Communication Server 2100

Product Guide

555-4001-806

Document status: Standard
Document version: 04.04
Document date: 20 October 2006

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

Contents

New in this release

The following sections detail what's new in the *Communication Server 2100 Product Guide* (555-4001-806) for release 9.0 (SE09).

Features

See the following sections for information about feature changes:

Note 1: New SE09 applications are described in the SE09 version of the *Communication Server 2100 Application Planning Guide* (555-4001-108).

Note 2: New SE09 Defence Switched Network (DSN) elements and applications are described in the *Meridian SL-100/Communication Server 2100 DSN General Description* (555-4021-108).

Communication Server 2100 Compact Motorola MCPN905 support

The Motorola MCPN905 board is supported as a Call Agent card type. This feature affects the following section:

- "Processor complex for Communication Server 2100 Compact (Call Agent)" (page 31)

Controlled hot switch of activity (SWACT) on compact

This release provides a controlled hot Switch of Activity (SWACT) capability for the Call Agent to the same load on the inactive side. This feature affects the following section:

- "Processor complex for Communication Server 2100 Compact (Call Agent)" (page 31)

Fully provisionable Codec lists for G.711 and G.729

This feature extends the IW SPM-IP codec list to be fully provisionable for G.711 and G.729. This feature affects the following section:

- "Interworking Spectrum Peripheral Module IP" (page 46)

GbE interface for sparing for Compact Call Agent cards

This feature provides a Gigabit Ethernet (GbE) interface for data synchronization or sparing for MCPN905-based Compact Call Agent (CCA) cards. This feature affects the following sections:

- "Processor complex (Core)" (page 26)
- "Communication Server 2100 Compact" (page 51)

Media Gateway 15000 Periodic routine exercise

This feature provides automated periodic routine-protected equipment testing on Media Gateway 15000 nodes. This feature affects the following section:

- "Nortel Media Gateway 15000" (page 62)

IEMS - MG 3200 (FCPS) Integration

Media Gateway 3200 is integrated into Integrated Element Management System (IEMS). IEMS provides integrated fault, performance, and security information for the Media Gateway 3200. This feature affects the following sections:

- "Media Gateway 3200 on Integrated Element Management System (IEMS)" (page 69)

- "Launching applications from IEMS" (page 152)

IP Client Manager (IPCM) additional phone support

These additional phone sets are supported:

- IP Phone 2007
- IP Phones 1120E and 1140E
- Wireless IP Phones 2210, 2211 and 2212

This feature affects the following section:

- "IP Client Manager" (page 77)

Pre-answer and mid-call SDP renegotiation

When interworking with a Multimedia Call Server (MCS), a Centrex IP Client Manager (CICM) node is supported for pre-answer and mid-call IP address and codec renegotiation. This feature affects the following section:

- "IP Client Manager" (page 77)

Removal of use of Border Control Point when user not logged in

A call terminating to a CICM line is allowed to complete even when the user associated with the directory number (DN) is not logged into a CICM client (IP Phone or m6350 SoftClient) at the time of the call. This feature affects the following section

- "IP Client Manager" (page 77)

Quality of Service reporting for CICM node calls

QoS statistics can be enabled to collect statistics for active calls on Nortel IP Phones. This feature affects the following section:

- "IP Client Manager" (page 77)

Media Gateway 9000 Global Line Card (GLC) 32 support

The feature provides support for the GLC 32 on the MG 9000. This feature affects the following section:

- "Nortel Media Gateway 9000" (page 85)

Border Control Point 7200

Border Control Point 7200 provides support of the IBM BladeCenter-T. The BladeCenter-T unit is a rack-mounted, high-density, high-performance, blade-server system developed for NEBS telecommunications network applications and other applications requiring additional physical robustness. This feature affects the following section:

- "Nortel Border Control Point 7000 series" (page 106)

CS 2100 OAM security enhancements

This feature provides security enhancements for user inactivity, lockout, or termination and centralization of MAPCI login. This feature affects the following sections:

- "OAMP security" (page 167)
- "Security and administration management" (page 174)
- "User management" (page 176)

Other changes

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

Ethernet Routing Switch 5520

Information was added to the Ethernet Routing Switches chapter to include the Ethernet Routing Switch (ERS) 5520. This information affects the following section:

- "Ethernet Routing Switch 5520" (page 134)

Introduction

Meridian SL-100 evolution

For more than two decades, large enterprise networks with 4,000 or more lines have used the Meridian SL-100. Advances in Internet telephony technology are changing the way Private Branch Exchanges (PBXs) provide communication services to enterprises around the world. SE09 uses this growing technology to offer businesses choices for how to evolve and grow their communication systems to the world of Internet Protocol (IP) telephony.

The evolution to IP telephony leverages Nortel products for other IP solutions. The Nortel Communication Server 2100 (CS 2100) delivers the same features as the Meridian SL-100, while paving the way for a new suite of services that result from the converging of telephony and data networks.

Software release SE09 builds on the evolution of the Meridian SL-100 to packet-based switching and all of its corresponding benefits. SE06 was the first release that bridged the Meridian SL-100 to the Nortel IP product portfolio. Previous Meridian SL-100 software releases have migrated to the SE software stream.

The CS 2100 provides central call processing and control between network components. Using the Real-time Transport Protocol (RTP), the CS 2100 provides translations and routing control for the entire IP telephony network. The CS 2100 also supports Dynamic Packet Trunks (DPTs) between IP telephony networks to optimize the bearer path for calls over DPT trunks.

The CS 2100 solution is based on using a single packet backbone network. Packet switching technology provides an alternative to current configurations in which voice and data networks exist in parallel and are managed separately. A migration to IP telephony reduces costs

- by eliminating hardware duplications,
- by simplifying and standardizing the management of networks and Network Elements, and
- by using bandwidths with maximum efficiency because circuit-switched connections are no longer needed.

The CS 2100 solution uses Communication Servers that offer large enterprises the opportunity to adopt the new packet-based network architecture without restricting themselves in terms of the capabilities and services they can offer their employees. The CS 2100 software includes call-processing agents, translations, routing, billing, and services software proven on other Nortel platforms in a wide range of markets. Because the CS 2100 supports interconnect interfaces, it can be deployed immediately alongside existing Public Switched Telephone Networks (PSTNs), while its support of value-added services ensures increased employee productivity.

With CS 2100, the transition from a Time Division Multiplexing (TDM) to packet architecture is seamless, with existing services remaining fully operational throughout the upgrade process. Traditional circuit-switched TDM and packet capabilities can be supported in parallel by the same software, with the Interworking Spectrum Peripheral Module IP (IW SPM-IP) providing connections between the TDM and the packet environments. This offers medium- to large-enterprise customers a second layer of flexibility they decide the best way, and the best time, to reap the benefits of IP switching. The CS 2100 uses the term "hybrid" to indicate that this Communication Server can deliver both IP and traditional TDM telephony services.

Available configurations

To provide Meridian SL-100 customers maximum flexibility in any upgrade to IP telephony, the following two base platforms, which deliver carrier-grade reliability, are supported:

- **Communication Server 2100 XA-Core (CS 2100 XA-Core)** - provides packet switching by leveraging current investment through the use of the Nortel proprietary Extended Architecture Core (XA-Core) processor currently used in existing Meridian SL-100s. For more information about this solution, see "Communication Server 2100 XA-Core" (page 58).

  Note: This platform can be based on a full SuperNode, or a streamlined SuperNode Size Enhanced (SNSE) configuration.

- **Communication Server 2100 Compact (CS 2100 Compact)** - provides packet switching by using an industry-standard compact Peripheral Component Interconnect (cPCI) processor. This configuration is sometimes referred to as the "Compact." This open platform, based on a Motorola cPCI circuit card, runs the same software as the XA-Core. For more information about this solution, see "Communication Server 2100 Compact" (page 51).

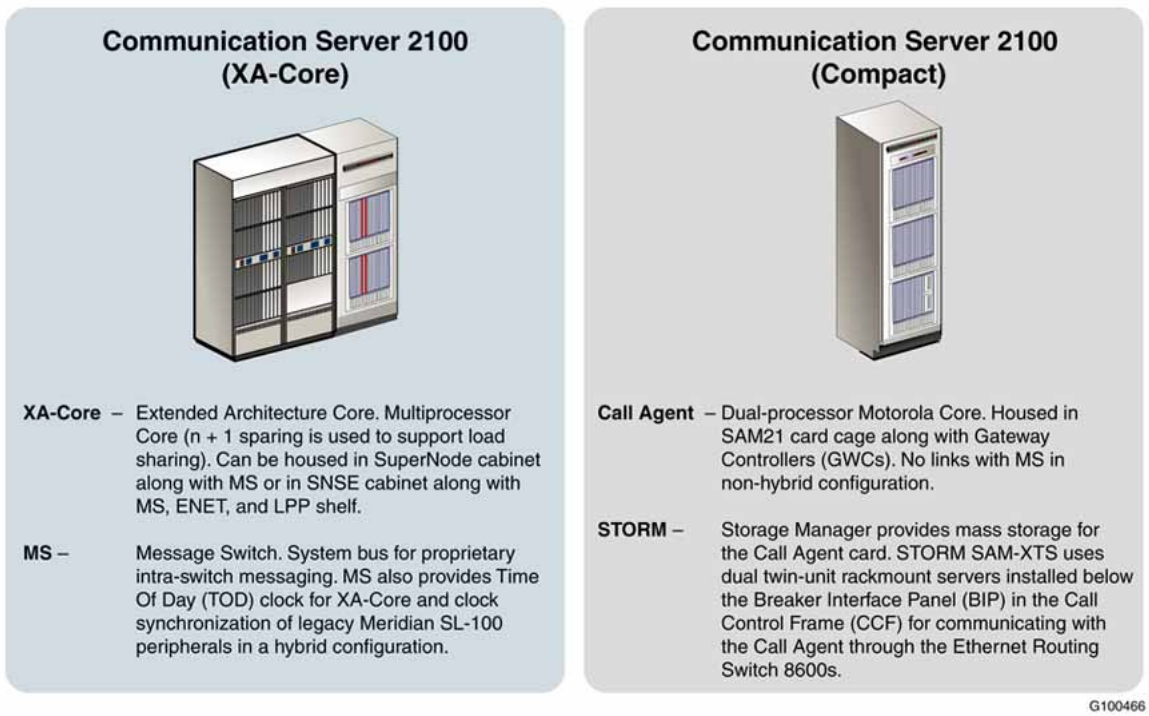
The term "Nortel Communication Server 2100", or "Communication Server 2100," is used to describe both of the above platforms.

Both configurations support the same range of call-processing agents, protocols, and telephony features. The main differences are that the CS 2100 Compact uses a different processor complex, has a significantly smaller system footprint and delivers reduced call processing capacity. CS 2100 Compact is, therefore, more appropriate for medium-sized enterprises where minimizing initial capital cost and system footprint is more important than switching capacity.

The CS 2100 is a distributed system comprising a number of different functional elements. The system uses the central processor to control all end points. The main functional elements are common to both configurations, but differences exist between the standard and compact configurations in terms of hardware components used to implement certain functions. See "Communication Server 2100 hardware" (page 23) for further information.

"Summary of processing differences between the two configurations" (page 15) summarizes the basic differences in hardware components between the two systems.

Summary of processing differences between the two configurations



Features and services

The CS 2100 supports the same wide range of features and applications that are currently supported on the Meridian SL-100.

ATTENTION

This document focuses on the base platform of the Communication Server 2100. See the *Communication Server 2100 Application Planning Guide* (555-4001-108) for a comprehensive description of features and services that the Communication Server 2100 supports.

Capacity

In "System capacities" (page 16) all figures quoted are general and are subject to variation depending on the network call model and capacity requirements. You should determine Nortel-specific estimates in consultation with Nortel Sales Engineering.

System capacities

Item	Communication Server 2100 XA-Core	Communication Server 2100 Compact
Call processing	• Maximum 1.65 million Busy Hour Call Attempts (BHCAs) • Maximum of 150,000 clients (not including trunks) • Maximum 56,000 simultaneous calls	• Maximum 1.3 million Busy Hour Call Attempts (BHCAs) • Maximum of 150,000 clients (not including trunks) • Maximum 32,000 simultaneous calls
Trunks and/or endpoints	Overall maximum of 200,000 trunk and/or endpoints. Within this, the limits that apply to different endpoint types are • 48,000 Primary Rate Interface (PRI/H.323) trunks • 150,000 analog subscriber lines	

Network topology

This chapter contains the following sections:

IP network architecture

The network architecture for the Communication Server 2100 (CS 2100) is based on a conceptual model defined by the Internet Engineering Task Force (IETF). This model specifies the logical functions that must be provided in a packet backbone network used to support multimedia traffic. Some of these logical functions exist within the packet network, whereas others exist at its periphery supporting access to the packet network from TDM networks and various types of access networks.

A "gateway" provides an interface between two domains (for example, between a packet network and a TDM network). There are two types of gateway functions as follows:

- **Media gateway** - provides an interface for bearer connections (for example, mapping a packet-based media stream onto a circuit-based media stream, seamlessly converting formats as necessary while maintaining content integrity).
- **Signaling gateway** - provides an interface for signaling connections. The signaling gateway terminates legacy network signaling on one side and packet network signaling on the other and supports all necessary interpretation and conversion between the two.

Media and signaling gateways are logical functions, not node types. A given node can provide the media gateway functions, signaling gateway function, or both. Similarly, gateway functions can be provided by a combination

of nodes, rather than by a single node. For more information about the supported gateways, see "Communication Server 2100 hardware" (page 23).

Gateways provide basic connectivity across the packet network. Additional capabilities are provided by various kinds of servers within the packet network. In-band services such as announcements and video are provided by media servers. Call-processing capabilities and related features are provided by Communication Servers (also known as Call Servers).

A Media Gateway Control (MGC) controls and coordinates packet network gateways to support applications such as IP telephony. As with gateways, a Media Gateway Controller is a logical function, not a node type. Media Gateway Controller functions can be provided by a combination of nodes, rather than a single node. A node can also provide server functions and Media Gateway Controller functions.

Communication Server 2100 implementation of IP architecture

In terms of IP network architecture, the CS 2100 is a Communication Server providing call-processing capabilities. It also provides Media Gateway Controller functions. Together with various types of gateways and servers, CS 2100 supports IP telephony. Specifically, CS 2100 capabilities include the following:

- **Basic connectivity and Network Element control**
  - Control over the media gateways that provides the bearer connection interface between the packet network environment and other TDM or access networks. CS 2100 provides the following three types of access using gateways:
    - Access to and from the Public Switched Telephone Network (PSTN) or other TDM network.
    - Integrated Services Digital Network (ISDN) Primary Rate Interface (PRI) access for digital Private Branch Exchanges (PBXs) and other PRI-enabled devices.
    - Analog line access.
  - Control over media servers that support announcements and conferencing over the packet network.
  - Originations and terminations for inter-Communication Server signaling across the packet network to and from other CS 2100s and to and from compatible Media Gateway Controllers.
  - Originations and terminations for TDM-side signaling.
- **Call processing**

- Support for a wide range of proven call-processing agents.
- Support for translations and routing of calls entering, exiting, and crossing the packet network.
- Support for requests to apply tones and announcements.
- Support for billing, event reporting, and performance monitoring.

- **Service support**
  - Support for specific sets of value-added features.
  - Support for general-purpose, service-delivery platforms.

CS 2100 can be regarded as single node; however, separate components provide the capabilities listed above. The Gateway Controllers (GWCs) are essential to the Communication Server and are typically used for the following purposes:

- To serve as controllers for media gateways, controlling their operation through device and or media control signaling based on packet network protocols.

  Note: Depending on the supported access type, a gateway can provide signaling gateway functions, as well as media gateway functions, in which case the Gateway Controller and the gateway exchange call control signaling and media control signaling, as is the case with PRI and analog line access.

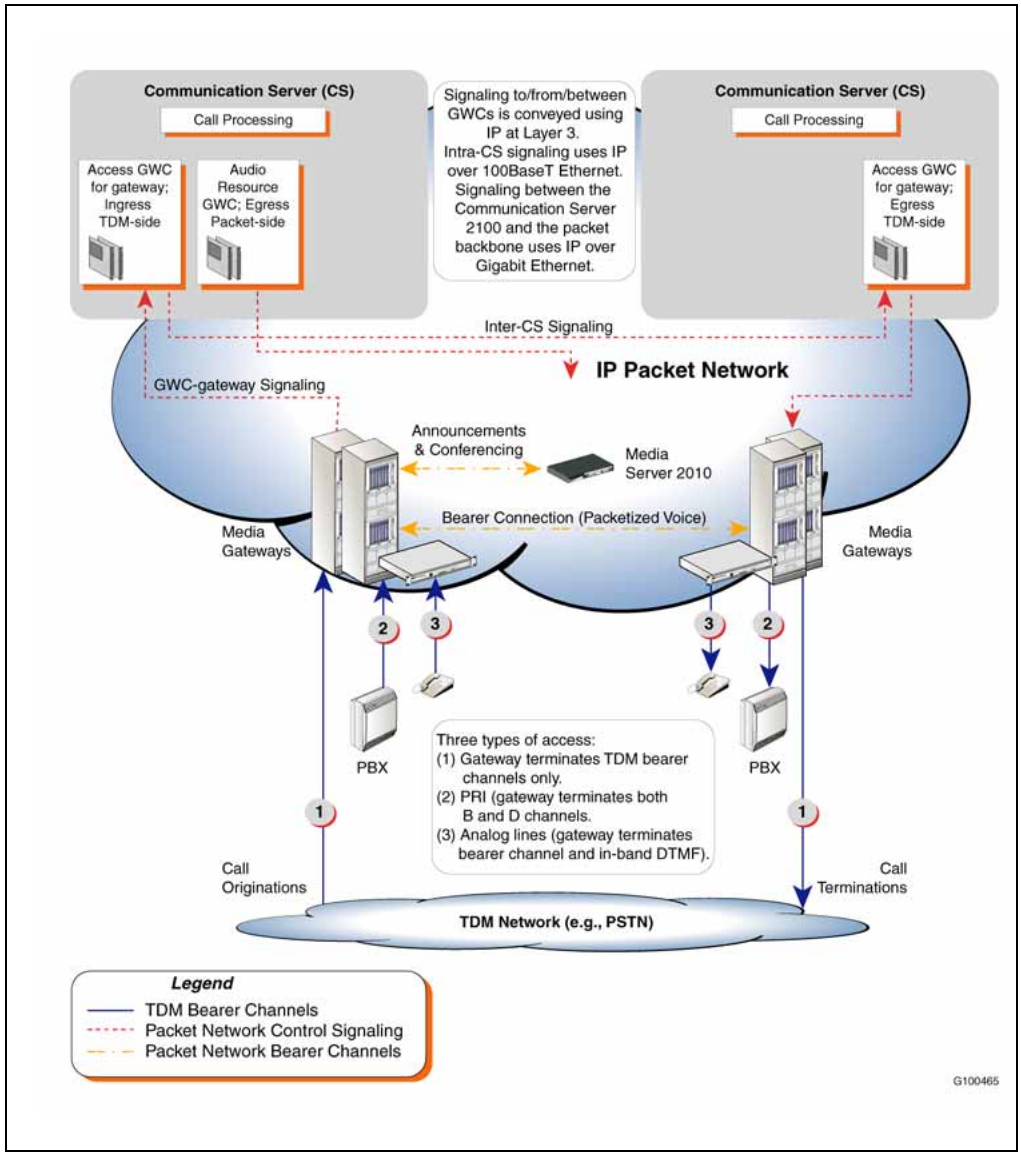
- To support communication between peer Communication Servers to handle networked calls. This support is accomplished through inter-Communication Server signaling, which is also based on packet network protocols.

In the CS 2100 architecture, you configure Gateway Controllers as CS 2100 peripherals, but from an IP network perspective a Gateway Controller is an independent host with its own IP address.

A range of packet network protocols are available for different types of communication involving Gateway Controllers.

"Communication Server network architecture for IP telephony" (page 20) shows a functional overview of the CS 2100 network architecture for IP telephony. The figure focuses on the roles of the different Gateway Controller types. For simplicity, Operations, Administration, Maintenance and Provisioning (OAMP) components are not shown (OAMP components are described in "Communication Server 2100 hardware" (page 23)).

Communication Server network architecture for IP telephony



Communication Server 2100 support for network architecture

Hardware support

Components

The Communication Server function is allocated to the CS 2100 as follows:

- Call processing is supported by the CS 2100 processor complex (Core).
- Different types of Gateway Controller functions are provided by Gateway Controllers housed in Service Application Module 21 (SAM21) card slots:
  - Gateway Controllers for media gateways supporting access to the packet network as follows:

– Trunk gateways support Primary Rate Interface (PRI/H.323) access.

– Line gateways provide support of analog lines.

A given gateway supports trunk or line access, but not both. An access Gateway Controller can control either trunk gateways or line gateways.

— Audio Gateway Controller for the Media Server 2010 that supports announcements and conferencing.

Gateways

The following gateway types are supported:

- Access gateways
  - — Media Gateway 15000 supporting IP telephony.
  - — Line media gateways attached to customer Local Area Networks (LANs) to support IP telephony.
  - — Media Gateway 9000.
  - — Media Gateway 3000 Series.
- Media Server 2010 that supports packetized announcements and conferencing.

Software support

Because the CS 2100 is a distributed system, you must consider the support for protocols that are internal to the network, as well as the PSTN interfaces CS 2100 supports externally. The SE09 software delivers protocol stacks that support three types of IP signaling involved in setting up calls across the packet network as shown in the following list:

Note: All packet network signaling is conveyed using IP at Layer 3.

- Access signaling between Gateway Controllers and media gateways. The following types of access signaling are supported:
  - — Media or device control signaling used by the Gateway Controller to control the characteristics of the packet network bearer connections used for a call.
  - — Call control signaling (setup and clearing messages) for message-based interfaces such as Integrated Services Digital Network (ISDN) PRI. Access network signaling is terminated at the media gateway.
  - — Call control signaling for analog subscriber lines.

- Network signaling between Communication Servers.
- Session Description Protocol (SDP) used to complement both Gateway Controller gateway signaling and inter-Communication Server signaling by specifying bearer capabilities and IP address information.

SE09 software load

SE09 is the fourth CS 2100 release for the Meridian SL-100. The SE09 software provides all of the required software functions for packet-based signaling. In addition, you can install SE09 on legacy Meridian SL-100 hardware platforms; in which case, the software is referred to as SE09 (TDM). You can install the SE09 software load in a hybrid configuration that simultaneously comprises circuit-switched and packet-switched capabilities.

The backbone packet network

The backbone packet network comprises the following two logically distinct networks:

- The bearer network is used to convey media streams such as speech, data, or video.
- The control network is used to convey signaling (that is, to set up and control bearer connections between media gateways).

References in this document to an IP backbone packet network denote the bearer network, not the control network. The control network uses IP at Layer 3.

Note: CS 2100 does not support Asynchronous Transport Mode (ATM) as the backbone network.

Communication Server 2100 hardware

Overview

This chapter describes the Communication Server 2100 (CS 2100) hardware. The chapter also summarizes the differences between the Communication Server 2100 XA-Core hardware platform and the CS 2100 Compact hardware platform.

The CS 2100 is based on a distributed modular architecture that provides inherent scalability, whereby the capacity of each CS 2100 can be tailored for its network role. Most call processing and feature support is provided by the central processor complex or Core, but specialized processing is delegated where possible to peripherals and Gateway Controllers to ensure optimum use of Core capacity.

Hardware availability is defined in terms of software releases because many hardware components have software dependencies and vice versa.

To meet the divergent needs of large enterprise customers, the following two hardware configurations are supported:

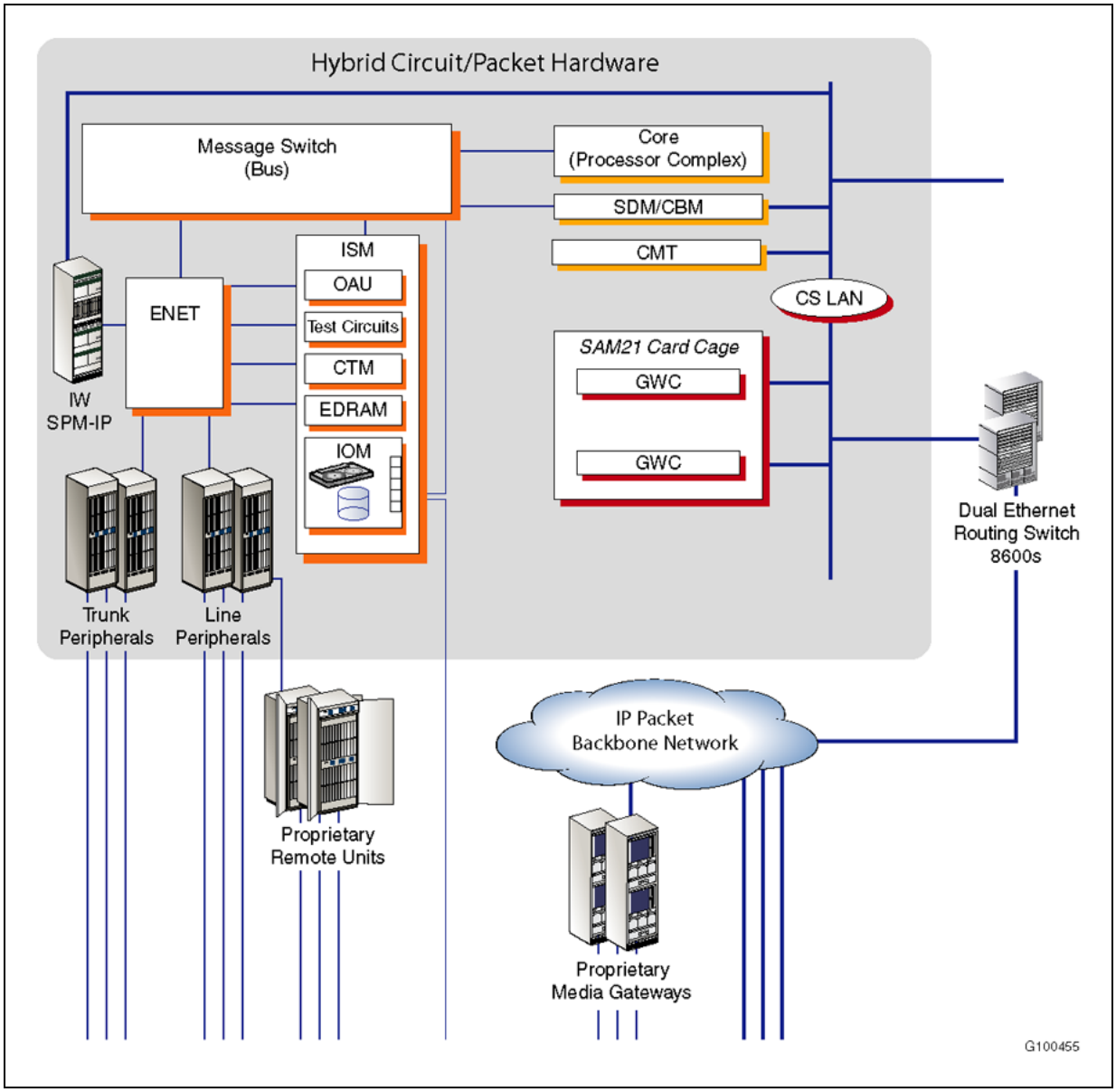
- CS 2100 XA-Core, which can be either a full SuperNode configuration or a streamlined SuperNode Size Enhanced (SNSE) configuration.
- CS 2100 Compact configuration with minimized footprint.

A CS 2100 Communication Server is a distributed system comprising a number of different functional elements. "Functional overview of the Communication Server 2100 hardware and CS LAN" (page 24) provides a high-level logical view of the interaction between the main functional elements, which are common to both configurations. Some functions are, however, provided by different hardware components in XA-Core and Compact configurations.

"Functional overview of the Communication Server 2100 hardware and CS LAN" (page 24) shows a logical view of the Communication Server 2100. Physically, the Communication Server 2100 consists of circuit cards housed in shelves, which are in turn packaged into cabinets to form a cabinet lineup. Many CS 2100 components are duplicated for reliability.

Others operate in load-sharing mode using N+1 sparing. In both cases, the objective is for a functional element to survive the failure of one of its constituent hardware units.

Functional overview of the Communication Server 2100 hardware and CS LAN

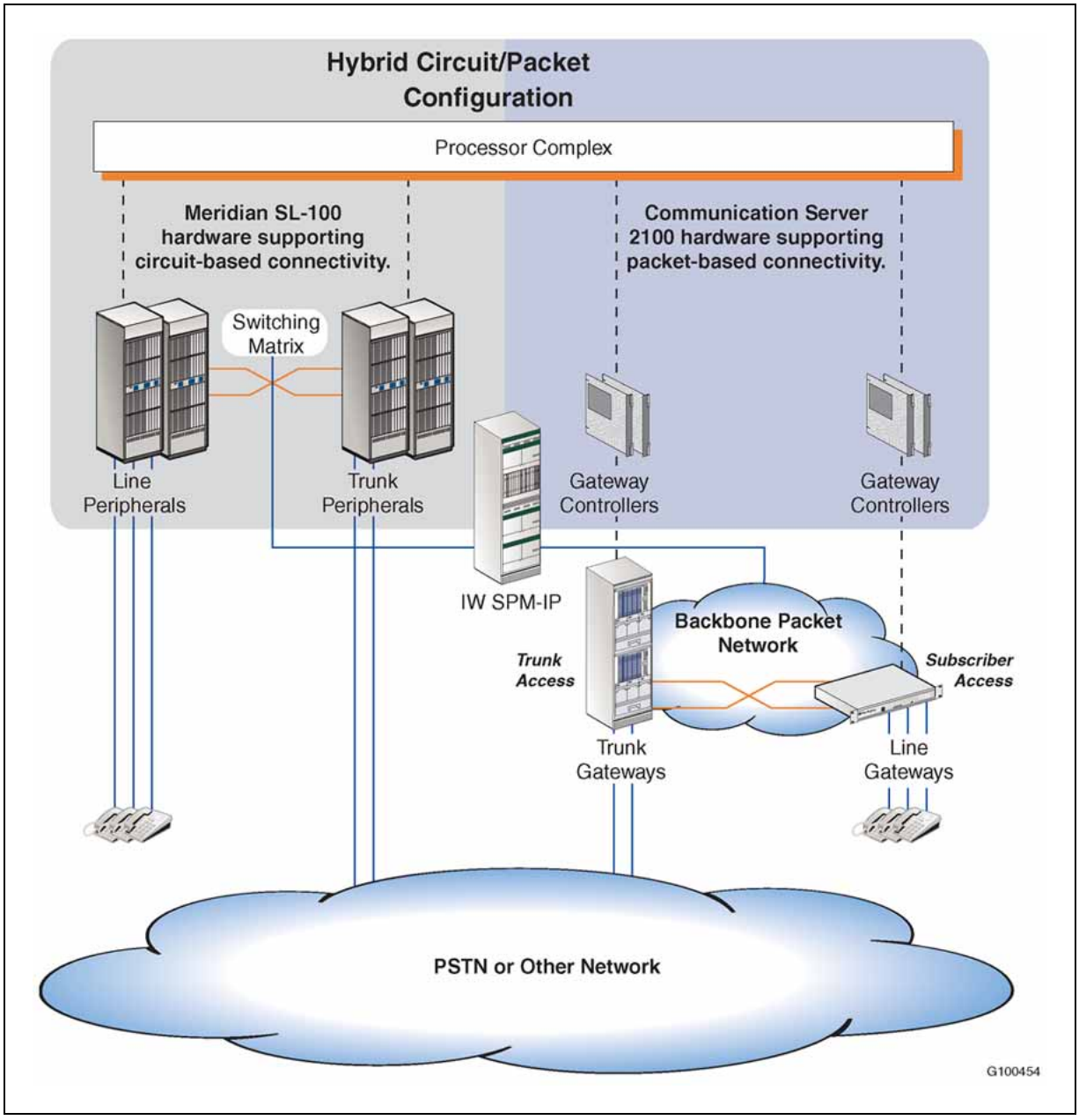


Hybrid support

"Functional view of hybrid circuit/packet configuration" (page 25) breaks out "Functional overview of the Communication Server 2100 hardware and CS LAN" (page 24) to provide a simplified functional view of the different

roles the CS 2100 and legacy Meridian SL-100 switches. The figure shows how to combine these units in a hybrid configuration to support both circuit-switched and packet-switched capabilities.

Functional view of hybrid circuit/packet configuration



For more information about the Meridian SL-100 circuit-switched hardware components, see *Communication Server 2100 Meridian SL-100 Product Guide,* (555-4001-103).

Chapter format

This chapter describes the internal hardware components of the CS 2100. Gateways that complement the solution, and media servers such as the Media Server 2010, are described in separate chapters.

This chapter contains the following sections:

- "Processor complex (Core)" (page 26)
- "Internal communication (Communication Server LAN and Message Switch)" (page 34)
- "Gateway Controllers" (page 38)
- "Interworking Spectrum Peripheral Module IP" (page 46)

OAMP platforms are described in"OAMP for Communication Server 2100 networks" (page 137). In addition, to distinguish between the two CS 2100 hardware configurations, this chapter includes the following sections:

- "Communication Server 2100 Compact" (page 51)
- "Communication Server 2100 XA-Core" (page 58)

Processor complex (Core)

The processor complex, or Core, is the central computing engine of a CS 2100. The Core is where you install the Product Computing-module Load (PCL) for the current software release. Although specialized processing is delegated to other components where possible, the centrally-located Product Computing-module Load supports call-processing agents for telephony interfaces, translations and routing, and service logic for delivering value-added features and services. The Product Computing-module Load also includes software for controlling packet network bearer connections established through Gateway Controllers and media gateways.

Depending on the configuration type, the CS 2100 supports two different Cores as follows:

- The Extended Architecture Core (XA-Core), as described in "XA-Core" (page 26), provides processing power for CS 2100 XA-Core configurations. XA-Core is also a processor complex for legacy Meridian SL-100 switches.
- The Call Agent as described in "Processor complex for Communication Server 2100 Compact (Call Agent)" (page 31), provides processing power for CS 2100 Compact configurations.

XA-Core

The XA-Core is the call-processing platform for the CS 2100 XA-Core. The XA-Core provides an OC-3c network connection provisioned for two Permanent Virtual Connections between each trunk gateway for signaling

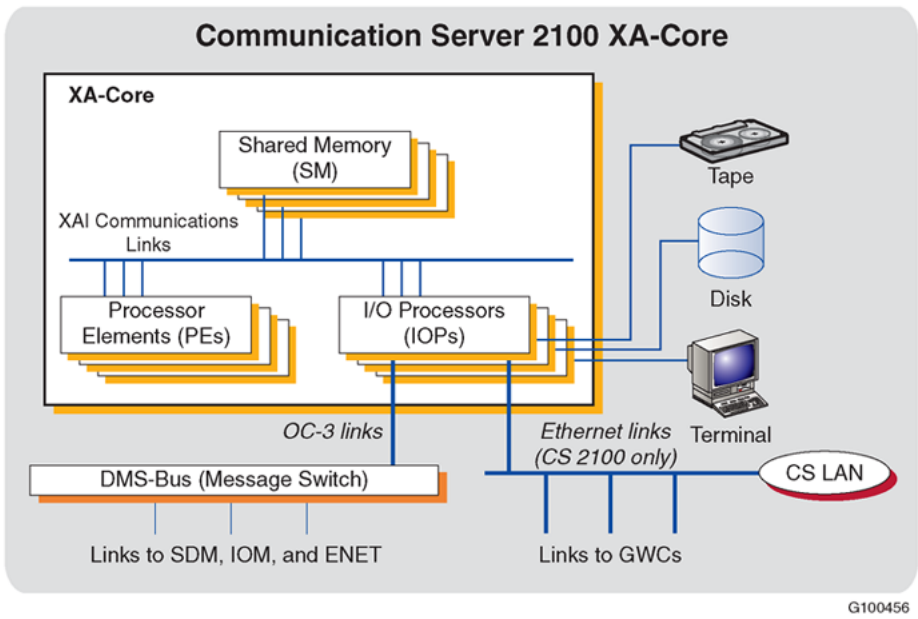
data and a 10/100BaseT interface to the CS LAN for OAMP data. The XA-Core connects to the Message Switch using an OC-3 connection. Network element provisioning, configuration, alarms, logs, and maintenance are supported by XA-Core software and are accessed by software applications on the Core Manager.

XA-Core design is based on the principle of using independently scalable subsystems to deliver call-processing capacity. You can tailor these subsystems incrementally to meet the requirements of your organization, without the need for replacements or upgrades. The XA-Core subsystem consists of the following subsystems:

- Processor subsystem
- Shared memory
- Input/output processors

A set of independent communications links referred to as the Extended Architecture Interconnect (XAI) provide links between subsystems (bus capabilities). " XA-Core logical architecture" (page 27) illustrates XA-Core architecture at the logical level.

XA-Core logical architecture



Physically, the processor complex implements each type of XA-Core subsystem as a circuit card. XA-Core as a whole consists of a single shelf that provides slots for inserting circuit cards. A SuperNode C42 cabinet houses the XA-Core shelf.

The XA-Core shelf can be included in a cabinet with the Message Switch and Enhanced Network (ENET) in separate cabinets. Alternatively, the XA-Core can be included in a SuperNode SE Combined Core cabinet along with a streamlined version of the Message Switch and ENET.

Processor subsystem

Each Processor Element (PE) consists of twin Power MCPN7410 processors and has 512 MB of on-board memory.

The system uses 2+1 XA-Core sparing (that is, three active load-sharing Processor Elements handling a workload engineered for two, --theoretically leaving one spare). The system can handle a full workload, even if a Processor Element fails.

Shared memory

Each shared memory element is a card housing two or three 128-MB memory modules. The maximum memory that can be provided by the shared memory subsystem for XA-Core is 1728 MB (1152 MB for SuperNode SE).

Mated pairs of 32-MB memory blocks on different memory cards, each storing duplicated data, provide the memory. In this configuration, the system retains one copy of the data in the event of a memory failure. Pairs of memory blocks are independently mated, so that problems with one mated pair have no impact on any other mated pair.

Input/output system

Input/Output Processors (IOPs) provide system load capacities and support communications links with other CS 2100 XA-Core components. Each Input/Output Processor motherboard houses one or two dedicated application-specific packlets designed to support capabilities such as the following:

- Ethernet ports for Internet Protocol (IP) communication using the Communication Server LAN (CS LAN) with other IP hosts, especially Gateway Controllers housed in SAM21 card cages. XA-Core is equipped with two High-capacity Input/Output Processor (HIOP) cards, which you connect to the Ethernet Routing Switch (ERs) 8600s through 100BaseT full duplex links. During normal operation, both HIOPs are active and operate in load-balancing mode.
- An interface to the CS 2100 XA-Core Message Switch (bus) for communication with the SuperNode Data Manager. Each Input/Output Processor used for this purpose supports ports for terminating Asynchronous Transport Mode (ATM) over Synchronous Optical Network (SONET) OC-3 links operating at 155 Mbps.
- Disk storage with capacity of 4 GB.

- Tape storage (DAT) with capacity of 1.3, 2, or 4 GB.

Physical layout

The XA-Core fits in a single shelf in a traditional Meridian SL-100 frame. The shelf contains the following types of circuit cards:

- Processing Element (PE) cards execute all call-processing software processes including the computing module software that provides a user interface through a Maintenance and Administration Position (MAP) terminal, central database functions, call-processing services, and system-level maintenance functions.
- Input/Output Processor (IOP) cards handle input and output processing. Each Input/Output Processor uses a generic processor card and one or two daughterboards, called packlets, which provide I/O services (for example, disk and tape drives; and serial, OC-3, and Ethernet interfaces).
- High-Performance Input/Output Processor (HIOP) cards provide a hardware upgrade for Input/Output Processor cards supporting 100BaseT Ethernet.
- Shared Memory (SM) cards contain all XA-Core data that can be shared with software processes running on Processing Element and Input/Output Processor cards. These cards also control data access by Processing Element and Input/Output Processor cards.

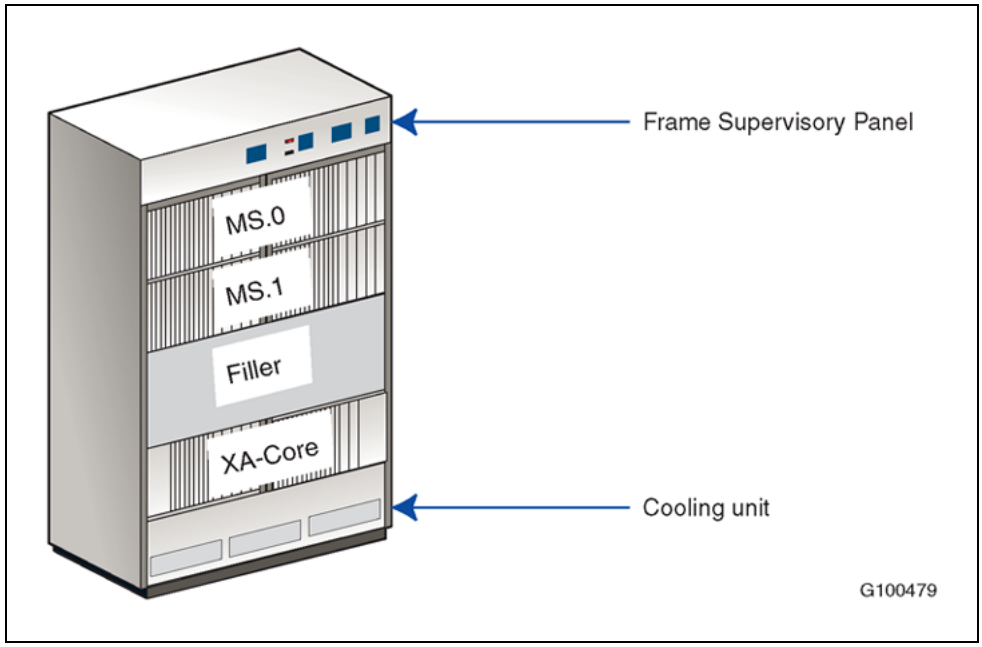
Together these circuit cards form a high-performance, multiprocessing computing engine that is completely scalable in terms of processing, memory, and I/O capability. Adjusting system capacity, or adding another interface, requires that you only plug in a new card.

SuperNode frame

The XA-Core is housed in a SuperNode cabinet and, depending on the configuration, can also contain a Frame Supervisory Panel (FSP), one standard XA-Core shelf, two Message Switch shelves, one filler shelf, and a cooling unit. XA-core components reside on a single shelf with a mid-plane design that houses front- and rear-mounted cards.

"XA-Core frame layout" (page 30) shows the cabinet configuration when the XA-Core and Message Switch shelves are in the same cabinet.

XA-Core frame layout



For additional information about XA-Core-based systems, see "Communication Server 2100 XA-Core" (page 58).

References

"Documentation references" (page 30) shows where you can find more information about the hardware components used with the CS 2100 XA-Core.

Documentation references

Document title	Document Number
Summary of TDM components (including Core and Message Switch)	
Communication Server 2100 Meridian SL-100 Product Guide	555-4001-103
DMS-100 Family Hardware Description Manual	297-8991-805
DMS SuperNode and DMS SuperNode SE Switch	297-5001-549
XA-Core Reference Manual	297-8991-810
XA-Core	

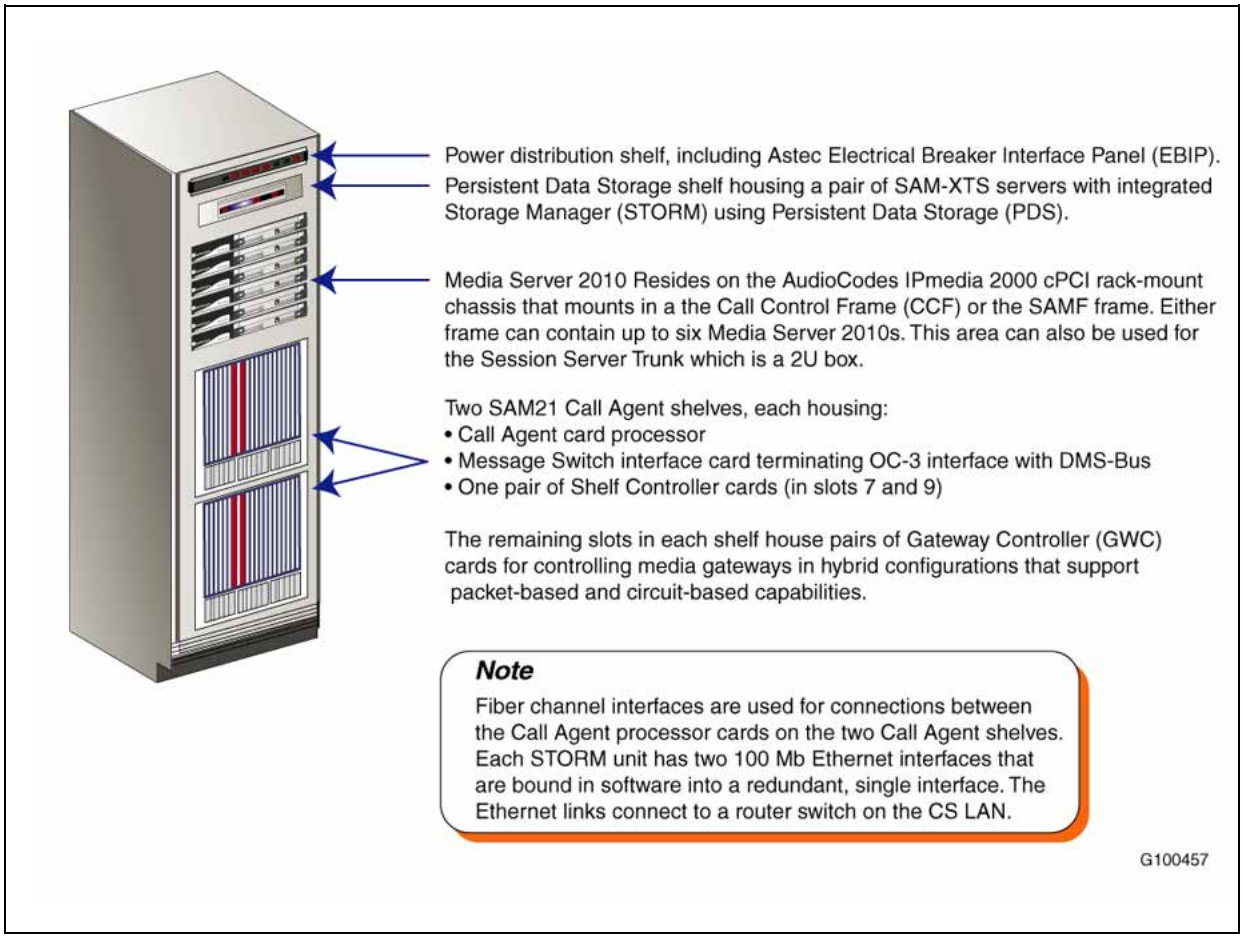
Document title	Document Number
Communication Server 2000 Basics ***Note:*** Due to the commonality between the two systems, these documents also apply to the CS 2100.	NN10448-111
Communication Server 2000 Fault Management	NN10083-911
Communication Server 2000 Configuration Management *Communication Server 2000 Configuration Management (IAW & IAC)*	NN10193-511 NN10188-511
North American ATM/IP Solution-Level Accounting	NN10400-800
Communication Server 2000 Performance Management	NN10149-711
Communication Server 2000 Security and Administration	NN10171-611
Upgrading the CS 2000 Core Manager	NN10061-461
Upgrading the Carrier Voice over IP Network	NN10444-450

Processor complex for Communication Server 2100 Compact (Call Agent)

The processor complex for the CS 2100 Compact is referred to as the Call Agent. The Call Agent is a non-proprietary processor, which consists of a pair of Motorola MCPN765 or MCPN905 cards, also known as blades. The Call Agent supports call processing and service logic with the SE09 load running on a combination of Linux operating system and Protel Environment Emulation Layer (PEEL) software.

A SAM21 shelf in a Packet Telephony Equipment 2000 (PTE2000) frame houses the Call Agent. This frame is referred to as a Call Control Frame (CCF). The SAM21 is so called because it is a Service Application Module shelf with 21 slots. A PTE frame is 61 cm wide x 213 cm high x 61 cm deep (24in x 84in x 24in) walled frame with a door. "Communication Server 2100 Compact Call Control Frame" (page 32) illustrates the Call Control Frame and its contents.

Communication Server 2100 Compact Call Control Frame



Frame layout

The CS 2100 Compact resides in a Call Control Frame (CCF) in a Packet Telephony Equipment (PTE2000) frame. Each Call Control Frame consists of the following components:

- Two CS 2100 Compact Call Agent/SAM21 shelves.
- One Astec Breaker Interface Panel (BIC) that serves as the power distribution shelf.
- Two STORM SAM-XTS server units that store data on internal disk drives and use RAID level one (RAID-1) mirroring for data redundancy. With RAID-1, one of the two drives can fail without loss of data.

In addition to the Call Control Frame, a CS 2100 Compact cabinet lineup includes a cabinet housing a CBM that resides in the COAM, the CS 2000 Manager and a PTE2000 frame housing OAMP servers for Gateway Controllers, and other CS 2100 Compact components (see "Communication Server 2100 Compact" (page 51) for more information).

Shelf layout

Each CS 2100 Compact resides in a SAM21 shelf. Each shelf consists of the following components:

- one alarm panel
- one card cage that consists of the following cards:
  - one Call Agent card
  - seven pairs of Gateway Controller cards
  - one pair of Shelf Controller cards that manage the SAM21 shelf
- three power supply and fan modules

Call Agent card

The Call Agent card is easy to insert, remove and replace at the card level. The shelf supports the hot swapping of cards.

The Call Agent card increases the density of processing within a given space. The Call Agent card is of two types:

- A Motorola MCPN905 board (NTRX51HZ), with MCP755X 1 GHz processor and 2.0 GB RAM, running LinuxPPC (Nortel distribution). The Ethernet ports are on the rear Transition Module. The fiber channel interface is provided by a Systran fiber channel PMC. A Motorola PrPMC815 provides persistent memory. An NTRX51HS transition module is needed for each Call Agent card. The card supports improved Call Agent restart and failover times, and capacity improvements.
- A Motorola MCPN765 board (NTRX51GZ), with MPC7410 500 MHz processor and 1.5 GB RAM, running Nortel Carrier Grade Linux (NCGL) operating system. Ethernet ports are on the rear Transition Module. The fiber channel interface is provided by a Systran fiber channel PCI Mezzanine Card (PMC). An NTRX51FS transition module is needed for each Call Agent card.

The Nortel Call Agent card is designed for survivability. The two Call Agent units are distributed on separate shelves. They are interconnected through IP for messaging and Fiber Channel (FC) for data synchronization or sparing, with a backup serial link, to eliminate the need for colocating the two shelves.

Note: MCPN905-based Call Agent cards can also be configured to use Gigabit Ethernet (GbE) instead of FC for sparing in geographically survivable configurations.

Release SE09 provides a controlled hot Switch of Activity (SWACT) capability for the Call Agent to the same load on the inactive side. A controlled hot SWACT reduces the restart period to less than three seconds. With the reduced restart period, the controlled hot SWACT feature introduces the following changed behavior and scheduling flexibility:

- Warm restarts are eliminated if the controlled SWACT is to the inactive Call Agent, which is in hot sync with its mate and on the same load.
- A SWACT after FULL REx tests is initiated.
- The user can set the day of the FULL REx test. Before this feature existed, the day of the FULL REx test was hard coded to Thursday.

References

"Documentation references" (page 34) shows where you can find detailed information about the Call Agent.

Documentation references

Document title	Document Number
Call Agent (equivalent of the core)	
Call Agent Basics	NN10023-111
Call Agent Fault Management	NN10087-911
Call Agent Configuration Management	NN10109-511
Call Agent Accounting Management	NN10131-811
Call Agent Performance Management	NN10153-711
Call Agent Administration and Security	NN10175-611
Upgrading the Call Agent	NN10065-461
Storage Management (STORM) (the Call Agent requires persistent storage)	
STORM Basics	NN10024-111
STORM Fault Management	NN10088-911
STORM Configuration	NN10110-511
STORM Performance Management	NN10054-711
STORM Security and Administration	NN10176-611
Upgrading the STORM	NN10066-461

Internal communication (Communication Server LAN and Message Switch)

Internal communication between components of a CS 2100 is based on one or both of the following:

- The Communication Server Local Area Network (CS LAN)

Primarily supports communication between Gateway Controllers and other components, such as the Core and the SuperNode Data Manager.

Note: In carrier network configurations, the CS LAN sometimes is referred to as the Central Office LAN (CO LAN).

- The Message Switch (bus)

  Provide a system bus for peer-to-peer messaging between the XA-Core and other Meridian SL-100 legacy components in a CS 2100 XA-Core configuration, such as the SuperNode Data Manager.

  Note: The Message Switch is not required, or used, in CS 2100 Compact configurations.

Communication Server Local Area Network

"Functional overview of the Communication Server 2100 hardware and CS LAN" (page 24) depicts how the CS LAN supports communication between CS 2100 components.

Communication Server 2100 components linked by the CS LAN

The CS LAN supports Ethernet communication between CS 2100 hardware components, especially between Gateway Controllers and other units, as follows:

- Components connected though the CS LAN in a CS 2100 XA-Core include the following:
  - Gateway Controllers
  - XA-Core
  - SuperNode Data Manager
- Components connected though the CS LAN in a CS 2100 Compact include the following:
  - Gateway Controllers
  - Call Agent
  - SuperNode Data Manager

The CS LAN also supports communication between CS 2100 components and some colocated non-CS 2100 components, including the following types of server:

- Media Server 2010 supporting the following capabilities:
  - Announcements
  - Conferencing
  - Monitoring

For more information about the Media Server 2010, see "Nortel Media Server 2010" (page 95).

- Sun Netra 240 servers housed in a dedicated PTE2000 OAMP frame, supporting Device Managers and management applications for Gateway Controllers and non-CS 2100 units such as media gateways.
- Trivial File Transfer Protocol (TFTP) server.

CS LAN characteristics and connectivity

The CS LAN is an Ethernet 100BaseT network based on the Ethernet Routing Switch (ERS) 8600. Physically, the CS LAN consists of direct Ethernet cable connections between ports on the ERS 8600 and ports on the CS 2100 hardware components.

See "Communication Server 2100 hardware" (page 23) for more information about the ERS 8600.

To provide redundancy, each CS LAN uses two ERS 8600s. A CS 2100 component, such as a Gateway Controller, connects to both ERS 8600s, using one as a default router and the other as a backup. The configuration implements load sharing over the CS LAN by configuring half of the devices on the LAN to Router A as the default gateway and configuring the other half to use Router B. The dual ERS 8600s serve as a hub for the CS LAN subnetwork providing all the necessary routing functions for communication across the LAN.

ATTENTION

See the *Packet Trunking-IP (PT-IP) SN06 Engineering Guidelines*, (SEB-02-10-001) for comprehensive recommendations for configuring the CS LAN.

The CS LAN supports intra-CS 2100 communication, and provides the interface between the CS LAN and the external managed IP network.

Message Switch (Communication Server 2100 XA-Core bus)

"Functional view of hybrid circuit/packet configuration" (page 25) depicts how the Message Switch supports communication between CS 2100 components using an OC-3 link (the Message Switch is not used in CS 2100 Compact configurations).

Communication Server 2100 XA-Core components linked by the Message Switch

The CS 2100 XA-Core configuration uses the Message Switch to support peer-to-peer messaging between the following components:

- XA-Core

- SuperNode Data Manager
- Enhanced Network (ENET)
- Input/Output Module and Integrated Service Module (ISM)

The system uses an Input/Output Module datalink housed in an Integrated Service Module shelf to bring the SuperNode Data Manager and the CS 2100 XA-Core into service.

ENET

The Enhanced Network (ENET), a fully duplicated switching fabric, performs TDM-based call switching for legacy services. The ENET shelf mounts in a C42 cabinet. The ENET switches calls between TDM-based peripherals and the Interwoking Spectrum Peripheral Module IP. The ENET is also used to access Integrated Services Module test and service circuits and to access alarms.

Integrated Services Module

The Integrated Services Module is a specialized module to accommodate test and service circuit cards used in switch and facility maintenance.

In the CS 2100 XA-Core configuration, the Integrated Services Module houses Input/Output Modules. Input/Output Modules provide ports for serial input and output, enabling local and remote devices to communicate with the rest of the CS 2100 XA-Core through the Message Switch. CS 2100 XA-Core Input/Output Modules support datalinks used to bring the SuperNode Data Manager platform and XA-Core into service.

Each single-slot Input/Output Module FX30 Communications Card (CC) supports 16 ports for

- 64 kbps synchronous V.35 links
- 28.6 kbps asynchronous RS-232 links

The system supports X.25 data communications over either V.35 or RS-232.

Message Switch hardware

The bus consists of two identical load-sharing planes called Message Switches, each with the capacity and connectivity to support the full internal messaging load if the other plane fails. The switch plane consists of the following:

- A 32-bit Motorola 68000 Series control processor with on-board memory.
- The following two buses for communication:
  - The Transaction Bus (T-Bus) carries the messaging payload (that is, the messages sent from one CS 2100 XA-Core component to another through the Message Switch). The Transaction Bus operates

at 128 Mbps, with a typical throughput of 250,000 64-byte messages per second and an average port-to-port delay of less than 100 ms.

— The Processor Bus (P-Bus) carries internal messages used to control Message Switch operation.

- A mapper subsystem that converts physical addresses (port numbers within the Message Switch) to or from the logical addresses of switch components.
- A port interface subsystem consisting of a number of Port Interface Units (PIUs), each including the following:
  — An interface card that logically faces toward the Message Switch Transaction Bus and provides Message Switch addressable ports.
  — A paddleboard supporting one or more links to the following switch components:
    – DS-512 optical fiber links for XA-Core and the SuperNode Data Manager
    – DS-30 copper links for Integrated Service Module Input/Output Modules
- A clock synchronization subsystem that provides the XA-Core with a clock for Time-of-Day synchronization. For accuracy, this clock subsystem connects to an external clock source such as a Building Integrated Timing System or a Global Positioning System (GPS) clock system.

  Note: In a hybrid configuration, the clock subsystem also provides the system clock and network synchronization for components such as trunk and line peripherals.

Gateway Controllers

Introduction

The Gateway Controllers manage and manipulate bearer connections on various types of media gateways. Gateway Controllers receive instructions from the XA-Core, or Call Agent, to perform operations such as the following:

- create a connection
- release a connection
- collect in-band digits
- provide echo cancellation

The software that the Gateway Controllers uses is based on the XPM peripheral loads used in the Meridian SL-100, with some exceptions.

Gateway Controller types and functions

Gateway Controllers enable the CS 2100 to access the packet backbone network. Gateway Controllers perform low-level call setup, protocol mediation and tasks to support call processing. The most important functions of Gateway Controllers include the following:

- Controlling the operation of media gateways that support trunk and line access to the packet network.
- Communicating with remote CS 2100 softswitches across the packet network.

The CS 2100 uses the following types of Gateway Controller:

- Gateway Controllers for media gateways including
  - Trunk gateways such as Nortel Media Gateway15000 (see "Nortel Media Gateway 15000" (page 62)) or the Nortel Media Gateway 3000 Series (see "Nortel Media Gateway 3000 Series" (page 68)). A given Gateway Controller can support up to 4,000 PRI trunks distributed between a number of different media gateways with a maximum of 1,024 on a given gateway.
  - Line gateways such as Nortel Media Gateway 9000 (see "Nortel Media Gateway 9000" (page 85)or IP Client Manager (see "IP Client Manager" (page 77)). A given Gateway Controller can support up to 6,000 lines distributed between a number of different media gateways, with a maximum of 1,024 on a given gateway.
- Gateway Controller for the Media Server 2010.
  - For more information on Media Server 2010 see "Nortel Media Server 2010" (page 95).

Note: In terms of the CS 2100 network architecture, the Media Server 2010 subtends the SAM21 and is therefore categorized as a media server, not as a CS 2100 component.

Hardware characteristics

SAM21 card cages or shelves house Gateway Controllers, along with a pair of Shelf Controller (SC) cards operating in hot standby mode to provide control and coordination for the entire shelf. In turn, cabinets house SAM21 shelves. The SAM21 is so called because it is a single-shelf Service Application Module (SAM) with 21 slots for housing circuit cards. The SAM21 uses a NEBS Level 3 Motorola CPX8221 industry-standard cPCI chassis with 21 slots. Two slots are reserved for the Shelf Controller cards. Sixteen slots are input/output slots reserved for up to eight Gateway Controllers, each consisting of two cards operating in standby mode.

Logically, a Gateway Controller is a single entity that you can access through a single IP address (that is, that of the currently active Gateway Controller unit).

Two 10/100 BaseT Ethernet links run from each Gateway Controller pair to the CS LAN. Each Gateway Controller pair requires four IP addresses. Each Shelf Controller card has one 10/100 BaseT Ethernet link to the CS LAN. Each Shelf Controller pair requires four IP addresses. You can equip a maximum of two Shelf Controllers for each SAM21 shelf.

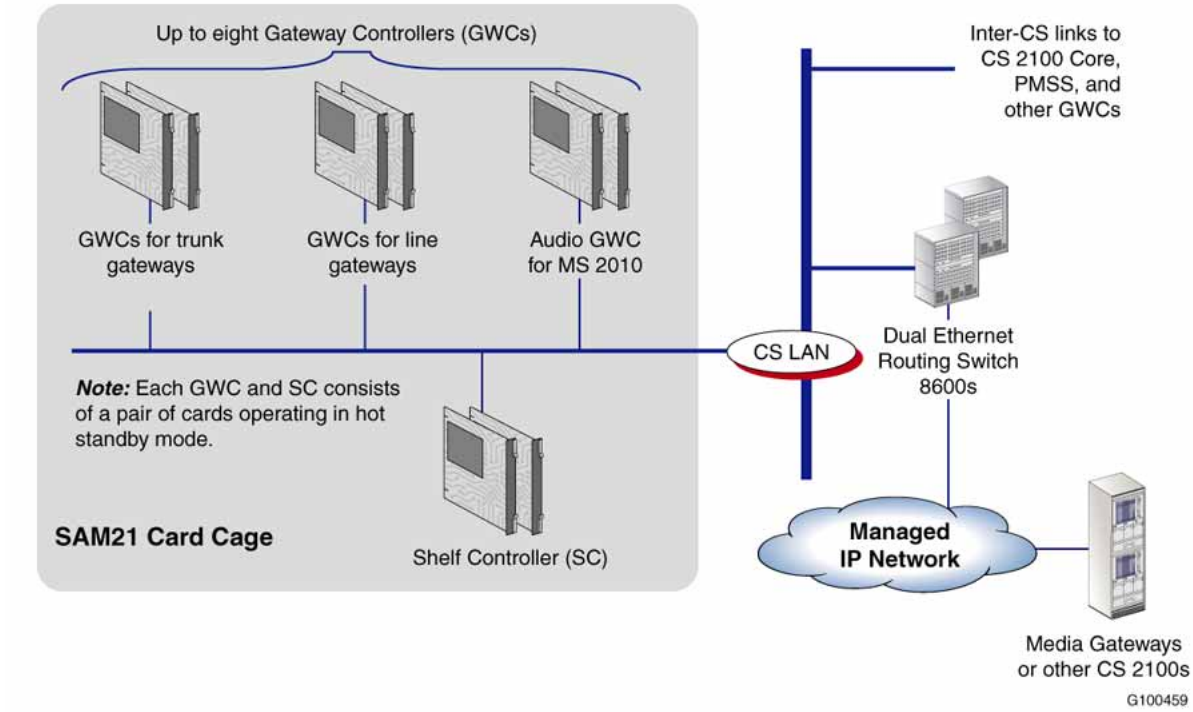
The backplane of the SAM21 card cage provides a compact Peripheral Component Interconnect (cPCI) bus for communication between circuit cards housed in the card cage. Ethernet 10/100BaseT ports on the cards themselves provide access to the Ethernet Routing Switch (ERS) 8600-based CS LAN. Gateway Controllers connect to both the cPCI bus on the SAM21 backplane and to the CS LAN. The cPCI bus enables the Shelf Controller to communicate with the Gateway Controllers to provide control and coordination of the shelf. The CS LAN enables Gateway Controllers to communicate with other CS 2100 components, including the XA-Core (CS 2100 XA-Core only) and other Gateway Controllers and through the LAN dual ERS 8600s with media gateways and other CS 2100 softswitches.

The Gateway Controller is based on the Motorola MCPN750 or MCPN905 single-board computer. Two redundant single-board computers make up each Gateway Controller node. The single-board computers are usually housed side-by-side in a SAM21 cPCI chassis. The Gateway Controller circuit cards host the Gateway Controller software that, together with the Core, provide the CS 2100 with its Media Gateway Controller (MGC) functions. Processing capacity is scalable by adding additional Gateway Controller card pairs.

The Gateway Controller is a single logical entity that physically resides on two cards. The two cards operate in active or hot standby mode: Unit 0 is the active card, while unit 1 is the inactive card operating in hot standby mode. If unit 0 fails, unit 1 assumes operations and becomes the active card. The two cards share an IP address.

"Logical view of different Gateway Controller types and their interaction" (page 41) shows the Gateway Controllers, and other units, that are housed in the SAM21. The figure also illustrates how Gateway Controllers use the CS LAN to communicate with each other and with other CS 2100 softswitches and packet network components. Communication between the Shelf Controllers and Gateway Controllers through the cPCI bus is not shown.

Logical view of different Gateway Controller types and their interaction



Cabinets used for Gateway Controllers/SAM21s in the Communication Server 2100 XA-Core

The PTE cabinet is equipped with an alarm panel, three power supply and cooling units, bridge extension modules, transition modules, and hot-swappable controllers. Two SAM21 Shelf Controller cards reside in the Call Agent shelves and include a 100bT interface for connection to the packet network.

Cabinets used for Gateway Controllers/SAM21s in the Communication Server 2100 Compact

In a CS 2100 Compact configuration, PTE2000 cabinets with three shelves house SAM21 card cages. Two SAM21 shelves are housed in the main Call Control Frame in the CS 2100 Compact configuration. These shelves not only house Gateway Controllers, but also the Call Agent processor cards. To increase capacity, a CS 2100 Compact lineup can include a PTE2000 Extension Frame, as well as the Call Control Frame, which houses up to three SAM21 shelves with additional Gateway Controllers.

For further information, see "Communication Server 2100 Compact Call Control Frame" (page 32) , which depicts the CS 2100 Compact Call Control Frame.

The Call Agent shelf is based on the Motorola CPX8221, which includes the following components:

- 17 I/O slots and four system slots per chassis
- redundant -48V DC. powered with power switch
- field replaceable units that are hot-pluggable
- alarm panel to indicate individual slot and system status
- NEBS 3-compliant

Gateway Controller access to the packet network

Media gateway configuration

You must provision Gateway Controllers and media gateways separately with the address information they need to communicate with each other. For each media gateway controlled by a Gateway Controller, you must specify Gateway Controller datafill information such as gateway IP address, User Datagram Protocol (UDP) port, and trunk or line endpoints available. Similarly, media gateway datafill specifies information about the controlling Gateway Controller, including its IP address and the User Datagram Protocol (UDP) port used for the device control messaging.

Gateway Controller protocol support

The primary purpose of a Gateway Controller is to act as an intermediary between packet network components (for example, gateways, other Communication Servers, and Media Server 2010) and the call-processing and service logic functions provided by the Core. The Gateway Controller acts as an intermediary by relaying requests and information from the packet network components to the Core and by relaying instructions and information from the Core. Gateway Controllers terminate packet network signaling and map this onto proprietary intra-CS 2100 signaling to and from the Core. Gateway Controllers must also provide protocol support for OAMP access from Device Managers and management applications.

The CS 2100 supports the Simple Network Management Protocol (SNMP) between Gateway Controllers and the Gateway Controller Manager running on a Sun Netra OAMP server.

Gateway Controller provisioning and capabilities

"Gateway Controller engineering guidelines" (page 43) describes capacity and provisioning requirements for Gateway Controllers.

Note: All figures quoted are general and are subject to variation depending on the network call model and capacity requirements.

Enterprise network planners should consult with Nortel Sales Engineering when determining network-specific estimates.

Gateway Controller engineering guidelines

Component	Description
SAM21s and Gateway Controllers	• A SAM21 has a maximum of 16 slots available for Gateway Controllers and, therefore, can house a maximum of eight Gateway Controllers of all types. In a CS 2100 Compact configuration, capacity is reduced to seven Gateway controllers because two slots must house the Call Agent cards. • The recommended maximum number of Gateway Controllers that you can provision on a CS 2100 is 60 Gateway Controllers of all types, of which 30 can be Gateway Controllers for media gateways, and 30 can be packet-side Gateway Controllers. • A Gateway Controller can support trunk access and line access.
Trunks, lines, and endpoints	• A CS 2100 can support an maximum of 165,000 trunk and/or line endpoints. Within this range, the following limits apply to different endpoint types: — 48,000 PRI/H.323 trunks — 4093 H.323 gateways — 150,000 lines • The allocation of the total number of supported trunks between access Gateway Controllers depends on the call model supported by the CS 2100.
Trunk access Gateway Controllers	• A trunk access Gateway Controller supports up to 30 media gateways. • A trunk access Gateway Controller supports up to 4,096 TDM-side trunk endpoints terminated on media gateways (up to 2,048 on a gateway). • The maximum BHCA is 76,800 (PRI). • The maximum number of simultaneous calls is 3,960 (PRI). • The maximum number of supported PRI D-channels is 132 and B-channels is 3,960.

Component	Description
Line access Gateway Controllers and gateways	• The maximum number of line endpoints supported by a line access Gateway Controller is 6,400. • The maximum BHCA supported by a line access Gateway Controller is 38,000. • CPE LAN line gateway guidelines are as follows: — Lines are assigned to line groups, with each group consisting of a maximum of 1,024 lines (actually 1,023, as one is reserved for maintenance). All of the lines belonging to line group (that is, all the gateways serving those lines) must be supported by one Gateway Controller. — A maximum of 2,000 simultaneous calls can occur per line Gateway Controller.
Audio Controller Gateway Controller for Media Server 2010	• A maximum of 4096ports for IP telephony connections (subject to feature-related limits) as follows: — One port is used for each announcement played to a call party. — One port per call party is used for conferencing. — Four ports are used for a call subject to monitoring. • A maximum of 468 simultaneous announcements for IP is provided. • The maximum BHCA is 40,000 or 60,000 depending on the CPU, with a maximum of 20,000 on one interface card.
Audio Controller Gateway Controller for Media Server 2010	• A maximum BHCA of 80,000 is provided. • There are 120 or 240 ports for conferencing and/or monitoring. • There are 240 ports for announcements.

Supported protocols

"Protocol summary" (page 44) describes the protocols that Gateway Controllers support.

Protocol summary

Protocol	Description
H.248	Call Control protocol for communication between the Gateway Controllers and Media Server 2010. The Gateway Controller instructs the Media Server 2010 to interact with a media gateway for announcements, conferencing, and monitoring.

Protocol	Description
ISDN User Adaptation (IUA)	The system transports IUA over SCTP v5 for call control to gateway Controllers for PRI.
Simple Network Management Protocol (SNMP)	Enables the Shelf Controller to manage the Gateway Controllers.
Real-time Transport Protocol (RTP)	An IETF standard (RFC 1889) for streaming real-time multimedia over IP in packets. RTP carries data that has real-time properties, such as voice and video over packetized networks. The Media Gateway 15000 uses RTP to encapsulate voice packets, which are then carried over User Datagram Protocol (UDP) over IP across the packet network to the terminating media gateway.
Real-time Control Protocol (RTCP)	This protocol monitors the Quality of Service (QoS) and conveys information about the participants in an on going RTP session. The system sends feedback about the session to the sending parties in the form of RTCP reports.
H.323	The ITU-T standard for sending voice (audio) and video using IP on a LAN without QoS. H.323 includes Q.931 for call setup, H.225 for call signalling, H.245 for exchanging terminal capabilities, RTP/RTCP for packet streaming, G.711/G.712 for CODECs, and several other protocols, many of which must be negotiated to set up a simple voice call.
Media Gateway Control Protocol (MGCP)	A protocol used within a Voice over IP system. MGCP is an IETF work in progress. MGCP is an internal protocol used within a distributed system that appears to the outside world as a single VoIP gateway. This system is composed of a Call Agent and a set of gateways, including at least one "media gateway" that converts media signals between circuits and packets and at least one "signalling gateway."
Session Initiation Protocol (SIP)	Session Server support for SIP signaling and CCS7 encapsulation is designed to be compliant with RFC3261, which defines a SIP interface for open interoperability between call servers and other Network Elements. In this implementation, SIP signaling terminates on the Session Server, which extracts the CCS7 signaling and passes it to the Dynamic Packet Trunk (DPT) Gateway Controller.
Real-time Control Protocol Extended Reports (RTCP XR)	A new VoIP management protocol, RTP Control Protocol Extended Reports (RTCP XR), defines a set of metrics that contain information for assessing VoIP call quality and for diagnosing problems. RTCP XR messages containing key call-quality-related metrics are exchanged periodically between IP phones and gateways. A probe or analyzer monitors these metrics midstream to support problem resolution.

References

"Documentation references" (page 46) shows where you can find more information about Gateway Controllers and Shelf Controllers.

Documentation references

Document title	Document Number
Gateway Controllers (GWCs) (provide the equivalent of XPMs)	
Gateway Controller Basics	NN10189-111
Gateway Controller Fault Management	NN10202-911
Gateway Controller Configuration Management	NN10205-511
Gateway Controller Performance Management	NN10208-711
Gateway Controller Security and Administration	NN10213-611
Upgrading the Gateway Controller	NN10196-461
SAM21 Shelf Controllers (play a role in hot swapping cards in the shelf and provide some fault assistance to all the cards)	
SAM21 Shelf Controller Basics	NN10025-111
SAM21 Shelf Controller Fault Management	NN10089-911
SAM21 Shelf Controller Configuration Management	NN10111-511
SAM21 Shelf Controller Performance Management	NN10155-711
SAM21 Shelf Controller Security and Administration	NN10177-611
Upgrading the SAM Shelf Controller	NN10067-461

Interworking Spectrum Peripheral Module IP

Introduction

The Interworking Spectrum Peripheral Module Internet Protocol (IW SPM-IP) transcodes voice between the TDM network and the IP network. The IW SPM-IP is a legacy-based, fault-tolerant peripheral with the following network connections:

- DS-512 connection to the ENET
- Gigabit Ethernet (GbE) connections to the packet network

The IW SPM-IP supports the following features:

- G.711 and G.729 voice coder/decoder (CODEC)
- silence insertion, detection and suppression
- comfort noise generation
- fax and modem detection
- adjustable jitter buffer

Supported call types

The IW SPM-IP supports the following types of call:

- trunk testing call on the gateway trunk using a legacy Maintenance Trunk Module (MTM) test circuit
- legacy TDM trunk and gateway TDM trunk interworking calls
- legacy TDM trunk and Dynamic Packet Trunk interworking calls

Functions

The IW SPM-IP bridges calls between the existing Nortel Meridian SL-100 Time Division Multiplexing (TDM) switch and the IP network. As mentioned previously, this solution is referred to as a "hybrid" configuration.

Note: Non-hybrid configurations do not require an IW SPM-IP.

The IW SPM-IP connects to an ENET over C-side DS-512 fiber links and to the IP network over GbE on the P-side. Between these two connections are the following components:

- Common Equipment Module (CEM) - connects to the DS-512 links and performs the bridge management function.
- Gigabit Ethernet Resource Module (GEM) - provides the means to connect these bridges to the IP network over GbE.

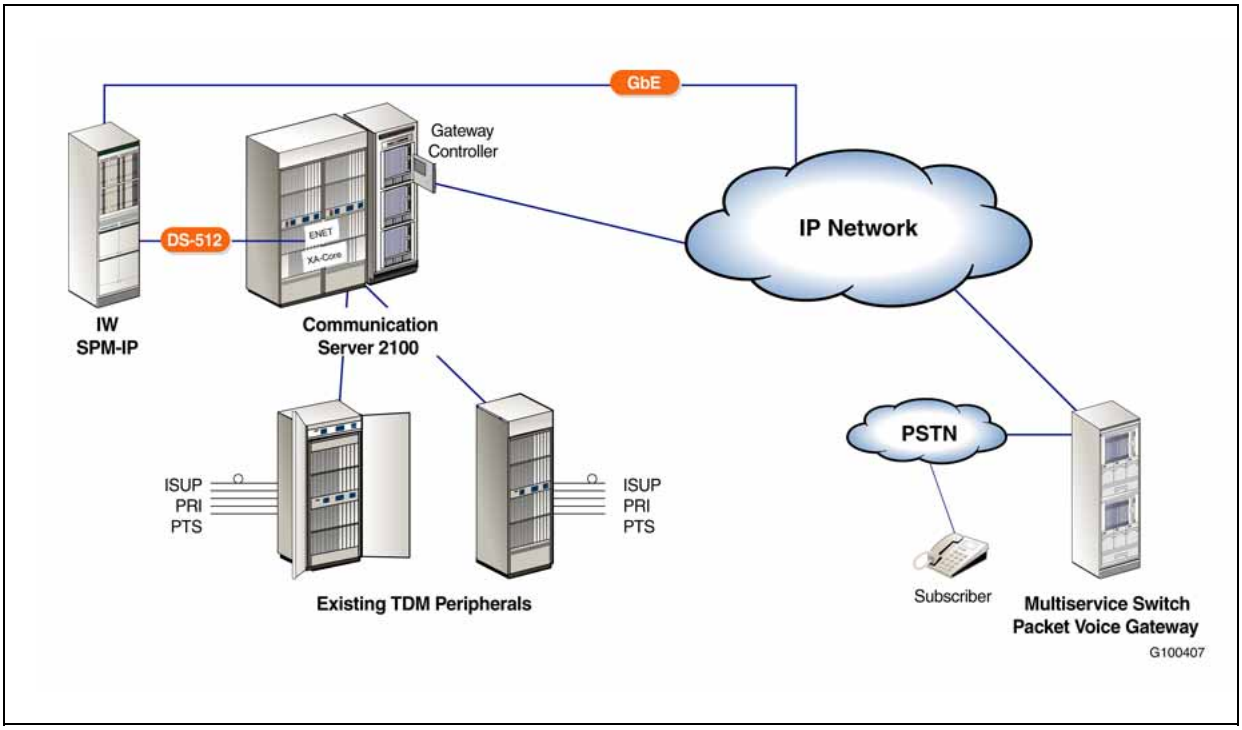
The IW SPM-IP provides interworking capability to legacy Meridian SL-100 TDM peripherals. IW SPM-IP enables the legacy TDM equipment to access Dynamic Packet Trunks (DPTs) and makes connections to far-end nodes. The IW SPM-IP also provides interworking to test trunk services for media gateways.

The IW SPM-IP is required for both the CS 2100 XA-Core and the CS 2100 Compact hybrid TDM and IP deployment off a single Communication Server. By creating a new resource module that supports an IP packet interface, which can be housed in the existing Spectrum Peripheral Module platform, the Spectrum Peripheral Module platform is transformed into an Interworking Spectrum Peripheral Module that can interface with elements of a packet network, such as the Media Gateway 15000. The new resource module, GEM, is easily added to an existing Spectrum Peripheral Module to support a Gigabit interface to the network.

Technicians perform IW SPM-IP maintenance functions, such as monitoring alarms and logs, by accessing the Maintenance and Administration Position Command Interpreter (MAPCI) on the XA-Core. High density is available with a minimum of 2016 DS0s per shelf/4032 DS0s per frame. The configuration supports Diffuser Quality of Service (QoS) and Remote Monitoring (RMON) statistics.

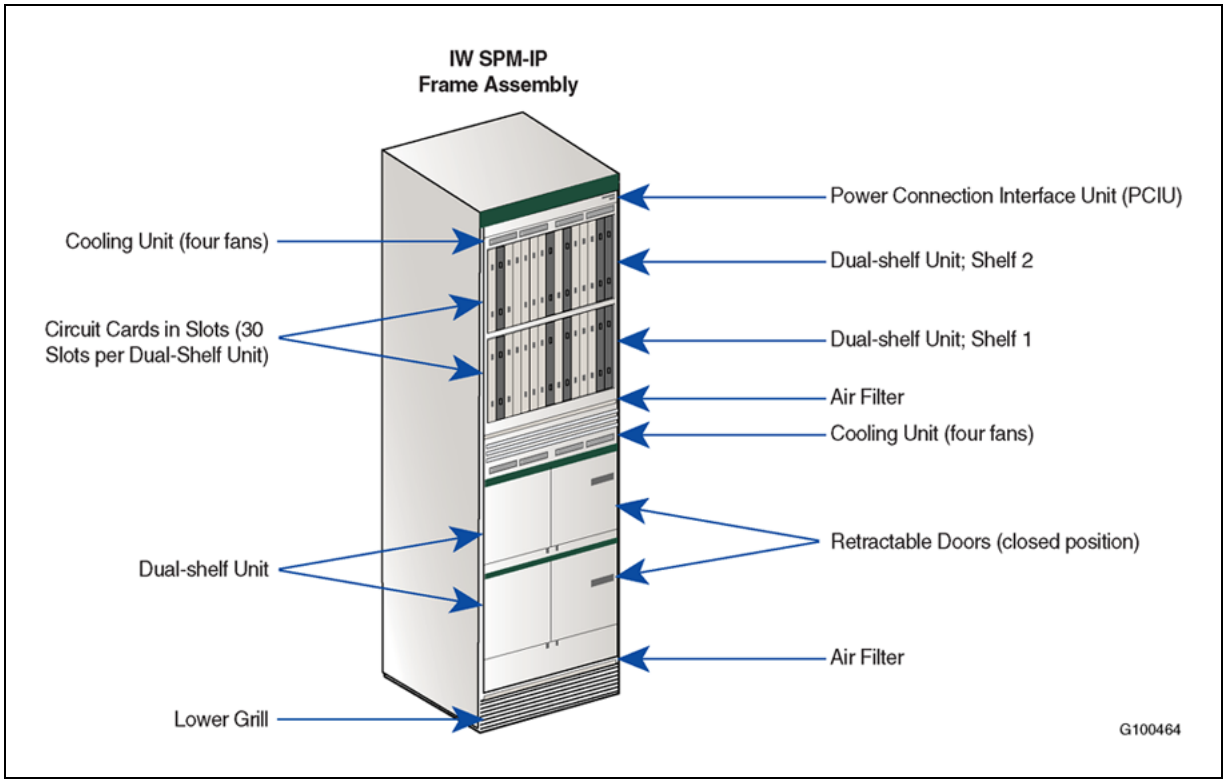
"IW SPM-IP enterprise network configuration example" (page 48) shows an example of how the IW SPM-IP is configured on an enterprise network.

IW SPM-IP enterprise network configuration example



"Interworking Spectrum Peripheral Module Internet Protocol frame assembly" (page 49) illustrates the layout of an IW SPM-IP cabinet.

Interworking Spectrum Peripheral Module Internet Protocol frame assembly



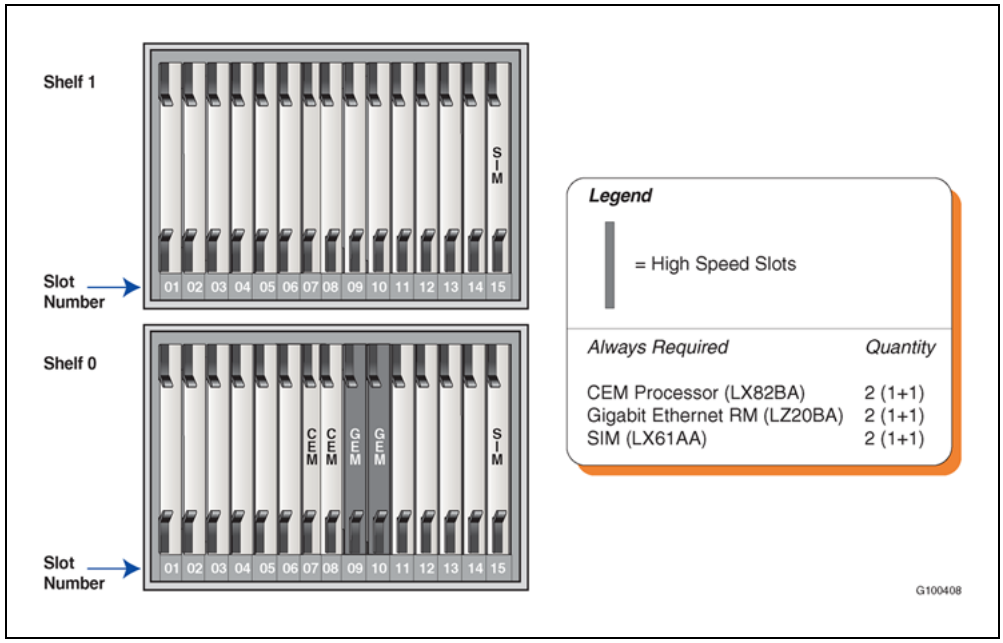
The IW SPM-IP is an ENET-hosted Spectrum Peripheral Module that has four C-side DS-512 links connecting the Common Equipment Module of the IW SPM-IP to the ENET. On the P-side (facing the packet network) the IW SPM-IP has two GbE links to the ERS 8600s in the CS LAN.

The IW SPM-IP uses Peripheral Processor Virtual Machine (PPVM, an internal CS 2100 protocol) for communication with the XA-Core. The IW SPM-IP uses Real Time Protocol (RTP), or Real Time Control Protocol (RTCP,) which complements RTP by monitoring data delivery for bearer connections to the Media Gateway 15000.

Shelf layout and physical interfaces

"IW SPM-IP shelf layout" (page 50) shows the recommended card configuration for the IW SPM-IP.

IW SPM-IP shelf layout



The IW SPM-IP shelf assembly consists of the following components:

- cooling unit with four fans for forced-air cooling
- two 30-slot shelves that house the following types of modules:
  - The Shelf Interface Module (SIM) provides power to the shelf. Each shelf has one Shelf Interface Module.
  - The Common Equipment Module (CEM) provides the following functions:
    - operational control of the IW SPM-IP
    - control of signal processing
    - system clock
    - physical connection to ENET
  - The Gigabit Ethernet Resource Module (GEM) provides the physical connection to the packet network. The GEM transcodes voice signals. Each shelf assembly contains two GEMs.

Operating parameters

The following operating parameters apply to the IW SPM-IP:

- Junctored Network is not supported.
- The Input/Output Controller (IOC) does not support the magnetic tape drive for a disk drive supported by a NT1X55xx-based disk drive controller.

- The following peripheral modules are not supported:
  - Line Module (LM)
  - Remote Line Module (RLM)
  - Digital Carrier Module (DCM)
  - PCM-30 Digital Trunk Controller (PDTC/PDTC-I)
  - Autovon Trunk Module (ATM)
  - Ethernet Interface Unit (EIU) supporting Intelligent Call Management (ICM) only, with telnet available through the SuperNode Data Manager (SDM)
- 2016 simultaneous calls over G.711 or G.729
- Fax and modem support using G.729

References

"Documentation references" (page 51) shows where you can find more information about the IW SPM-IP.

Documentation references

Document title	Document number
IW SPM-IP Basics	NN10015-111
IW SPM-IP Fault Management	NN10078-911
IW SPM-IP Configuration Management	NN10100-511
IW SPM-IP Performance Management	NN10144-711
IW SPM-IP Security and Administration	NN10166-611
Upgrading the IW SPM-IP	NN10056-461

Communication Server 2100 Compact

Description

The CS 2100 Compact architecture changes the dynamics of traditional switching by distributing its three fundamental elements as follows:

- intelligence or call control
- switching
- connectivity

Media Gateway Controllers carry out the call control. A distributed packet-based network with the line and trunk connectivity through the Media Gateways replaces the TDM switching layer. The Media Gateways themselves are under the direct control of the Media Gateway Controllers.

The Gateway Controller acts as a call-processing protocol converter to create a bridge between media gateways and CS 2100 Compact call processing.

Enterprise customers have a second core processor option, the CS 2100 Compact. The off-the-shelf hardware platform is based on the Compact PCI standard, which delivers manufacturer inter-operability that has its roots in the personal computer, but delivers flexibility in a standards-based manner.

The off-the-shelf software is the most open software available today, Linux©. But this Linux goes beyond standard operating system. This operating system has been hardened by Motorola and Nortel to deliver the same reliability and operability that is expected from other Nortel products.

The CS 2100 Compact provides flexible, distributed call and service control across a packet network over an IP backbone. The CS 2100 Compact performs all call control processing functions for your network including translations, routing, and central service delivery. You can deploy next-generation services on a single CS 2100 Compact and make them available to multiple customer groups.

ATTENTION

For more information about the IP telephony solution, see the *Communication Server 2100 Application Planning Guide* (555-4001-108).

Two 10/100 BaseT Ethernet interfaces run from the Call Agent on the CS 2100 Compact to the CS LAN. Each Ethernet link connects to a different ERS 8600.

Communication Server 2100 Compact hardware

The CS 2100 consists of the following components:

- Call Agent
- Storage Management (STORM)
- Gateway Controllers

Call Agent

The Call Agent is the call-processing engine of the CS 2100 Compact. The Call Agent hardware is a Single Board Computer (SBC) that resides in a SAM21 shelf. Two Call Agent cards and two SAM21 shelves are required for redundancy. A single Call Control Frame houses the two shelves. The Call Agent provides the following functions:

- call processing services on line and trunk endpoints
- translation and routing support for all endpoints served by the CS 2100 Compact

- a provisioned view of profiles of
  - — subscriber services
  - — trunk group services
- billing data collection and formatting, before sending the data to the Element Management System (EMS)
- log, alarm, and Operational Measurement (OM) information collection for use in downstream network management systems

The Call Agent resides on the Call Agent card in the CS 2100 Compact.

Storage Management (STORM)

Storage Management provides Network File System (NFS) services to applications running on the CS 2100 Compact. An NFS is a distributed file system used by applications to access files and directories on remote computers. STORM acts as an NFS for Call Agent clients.

Storage Management resides on two STORM SAM-XTS server units. Each Call Agent card uses one STORM unit as a primary storage device and the other STORM unit as a secondary storage device. The STORM units provide no redundancy between themselves. All component applications using the STORM services provide their own data redundancy (if required) by ensuring that any important data is written to both STORM units. If a STORM unit is out of service, access to data stored on it is interrupted until the STORM unit is recovered. Each unit is NEBS-compliant and has two 72-GB hot-swappable disk drives. A CDROM drive on the front of each unit is used for initial software loading and is available for software upgrade media.

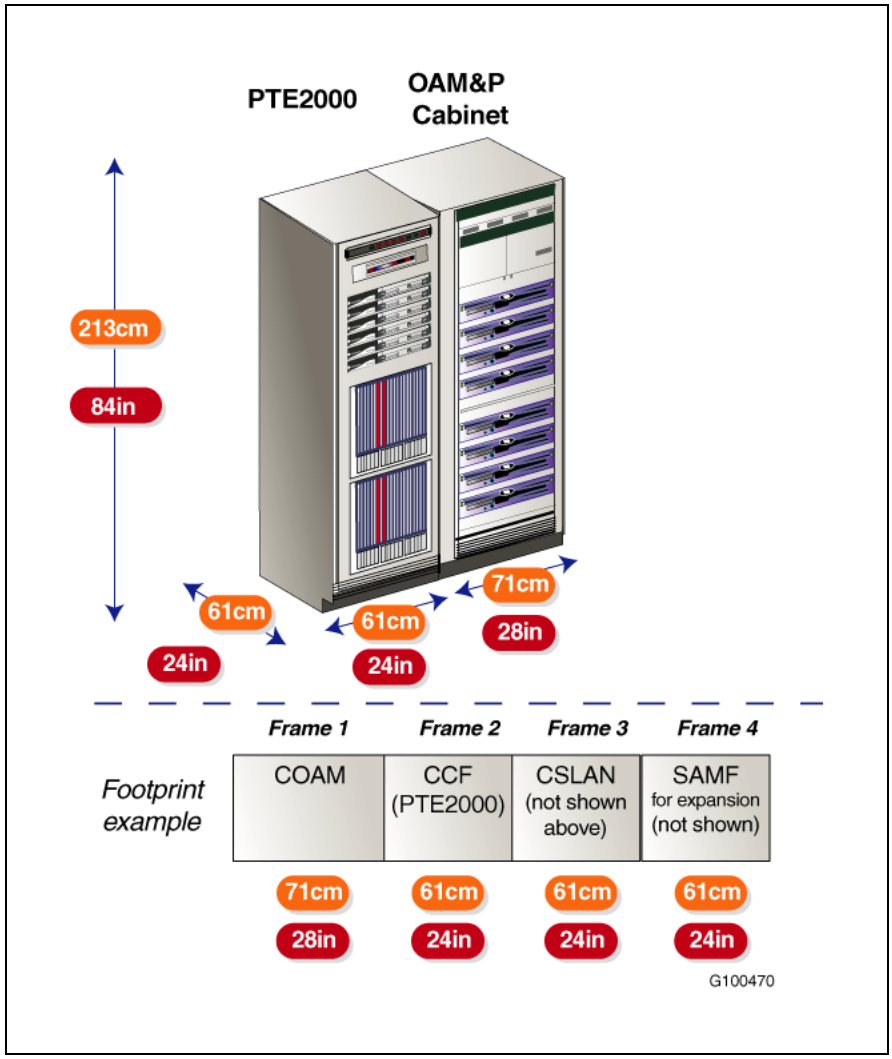
Frame layout

The CS 2100 Compact resides in a Call Control Frame in a PTE2000 frame. Each Call Control Frame consists of the following components:

- two Call Agent/SAM21 shelves
- two STORM SAM-XTS server units that store data on internal disk drives
- one Astec Breaker Interface Panel (BIP) that serves as the power distribution shelf

"Communication Server 2100 Compact Call Control Frame" (page 32) shows the Call Control Frame. "Sample Communication Server 2100 Compact cabinet lineup" (page 54) shows a sample cabinet lineup.

Sample Communication Server 2100 Compact cabinet lineup



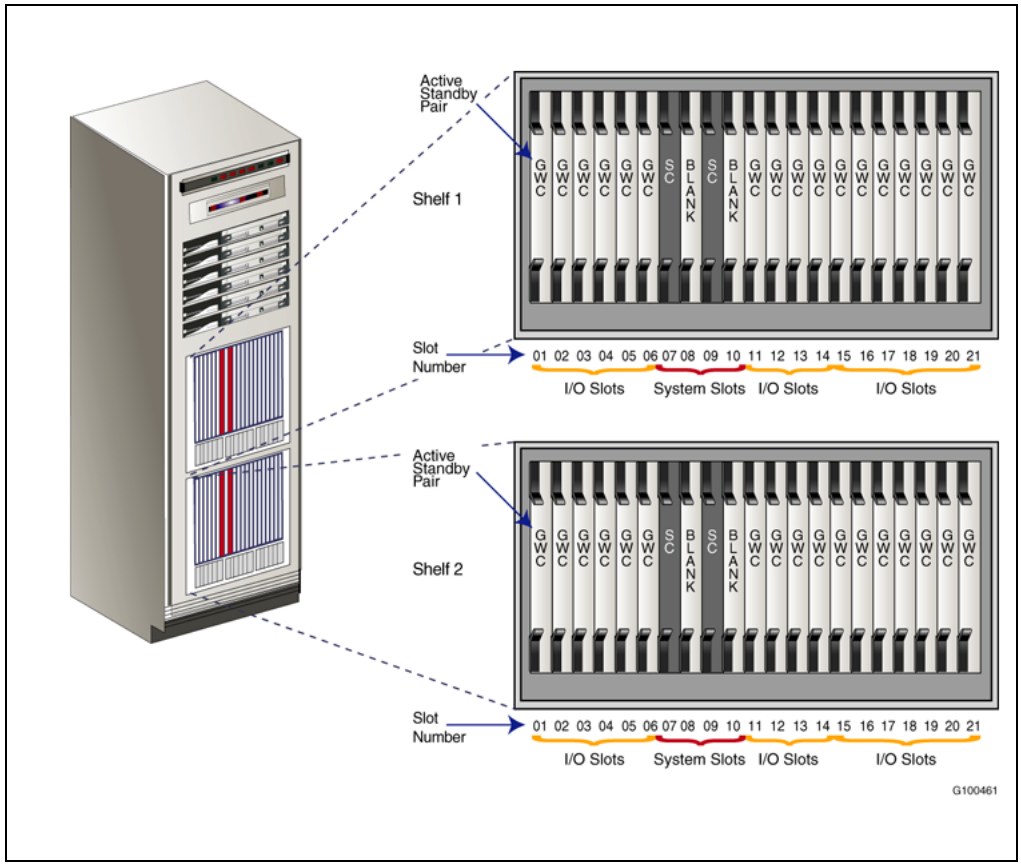
Card configuration

The Gateway Controller circuit card is based on the Motorola MCPN750 or MCPN905 Single Board Computer (SBC). Two redundant SBCs make up each Gateway Controller. The Gateway Controller circuit cards host the Gateway Controller software that, together with the Call Agent, provides the CS 2100 Compact with its Media Gateway Controller functions. Processing capacity is scalable by adding Gateway Controller circuit card pairs. A maximum of eight Gateway Controller card pairs exist for each SAM21 shelf. The 21st slot (front and rear) should always be empty.

The SAM21 Shelf Controllers (SCs) provide physical management of the SAM21 shelf and support the resident Gateway Controller or other cards. You can fill all 16 Input/Output slots in the SAM21 shelf with Gateway

Controller cards, as shown in "Communication Server 2100 sample SAM21 shelf configuration" (page 55), depending on the network requirements of your organization.

Communication Server 2100 sample SAM21 shelf configuration

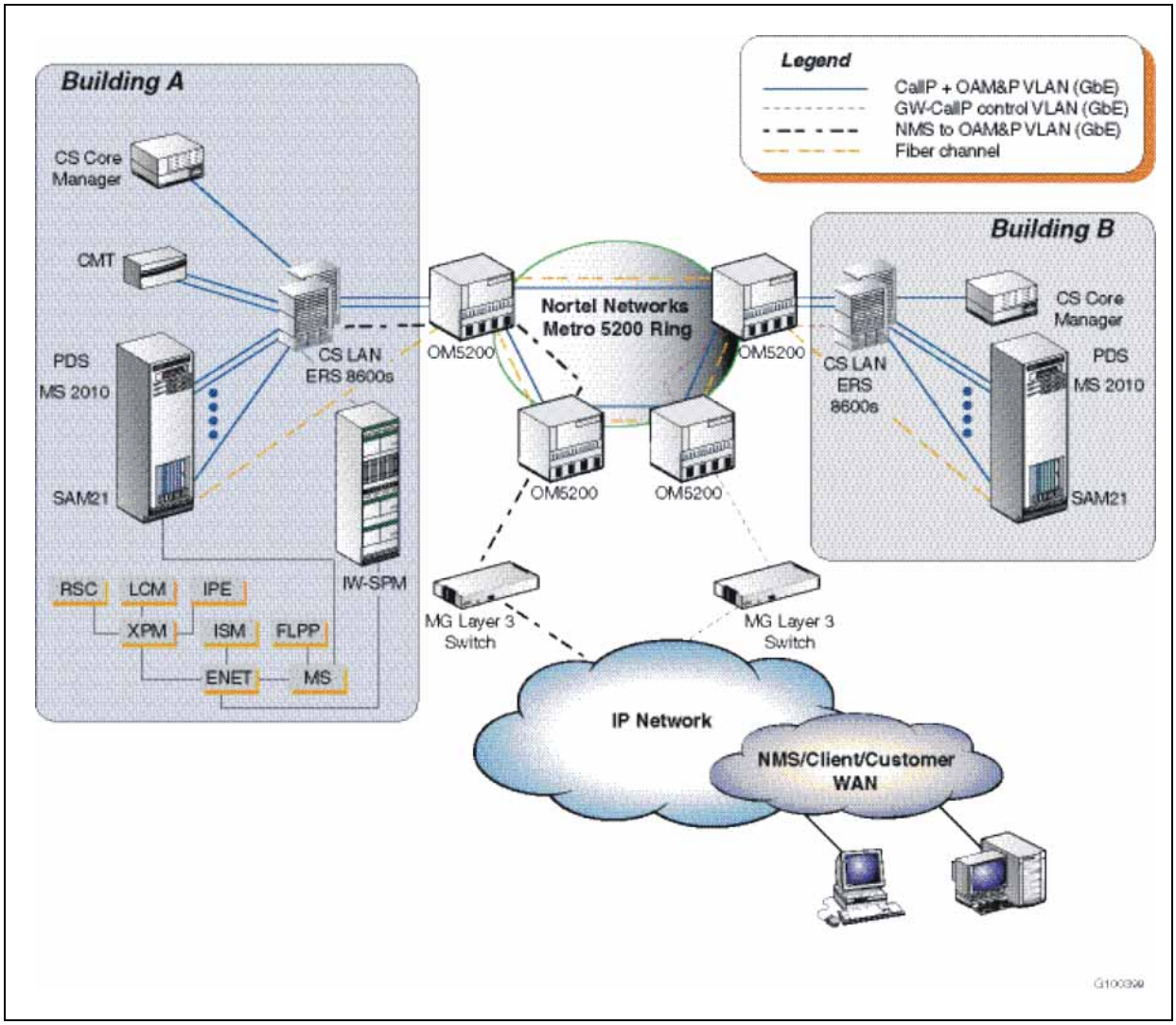


Geographic survivability

Geographic survivability allows services to continue in the event of a catastrophic loss of a call server site caused by a natural or man-made disaster. The Geographic Survivability for the CS 2100 platform distributes the redundancy of the CS 2100 Compact architecture in different physical locations and uses application layer protection. Nodes are connected over a fault-tolerant optical network that spans the distance between two sites. Compact Call Agent blades can alternately be synchronized by means of a Gigabit Ethernet (GbE) interface. There are mechanisms to select which of the two sites provides services and to allow load sharing and proper routing.

"Geographic survivability network configuration" (page 56) shows an example of the geographic survivability configuration of the CS 2100 Compact.

Geographic survivability network configuration



ATTENTION

See the *Communication Server 2100 Geographic Survivability Planning Guide* (555-4031-901), for more information about the geographic survivability.

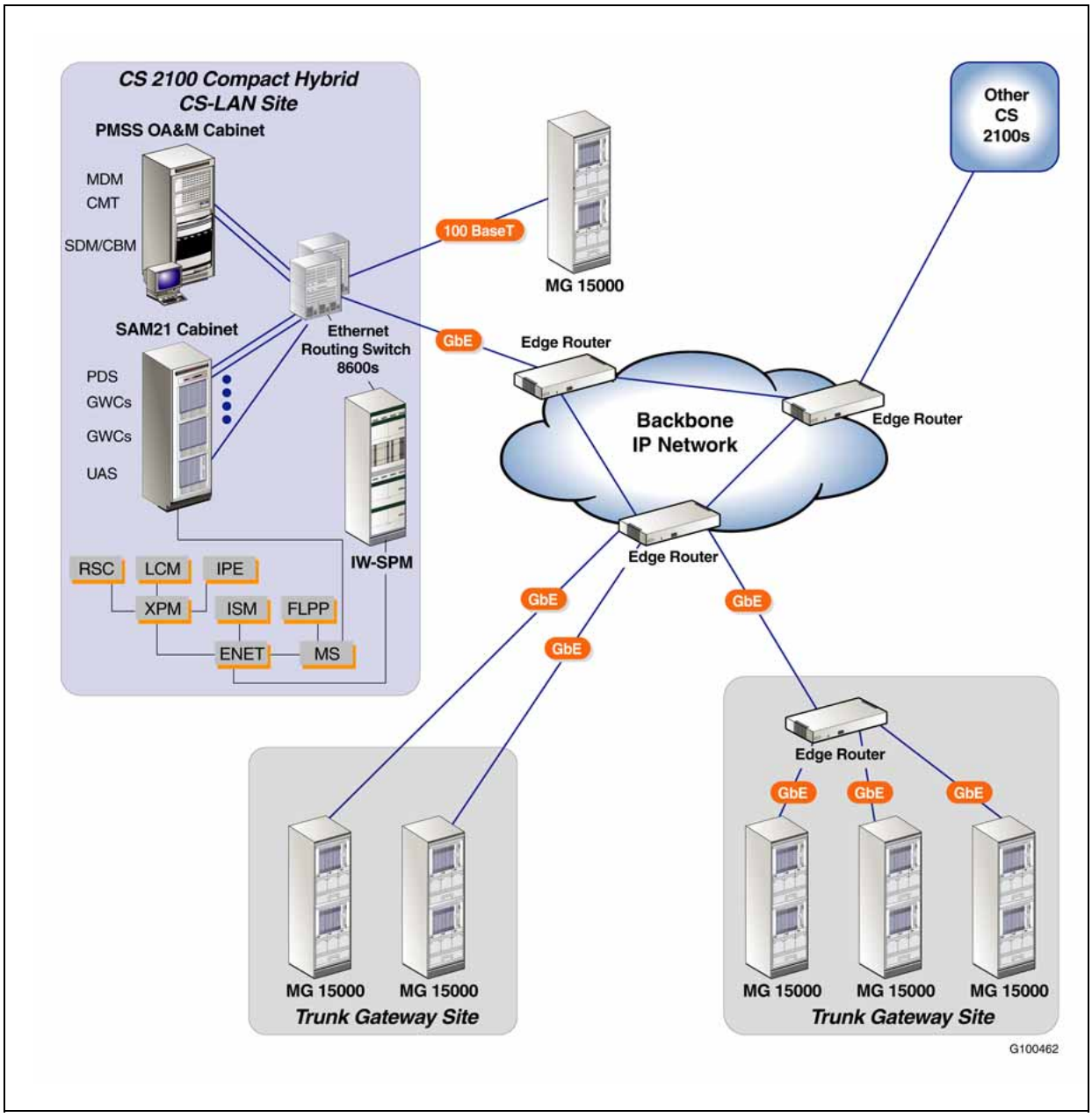
Hybrid support

The CS 2100 Compact provides the ability to support a Time Division Multiplexing and a packet softswitch from the same core. The CS 2100 Compact provides hybrid support through the Message Controller (MC) that resides within the MCPN765 processor card. It provides common commands for all subtending TDM components.

"Communication Server 2100 hardware" (page 23) lists the existing Meridian SL-100 peripherals that are supported on the TDM side of the network in a hybrid configuration.

"Example Communication Server 2100 Compact hybrid configuration" (page 57) shows the CS 2100 Compact in a hybrid configuration.

Example Communication Server 2100 Compact hybrid configuration



Signaling interfaces

"Telephony protocol support" (page 58) shows the telephony protocols to which the packetized portion can interface.

Telephony protocol support

Interface	Abbreviation
Primary Rate Interface National ISDN 1 (also known as NTNA)	PRI NI-1
Primary Rate Interface National ISDN 2	PRI NI-2
Digital Signaling Level 1 (on Media Gateway 15000 using demux)	DS1
Digital Signaling Level 3 (on Media Gateway 15000 using demux)	DS3
Optical Carrier Level 3 (on Media Gateway 15000)	OC-3
Multi Frequency	MF
Signaling System #7	SS7
Analog line	-

Operating parameters

The following operating parameters apply to the CS 2100 Compact:

- international protocols not currently supported
- Communication Servers are limited in capacity as follows:
  - 150,000 clients (not including trunks)
  - 1,300,000 Busy Hour Call Attempts (BHCA)
- NEBS-compliant
- in-service upgrades
- 99.999 percent availability

Communication Server 2100 XA-Core

Description

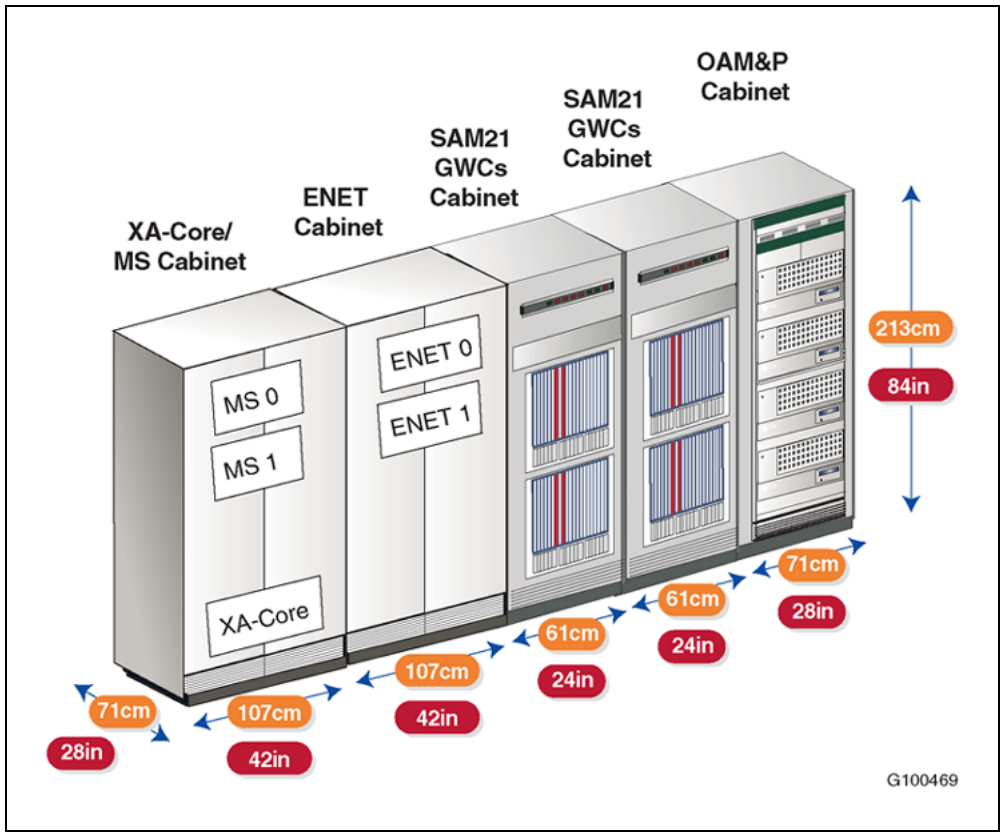
The CS 2100 XA-Core provides the foundation for the IP switching by building on the hardware of existing Meridian SL-100 digital switches. Specifically, it reuses the XA-Core as its processing engine.

Two 10/100 BaseT Ethernet links run from the High Performance I/O Processor (HIOP) cards on the CS 2100 XA-Core to the CS LAN. Each Ethernet link connects to a different Ethernet Routing Switch (ERS) 8600. The configuration requires 10 IP addresses.

In addition to the Ethernet interface, the XA-Core connects to both Message Switches by dual OC-3 connections. Each Message Switch has several DS-512 port interfaces. A DS-512 pair is used to interface to the Core Manager on the SuperNode Data Manager platform.

"Sample Communication Server 2100 XA-Core cabinet lineup" (page 59) shows a sample cabinet lineup.

Sample Communication Server 2100 XA-Core cabinet lineup



Hybrid support

The CS 2100 XA-Core can support a Time Division Multiplexing and packet softswitch from the same Core. The CS 2100 XA-Core provides hybrid support through the Ethernet IOP in the XA-Core shelf and delivers Meridian SL-100 TDM support for the following configuration:

- Message Switch in either a SuperNode SE or SuperNode
- Enhanced Network residing in either a SuperNode SE or Enhanced Network Combined cabinet
- Input/Output devices consist of the Input/Output Controller (IOC) and Input Output Module (IOM) supporting Current Loop, Electronic Industries Association (EIA), X.25, and V.35 devices. The CS 2100 XA-Core supports the NTFX32xx-based storage media.

- "Communication Server 2100 hardware" (page 23) lists the existing Meridian SL-100 peripherals that are supported on the TDM side of the network in a hybrid configuration.

Signaling interfaces

The CS 2100 XA-Core supports the same telephony protocols as the CS 2100 Compact (see "Telephony protocol support" (page 58)).

Operating parameters

The following operating parameters apply to the CS 2100 XA-Core:

- Junctored Network not supported
- Media Server 2010 not supported in a hybrid configuration.
- Input/Output Controller does not support the magnetic Tape Drive for a disk drive supported by a NT1X55xx-based disk drive controller
- international protocols not supported
- Communication Servers are limited in capacity as follows:
  - 150,000 clients (not including trunks)
  - 1,650,000 Busy Hour Call Attempts (BHCAs)
- NEBS-compliant
- in-service upgrades
- 99.999 percent availability

Gateways

Introduction

For a Communication Server 2100 (CS 2100) to perform its network role, you must deploy the server with one or more media gateways to handle packet network bearer connections. A media gateway provides an interface for bearer connections (for example, mapping a packet-based media stream to a circuit-based media stream, seamlessly providing any required format conversion while maintaining content integrity). Depending on the telephony interface supported, a media gateway can also provide signaling gateway functions.

Gateway Controllers convert between Proprietary Processing Virtual Machine (PPVM) messages and open standard protocols used by media gateways (for example, H.248 and MGCP).

This chapter contains the following sections:

Trunk gateways

- "Nortel Media Gateway 15000" (page 62)
- "Nortel Media Gateway 3000 Series" (page 68)

Line gateways

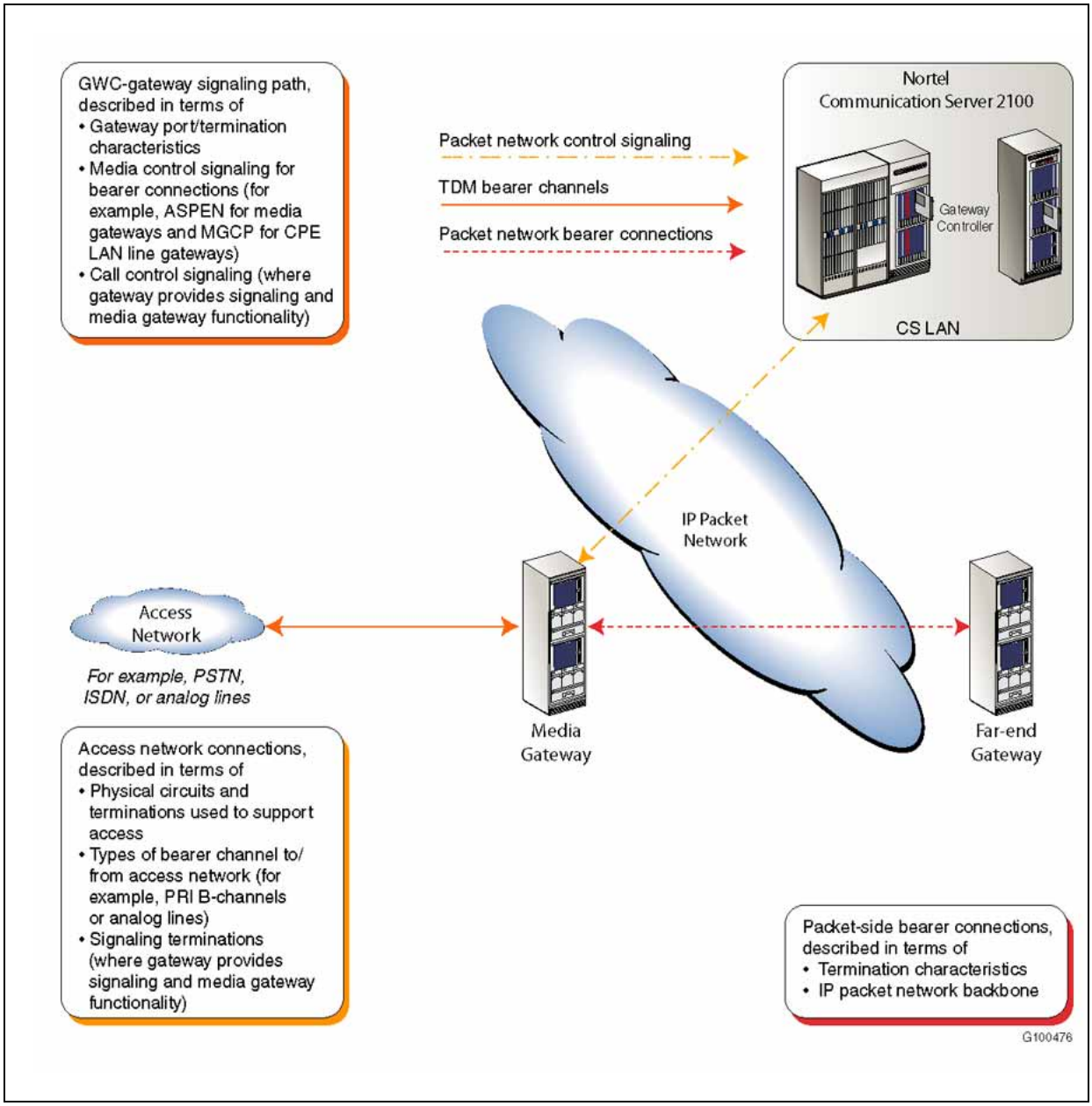
- "IP Client Manager" (page 77)

Multiservice gateways

- "Nortel Media Gateway 9000" (page 85)

"Media gateway capabilities" (page 62) summarizes how gateway capabilities can be categorized.

Media gateway capabilities



Nortel Media Gateway 15000

Description

The Media Gateway 15000 supports Primary Rate Interface (PRI) trunk access to the IP packet backbone network. The Media Gateway serves as an interface between the TDM network and an IP network.

The Media Gateway 15000 performs the following functions:

- converts TDM traffic into IP packets for transfer over an IP network

- converts the IP packets back into TDM format for transfer over the traditional circuit-switched network

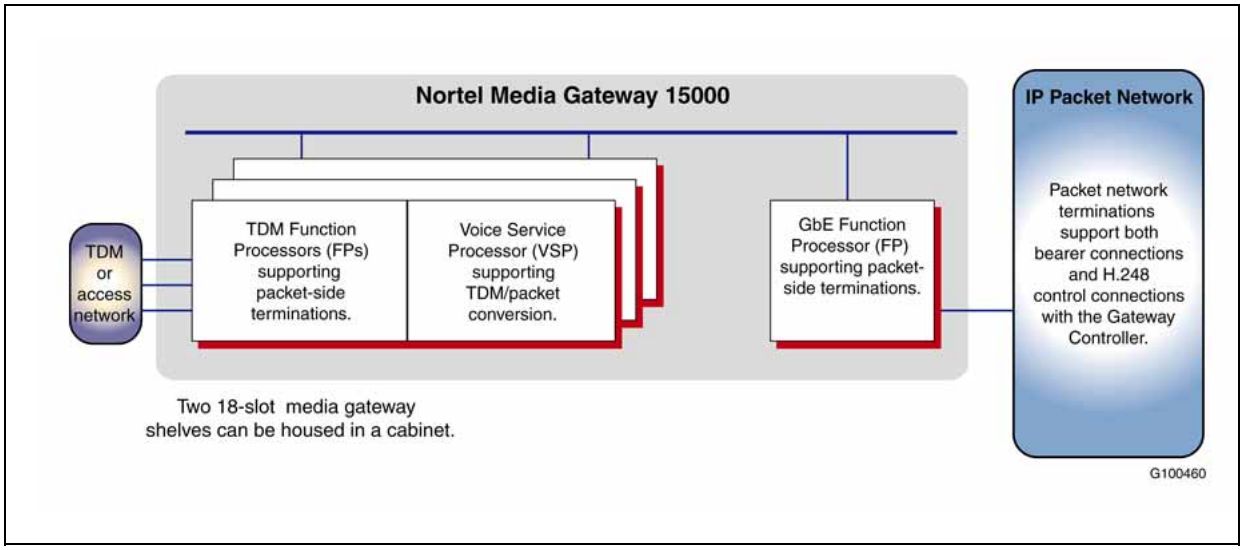
  Note: The Media Gateway 15000 was previously called the Passport 15000 Packet Voice Gateway.

The Media Gateway 15000 application is a carrier-grade integrated voice and data interworking service. With the Media Gateway 15000, the CS 2100 still manages the call. However, instead of using TDM bearer channels to transport the traffic, traffic is routed through IP circuits on the Media Gateway 15000. The Media Gateway 15000 uses the switched native IP configuration.

The Media Gateway 15000 provides signaling gateway functions, as well as media gateway functions. Media gateway functions for PRI means mapping ISDN B-channels onto packet network media streams under H.248 (a Gateway Controller-gateway device control protocol used for IP telephony) control. Signaling gateway functions for PRI means terminating ISDN D-channels and backhauling Layer 3 signaling across the packet network so that call processing can take place at the CS 2100.

"Logical configuration of a Media Gateway 15000" (page 63) illustrates Media Gateway 15000 components and their functions at a logical level.

Logical configuration of a Media Gateway 15000



The Voice Service Processor is the Media Gateway 15000 component that supports seamless conversion between network media streams (for example, circuit-based PSTN media streams) and packet media streams. For IP telephony, the Voice Service Processor handles packetization of

voice samples in Real Time Protocol (RTP). Codec capabilities are as follows (you can provision one default and one compression codec for each Media Gateway 15000):

- G.711, packet size 10 ms or 20 ms
- G.729 and G.729a, packet size 10 ms or 20 ms

From a network perspective, each Voice Service Processor is an independent unit with its own IP address. If more than one Voice Service Processor is housed in a Media Gateway 15000 shelf, the Gateway Controller perceives each as a separate entity. The trunks on a given TDM-side OC-3 carrier are all assigned to a particular Voice Service Processor and are not available to any other Voice Service Processor. Each Voice Service Processor can, therefore, be regarded as a logical gateway.

The IP interface for the MG 15000 is provided by a Gigabit Ethernet (GbE) Function Processor (NTHW49AA) which will provide a common interface for all Voice Service Processors within the MG 15000 chassis. The GbE Function Processor provides a hitless failover if one circuit pack or network interface fails, and it provides higher availability for the services provided within the MG 15000 over the VSP3 architecture.

Physical configuration

The Media Gateway 15000 serves as a media gateway in the CS 2100 network. The Media Gateway 15000 supports the H.248 protocol for communication between the Gateway Controllers and media gateways.

The Nortel Media Gateway 15000 is a multiservice data device that you can deploy as a backbone for existing Media Gateway 15000 edge node networks. It delivers a powerful range of standards-based interfaces and services, including frame relay and IP. Media Gateway 15000 nodes provide multiprotocol routing services, intelligent traffic management, and the nodes simultaneously support voice, data, video, and image traffic. It offers full redundancy, scalable high-capacity, high-speed access and trunking.

The Nortel Media Gateway 15000 device is installed in an NEBS-compliant PTE 2000 frame that can hold two independent devices. Each 18-slot Media Gateway 15000 shelf supports a maximum of 16 processor cards. The two fabric cards interconnect the processor cards. Each processor card has redundant serial links to the two fabric cards.

The Media Gateway 15000 supports the following functions:

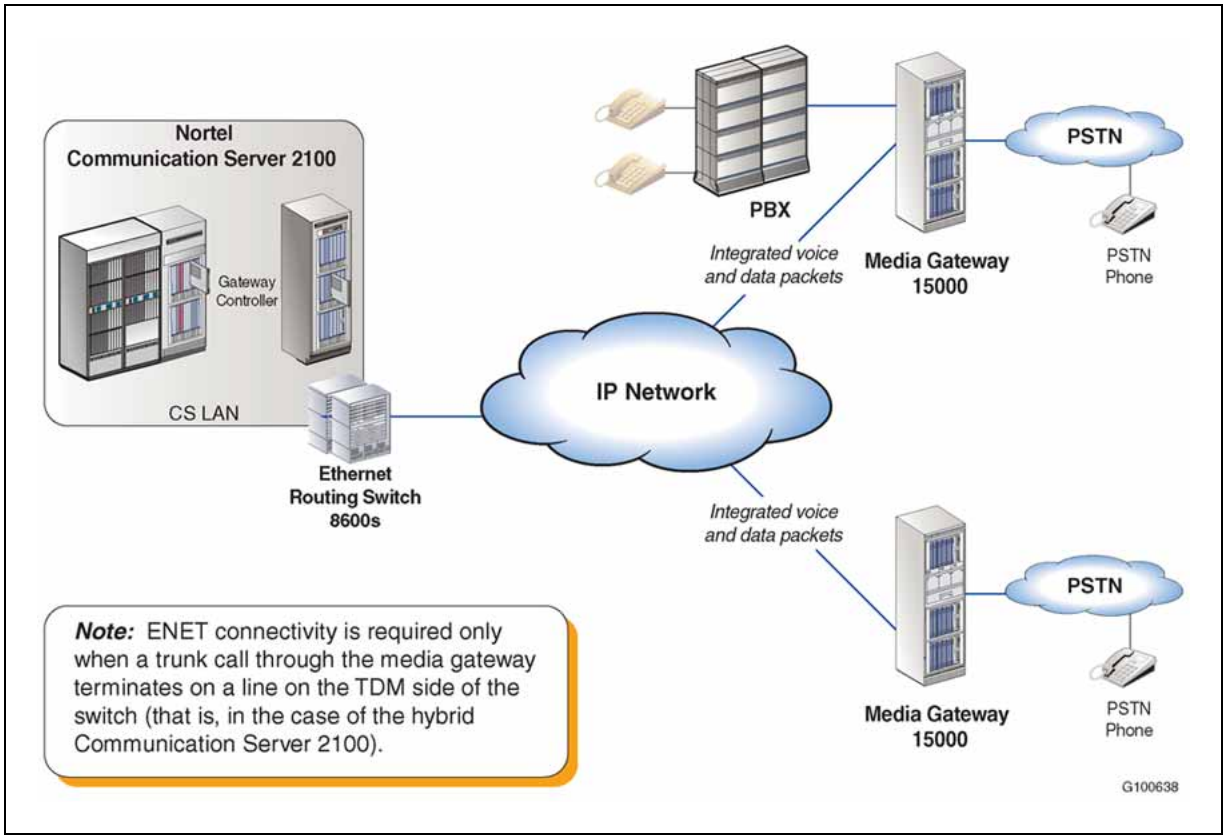
- VSP3-0 FP card
- Hitless Software Migration (HSM)
- Hot Equipment Protection
- Media Gateway Periodic Routine Exercise (REX)

The Media Gateway 15000 supports the following:

- toll-quality ITU-T G.711 PCM, G.726 PCM, G.726 ADPCM, or G.729 A/B CS-ACELP voice with silence suppression, comfort noise generation, and dynamic downspeeding capability for congestion management
- tone generation on the TDM side of the gateway, such as basic service tones, and basic and expanded call progress tones
- Dual-tone Multi frequency (DTMF) digit collection for ANSI PRI agencies
- 56/64 kbps clear-channel fax and modem support
- echo cancellation compliant with ITU-T G.165 and G.168
- tone detection compliant with ITU-T G.164 and G.165
- clear channel support for test trunk capability
- software maintenance and release upgrade support
- interworking with TDM trunks through the Interworking Spectrum Peripheral Module IP

"Media Gateway 15000 example configuration" (page 66) shows an example of a Media Gateway 15000 in a CS 2100 network. The IP channels transport voice and voice-band data traffic over virtual connections within the Media Gateway 15000.

Media Gateway 15000 example configuration



Requirements

To support a Media Gateway 15000, you must install the following hardware and software components:

- **Hardware**
  - a VSP3 optical Function Processor
  - a 1000BaseFX Ethernet Function Processor (for the native IP configuration)
- **Software**
  - Media Gateway base
  - Packet Voice Gateway
  - IP
  - Wide Area Network Data Terminating Equipment (WAN DTE)
  - Media Gateway networking

Operating parameters

The following operating parameters apply to the Media Gateway 15000:

- 99.9999 percent reliability
- NEBS level 3
- Supports OC-3; mux to deliver DS1 or DS3.
- The Media Gateway 15000 supports PRI, Signaling System #7, and Multi Frequency (MF) trunks.

Media Gateway 150000 physical interfaces depend on the type of Packet Voice Gateway and Voice Services Processor. "Media Gateway 15000s capacity summary" (page 67) lists the overall maximum number of 64-kbps bearer connections or DS0s that various Media Gateway 15000 configurations can support (the numbers are less if redundancy is in use).

Media Gateway 15000s capacity summary

Media Gateway type	Codec type	Maximum 64 kbps channels/DS0s per VSP
Media Gateway 15000 with VSP3 optical	G.711 (10 ms)	2,016
	G.711 (20 ms)	2,016
	G.729a/b (10 ms + digit collection)	1,512
	G.729a/b (20 ms + digit collection)	1,512

References

"Documentation references" (page 67) shows where you can find more information about the Media Gateway 15000s.

Documentation references

Document title	Document number
Nortel Multiservice Switch 7400/15000/20000 Overview	NN10600-030
Nortel Media Gateway 7480/15000 Technology Fundamentals	NN10600-780
Nortel Media Gateway 7480/15000 Configuring Switched Service Configuration Management	NN10600-782
Nortel Media Gateway 7480/15000 Periodic Routine Exercise	NN10600-783
Nortel Multiservice Switch 15000/20000 Hardware Description	NN10600-120

Document title	Document number
Nortel Multiservice Switch 15000/20000 Hardware Installation, Maintenance and Upgrades	NN10600-130
Nortel Multiservice Switch 7400/15000/20000 Software Installation	NN10600-270
Nortel Multiservice Switch 7400/15000/20000 Network Management Connectivity	NN10600-271
Nortel Multiservice Switch 7400/15000/20000 Upgrading Software	NN10600-272
Nortel Multiservice Switch 7400/15000/20000 Command Reference	NN10600-050
Nortel Multiservice Switch 7400/15000/20000 Command Job Aid	NN10600-053

Nortel Media Gateway 3000 Series

Description

Nortel is offering enterprise customers a small scale alternative to the Media Gateway 15000 traditionally deployed in the carrier market. The Media Gateway 3000 Series is made up of the Media Gateway 3200 and the Media Gateway 3500. The MG 3200 and the MG 3500 support the Trunkside T1 application.

Trunk gateways

In the CS 2100 configuration, trunk gateways provide access to the Public Switched Telephone Network. A key strategy of the Meridian SL-100 evolution to the CS 2100 is to provide customers with flexibility. Thus, a cost-effective Time Division Multiplexing (TDM) gateway must be delivered to access the PSTN in the CS 2100 product offering.

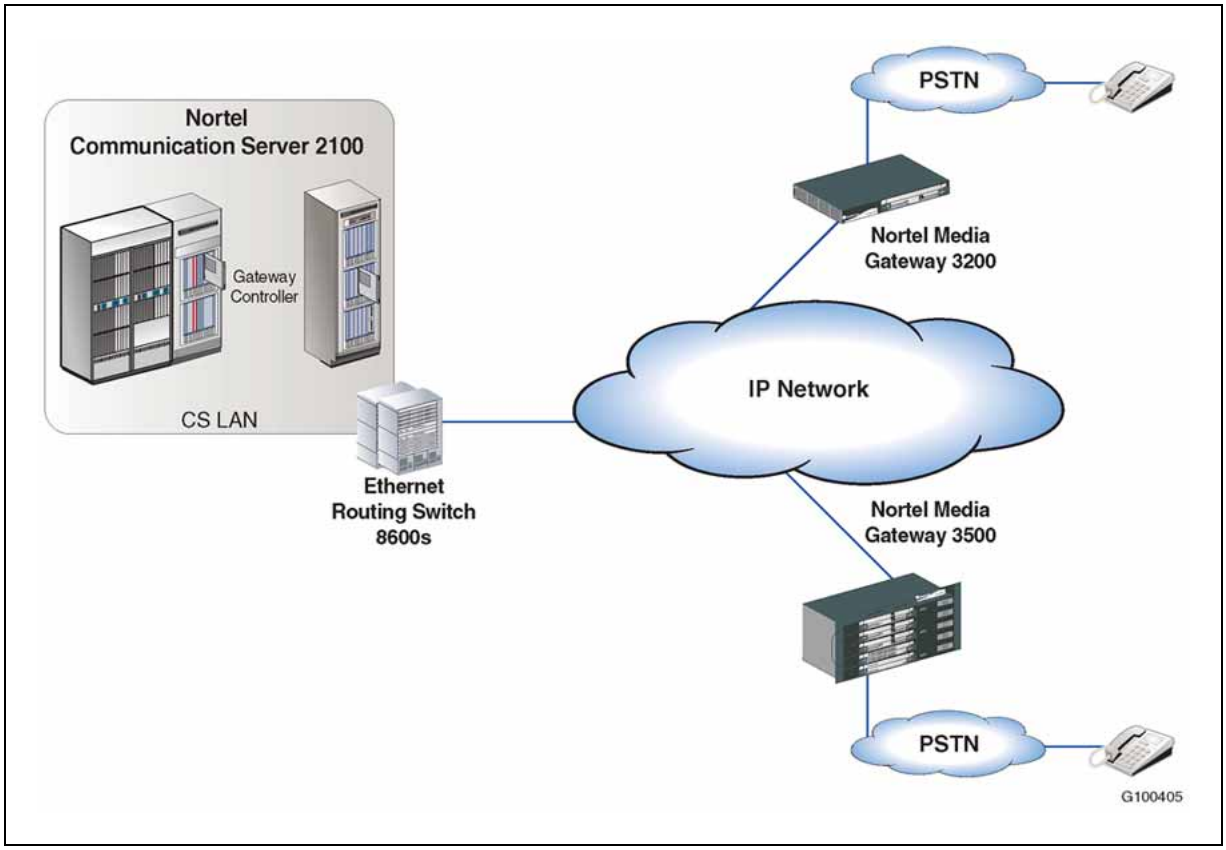
Media Gateway 3000 Series gateways communicate using the H.248 protocol and support Integrated Service Digital Network (ISDN) Primary Rate Interface (PRI). This section describes how you can integrate the Media Gateway 3000 Series gateways into the CS 2100 environment.

The two versions of the Nortel Media Gateway 3000 Series for trunk gateways are as follows:

- The Nortel Media Gateway 3200 provides options for 1, 2, 4, 8, and 16 spans of independent, simultaneous VoIP calls. It supports up to 16 T1 spans.
- The Nortel Media Gateway 3500 provides up to 2,304 independent IP to PSTN voice calls and supports up to 96 non-spared, or 80 spared, T1 spans.

"Nortel Media Gateway 3000 Series Trunkside T1 network configuration" (page 69) shows an example of Nortel Media Gateway 3000 Series Trunkside T1 in a CS 2100 configuration.

Nortel Media Gateway 3000 Series Trunkside T1 network configuration



The D-channel of the trunk gateway terminates at the Gateway Controller (GWC) of the CS 2100.

Media Gateway 3500 Element Management System

The Nortel Media Gateway 3500 is supplied with an Element Management System that covers all areas vital for efficient operation, administration, management, and provisioning. The standards-compliant EMS for Media Gateways uses distributed SNMP-based management software optimized to support day-to-day element management activities. It supports fault management, configuration, and security.

Media Gateway 3200 on Integrated Element Management System (IEMS)

Media Gateway 3200 is integrated into IEMS. IEMS provides integrated fault, configuration, and performance for the Media Gateway 3200. Media Gateway 3200 on IEMS is available to all customers who deploy Media

Gateway 3200 except when the Media Gateway 3200 is deployed behind a customer NAT. In SE09, IEMS does not support a Media Gateway 3200 behind a NAT.

Feature support

NI-1 Primary Rate Interface (PRI) features

"NI-1 features" (page 70) describes the NI-1 features supported by the Nortel Media Gateway 3000 Series gateways.

Note: NI-1 features are not supported on the Meridian 1 or Communication Server 1000. For the Meridian 1 and Communication Server 1000, the only features supported are network-side and subtending subscriber features.

ATTENTION

See the *Meridian SL-100 ISDN Primary Rate Interface Reference Manual* (555-4001-106), for detailed information about the PRI features that the Meridian SL-100 supports.

NI-1 features

Feature	Description
PRI user services	
Calling Line Identification (CLID)	Enables a called terminal to be notified by the network of the address from which the call originated.
Network Redirection and Reason	Informs the calling and called parties about redirections that occur during the life of a call. The following redirection services are supported: • Call Forwarding Universal (CFU) • Call Forwarding Busy (CFB) • Call Forwarding No Reply (CFNR) • Call Transfer • Call Pickup Features of the Network Redirection and Reason are as follows:
Notification of redirection before answer	The calling party is informed of the reason for redirection and the Directory Number (DN) of the new destination by means of the "Redirection number" Information Element (IE) in the NOTIFY message.
Notification of redirection after answer	The connected parties are informed of the reason for redirection and the DN of the new connected party by means of the "Connected number" IE in the NOTIFY message.

Feature	Description
Notification of redirected call	The new destination of the redirected call is informed of the original destination and the reason for redirection by means of the "Original called number" IE delivered in the SETUP message.
Network Name CLID	Transports the calling, redirecting, and called parties' names across the PRI. An originating node receives the name of the terminating party and delivers the originator's name to the terminating node. When a call is redirected, the name of the connected party is delivered.
Network Ring Again (NRAG)	Notifies calling user when a busy called party becomes idle. For example, a user (A) encountering a busy user (B) can monitor that user and be recalled when user (B) becomes idle. If user (A) accepts the recall, the original call is set up again automatically.
Network Automatic Call Distribution (NACD)	Distributes incoming calls to a set of answering positions (agent positions). These positions are at a local node or remote nodes, where each node is served by a similar or like node (for example, CS 2100 to CS 2100). Information exchanged between nodes is used to determine the best routing to evenly distribute calls among the answering positions.
Special Number Services	Provides access any Special Number Services available in the public network. These special numbers may not conform to any numbering plans. As such, they are specified in the public network dialing plan to access certain network services (for example, 0 for operator services and 411 for directory information). The special number digits are sent by the user in the "Called party number" IE in a SETUP message. The called party number is coded as conforming to the E.164 numbering plan (for example, an NPI of "E.164" and type of number of "unknown"). All special numbers accessible to public network subscribers can be accessed over PRI, including the following: • 0 • 411 • 911 • 611 • 1-800 • 1-900 • 0+ (operator assisted calls)

Feature	Description
10-Digit Local Display	Displays the three-digit area code, and the seven-digit DN of the calling party on the called party's display phone in the following situations: • the call is a non-intragroup call from a PRI of a Signaling System #7 (SS7) trunk • both calling and called parties are in the same Serving Numbering Plan Area (SNPA) • both calling and called parties use CLID
Network Message Service	The following types of Network Message Service are supported: • Network Message Waiting Indicator (NMWI) - A Message Service on one node activates or deactivates the message waiting indicator of a subscriber at a different node. • Network Executive Message Waiting (NEMW) - The Executive Message Waiting (EMW) feature on one node activates the message waiting indicator of a subscriber at a different node.
Release Link Trunk (RLT) Enhancement	RLT optimizes the use of NTNA PRI trunks and is optional. This feature includes the ability to drop PRI trunks between two CS 2100s. RLT also enables a CS 2100 to receive a call from another CS 2100, to transfer the call back to the originating CS 2100, and to release the redundant trunk.
Integrated Services Access (ISA)	One PRI interface can replace several dedicated trunk groups, resulting in efficiencies and simplified administration. ISA provides the capability to signal information that specifies the trunk type needed to complete a call. While the individual services continue to exist in the network for INWATS, OUTWATS, TIE, and FX calls, a single PRI connection allows access to all of these services. ISA is supported for both incoming and outgoing calls on a PRI. An ISA call follows normal call control procedures. The "Network specific facilities" (NSF) and "Called party number" (CDN) IEs within the SETUP message are used to select the appropriate service. The following services are supported: • OUTWATS--A service provided by telephone companies which permits a customer to originate calls to destinations in specific geographical areas, sometimes identified as a zone or band. The user can request a specific zone or band number. • INWATS--A form of long distance service that allows a subscriber to receive calls originating within specified service areas (zones or bands) without charge to the caller. Typically, the caller dials 1-800 to identify the call as an INWATS call. • Foreign Exchange (FX)--A dedicated line service between the customer's location and a remote public network exchange that provides the equivalent of local service at the distant exchange.

Feature	Description
	• TIE--Private dedicated facilities between two private network switches (for example, PBX, and Centrex). • PRIVATE--Private calls allow PRI users to access customer-specific routing and number translations. • PUBLIC--Allows PRI users to access the public switched network.
PRI administration services	
Backup D-channel	Increases the reliability of signaling for non-facility associated signaling (that is, when a single D-channel is used to provide call control signaling for more than one interface). This service provides a procedure for employing a standby D-channel that is used if the primary D-channel fails. All active calls are maintained during the switch over to the standby D-channel.

NI-2 Primary Rate Interface features

"NI-2 features" (page 73) describes the NI-2 features supported by the Nortel Media Gateway 3000 Series gateways.

Note: NI-2 features are not supported on the Meridian 1 or Communication Server 1000. For the Meridian 1 and Communication Server 1000, the only features supported are subtending subscriber features.

NI-2 features

Feature	Description
PRI call processing services	
CLID Delivery	For PRI origination, CLID and Redirecting Number Delivery (RND) screening are available as a single option on a per ISDN PRI basis.
Call-by-Call Service	Conveys signaling information over an ISDN PRI that indicates, on a per-call basis, the specific service type associated with the call. Service types include the following: • FX • TIE • OUTWATS • INWATS • Hotel/Motel • Selective Class of Call Screening (SCOCS) • Public Network

Feature	Description
Calling Name	Provides information to the terminating circuit. The service delivers the calling party's name toward the called party (in this description, the called party is connected to the CS 2100 through an NTNI PRI). Several factors can determine if the calling name is delivered, including whether • the PRI has subscribed to the calling name delivery • the calling line number presentation is allowed • the calling line number is available • the calling name can be successfully retrieved
Message Service	Subscribers can retrieve messages previously left for them. Subscribers to Message Service are referred to as client users. Client users can select any call forward variant to route the incoming calls to a Message Storage and Retrieval (MSR) system. The MSR is connected to the Stored Program Control Switch (SPCS) through NTNI PRI. When a call is forwarded by a client user to the MSR, the client user number is delivered to the MSR. Typically, the MSR provides a personalized greeting from the client user and stores the caller's message. When a message is waiting to be retrieved, the MSR sends a PRI D-channel message to the SPCS requesting that the client user's message-waiting indicator be activated. After the network activates the message-waiting indicator, the SPCS sends an acknowledgement message to the MSR. The client can directly call the MSR to retrieve waiting messages. Typically, the MSR requires the client user to provide a user ID and password through in-band signaling. When all messages are retrieved, the MSR sends a PRI D-channel message to the SPCS requesting that the client user's message-waiting indicator be deactivated. After the network deactivates the message-waiting indicator, the SPCS sends an acknowledgement message to the MSR.
PRI administration and maintenance services	
Back-up D-channel	Increase the reliability of signaling for non-facility associated signaling (that is, when a single D-channel is used to provide call control for more than one DS1 interface). This service provides a procedure for employing a standby D-channel that is used if the primary D-channel fails. All active calls are maintained during the switch over to the standby D-channel, assuming the associated B-channels remain functional. Back-up D-channel service is optional on a per ISDN PRI basis.

Feature	Description
Restart Signaling	B-channel restart procedures return a single B-channel, all B-channels on a DS1, or all B-channels associated with a PRI to an Idle condition. Restart procedures clear all calls on the identified B-channels. Additional calls on these B-channels are prohibited until a REST ACK messages is received in response to the REST message. Restart procedures are invoked • after a data link reset following a data link failure (that is, after T309 timer expires) • after the T308 timer expires for a second time caused by the absence of a response to the RELEASE message • when a data link is established at system initialization • when you add or return B-channels to service from a Maintenance or Out-of-Service state
B-channel Availability	In order of decreasing availability, B-channel states are defined as follows: • In Service (IS)--the B-channel can be allocated to a call by Layer 3 call control. • Out of Service (OOS)--the B-channel is unavailable for use by Layer 3 call control. The Out-of-Service state is further categorized to identify which end of the interface initiated the move to that state as follows: — near end (NE) — far end (FE) These categories ensure that only the side of the interface that initiated the move to OOS state can subsequently return the B-channel to IS state. The categories, in order of increasing priority, are IS, OOS/FE, and OOS/NE. The network can track NE and FE status separately, but the NE status procedures take precedence over the FE procedures. Therefore, if the NE status of the channel is OOS/NE and the NE receives a request to change the OOS state, the status of NE remains OOS/NE. OOS state is considered busy for normal call processing. A switch does not assign a channel in OOS state for normal outgoing traffic. A switch assigns B-channels with an IS state for calls and the B-channels can be used for calls offered from the Customer Premises Equipment (CPE). Test calls using the channel are not supported.

Feature	Description
	If a channel carrying a call reaches the OOS state after the call ceases, signaling procedures notify the CPE of the new OOS/NE status. However, the channel remains IS until the call ceases, at which time the state changes to OOS. If a channel is placed in OOS state without waiting for the call to cease, signaling procedures notify the CPE of the new OOS/NE status, the call is cleared, and the state changes to OOS. This is achieved by issuing a Force Release (FRLS) command to the channel.

Limitations and restrictions for PRI variants NTNA and NI-2

With the following SLE features, restrictions and limitations exist with both NTNA and NI-2. Announcements need to be set up for these features to provide appropriate treatment:

- Distinctive Ring/Call Waiting Tone (DRCW)
- Selective Call Acceptance (SCA)
- Selective Call Forward (SCF)
- Selective Call Rejection (SRFJ)

Additional NI-1 and NI-2 limitations a described in the Custom Local Area Signaling (CLASS) chapter of the *Communication Server 2100 Application Planning Guide* (555-4001-108).

Operating parameters

The following operating parameters apply to the Nortel Media Gateway 3000 Series:

- multiple density options (from one T1 to 16 T1s)
- NEBS level 3 compliant
- Packet Telephony standards compliant
- IETF standards compliant
- optional AC power supply redundancy
- hot-swappable enabled

References

"Documentation references" (page 77) shows where you can find more information about the Nortel Media Gateway 3000 Series. Note: The Nortel Media Gateway 3000 Series gateways were previously called the Audiocodes Mediant gateways.

Documentation references

Document title	Document number
MG 3200 H.248 User's Manual	LTRT-72704
MG 3200 Gateway Configuration Guide	LTRT-72904
MG 3200 H.248 Fast Track Installation Guide	LTRT-73804
MG 3500 EMS User's Manual	LTRT-74004
MG 3500 EMS Product Description	LTRT-74104
MG 3500 Gateway Product Description	LTRT-74604
MG 3500 EMS Server Installation and Maintenance Manual	LTRT-74204
MG 3500 Gateway Installation, Operation & Maintenance	LTRT-74504
Detailed hardware specifications are available at www.audiocodes.com.	N/A

IP Client Manager

Description

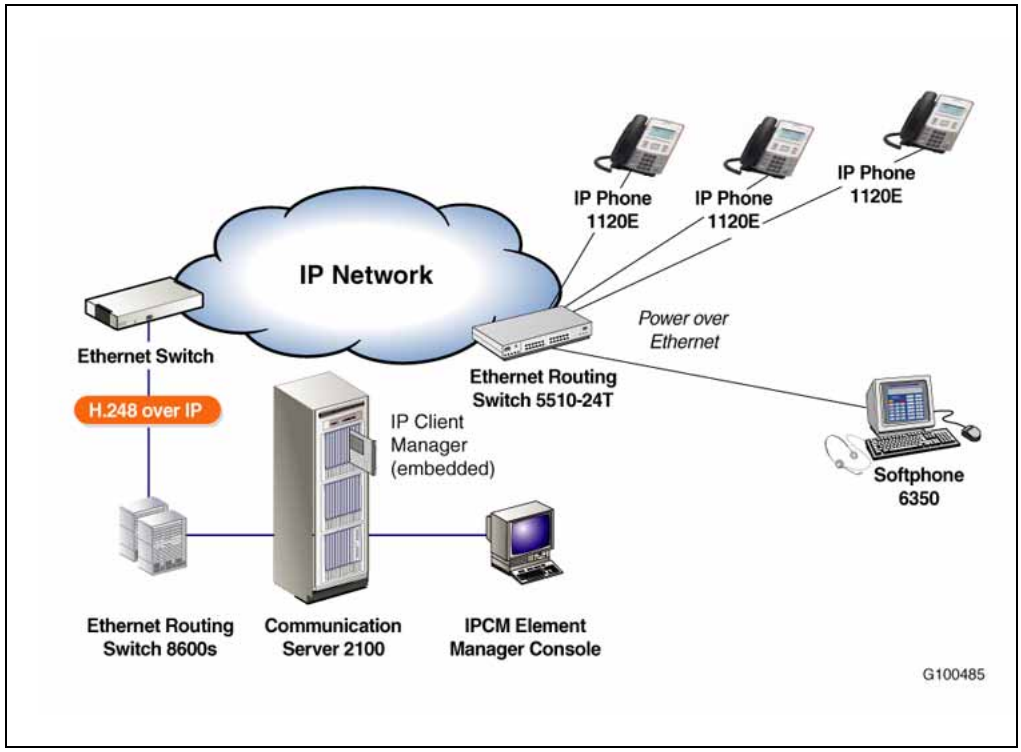
The IP Client Manager (IPCM) uses IP technology to deliver the full Meridian business features sets and capabilities to users connected to a managed IP network. The IP Client Manager connects to a Gateway Controller (GWC) of the CS 2100.

A pair of IP Client Manager Element Managers (IPCM-EMs) can manage up to 100 IP Client Managers. The two IPCM-EMs provide the OAMP interface.

From IPCM 7.0 onwards, the IPCM is configured so the IP Client Manager, including the Element Manager, resides in a SAM21 chassis (on Motorola 5385 CPUs).

"IP Client Manager embedded network configuration" (page 78) shows how the IP Client Manager resides in a SAM 21.

IP Client Manager embedded network configuration



The IP Client Manager provides the control interface between the Gateway Controller and distributed IP clients on a managed IP network. The IP Client Manager communicates with the Gateway Controller using the H.248 IP interface. In this configuration, the IP Client Manager can be considered as a "terminal server" or "signaling gateway".

Media streams in a CS 2100 IP solution are routed directly between media endpoints. The IP Client Manager terminals (for example, the IP Phone 1120E) are media endpoints. Other endpoints in a CS 2100 IP network include the following:

- TDM trunk gateways (for example, the Media Gateway 15000)
- Analog line gateways
- Voice-processing servers (for example, the Media Server 2010)
- IP terminals hosted on another IP Client Manager

Capacity

Each IP Client Manager processor pair supports up to 3,069 users. It supports one or more pairs of CPV5385 CPU processor cards per shelf.

Features

The IP Client Manager offers the following features:

- support of the IPCM (including EM) in a SAM21 chassis (on Motorola 5385 CPUs)
- Windows XP Embedded OS)
- support for IP Phones 2001, 2002 and 2004
- support for the IP Softphone 6350 PC-based telephone
- support for the IP Phone 2002 and 2004 Key Expansion Module
- support for the IP Conference Phone 2033
- support for IP Phones 1120E and 1140E
- support for IP Phone 2007
- support for Wireless IP Phones 2210, 2211 and 2212
- UNIStim security (gateway to 200x)
- UNIStim security (gateway to soft client)
- alignment of the Element Manager with CS 2100 Integrated Element Management System (IEMS) (see "Nortel Integrated Element Management System" (page 147)).
- flow-through provisioning
- faults and alarms (reporting to Network Management Systems)
- performance and Operational Measurements (reporting to Network Management Systems)
- hitless in-service upgrades
- enterprise administrator controls
- end user web management
- geographic survivability similar to the Gateway Controller capability (see "Geographic survivability" (page 55))
- support of the a wide range of IP Phone features described in *CICM Basics* (NN10044-111). Contact your Nortel representative for a complete list of features supported on the IP Phones and IP Softphone, many of which are explicitly for Meridian SL-100 customers but now operate off the CS 2100.

  Note: Centrex IP Client (CICM) is the carrier name for the IP Client Manager (IPCM).

Line Option for IPCM Phones feature

Prior to the Line Option for IPCM Phones feature (A00003653), technicians provisioned IP phones as M5216 sets on the switch using the M5216 Line Class Code (LCC). However, no indication was available in the Core of a line being an IPCM line (for example, as in a QLEN or QDN output).

The Line Option for IPCM Phones feature delivers the IPCLIENT line option. This option distinguishes lines with actual M5216 phones from IPCM lines that have UNIStim phones. The Line Option for IPCM Phones feature provides the ability to use SERVORD to provision the IPCLIENT option to indicate that a line with the M5216 LCC is an IPCM line.

You can assign or remove the IPCLIENT option from a line using the following SERVORD commands:

- NEW
- NEWACD
- ADO
- EST
- ADD
- DEO

In addition, the COPYSET, CKLN and CHF commands are supported.

End users can "hot-desk" from IPCM phone to IPCM phone. However, hot-desking may be infrequent and the phone might be the end-user's primary phone. Therefore, when IPCLIENT is entered as an option, the system prompts the technician for the primary set type. The available options are as follows:

- I2001
- I2002
- I2004
- SOFTCLIENT
- OTHER

ATTENTION

See the *Communication Server 2100 Commercial Systems Feature Description Manual* (555-4031-801) for information about how to configure and administer the Line Option for IPCM Phones feature.

Active Call Failover

Prior to SE08, IP terminals could connect to either node of an IP Client Manager for service. Should a node fail, all terminals hosted by the defunct node experience an outage (possibly losing one or more calls) while they

rebooted and reconnected to the mate node. The Active Call Failover (ACF) function transitions the IP Client Manager from a load-sharing model to a full takeover redundancy model.

With Active Call Failover, all terminals connect to the master node of the IP Client Manager through a single IP address. If the master node fails, the mate assumes the role of master node, takes over this floating IP address, and begins to recover of terminals while maintaining active calls.

A Switch of Activity (SWACT) occurs when the role of master is transitioned from one node to another. "IP Client Manager Active Call Failover configuration" (page 82) shows the IP Client Manager architecture when it is configured for Active Call Failover. This figure is based on the assumption that following a SWACT, communication with the Gateway Controller and terminals is maintained by the newly promoted master, which in this example is Node B.

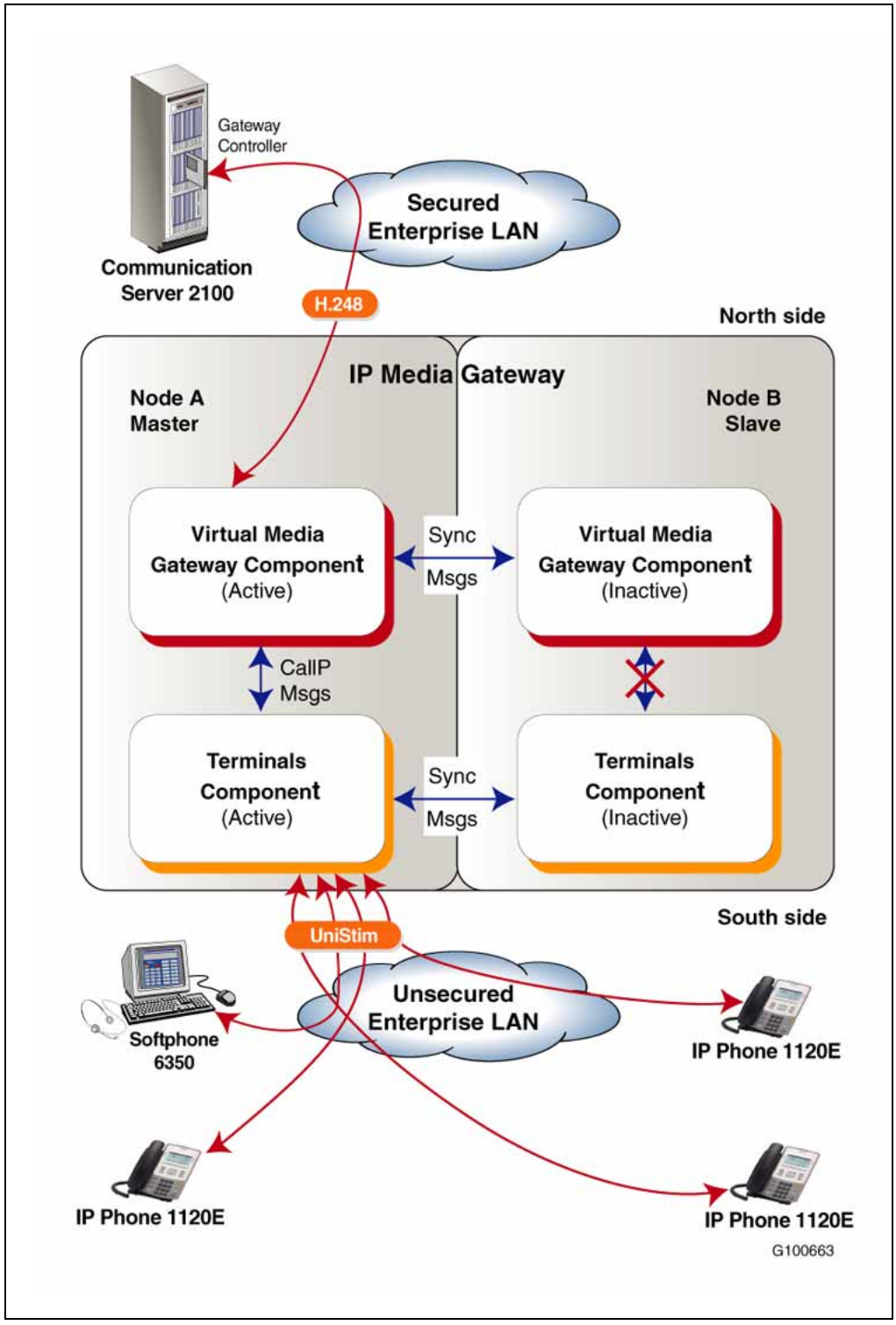
As shown, the north side of the IP Client Manager continues to communicate with the Gateway Controller using the H.248 protocol over a single interface. However, Active Call Failover changes the architecture of the IP Client Manager so that the south side now also presents a single, but unique interface. Terminals can no longer connect to one or the other nodes. Instead, terminals are now aware only of a single IP address towards which all UNIStim messaging must be directed. This address is bound to the master node.

Therefore, both the H.248 and UNIStim interfaces make use of their own "floating" IP address that is bound dynamically to the master node interface. Each component shown in "IP Client Manager Active Call Failover configuration" (page 82) manages its floating IP address and ensure it is swapped with its mate during a SWACT.

The inactive Virtual Media Gateway component keeps a constant near-full synchronization with the active side. The double-sided arrow connecting the components on both nodes of the IP Client Manager illustrates this. This configuration is necessary to ensure that both nodes accurately view the state of call processing at all times, thus enabling the inactive side to take control of these operations during a SWACT.

As for the Terminals component, the active component also maintains a state of synchronization with the inactive component.

IP Client Manager Active Call Failover configuration



Active Call Failover requirements The Active Call Failover feature has no new hardware requirements. The Active Call Failover feature was introduced in the IP Client Manager 8.0 release (SE08).

The 8.0 IP Client Manager release introduces no mandatory requirements either to the IP Phone or to the IP Softphone firmware. However, enhancements were made to both the firmware and IP Softphone 6350 software to minimize the impact on the user during a SWACT. Nortel therefore recommends that you upgrade the IP Phones/Softphones to the latest versions that ship as part of the IP Client Manager release.

Pre-answer and mid-call SDP renegotiation During each call setup, a CICM node negotiates:

- which codecs to use
- the duration of the packetization times
- the destination IP information through exchanging SDP messages with the far end of the connection

A CICM node cannot process SDP renegotiation attempts from the peer gateway. Problems occur when interworking with gateways that rely on SDP renegotiation to change codecs or destination IP address pre-answer or mid-call.

With SE09 and later, when interworking with a Multimedia Call Server (MCS), a CICM node is supported for pre-answer and mid-call IP address and codec renegotiation.

Removal of use of Border Control Point when user not logged in With SE09 and later, a call terminating to a CICM line can complete even when the user associated with the directory number (DN) is not logged into a CICM client (IP Phone or m6350 SoftClient) at the time of the call. Therefore, interactions with features such as call forwarding and voice mail can occur while the user is not logged in. Also, the user can log into the CICM client while receiving the call, be alerted to the call, and answer the call.

Prior to SE09, a Border Control Point 7000 series (BCP 7100/7200) is required between a CICM node and its gateway into the network (even a network that does not have NAT traversal). The Border Control Point 7000 series terminates calls made to CICM users who are not logged in so that features such as call forwarding or voice mail can be used. The portal also enables users who log in while being called to be alerted and to respond to the call.

With SE09 and later, the requirement for the Border Control Point 7000 series no longer applies to a CICM call that does not use the NAT traversal capability. A Border Control Point 7000 Series is still required when a CICM user wants carrier-hosted Centrex IP feature interactions enabled or to fulfill media NAT traversal and media anchoring for Lawful Intercept (LI).

> ***Note:*** The Border Control Point 7000 series was previously known as real-time transport (RTP) media portal.

Quality of Service reporting for CICM node calls In Voice over IP (VoIP) networks, the Quality of Service (QoS) of calls can be adversely affected by the components in the network. Unlike Time Division Multiplexed (TDM) networks where the voice quality is consistent for all calls, VoIP networks can experience a different voice quality on each call.

When QoS statistics are enabled, they accumulate on active calls on Nortel IP Phones.

QoS statistics can be used for:

- network engineering
- trend analysis
- trouble-shooting network problems
- service-level agreement (SLA) validation.

References

"Documentation references" (page 84) shows where you can find more information about the IP Client Manager.

> ***Note:*** Centrex IP Client Manager (CICM) is the carrier name for the IP Client Manager (IPCM).

Documentation references

Document	Order number
CICM Etherset Installation Guide and User Manual	NN10027-113
CICM m6350 SoftClient Branding Kit	NN10183-114
m6350 Installation Guide	NN10182-113
Nortel IP Phone 2001 User Guide	NN10300-005
Nortel IP Phone 2002 User Guide	NN10300-007
Nortel IP Phone 2004 User Guide	NN10300-009
Nortel IP Audio Conference Phone 2033 User Guide	555-4001-605
Nortel IP Phone Key Expansion Module User Guide	NN10300-011

Document	Order number
IP Phones Description, Installation, and Operation (refer to the Appendix on IP Phone diagnostic utilities)	555-3001-368
CICM Basics	NN10044-111
Upgrading CICM	NN10230-461
CICM Fault Management	NN10233-911
CICM Configuration Management	NN10240-511
CICM Accounting Management	NN10244-811
CICM Performance Management	NN110248-711
CICM Security and Administration	NN10252-611
Communication Server 2100 Commercial Systems Feature Description Manual (refer to the Line Option for IP Phones feature description)	555-4031-801
Communication Server 2100 Commercial Systems Service Order Reference Manual (refer to the IPCLIENT - IP Client section)	555-4031-808
Communication Server 2100 Commercial Systems Data Schema Reference Manual (refer to the KSETFEAT Feature IP Client section)	555-4031-851
m6350 TAPI Service Provider Installation and Troubleshooting Guide	297-5551-901

Nortel Media Gateway 9000

Description

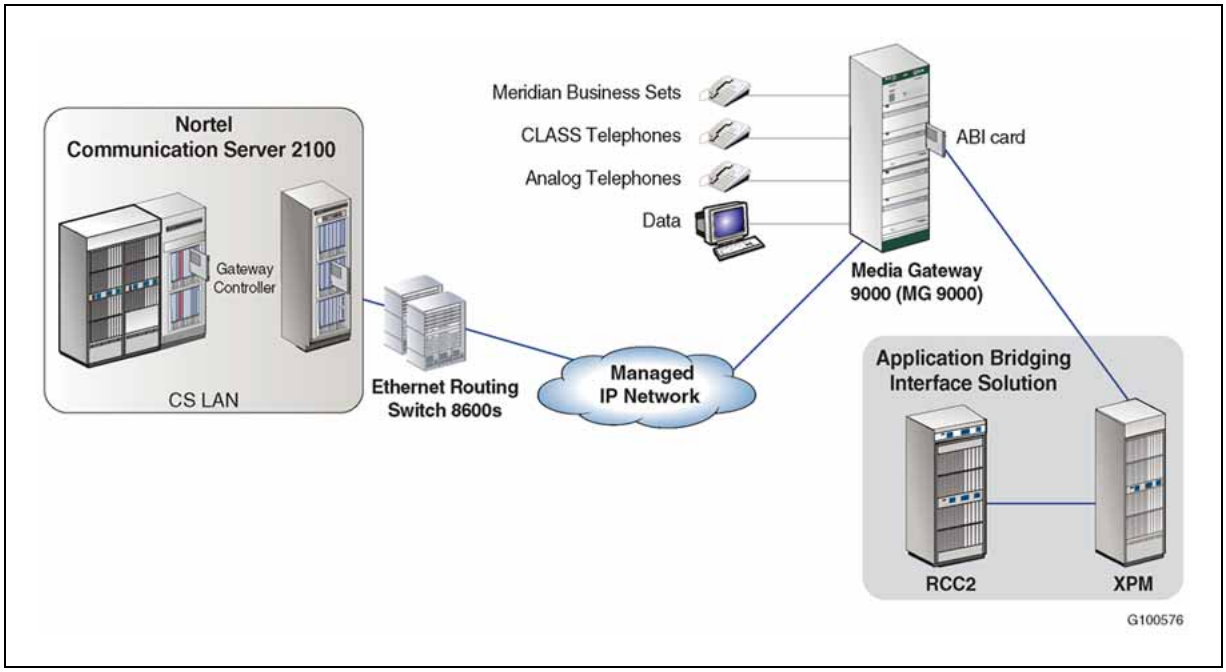
The Nortel Media Gateway 9000 (MG 9000) is a multiservice media gateway that enables large enterprises to use a single-access platform for a wide range of services. Positioned at the edge of an IP network, the Media Gateway 9000 combines voice and data services into a single-access gateway, with a single network interface and management infrastructure.

The Media Gateway 9000 has the following features:

- provides enterprises with the capability to support POTS, P-Phone, Ground Start and line services
- connects subscriber interfaces directly to packet backbone networks
- supports the Access Bridging Interface (ABI)
- supports Emergency Stand Alone (ESA)
- deploys in an enterprise's IP network which it uses to carry packetized voice, call control signaling, Operations, Administration, Maintenance and Provisioning (OAMP), and data traffic
- defense Switched Network support in normal operation

"MG 9000 example configuration" (page 86) shows an example of a Media Gateway 9000 network configuration.

MG 9000 example configuration



Benefits

The MG 9000 simplifies the network and in the process provides the following benefits:

- reduces floor space (up to 80 percent)
- requires fewer cards (up to 50 percent fewer)
- reduces power and Heating, Ventilation and Air Conditioning (HVAC) (up to 50 percent reduction)
- supports peripheral hosting using the Access Bridging Interface function to extend its reach, while at the same time providing investment protection

Applications

The Media Gateway 9000 supports the following applications:

- Access Bridging Interface
- switched lines

Each application can reside in the same shelf or in different shelves. The type and number of individual circuits are limited by the hardware restrictions for each application.

Access Bridging Interface

The Access Bridging Interface (ABI) on the MG 9000 is another attribute enterprises can use in their packet evolution strategies. This MG 9000 feature facilitates PBX consolidation and office collapse for organizations that wish to leverage their TDM access equipment. In addition to the native lines hosted from the MG 9000, the Access Bridging Interface can support most TDM-based line equipment (for example, LCM, LCM-based remotes, GR-303, and TR-08) that subtend from Meridian SL-100 offices.

During an office collapse, the LCM, GR-303, and TR-08 equipment can remain in place as the office core is removed. Their links migrate to the MG 9000 Access Bridging Interface for call control through the CS 2100. The MG 9000 packetizes the voice for transport over the packet network. Therefore, the Access Bridging Interface facilitates office collapse by providing access device reuse, less rewiring, and fast upgrades.

The ABI DS-512 Interface cards (NTNY43BA) support DS-512 fiber link connections between Expanded Subscriber Carrier Module Access (ESMA) and Line Group Controller ISDN (LGCI) peripherals and the MG 9000. Each DS-512 cards hosts a single fiber link, consisting of one downstream/TX fiber and one upstream/RX fiber.

The following XPM types can connect to an MG 9000 through the ABI cards:

- Line Group Controller (LGC), Line Group Controller ISDN (LGCI), Line Trunk Controller (LTC), Line Trunk Controller ISDN (LTCI) with the following subtending devices:
  - Line Concentrating Module (LCM)
  - Remote Line Concentration Module (RLCM)
  - Intelligent Peripheral Equipment (IPE)
  - Line Concentrating Module Enhance (LCME)
  - Remote Switching Center (RSC)
  - Remote Switching Center SONET (RSC-S)

The RSC and RSC-S can support LCM, RLCM, IPE, and LCME line peripherals.

The ABI functions also add support for hosting a Remote Maintenance Module (RMM) from ABI-based XPMs, specifically the LTC, LTCI, LGC, LGCI, and Subscriber Carrier Module-100 Access Second Version (SMA2).

The ABI cards in the MG 9000 are configured in pairs with “network side/user side” unit status using a one-to-one protection group type. Each ABI card in the pair carries DS30 messaging and bearer traffic to the subtending XPM over DS-512 links. Both cards that comprise the ABI pair can be viewed as a small ENET where each plane (represented by an ABI

card) is connected to the XPM the same as a true ENET-configured XPM. A subset of line diagnostics are provided for ABI lines when the switching platform is configured as pure IP.

The “network-side” ABI card controls the MIB data, setting up connections, and delegating to the “user-side” card as appropriate for data syncing call setup and supervision.

Access Bridging Interface Emergency Stand Alone capability
The Emergency Stand Alone (ESA) feature extends the ESA capability, available for MG 9000-based lines to all lines, on subtending peripheral modules that use the MG 9000 Access Bridging Interface. The MG 9000 can continue processing calls for MG 9000 lines and any subtending Access Bridging Interface lines when call control links to the CS 2100 have been lost. ESA is not available for ABI ISDN BRI lines connected to an LCME.

The main advantage of this feature is that the MG 9000 maintains call processing for MG 9000 lines and MG 9000 Access Bridging Interface subtending lines even when a failure occurs on the call control link back to the CS 2100.

Switched lines

The Media Gateway 9000 is a scalable platform providing tip and ring subscriber interfaces and redundant Optical Carrier Level 3 (OC-3)/Synchronous Transport Mode 1 (STM-1) and GbE interfaces to the enterprise IP network.

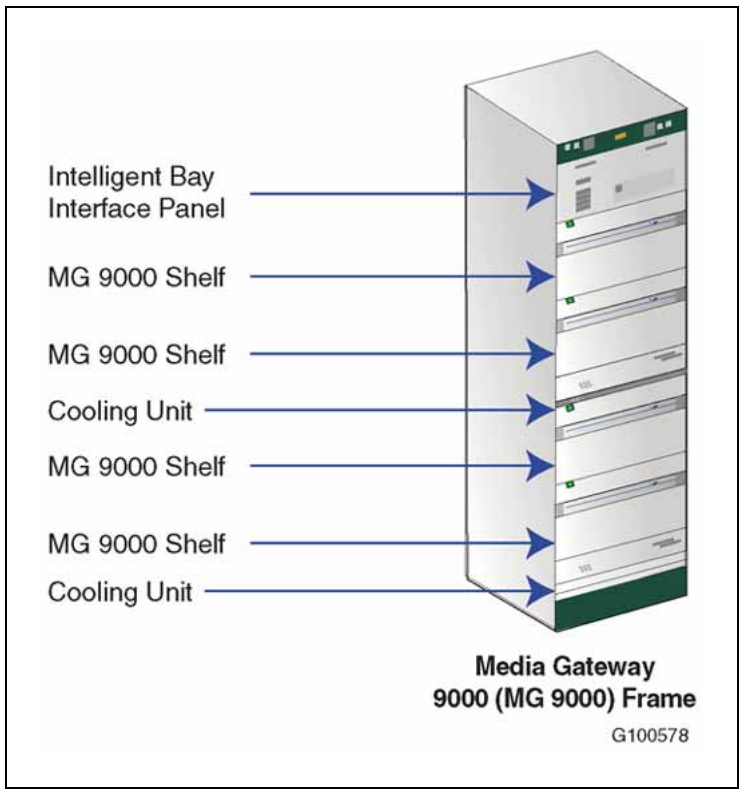
Switched line services include wireline access on the Media Gateway 9000 and the services required to support the lines. The switched lines application brings narrowband voice services onto the enterprise IP network and acts as a switch replacement.

Physical description

The Media Gateway 9000 contains a master shelf for switched lines communication. The master shelf contains the common equipment cards for the node. The master shelf is the first Media Gateway 9000 shelf in the node (typically the bottom shelf in the frame). Additional shelves are subtended from the master shelf by the use of connections through the Internet Telephony Processor (ITP) card and Internet Telephony Extender (ITX) card. The master shelf contains common equipment cards for the switched lines application.

The Media Gateway 9000 is used as a single- or multiple-shelf node depending on the customer line capacity requirements. The term node is used to describe a Media Gateway Network Element connected to an IP network. "NTNY01BB Media Gateway 9000 frame" (page 89) shows a Media Gateway 9000 frame.

NTNY01BB Media Gateway 9000 frame



"NTNY01BB frame components" (page 89) describes the components that reside in a Media Gateway 9000 frame.

NTNY01BB frame components

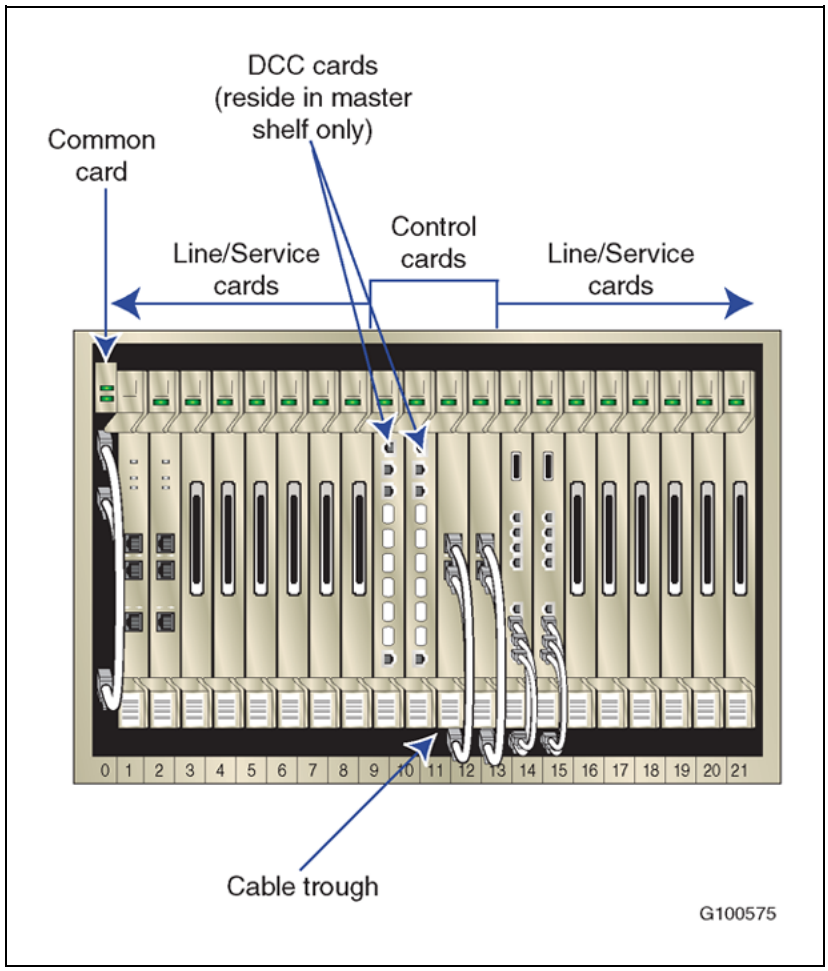
Component	Description
Intelligent Bay Interface Panel (IBIP)	The Intelligent Bay Interface Panel contains the following items: • Fuse panel - The fuse panel on the IBIP front panel protects the individual DCloads in the MG 9000 frame, such as shelves and cooling units, and permits them to be disconnected in a maintenance scenario. The assemblies are protected by 20 fuses. • NTNY25BA Dual Talk Battery Filter cards - The two NTNY25BA Dual Talk Battery Filter cards in the IBIP provide a clean -48 V DC power supply for POTS loop feed. Each card serves as the talk battery filter capacitor for both A or both B talk battery feeds.

Component	Description
	• NTNY27AA Current Sensors - The NTNY27AA Current Sensors monitor both the A and B -48V talk battery power feed currents to each shelf. • NTNY28AA Alarm Relay card and NTNY29AA Alarm Processor card - The alarm and system monitoring functions of the IBIP are split between the NTNY29AA Alarm Processor card and the NTNY28AA Alarm Relay Card.
Data Control Card (DCC), Internet Telephony Processor (ITP) and Internet Telephony Extender (ITX) cards	The functions of these cards are as follows: • NTNY45FA Data Control Card - The NTNY45 is the control complex and Wide Area Network (WAN) for the Media Gateway 9000. The Data Control Card is used in pairs for redundancy and is always provisioned in slots 10 and 11 of the Media Gateway 9000 master shelf. • NTNY30 Internet Telephony Processor card - Provides subtending to additional Media Gateway 9000 shelves and connects with corresponding Internet Telephony Extender cards. The Internet Telephony Processor card processes the ATM-25 line the Internet Telephony Extender card creates. Each Media Gateway 9000 shelf contains two Internet Telephony Processor cards. • NTNY41BA Internet Telephony Extender card - Supports subtended Media Gateway 9000 shelves, creates an ATM-25 link to transmit data to the main control shelf, connects to corresponding Internet Telephony Processor cards, and works in pairs. Each Media Gateway 9000 master shelf requires a minimum of two Internet Telephony Extender cards. Each Internet Telephony Extender pair supports a maximum of eight additional Media Gateway 9000 shelves.
Cooling units	Each frame contains two cooling units.
Media Gateway 9000 shelves	Each frame contains four shelves that are used for POTS/combination lines. Media Gateway 9000 shelves support switched line applications. • switched lines

You provision the Media Gateway 9000 shelves from the bottom shelf up, starting with the MG9K00 shelf and proceeding to the MG9K03 shelf. Frames with fewer than four shelves require plenums in the empty shelf spaces to maintain proper air flow for cooling.

The bottom shelf (first shelf) in the frame of an initial Media Gateway 9000 is considered the master shelf for the node. A Media Gateway 9000 frame supports a maximum of four switched line shelves. "Media Gateway 9000 shelf" (page 91) shows an example of a Media Gateway 9000 shelf. The Media Gateway 9000 contains up to 16 service slots in each shelf.

Media Gateway 9000 shelf



"Media Gateway 9000 shelves" (page 91) describes the shelves in a Media Gateway 9000 frame.

Media Gateway 9000 shelves

PEC	Description
NTNY11AA	Media Gateway 9000 shelf. The MG 9000 shelf contains voice and data domains. The domains are independent in the hardware architecture, and prevent traffic conditions in one domain from degrading the operating capacity in the other domain.
NTNY15AA	Air filter assembly.

PEC	Description
NTNY17BA	Media Gateway 9000 Intelligent Bay Interface Panel shelf.
NTNY18AA	Media Gateway 9000 Cooling Unit shelf with NTNY16AA Local Craft Access Panel (LCAP) (that is, the middle cooling unit).

"Media Gateway 9000 line/service cards" (page 92) lists the Media Gateway 9000 line/service cards that are supported in a CS 2100 network.

Media Gateway 9000 line/service cards

Card	Description
POTS 32	Traditional telephone service cards with 32 ports.
Global Line Card (GLC) 32	Supports up to 32 POTS ports for almost any country.

Global Line Card (GLC) 32

The Global Line Card (GLC) 32 was introduced in SE09. The GLC 32 line card (NTNY53BA) supports 32 subscribers and it provides global services for the MG 9000. The GLC enables the MG 9000 to terminate subscriber POTS loops for almost any country. Voice services comply to both LATA Switching System Generic Requirement (LSSGR) and Digital Loop Carrier (DLC) specifications for North America, as well as the application specifications for other countries.

The GLC 32 can terminate P-phone/Electronic Business Set (EBS), and Ground start lines. The analog voice traffic is converted to either A-law or the U-law PCM and aggregated into a serial PCM stream. This PCM stream is sent to the Internet Telephony Processor (ITP), where it is converted to packets and sent to the Data Control Card (DCC) and on to the packet network.

For more information about the GLC 32, see *MG 9000 Basics* (NN10011-111).

Emergency Stand Alone

Emergency Stand Alone (ESA) in the Media Gateway 9000 supports basic calls within the Media Gateway 9000, while one or more of the Virtual Media Gateways (VMGs) in the Media Gateway 9000 are out of communication with its assigned Gateway Controller (GWC). ESA also provides basic emergency service access codes such as 911, 411 and 611. During ESA, the service codes 911, 411 and 611 translate to a local 7- or 10-digit DN hosted by the Media Gateway 9000 line gateway. In an IP configuration, 6- to 13-digit dialing plan lengths are supported.

As mentioned previously, Emergency Stand Alone is also supported with the Access Bridging Interface function, in which case the subtending peripherals maintain service (except the RSC, which maintains its own ESA mode).

Protocol support

"Media Gateway 9000 protocols" (page 93) lists the industry-standard protocols that are applicable to the Media Gateway 9000.

Media Gateway 9000 protocols

Function	Standard	Description
Call control	ITU H.248	The ITU H.248 media gateway control messaging is used between the CS 2100 and the Media Gateway 9000 to establish calls.
Management	SNMP 2.0	The Simple Network Management Protocol 2.0 sends management information between the Media Gateway 9000 Manager and the Media Gateway 9000.
Switched lines over IP	RTP	The Real Time Protocol is an Internet Engineering Task Force (IETF) protocol used for switched lines over IP solutions.

Operating parameters

The following operating parameters apply to the Media Gateway 9000:

- The Media Gateway 9000 is supported with SE07 or higher software releases.
- Connection to an Asynchronous Transport Mode (ATM) backbone is not supported in SE09.
- The Universal Access AALI multiservice ATM network solution is not supported in a CS 2100 network.
- The DS1 private lines application is not supported in a CS 2100 network.
- The Media Gateway 9000 is used as a single or multiple node, depending on customer capacity requirements.
- The NTNY01BB Media Gateway 9000 frame supports up to 2,016 lines in subtended frames.
- The NTNY01BB Media Gateway 9000 frame supports up to 1,952 POTS lines in the first frame.
- The Media Gateway 9000 supports a configuration having up to three frames and 12 shelves.

- The following user interfaces are supported:
  - SERVORD, though the Maintenance and Administration Position (MAP)
  - Media Gateway 9000 Element Manager

References

"Documentation references" (page 94) shows where you can find more information about the Media Gateway 9000.

Documentation references

Document title	Document number
MG 9000 Basics	NN10011-111
Upgrading the MG 9000	NN10048-461
MG 9000 Configuration Management	NN10096-511
MG 9000 Security and Administration	NN10162-611
MG 9000 Performance Management	NN10140-711
MG 9000 Fault Management	NN10074-911

Media servers

Introduction

A media server is a central resource for delivering, managing and manipulating packet-based media streams and services over the backbone network. For SE08 and onward, the Communication Server 2100 (CS 2100) supports the Nortel Media Server 2010. This media server delivers the following capabilities:

- Packetized announcements provided to call parties in response to a request from the CS 2100.
- Conference circuits for multiparty calls across the packet network.

This chapter contains the following section:

- "Nortel Media Server 2010" (page 95)

Nortel Media Server 2010

The Nortel Media Server 2010 (MS 2010) offers advanced IP packet audio and conferencing services in a CS 2100 enterprise network. Ms 2010 replaced the Universal Audio Server (UAS) beginning in the SE07 software release.

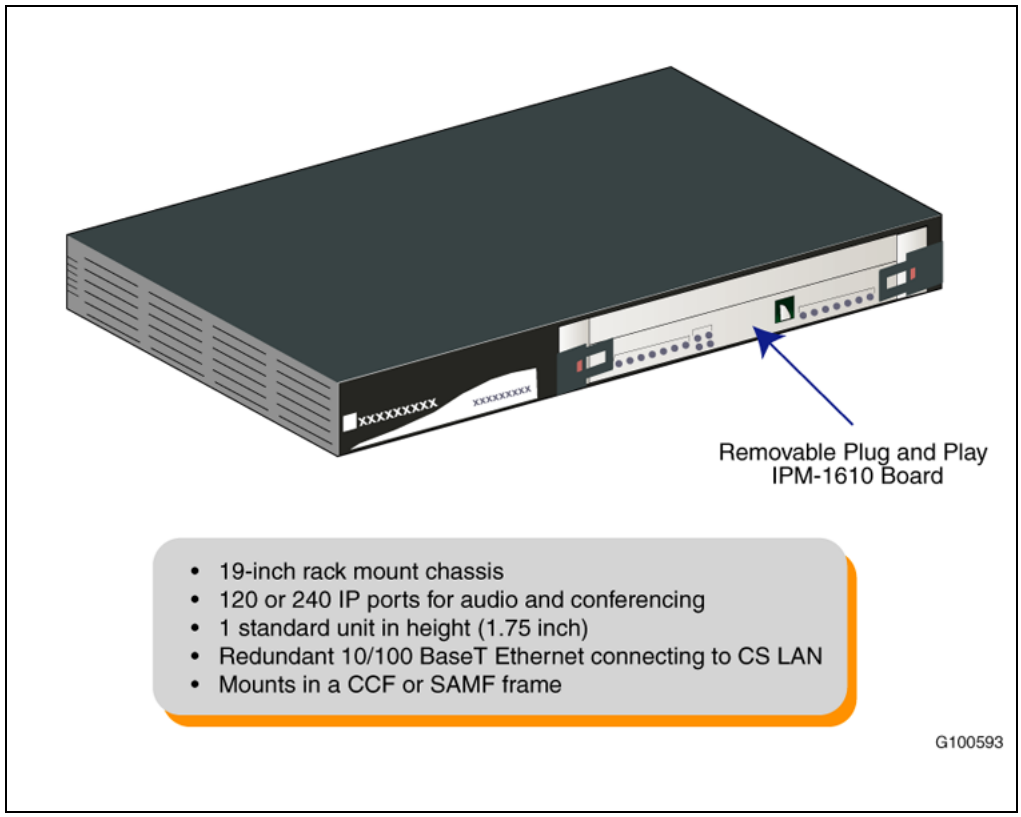
The key features of the MS 2010 are listed below:

- The MS 2010 is a compact media server that provides leading-edge IP-based packet audio services for the CS 2100.
- The MS 2010 supports the following audio and conferencing capabilities:
  - audio conferencing
  - recorded announcements such as branding messages, treatments, and broadcast announcements. These announcements can be interruptible by Dual-tone Multifrequency (DTMF) digit entry.
  - Bearer Channel Tandeming (BCT) for monitoring (that is, Lawful Intercept)
  - Flexible platform to support future revenue-enabling audio services.

- The MS 2010 uses the Audio Provisioning Server (APS). The APS provides a central database for network-wide provisioning and maintenance of announcements. The APS assures that all Media Server 2010s in the network use the same announcements. The APS is required whenever the Media Server 2010 is used as an announcement server.

"Media Server 2010" (page 96) shows the Media Server 2010.

Media Server 2010



"Media Server 2010 features" (page 96) describes the features offered by the Media Server 2010.

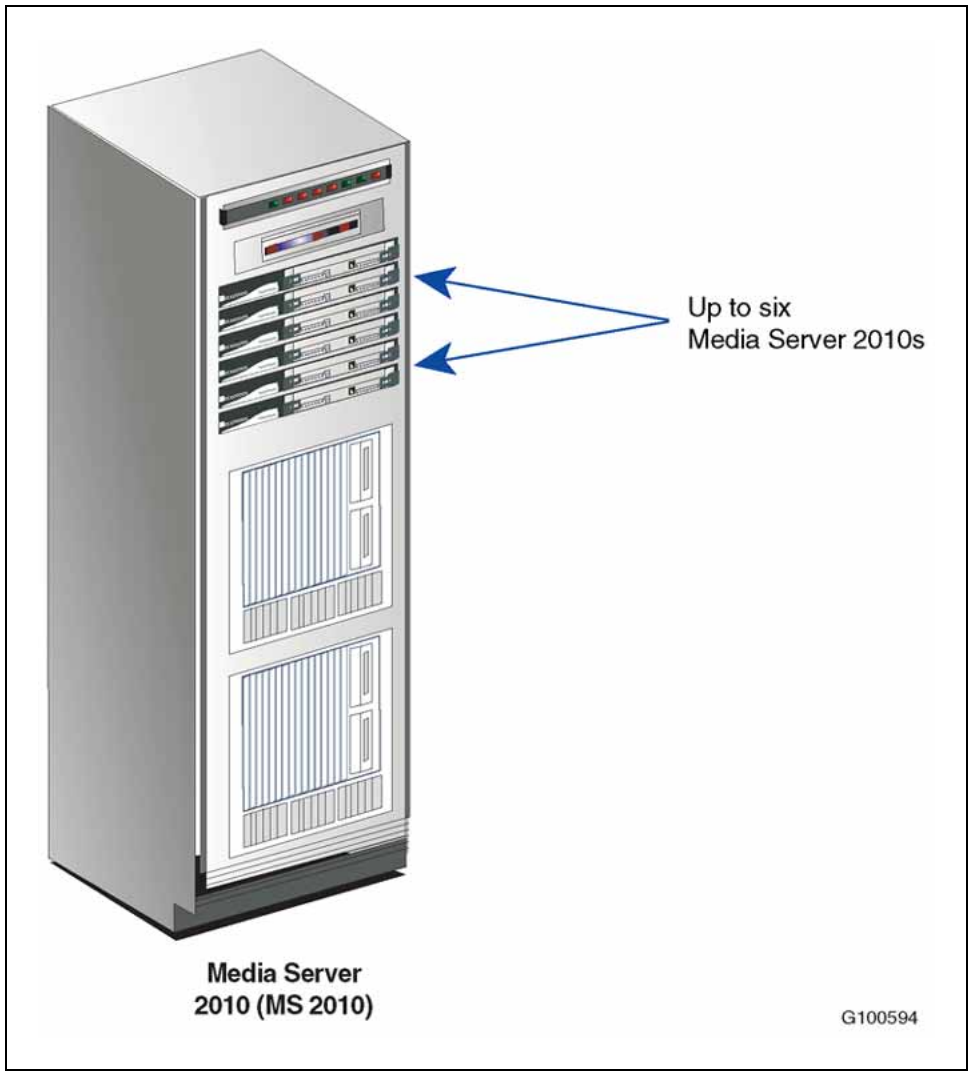
Media Server 2010 features

Feature	Description
Announcements	Play, Play Collect, and Play Record.
Conferencing	Conferencing, Optional Deletion of Last Port, Play to Conference, Record from Conference, and Monitor only Conference.

Feature	Description
Flexible, Centralized Audio Management and Provisioning	Together with the Audio Provisioning Server (APS), the Media Server 2010 provides a web-based interface for managing and provisioning audio, ensuring consistent error-free audio network wide.
Bearer channel tandeming	Bearer channel of all monitored calls is tandemed through the Media Server 2010 where the content is replicated.
Multiple Languages	The Media Server 2010 provides the customer options for multiple language models for global delivery and support of static audio services (numbers, time, currency, and so on).
Industry-standard Protocols and Interfaces	The MS 2010 supports industry-standard protocols and interfaces: • H.248 is used for call signaling • SNMP v3 is supported for OAM messaging • Audio files are transferred using FTP • IP connectivity is 10/100BaseT

"Media Server 2010s in a SAMF Frame" (page 98) illustrates Media Server 2010s in a SAMF Frame.

Media Server 2010s in a SAMF Frame



Hardware and software requirements for the Media Server 2010

The following hardware and software are required for the Media Server 2010 in a CS 2100 enterprise network:

- CS 2100 network configuration with SE07 Release or higher.
- The Media Server 2010 hardware and software. The MS 2010 has the following features:
  - — A NEBS 3-compliant 48.3-cm (19-inch) rack-mount chassis that is one standard unit (1u) high (4.4 cm or 1.75 inches).
  - — Resides on the AudioCodes IPmedia 2000 cPCI rackmount chassis that mounts in a the Call Control Frame (CCF) or the SAMF frame. Either frame can contain up to six Media Server 2010s.

The IPmedia 2000 cPCI rackmount chassis contains the following components:

  – one removable plug and play IPM-1610 board

  – one rear transition module with an Ethernet interface

— Supports 120 or 240 IP ports for Conferencing, or Bearer Channel Tandeming (for monitoring), in addition to 240 channels of Recorded Announcements.

— Supports 80,000 Busy Hour Call Attempts (BHCAs) per unit.

— Stores up to 20 minutes of audio with real-time update capabilities. Up to 40 minutes of storage are available if updates in real-time are not required.

— Uses the Real Time Operating System (RTOS) that provides a high-performance software environment with reduced security vulnerabilities.

— Incorporates open, standards-based protocols and supports H.248 and Real Time Protocol/Real Time Control Protocol (RTP/RTCP). H.248 is used to transmit call control signals over packet networks. RTP/RTCP are used to transmit audio on the bearer network.

— Supports an industry-standard suite of compressed and uncompressed packet voice encoding including G.711 (mu-law and A-law), G.723.1 and G.729a/b.

— Provides redundant 10/100BaseT Ethernet for IP interfaces that connect to the CS LAN. Each pair of interfaces uses one IP address and operates in active/standby mode.

- The Audio Provisioning Server (APS) hardware and software. The APS has the following features:

  — Provides a database to store all recorded audio segments. The database can store over 100 hours of audio information.

  — Uses a web-based interface to easily configure and assemble audio announcements for download to the MS 2010 Media Servers and any supported gateway.

  — Runs on a NEBS-compliant Sun Netra 240 that uses the Sun Solaris operating system.

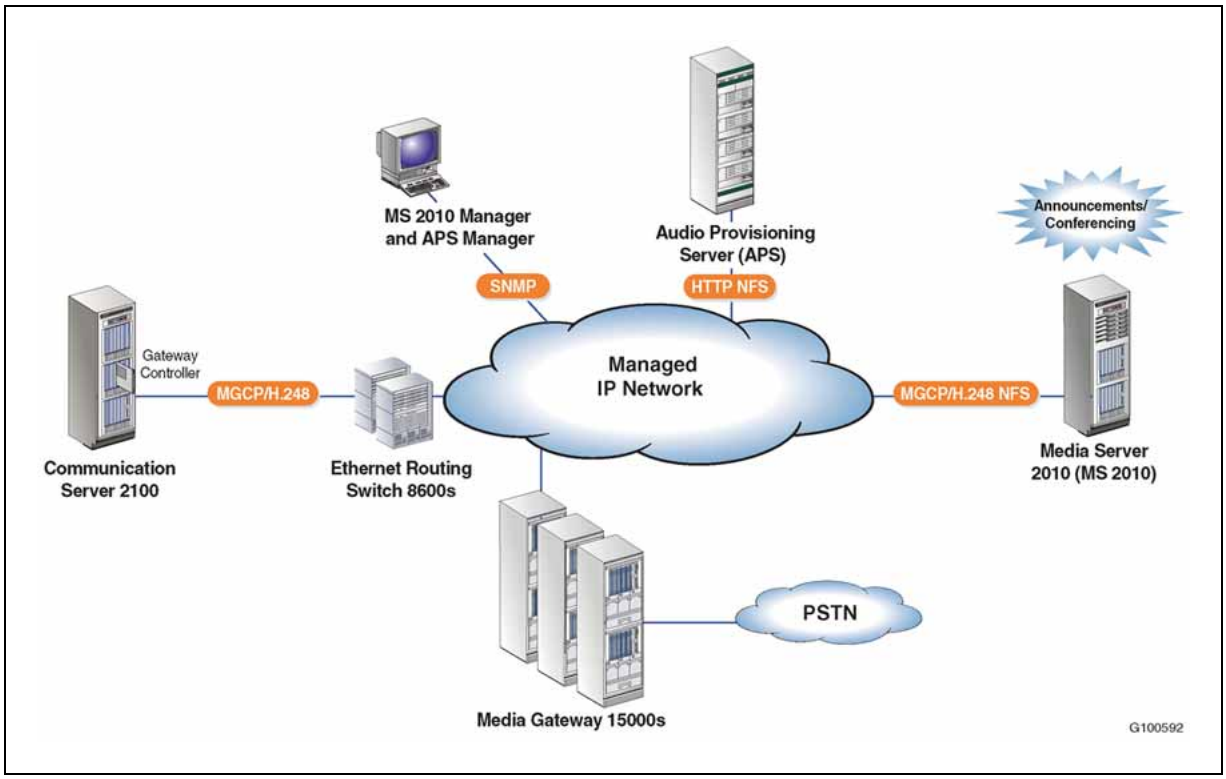
  — Lowers the cost and complexity of changing or adding announcements within a network as changes are made centrally and exported to every Media Server 2010 in the network.

  — Provides for monitoring, management of faults, and reporting and clearing of logs and alarms using SNMP.

— Uses redundant 10/100BaseT Ethernet to connect to the CS LAN. Each pair of interfaces uses one IP address and operates in active/standby mode.

"Media Server 2010s in a typical Communication Server 2100 configuration" (page 100) illustrates a typical CS 2100 network configuration with Media Server 2010s. The CS 2100 directs the Media Server 2010 to play audio or to provide conferencing resources. The Media Server 2010 interprets the messages sent by the CS 2100 and retrieves the audio or initiates the conferencing request.

Media Server 2010s in a typical Communication Server 2100 configuration



Audio is added to the system through the provisioning client (APS manager) and sent to the Audio Provisioning Server (APS). The APS stores the audio in an Oracle database and forwards it to the other MS 2010 nodes in the network on startup of a node or on a periodic basis.

The conferencing capacity of the MS 2010 is based on the total number of conferences that occur simultaneously. An MS 2010 supporting 120 channels can support 120 conference participants. Each conference can accommodate from 3 through 64 participants. Therefore, the maximum number of simultaneous conferences that can be supported is 40.

Features and benefits of the Media Server 2010

The Media Server 2010 includes the following features and benefits:

- Delivers advanced audio and conferencing services in IP packet networks.
- Provides consistent announcements throughout the network using Audio Provisioning Server (APS), the central audio management tool of the Media Server 2010. The APS provides simultaneous, error-free audio updates to all Media Servers in the network, resulting in announcement consistency network-wide.
- Eliminates the need to support traffic between TDM and packet networks for audio services.
- Offers ease in provisioning, network-wide. The APS provides provisioning and element management for the Media Server 2010. The APS enables provisioning of IP connections for conference and announcement functions on all Media Server 2010s in the network. The APS also provides for monitoring, management of faults, and reporting and clearing of logs and alarms using SNMP.
- Assures interoperability. The Media Server 2010 incorporates open, standards-based protocols, such as H.248, and RTP/RTCP for provisioning in an IP network.
- Delivers a rich set of advanced audio services. The Media Server 2010 has state-of-the-art Digital Signal Processing technology. Enhanced capabilities developed for the Media Server 2010 enable customers to offer new features delivered across CS 2100 networks.
- Engineered system availability is over 99.999 percent or less than five minutes of degraded availability per year.

Document references for the Media Server 2010

"Document references for the Media Server 2010" (page 101) lists documentation references for the Media Server 2010.

Document references for the Media Server 2010

Document title	Document number
Media Server 2000 Series Basics	NN10323-111
Media Server 2000 Series Fault Management	NN10328-911
Media Server 2000 Series Configuration Management	NN10340-511
Media Server 2000 Series Performance Management	NN10331-711

Document title	Document number
Media Server 2000 Series Security and Administration	NN10337-611
Upgrading the Media Server 2000 Series	NN10335-461

Media proxies

Introduction

A media proxy (strictly speaking, a media transport proxy) is a Network Element that terminates and re-originates the transport layer for media traffic. A media proxy acts as an intermediary in a call between two packet network endpoints when the media stream for the call is routed through one or more Network Address Translations (NATS) and NAT traversal is, therefore, required. The first section of this chapter describes the media proxy functions and NAT traversal in generic terms. The second section describes the capabilities of the Border Control Point 7000 series, which is the media proxy implementation supported by the Communication Server 2100 (CS 2100)beginning in SE07.

This chapter contains the following sections:

Note: The Border Control Point 7000 series was previously called the Real-time Transport Protocol (RTP) Media Portal.

Network Address Translation (NAT) functionality

Introduction

A media proxy is a Network Element that acts as an intermediary in a call between two packet network endpoints when Network Address Translation (NAT) traversal is required for the call media stream. The media proxy examines incoming packets on each of its ports to determine their origin and can thus work out the destination to which return packets in the other direction should be sent. Two media proxy ports are used to handle a typical call, each proxy presenting an interface to one of the endpoints involved in the call. A connection exists across the media proxy between the two ports to support end-to-end communication between the two packet network endpoints.

The necessity for using a media proxy on a packet network call arises when one of the call endpoints is behind a Network Address Translation, typically because the call endpoint belongs to a private network that is kept secure

from the carrier's public network. The carrier's public network is actually a private network owned and operated by the carrier, but it is described as public because it can be accessed by all of the carrier's customers to support communication between them, including customers served by different private networks.

For packets that originate from a private network endpoint and traverse a carrier's public network, a NAT changes the originating IP address. Instead of the private IP address of the endpoint, which is not made visible over the public network, the originating IP address of packets routed through the NAT is the public network address of a port on the NAT. The NAT performs mapping or binding between such externally visible public network addresses and the private addresses used within the private network.

Note: If translation is applied to ports as well as to IP addresses, the device is referred to as a Network Address and Port Translator (NAPT).

NAT traversal

NAT traversal for signaling

To support NAT traversal for signaling traffic, media gateways and other hosts that are behind a NAT must perform the following:

- Initiate communication with their GWCs (a GWC cannot initiate communication with a gateway behind a NAT).
- Provide their GWCs with address information embedded in signaling packets, which the GWC can then map on to the source address in the packet header (which is that of the NAT, rather than the gateway).
- Use keep-alive messaging to ensure that communication with their GWCs is maintained when no call is in progress (the GWC otherwise cannot send setup messages for calls incoming to the gateway).

NAT traversal for bearer traffic

For VoIP, bearer connections across the packet network are established between RTP/RTCP endpoints (that is, ports on media gateways). When a call is established, each gateway uses device/media control signaling to inform its GWC of the bearer capabilities it can support (for example, codecs, and packetization rates). The gateway also tells the GWC the IP address and RTP port number to which bearer packets destined for it should be sent.

Bearer capability and media address information is conveyed and embedded in device/media control signaling, either in Session Description Protocol (SDP) session description lines in MGCP messages or in UNIStim commands. A problem arises if NAT is in use; however, because media address information embedded in signaling packets is of no use to a remote terminating endpoint that receives it; it identifies the originating endpoint using a private address to which the terminating endpoint has no access.

NAT traversal for media streams requires knowledge not only of what media gateways can be accessed through a network, but also of which NAT (if any) needs to be traversed to reach a given gateway. Specifically, being able to send media packets to a given gateway requires knowledge of the public NAT address that is bound to the gateway private address. However, the public NAT address for a media stream cannot be discovered by a GWC in the same way as the public NAT address for a signaling connection because media packets are by definition not sent by a gateway to its GWC. RTP/RTCP provides no address discovery mechanism that can be used to set up a two-way connection between media gateways.

Hence a media proxy is needed as an intermediary. If a GWC knows that a given gateway is behind a NAT, it can insert a media proxy into a call as a destination for media packets from that gateway, and the media proxy can then discover the public NAT address from which those media packets are being sent. The media proxy can then receive media packets from the far-end gateway and send them to the correct public address on the NAT, which uses the previously created NAT bind to send the media to the private network endpoint behind the NAT. Two-way media streams for calls involving media gateways behind NATs can thus be set up, provided that media packets are routed using the media proxy.

To enable CS 2100 Gateway Controllers to determine whether a media proxy needs to be inserted in a given call, each Gateway Controller stores the following data:

- Information about all the middleboxes in the network, including NATs.
- Information about each media proxy available to the Gateway Controller.
- Information about which middleboxes, if any, needs to be traversed to reach each gateway or remote IP client in the network.

Using a Gateway Controller-controlled media proxy to support NAT traversal for media streams means that no changes are required to media gateway or NAT functions. In particular, it does not require gateways to be aware of network topology and middleboxes deployment. It is a scalable solution with no dependencies on factors outside the network operator’s control.

The situation for determining whether a media proxy needs to be inserted in a call to support NAT traversal is similar to the situation for determining whether Call Admission Control (CAC) should be applied. NATs and Limited Bandwidth Links (LBLs) can both be regarded as types of middlebox whose involvement in a call has an impact on call establishment at the Gateway Controller.

For more information about Call Admission Control, see "Communication Server 2100 hardware" (page 23).

Nortel Border Control Point 7000 series

Overview

The BCP 7000 series is a Gateway Controller-controlled media proxy. The primary purpose of the BCP 7000 series is to support public address discovery for media streams that are routed using a NAT. The BCP 7000 series examines incoming packets on each of its ports to determine their origin, and can thus work out the destination to which return packets in the other direction should be sent. In an enterprise network supporting a CS 2100 solution, each media proxy has two connections: one with the private VoIP network supporting the CS LAN, and one with the carrier's public network. This enables it to support the following two capabilities:

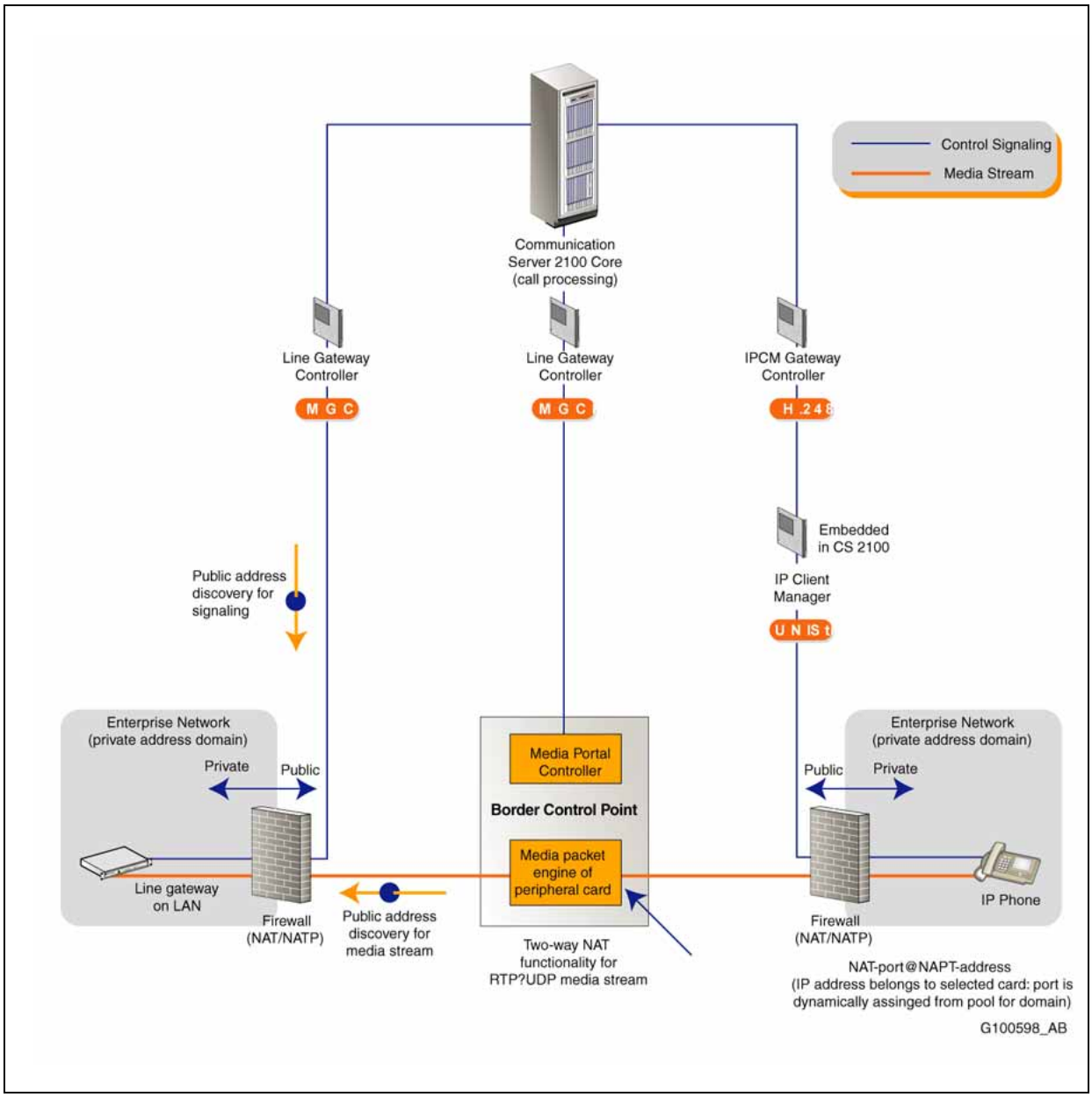
- The BCP 7000 series supports communication with and between private address domains (for example, for enterprise networks hosting line media gateways and IP Client Manager phones, by enabling media streams that traverse NATs to be routed across the carrier's public network).
- The BCP 7000 series can act as a firewall to control the traversal of media streams into the private VoIP address domain used for the CS 2100 CS LAN and large carrier-located gateways.

The BCP 7000 series is controlled by CS 2100 Gateway Controllers using the MGCP+ device/media control protocol.

The BCP 7000 series enables elements in the private network to securely communicate with elements in the public network in both directions. The BCP 7000 series acts as a Media Monitor, Media Directory, and Media Tap and provides Network Address and Port Translation (NAPT) functions that shield private network components from external exposure through leaks in the media streams.

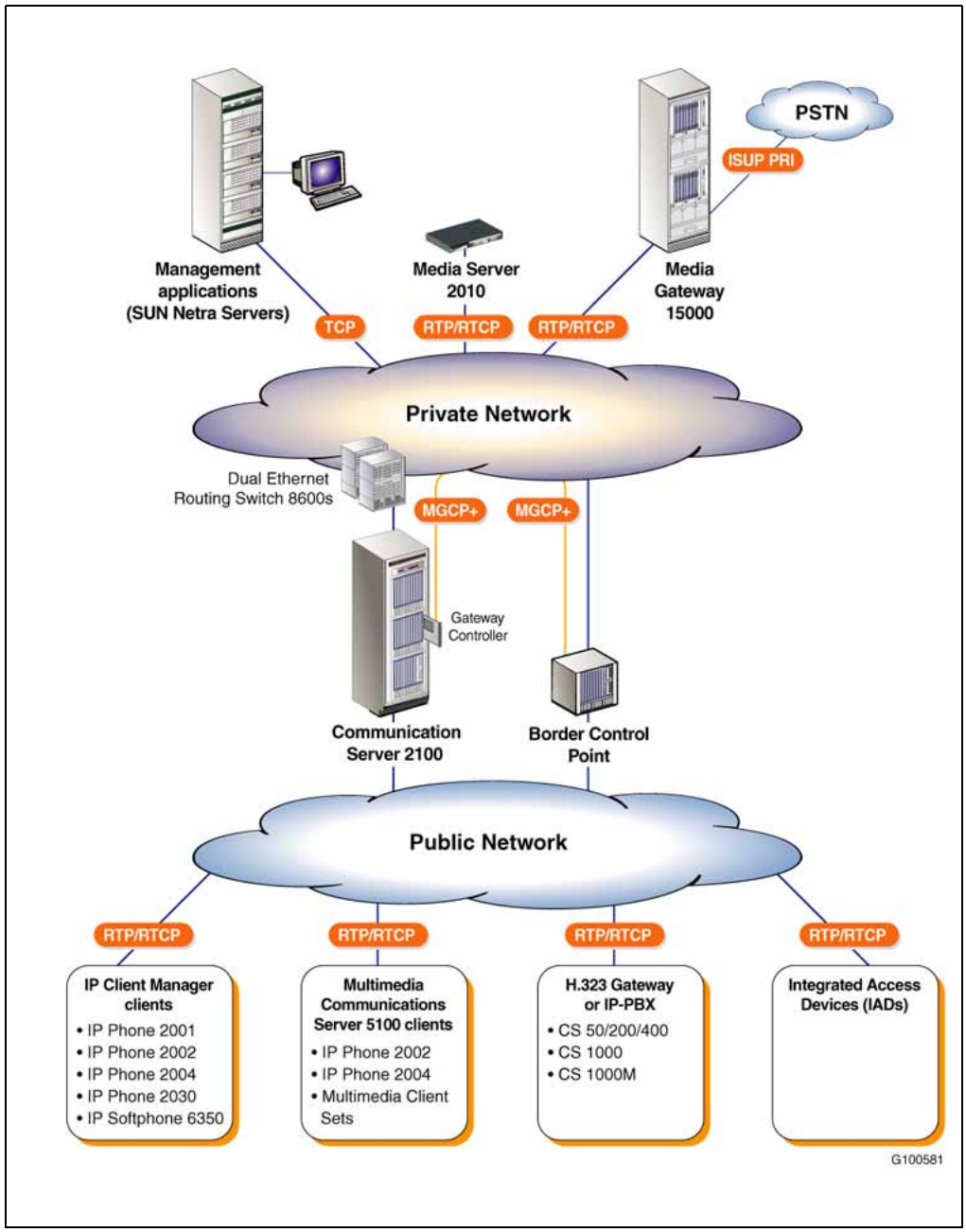
"Border Control Point 7000 series and NAT traversal" (page 107) illustrates the network role of the BCP 7000 series in supporting NAT traversal between two media gateways in private networks behind NAT devices.

Border Control Point 7000 series and NAT traversal



"BCP 7000 series in a Communication Server 2100 network" (page 108) shows an example of a BCP 7000 series network configuration.

BCP 7000 series in a Communication Server 2100 network



Note: In "BCP 7000 series in a Communication Server 2100 network" (page 108), the public and private networks should not be confused with public and private IP addressing. In addition, the list of clients and gateways is not complete.

The clouds in the illustration represent two distinct networks. The Private Network interacts with the Public Network through the various edge components. In addition to extending service reach to obscure multimedia

clients attached to the public network, the BCP 7000 series provides media-layer functions for the RTP, RTCP, and UDP transmissions that traverse between the public network and the private network.

Physical description

The BCP 7000 series is available on two platforms: the original CPX8216-T (BCP 7100) and the IBM BladeCenter-T (BCP 7200).

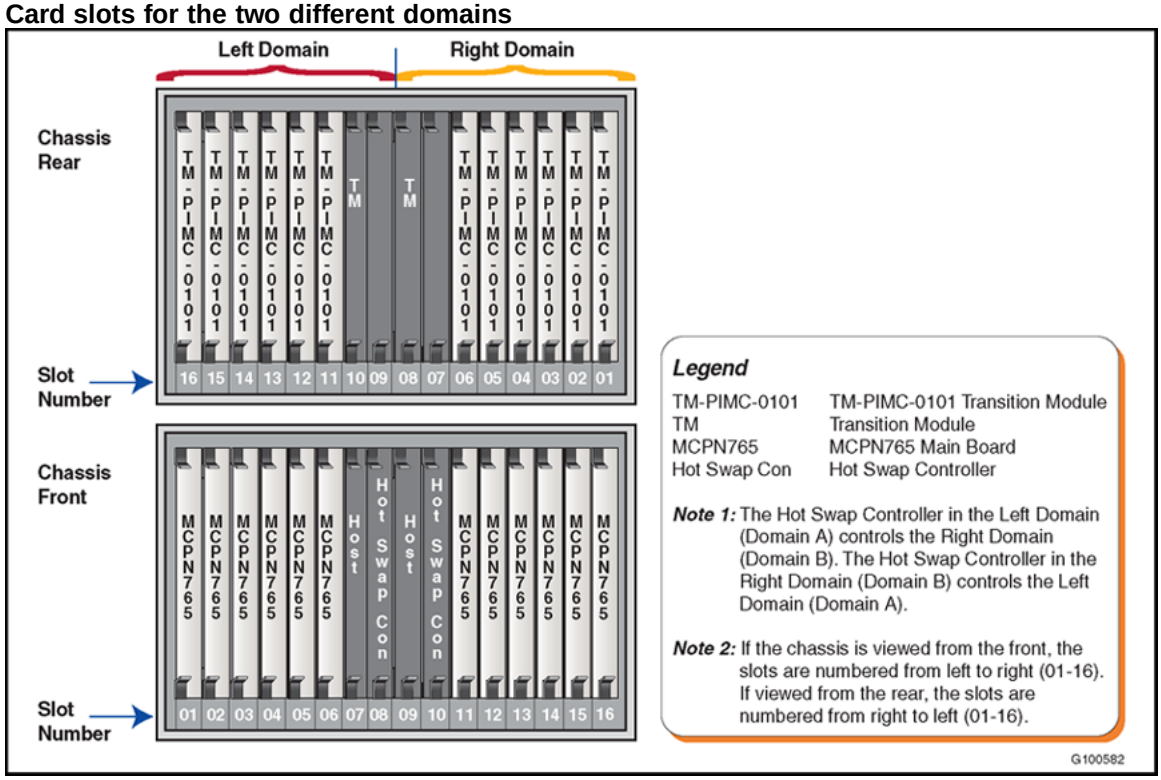
- ***CPX8216-T (BCP 7100)***

  The chassis offers a High Availability platform that provides the basic operating environment, such as power, cooling, and mounting slots, required to sustain the resident subcomponent single-board computers. The CPX8216-T partitions the chassis into two separate logical operating domains, dividing the chassis shelf into two half-shelves consisting of eight-slots each. A BCP 7100 occupies a single-chassis domain (side) on the CPX8216-T.

  The logical Domains of the chassis are not internet Domains. Rather, the term is used to identify Side A and Side B of the chassis. Other terms used interchangeably include: Domain A and Domain B, Left Domain and Right Domain, and half-shelf.

  "Card slots for the two different domains" (page 109) shows a typical card configuration used for the BCP 7100 series domains.

Card slots for the two different domains



Each chassis half-shelf, and therefore each BCP 7100 consists of the following hardware components:

— A single CPV5370 Intel processor board (the host card) with: 1 GB memory, a Small Computer System Interface (SCSI) Input/Output daughterboard, and rear Transition Module.

— Hot Swap Controller and Bridge (HSC) module.

— SCSI CD-ROM drive.

— SCSI hard drive.

— Floppy drive.

— One (or more) Motorola MCPN765 Power PC processor board (the media blade) with 64 MB RAM and associated Rear Transition Module.

— Available AC or DC power options.

The following additional non-Motorola items must be provided by the customer:

— mouse

— keyboard

— monitor

"Border Control Point 7000 series card summary" (page 110) describes the cards that are used in the BCP 7100.

Border Control Point 7000 series card summary

Card	Description
Host card	The Rear Transition Module for the host card (CPV5370) provides the following: • COM2 port for connection to a Terminal Server and local monitor. • Two Ethernet ports that provide connectivity to the private network. The connection carries control signaling and OAMP data. Ethernet ports are used as follows: — The Ethernet 1 port provides an active connection. — The Ethernet 2 port provides a standby connection. The standby Ethernet function is enabled by default through the "Active IP failover" property when you configure the BCP 7000 series. The Ethernet connections provide the following: • MCGP+ control signaling to communicate with the CS 2100.

Card	Description
	• OAMP data to the Management Module over TCP.
Media blades	Network interfaces on each of the media blades (MCPN765) in the BCP 7000 series provide a path for media streams to and from the private network and public network. A media blade consists of the following Input/Output cards: • MCPN765 Front Card • TM-PIMC-0101 Rear Transition Module ***Note:*** You must always deploy I/O cards in pairs. A 1:1 relationship exists between the Front Card and the Rear Transition Module. The Rear Transition Module contains two 10/100 BaseT Ethernet connections for RTP/RTCP/UDP media streams. Each media blade performs the following functions: • Address and Port Discovery (APD) for obscure media endpoints. • Provides connectivity for RTP/RTCP/UDP media streams to pass between the private network and the public network. • Relays media packets between endpoints. • Provides an array of NAT and/or NAPT functions. The NET ports are used for the following: • NET1 port = connectivity to public network. • NET2 port = connectively to private network.

- ***IBM BladeCenter-T (BCP 7200)***

  The BladeCenter-T unit is a rack-mounted, high-density, high-performance, blade-server system developed for NEBS telecommunications network applications and other applications requiring additional physical robustness.

  The BladeCenter-T unit uses blade servers, switches, and other components that are common to the IBM BladeCenter* product line. This common component strategy makes it ideal for applications in telecommunications networks that need high levels of computing power and access to common off-the-shelf middleware packages that are used in IT data centers.

  The BladeCenter-T unit supports up to eight blade servers, making it ideally suited for networking environments that require a large number of high-performance servers in a small amount of space.

The BladeCenter-T unit provides common resources that are shared by the blade servers, such as power, cooling, system management, network connections, backplane, and Input/Output (CD-ROM drive and connectors for USB, keyboard, video, mouse, and network interfaces).

The following is a list of parts for the IBM BladeCenter-T.

— Chassis (AC-powered chassis: Type 8730, DC-powered chassis Type 8720)

— Power Modules (AC or DC power)

— Media Tray

— Management Modules

— Blower Modules

— KVM Module

— LAN Module

— IO Modules

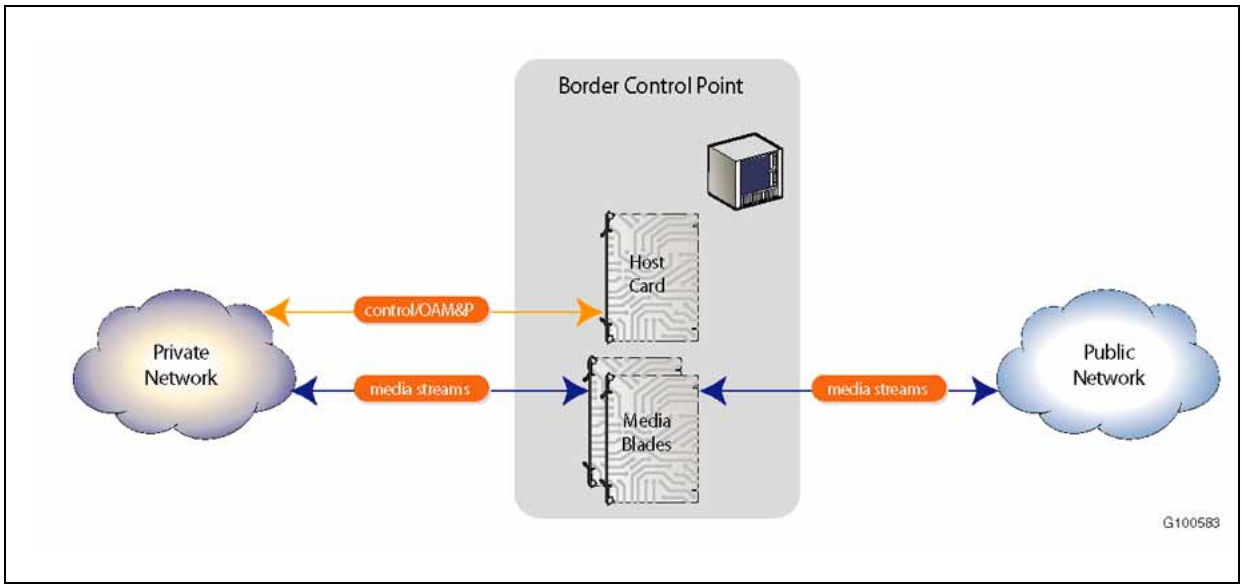
— Blade Servers

Network interfaces

The host card provides the MGCP+ control signaling and OAMP data interface to and from the private network through the use of its Rear Transition Module. Each media blade (Input/Output card) provides a media stream interface to the private network and a media stream interface to the public network.

The BCP 7000 series host card connects to the private network. The BCP 7000 series is an edge component that is dual-homed to the public network and the enterprise private network. The media blades span these two distinct networks (see "Border Control Point 7000 series interfaces" (page 113)).

Border Control Point 7000 series interfaces



OAMP strategy

The central location for OAMP management of the BCP 7000 series is the System Management Console. The System Management Console provides an overall view of the various components in the system, provides access to OAMP functions, and is used for fault and configuration management of the BCP 7000 series. BCP 7000 series management data is stored on the Management Module and in the database. The Management Module stores alarm, log, and Operational Measurement (OM) data. Configuration data is stored locally on the BCP 7000 series, as well as persistently in the database.

For more information about system management, see "Communication Server 2100 hardware" (page 23).

References

"Documentation references" (page 113) shows where you can find more information about the BCP 7000 series.

Documentation references

Document title	Document number
Carrier Voice over IP and Multimedia, Multimedia Communication Server 5200 Border Control Point 7000 Series Basics that contains the following modules: • Overview • Upgrades • Fault management	NN10035-111

Document title	Document number
• Configuration management • Accounting management • Performance management • Security and administration	
MCS 5200 System Management Console User Guide - describes the central location for OAMP management of the BCP 7000 series.	NN10247-111

Call Admission Control

What is Call Admission Control?

Call Admission Control (CAC) is required in packet networks to address problems that might otherwise be caused by network congestion.

In a TDM network, the effect of congestion is that new calls cannot be set up across the network because local exchanges at the edge of the network can seize trunk circuits. Accepting that some new calls are not set up is the price of maintaining voice quality for existing calls. The Grade of Service (GoS) for a TDM network is the likelihood of being able to set up a call. GoS is calculated by the probability of encountering blocking at a switch operating under normal load and is typically in the range of 0.1% to 0.5%.

In an IP network without Call Admission Control, the impact of congestion is that packet loss increases across the entire network, meaning that voice quality is degraded both for existing calls and for newly set up calls. Accepting some degradation in voice quality is the price of placing no restrictions on setting up new calls.

To achieve PSTN equivalence for VoIP calls over a packet network, devices at the edge of the packet network must perform a function similar to that of local exchanges in a TDM network. This means that these devices must be able to determine whether a new call being set up degrades Quality of Service (QoS). The edge devices provide a point where the probability of blocking can be measured and where appropriate trade-offs can be made between QoS and GoS targets. The IP network can use a variety of mechanisms to achieve this purpose. Collectively these mechanisms are referred to as Call Admission Control.

Call Admission Control is applied to call attempts that encounter bandwidth restrictions and should, therefore, not be set up.

Ensuring the availability of sufficient bandwidth in a carrier's core network is a network engineering task and is the responsibility of the network operator. The information in this document is based on the assumption that bandwidth in the core network is effectively unlimited. Typically, however, access and enterprise networks are connected to the core network. The network

operator is not responsible for engineering these subsidiary networks, but it is essential for the network operator to guarantee the performance of the core network. Aggregation takes place between access/enterprise networks and the core to ensure that links to and between core network routers operate at the same high capacity. Admission control depends on knowing how the overall network is structured in terms of routing/aggregation hierarchy and on being able to apply this knowledge to determine whether calls should be set up.

Communication Server 2100 support for Virtual Call Admission Control

The following two things are required to enable the Communication Server 2100 (CS 2100) to support Virtual Call Admission Control (VCAC):

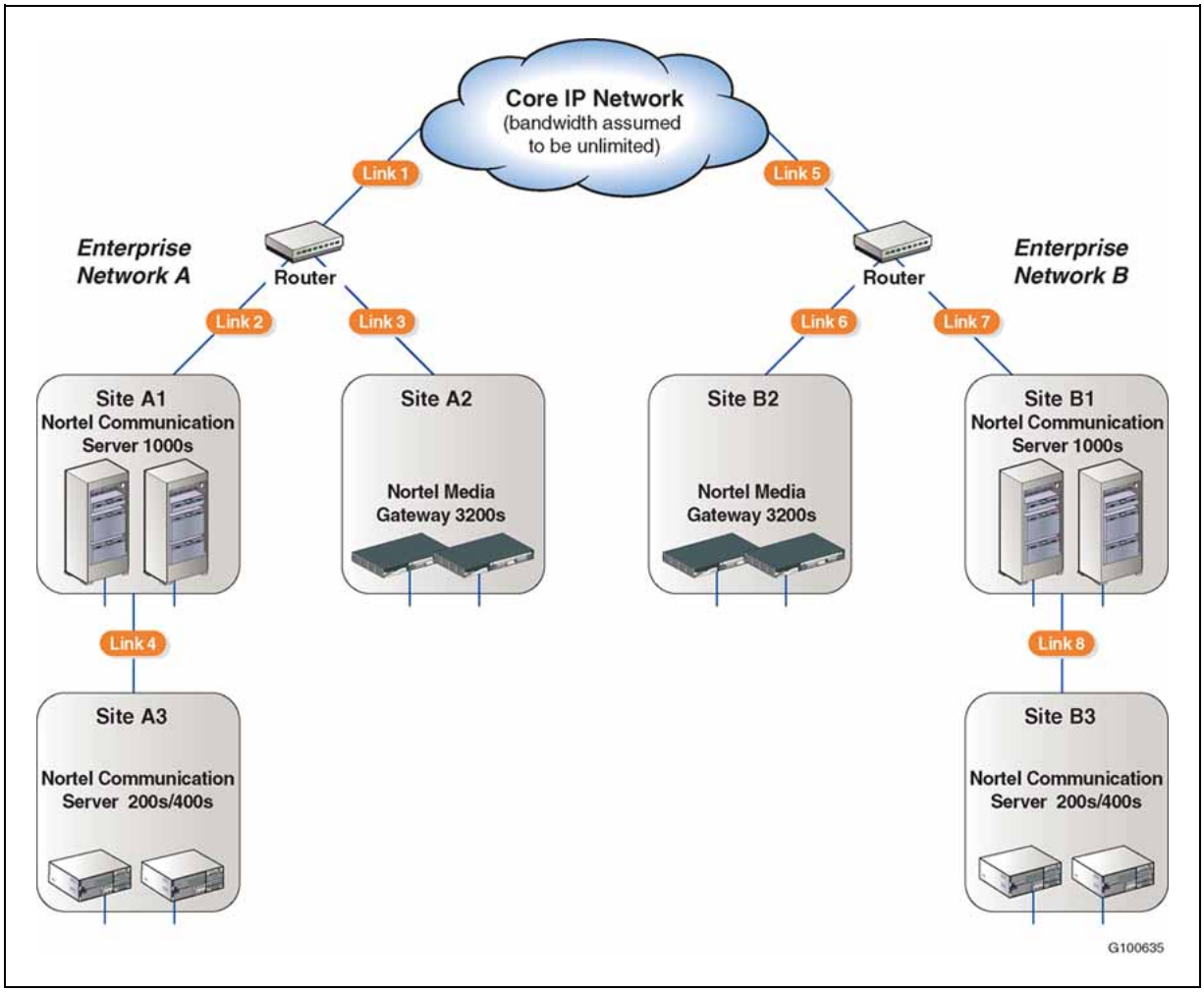
- A logical model of the overall network structure identifying which Limited Bandwidth Links (LBLs), if any, must be traversed to reach a given media gateway endpoint.
- A mechanism for capturing this network structure information in a standard way and making it available to the CS 2100 Gateway Controllers, enabling them to decide whether call setup should proceed if Limited Bandwidth Link traversal is involved.

Virtual Call Admission Control enables the CS 2100 to cancel post-dial, pre-ringing calls that overload a segment of the packet network.

Logical network model

You can view access and enterprise networks as radiating out from the core network. The routing/aggregation hierarchy for a given network begins with the links between the core network and the Customer Edge (CE) router. Behind the Customer Edge router is a hierarchy of links connecting the sites where media gateways are located (see "Example network with Limited Bandwidth Links" (page 117)).

Example network with Limited Bandwidth Links



The logical model that Virtual Call Admission Control uses is based on the links between the sites. Gateways are described as being behind a particular link. So, in Enterprise A in "Example network with Limited Bandwidth Links" (page 117), a gateway at Site A3 is behind Link 4, which is behind Link 2 which, in turn, is behind Link 1.

A link with restricted bandwidth is referred to as a Limited Bandwidth Link (LBL). The bandwidth restriction can be physical (for example, an ADSL line running at 500 kbps) or contractual (for example, a subscriber who purchases a maximum of 1 Mbps of simultaneous VoIP calls). In either case, the capacity available to reach the Limited Bandwidth Link can be defined.

The logical network model is a tree structure made up of Limited Bandwidth Links in accordance with the following rules:

- A top-level Limited Bandwidth Link must be connected to a non-bandwidth constrained "core network".

- A Limited Bandwidth Link can have only one parent, either a Limited Bandwidth Link closer to the core network or the core network itself.
- A Limited Bandwidth Link can have any number of children (subject to the maximum number of LBLs that can be datafilled per Gateway Controller).

These rules mean the following:

- no circular network paths
- one route can exist from a particular Limited Bandwidth Link back to the core network
- Any gateway has single path through the model to the core network and any other gateway that is within the model.

You can add gateways to any Limited Bandwidth Link in the logical model. A Limited Bandwidth Link can have any number of gateways attached to it, which is described as having gateway "leaves" on the Limited Bandwidth Link "tree".

Note: Media Gateway 15000 and Media Server 2010 gateways are assumed to be within the core network. Similarly, SIP-T trunks are assumed to start and finish in the core network.

After a call is made, the CS 2100 identifies the Limited Bandwidth Links and Network Address Translations along the speechpath between the two endpoints and calculates whether sufficient resources are available on all the Limited Bandwidth Links not to exceed the provisioned limits. If all the Limited Bandwidth Links can handle the new call, the call progresses as normal. If one or more Limited Bandwidth Links cannot handle the call, the originator receives a treatment provisioned by the network owner. The terminator has not reached a ringing stage, so is unaware of the call attempt.

Note: For more information about provisioning Gateway Controllers to support Virtual Call Admission Control, see*Policy Controller Configuration Management* , NN10205-511.

For example, assume a call exists between a gateway on Site A3 and a gateway on Site A2. This call uses resources on Links 2, 3, and 4, but not on Link 1 as the call does not leave the enterprise. An insufficient resources failure on any of Links 2, 3, or 4 results in the call going to treatment.

Gateway Controller support for LBL traversal and VCAC

Limited Bandwidth Link traversal for media streams requires knowledge not only of what media gateways can be accessed over a network, but also of which Limited Bandwidth Links, if any, need to be traversed to reach a given

gateway. To enable CS 2100 to determine whether bandwidth limitations mean that Call Admission Control should be applied for a call attempt, the Session Policy Controller stores the following data:

- Information about all the Limited Bandwidth Links in the network.
- Information about which Limited Bandwidth Links, if any, need to be traversed to reach each gateway or remote IP Client Manager client in the network.

The criteria for determining whether Call Admission Control should be applied for a call attempt is similar to the criteria for determining whether a media proxy needs to be inserted in a call to support Network Address Translation traversal. Limited Bandwidth Links and Network Address Translations can both be regarded as types of middlebox that, when involved in a call, impact call establishment at the Gateway Controller.

Virtual Call Admission Control operates by calculating the path between the originating and terminating gateways. Virtual Call Admission Control examines the negotiated codec and processing time (ptime) for the call and checks that each Limited Bandwidth Link in the path has sufficient resources are available for the call to be set up. If sufficient resources, the call proceeds as normal. If insufficient resources are available for the call to be set up, the call is released and a user-provisionable treatment (which must be a tone) is applied to the originator. The terminator does not reach the ringing stage.

Each Limited Bandwidth Link has the following set of properties:

- Resource Usage Factor - A value, based on the real, negotiated bearer characteristics for the call (that is, codec and packetization rate). The term "resource", rather than bandwidth is used, because the value may be normalized, or an engineering factor may be applied to increase or decrease the value away from the real "bits on the wire" value. With the Resource Usage Factor, customers can count calls on a Limited Bandwidth Link (all codec/ptime pairs use one unit of resource).

  The resource usage is per Limited Bandwidth Link, not common across the entire network, because resource usage can relate to a real Network Element (for example, a layer 3 value for a codec/ptime pair is consistent across the network, but the layer 2 values vary).

- Maximum Count - This is the maximum amount of resources on the Limited Bandwidth Link in the same units as the Resource Usage Factor.

Gateway Controller-Element Management Internet transparency VCAC provisioning

In SE08 the following enhancements were introduced to make it easy for technicians to provision Basic Virtual Call Admission Control:

- The creation of a provisioning capability on Succession Element and Subnetwork Manager (SESM) for the Virtual Call Admission Control function: Limited Bandwidth Link middleboxes and their associated Resource Usage data.
- The addition of the capability to provision "chained" middleboxes (where multiple middleboxes reside between a media gateway and the network core).
- The extension of the associated Operations Support System (OSS) interface to allow full read-write access for Network Address Translations, Limited Bandwidth Links, media proxies, and Resource Usage data.

The components impacted by this enhancement are as follows:

- Gateway Controller Element Manager
- CS 2000 Management Tools GUI
- OSSGate

Gateway Controller Element Manager

This feature provides the following capabilities for provisioning Limited Bandwidth Link middleboxes:

- The user can change or delete the Limited Bandwidth Link middleboxes using the (CORBA) interfaces and the GUI panel.
- The user can navigate a chain of middleboxes.
- Makes changes to the model to include Limited Bandwidth Link middleboxes.
- Makes changes to the database to accommodate new entries for Limited Bandwidth Link and Resource Usage.
- Provides a checksum for the dead shelf recovery.
- Provides a facility to link Limited Bandwidth Link middleboxes to each other or to a gateway.
- Enables Virtual Call Admission Control counting on Gateway Controllers that ensures the Gateway Controller understands whether the counter is local or on another Gateway Controller.

This feature provides the following capabilities for provisioning Resource Usage:

- Creates a new table in the database for Resource Usage table data.

- The user can add, change, and delete the Resource Usage table data using the (CORBA) interfaces and the GUI panel.
- Provides appropriate validation for changes to table data (for example, prevent deletion where entries are currently used by Limited Bandwidth Links).
- Provides the capability to query and display Resource Usage table data as appropriate (for example, select Resource Usage table entries required by a given Gateway Controller).

Policy Control Framework

The Policy Controller has a Policy Control Framework (PCF) that is responsible for processing requests for resources and applying the necessary policy enforcement mechanisms to the requests. All relevant network topology information is retrieved from a Topology Database.

The only policy supported is the Virtual Call Admissions Control (VCAC) Bandwidth Policy. This default policy carries out network resource reservation functions.

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

When an application server agrees to provide service to a client, it sends a request to the Policy Controller that contains the following information:

- Client identity and location
- FlowSpec specifying traffic requirement for the session

Policy Controller hardware platform

The Policy Controller units are deployed in a rack-mounted configuration that houses processing hardware, hard drives, ethernet interface ports (two currently reserved for inter-Policy Controller communication for fault tolerance), and redundant power supplies. This hardware platform uses Network Equipment Building Standards (NEBS) Level 3 compliant hardware designed for telecommunications central offices or data centers, based on the Hewlett PackardTM cc3310 carrier-grade server. With two chassis working together to provide carrier-grade level fault tolerance, this hardware configuration provides the platform for the Policy Controller application.

Features of each hardware platform unit include:

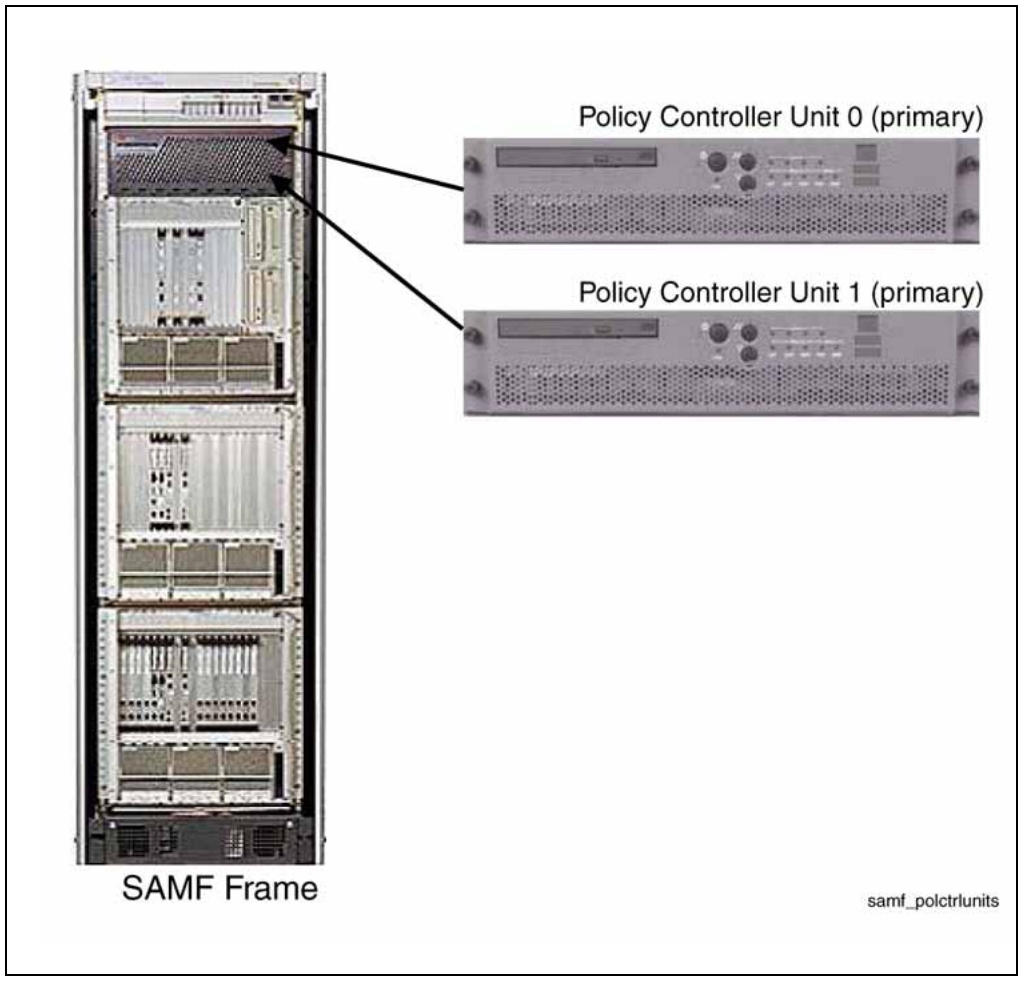
- Dual 2.4GHz Xeon Processors
- 4GB DDR Memory
- Dual 73GB Hot-Swappable Disk Drives

- CD-RW/DVD-R Drive
- Dual Hot-Swappable Power Supplies
- Dual GbE Interface network interface cards
- Service Application Module – eXtremely Thin Server (SAM-XTS) Platform is based on the compact HP cc3310 carrier-grade server.

shows one Policy Controller node (two units in total) positioned in a SAMF frame (NTRX51HA).

Typically, each Policy Controller unit is labeled for identification to distinguish it from other units in the frame, and to distinguish it from STORM units. The naming identification can be similar to the hostname of the node, made during commissioning of the node.

Policy Controller units in the same SAMF frame (NTRX51HA)



Call Server GUI

The network configuration GUI panel is extended to provision two new data entries (that is, Limited Bandwidth Link middlebox devices and Resource Usage). The Resource Usage (RU) entity is a data lookup table for use at Internet transparency call setup time on the Gateway Controller. The table supports data addition, change, deletion, and query (display). The Limited Bandwidth Link Middlebox entry supports the addition, deletion, modifications, and query (display) of the Limited Bandwidth Link Middlebox data. A search capability is also available.

OSSGate

Previously, OSSGate supported a limited set of XML operations to query middlebox and media proxy data and to associate a media gateway to a middlebox. The following capabilities are added:

- add, change, delete, and query operations for Network Address Translation middleboxes
- add, change, delete, and query operations for Limited Bandwidth Link middleboxes
- add, change, delete, and query operations for media proxies
- add, change, delete, and query operations for the Resource Usage lookup table
- other specific queries (for example, return middlebox chain for specified media gateway)

Transparency VCAC provisioning support for IP Client Managers

While IP Client Managers support Virtual Call Admission Control, a problem occurs because the IP Client Manager endpoints/users are not fixed lines. They are roaming users that can move from one area of an enterprise to another. This solution must address the fact that the endpoints/users can move from behind one internet transparency middlebox to another. To complicate matters, an IP Client Manager can also serve multiple enterprises, which requires multiple groups of middleboxes per IP Client Manager.

The E911 feature (A00003568) enables Virtual Call Admission Control for the IP Client Manager gateway, which, on user login, sends the adjacent middlebox identifier to the Gateway Controller. The identifier is used by the Gateway Controller to perform internet transparency tasks (that is, Virtual Call Admission Control and Network Address Translation traversal). However, for the E911 feature to work successfully, the IP Client Manager GWC must have the middlebox hierarchy (of the middlebox provided up to the top level middlebox) provisioned into the IP Client Manager GWC.

The E911 feature enhances the Virtual Call Admission Control provisioning function as follows:

- Ensures that middleboxes are sent to the Gateway Controller for the IP Client Manager endpoints.
- Increases the number of middleboxes allowed onto a large lines Gateway Controller.

The components impacted by this enhancement are as follows:

- Gateway Controller Element Manager
- CS 2000 Management Tools GUI
- OSSGate

Operating parameters

Virtual Call Admission Control is available for both CS 2100 XA-Core and Compact systems.

References

"Documentation references" (page 124) shows where you can find more information about Virtual Call Admission Control.

Documentation references

Document title	Document number
GWC Basics	NN10189-111
GWC Configuration Management	NN10205-511
OSSGate User's Guide	NE10004-512
Policy Controller Configuration Management	NE10432-511
For more information about the CS 2000 Management Tools GUI and the Gateway Controller Element Manager, see "OAMP for Communication Server 2100 networks" (page 137).	N/A

Ethernet Routing Switches

This chapter contains the following sections:

Ethernet Routing Switch 8600

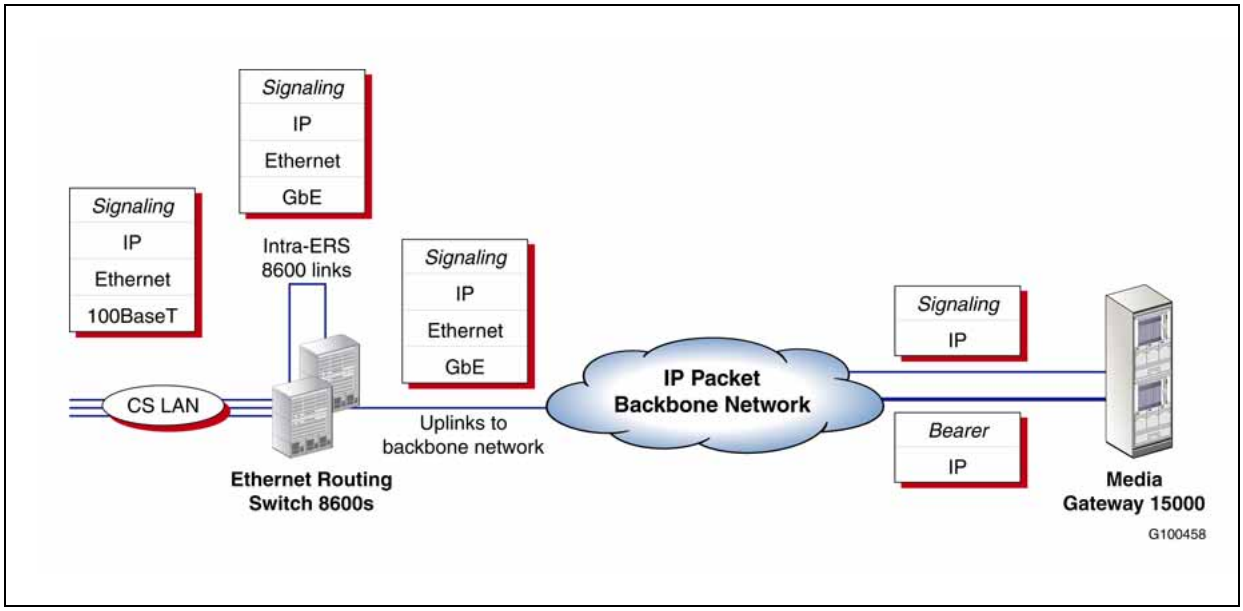
The Ethernet Routing Switch (ERS) 8600s (that is, the 8606 and 8610) described in this chapter are used in the Communication Server 2100 (CS 2100) network. Although the ERS 8600 is a product in its own right rather than a CS 2100 component, the ERS 8600 is an integral part of the CS 2100 Communication Server Local Area Network (CS LAN). The ERS 8600 is therefore described in this document as if it were a CS 2100 component.

> ***Note:*** The ERS 8600 series was previously called the Passport 8600 series.

The CS 2100 CS LAN is an Ethernet network based on the ERS 8600. Physically, the CS LAN has two ERS 8600s configured to use the Virtual Router Redundancy Protocol (VRRP) and to operate in load-sharing mode. A given CS 2100 component such as a Gateway Controller is connected to both ERS 8600s using one as its default router and the other as a backup. The dual ERS 8600s serve as a Communication Server LAN, providing all the necessary routing and Ethernet switching function for communication across the LAN.

The CS LAN not only supports intra-CS 2100 communication, but also provides the interface between the CS LAN and the external managed IP network (see "Connectivity for an IP backbone network" (page 126)).

Connectivity for an IP backbone network



The ERS 8600 passes signaling and management messages between the Network Elements. It provides control messages between the CS 2100 and gateways through the Gateway Controller and other components. It supports the following interfaces:

- Gigabit Ethernet (GbE)
- Multiport 10/100BaseT

The ERS 8600 also supports a redundant configuration to connect the following components:

- CS 2100
- XA-Core (through Enhanced Input/Output Processor/High-capacity Input/Output Processor) (XA-Core configurations only)
- Gateway Controller
- Media Server 2010
- Operations, Administration, Maintenance, and Provisioning
  - — Integrated Element Management System (IEMS)
  - — Multiservice Data Manager (MDM)
  - — SuperNode Data Manager (SDM)/Core and Billing Manager (CBM)
  - — Management Solutions (MS)
- Optivity

To provide secure access to different functions, the ERS 8600 is used to configure the CS LAN as a number of Virtual LANs (VLANs) as shown in "CS LAN Ethernet Routing Switch 8600 VLAN configuration" (page 128). The CS LAN ERS 8600s support three trusted VLANs:

- Call-processing (signaling) VLAN that interconnects the functional CS 2100 Network Elements (NEs), such as the CS 2100 Core, GWCs, and the Media Server 2010 that are involved in the call processing and service provision for end users.
- OAMP VLAN interconnects OAMP server applications, such as PMSS and Element Manager Systems (EMSs) that are the only entities that can access the NEs.
- The VLAN for media (bearer) connections.

The ERS 8600s also provide access to two types of external communication:

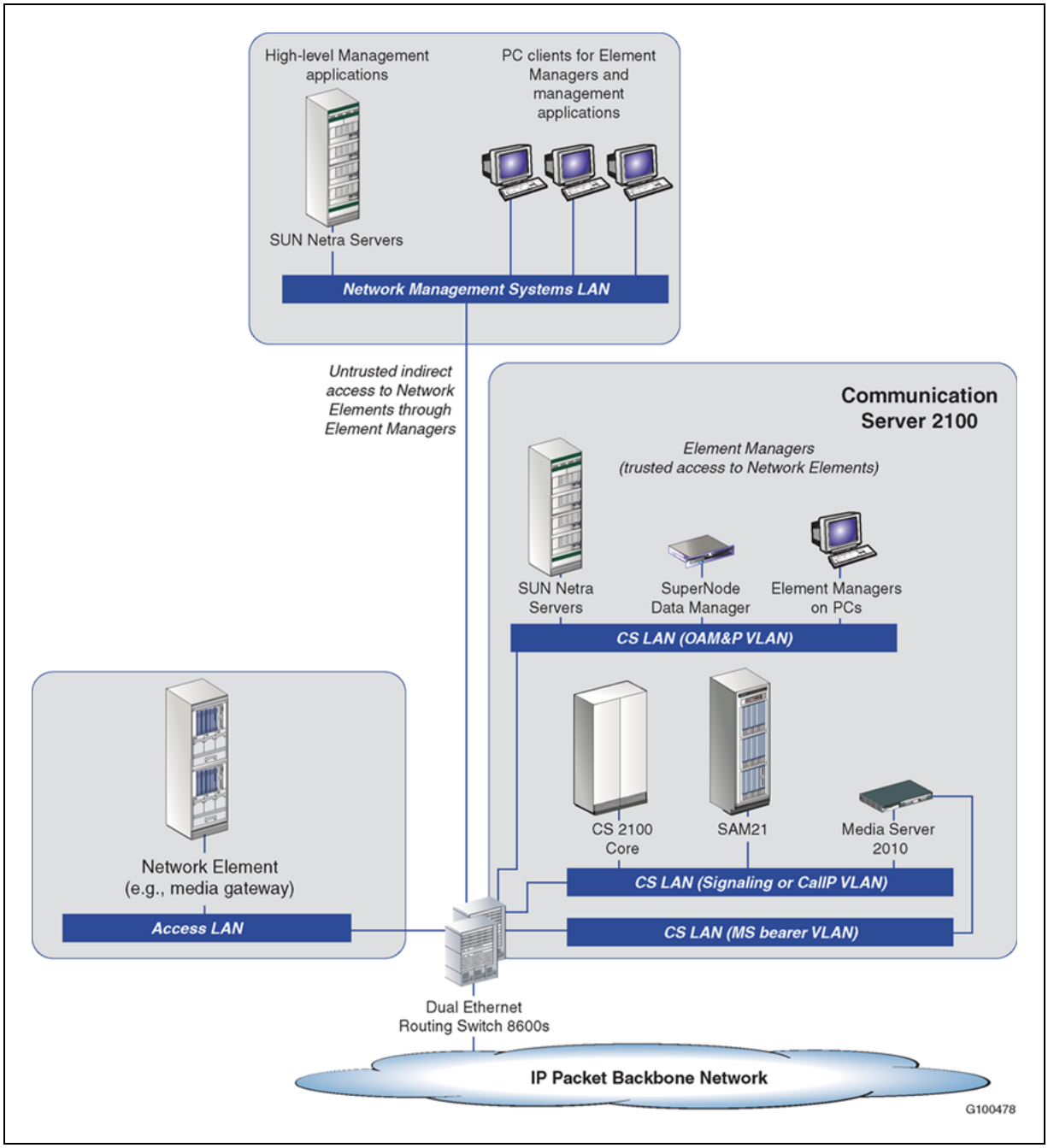
- Intranet connectivity such as access from separate (untrusted) LANs for OAMP clients such as a Network Management System (NMS).
- Backbone network connectivity through the Access LAN in the form of GbE uplinks to the backbone packet network. Backbone network connectivity is used for signaling between CS 2100 Gateway Controllers and their remote media gateways, and for peer-to-peer signaling between CS 2100 and compatible Media Gateway Controllers. They can also convey Media Server 2010 bearer traffic if required.

The main benefit of VLANs is to isolate certain types of network traffic to nodes within the same VLAN (creating a type of Layer 2 VPN with minimal security). Isolating certain types of network traffic is useful in preventing IP traffic from lesser trusted nodes and networks from reaching critical CS LAN elements.

"CS LAN Ethernet Routing Switch 8600 VLAN configuration" (page 128) shows an example of a CS LAN Ethernet Routing Switch VLAN configuration.

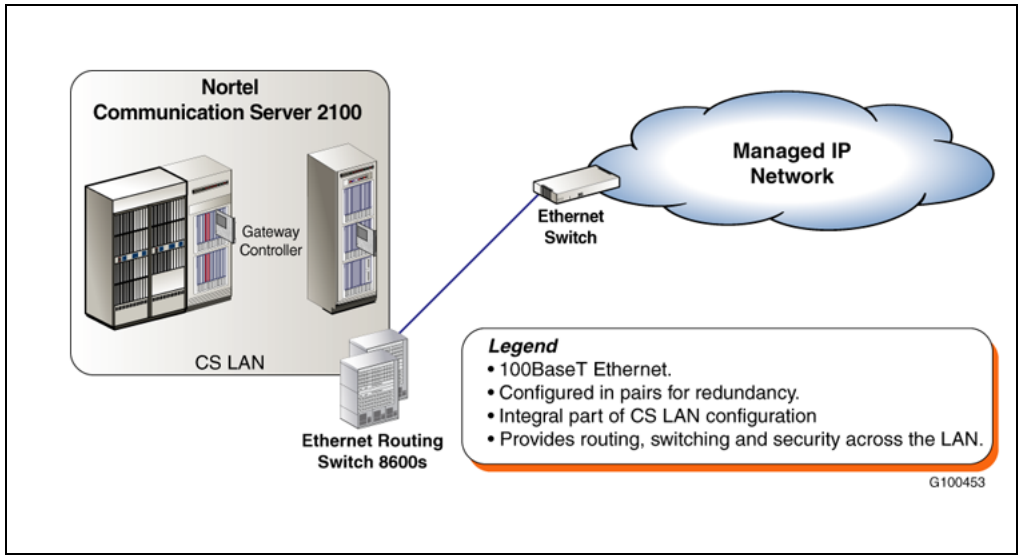
Note: For versions 3.6 and earlier, the SDM resides on both the OAMP and CallP VLANs.

CS LAN Ethernet Routing Switch 8600 VLAN configuration



"CS LAN Ethernet Routing Switch 8600 network configuration" (page 129) shows an example of the ERS 8600 in a network configuration.

CS LAN Ethernet Routing Switch 8600 network configuration



IP addressing

The VLANs use private IP addresses from within the CS 2100 IP address domain. Using private IP addresses protects functional CS 2100 Network Elements from all access, except access from known, secure applications.

> ***Note:*** These IP addresses are sometimes referred to as public addresses, which means only that they are external to the CS 2100 IP address domain to which functional Network Elements belong, not that they are public Internet addresses. In practice, the organization OAMP intranet is also a private network.

Each ERS 8600 requires the following IP addresses, which are allocated as follows:

- one for the management interface
- one Virtual IP address for VRRP
- one for each of configured VLANs

Filtering

The ERS 8600, along with other ERS 8000 series switches, provides filtering capabilities that allow the switch to filter out non-call-related traffic to prevent that traffic from interfering with CS 2100 applications. You can configure your network to prioritize specific types of traffic, ensuring that they receive the appropriate Quality of Service (QoS) level. This ensures that network resources are allocated where they are most needed.

Traffic prioritization features on the ERS 8000 series switches allow you to manage bandwidth allocation for traffic flows on the LAN at the Layer 2 level.

Traffic flows on the WAN are routed by the ERS 8600 at the Layer 3 level through a Differentiated Services (DiffServ) network architecture.

Traffic filtering is a mechanism that helps you manage traffic by defining filtering conditions and associating these conditions with specific actions. Within a DiffServ network, you can assign QoS levels that can be based on a range of filtering conditions using IP filtering.

CS LAN connections for Communication Server 2100 components

Within a CS 2100 CS LAN, communication is based on IP over 100BaseT Ethernet. "CS LAN connections supported by dual Ethernet Routing Switch 8600s" (page 130) summarizes how the 100BaseT Ethernet ports provided by the dual ERS 8600s are used to support CS LAN connections with other components.

CS LAN connections supported by dual Ethernet Routing Switch 8600s

Component	100BaseT terminations provided by	Connection characteristics
Communication Server 2100 Core		
XA-Core	LX04CA HIOP cards in XA-Core shelf	Redundancy provided by independent connections with both routers. Each High-capacity Input/Output Processor is connected to one ERS 8600, but not to the other. During normal operation, both High-capacity Input/Output Processors are active and operate in load-balancing mode.
Call Agent	Two Ethernet ports on NTRX51GZ/HZ processor cards, one in each SAM21 Call Agent shelf	Redundancy provided by independent connections with both routers. Two ports per processor card, each connected to one of the dual ERS 8600s.
Gateway Controllers in SAM21 chassis (connectivity identical for all Gateway Controller types)	Ethernet ports on Gateway Controller cards	Redundancy provided by independent connections with both routers. One port per Gateway Controller card, therefore two for a Gateway Controller pair. Each card is connected to one of the dual ERS 8600s.

Component	100BaseT terminations provided by	Connection characteristics
SAM21 Shelf Controllers	Ethernet ports on Shelf Controller cards	Redundancy provided by independent connections with both routers. One port per Shelf Controller card, therefore two for a Shelf Controller pair. Each card is connected to one of the dual ERS 8600s.
SuperNode Data Manager	NTRX50NK UMFIO Personality Module (PM) cards in SDM shelf.	Redundancy provided by independent connections with both routers. SuperNode Data Manager houses two PM cards, each connected to one of the ERS 8600s, but not the other.
Media Server 2010		
H.248 signaling connections	Dual Ethernet ports on Media Server 2010 processor card.	Redundancy provided by independent connections with both routers. Each port is connected to one of the ERS 8600s, but not the other.
Bearer connections (VoIP only)	Dual Ethernet ports on CG6000 DSP cards in the Media Server 2010.	Redundancy provided by independent connections with both routers. Each port is connected to one of the ERS 8600s, but not the other.
OAMP nodes		
CS 2000 Manager	Ethernet ports on Sun Netra 240 platform	Redundancy provided by independent connections with both routers. Each port is connected to one of the ERS 8600s, but not the other.

Component	100BaseT terminations provided by	Connection characteristics
Audio Provisioning System	Ethernet ports on Sun Netra 240 platform	Redundancy provided by independent connections with both routers. Each port is connected to one of the ERS 8600s, but not the other.
Multiservice Data Manager	Ethernet ports on Sun Netra 240 platform	Redundancy provided by independent connections with both routers. Each port is connected to one of the ERS 8600s, but not the other.

Requirements

The CS LAN is based on a ERS 8600 which is a modular product that offers Layer 2 switching along with wire-speed, IP-based Layer 3 switching functions in a single 10-slot 8010 chassis. The ERS 8600 has no single point of failure, with all system components being hot-swappable and redundant, and with takeover in the event of failure measured in microseconds.

Each CS LAN is based on two complementary ERS 8600s housed in a single cabinet, each in a separate shelf or chassis and provisioned as summarized in "Ethernet Routing Switch 8600 hardware" (page 132).

Ethernet Routing Switch 8600 hardware

Unit	Function	Provisioning
8010co chassis	Provides 10 slots for housing ERS 8600 cards.	Center slots (5 and 6) reserved for 8691 cards. Other slots (1-4 and 7-10) available for I/O support.
8691CPU/SF	ERS 8600 Central Processing Unit (CPU) and switching fabric.	One per chassis.

Unit	Function	Provisioning
8632TXE	Supports: • 32 Ethernet 100BaseT ports • two GbE ports	Two per chassis, supporting a minimum total of eight GbE ports for the CS LAN, allocated as follows: • Four GbE ports are used for fully redundant inter-chassis communication using at least two GbE links. • For IP telephony, at least two GbE ports are used for uplinks to the packet backbone network (four can be used if required).
8608GBE	Provides eight slots for Gigabit Interface Converter (GBIC) modules.	Each GbE port requires a dedicated Gigabit Interface Converter module or connection to provide its physical and optical interface characteristics. At least one 8608 card is, therefore, required per ERS 8600.
8608SXE	Equivalent to 8608GBE, but uses fixed GBIC connections instead of GBIC modules.	
8648TXE	Provides 48 10/100BaseT Ethernet ports (RJ-45).	Used to provide additional 100BaseT ports for CS LAN connectivity, if required.

Operating parameters

The following operating parameters apply to the ERS 8600:

- Supports DS1 using demux.
- Supports DS3.

References

"Documentation references" (page 133) shows where you can find more information about the ERS 8600.

Note: The ERS 8600 was previously called the Passport 8600 series.

Documentation references

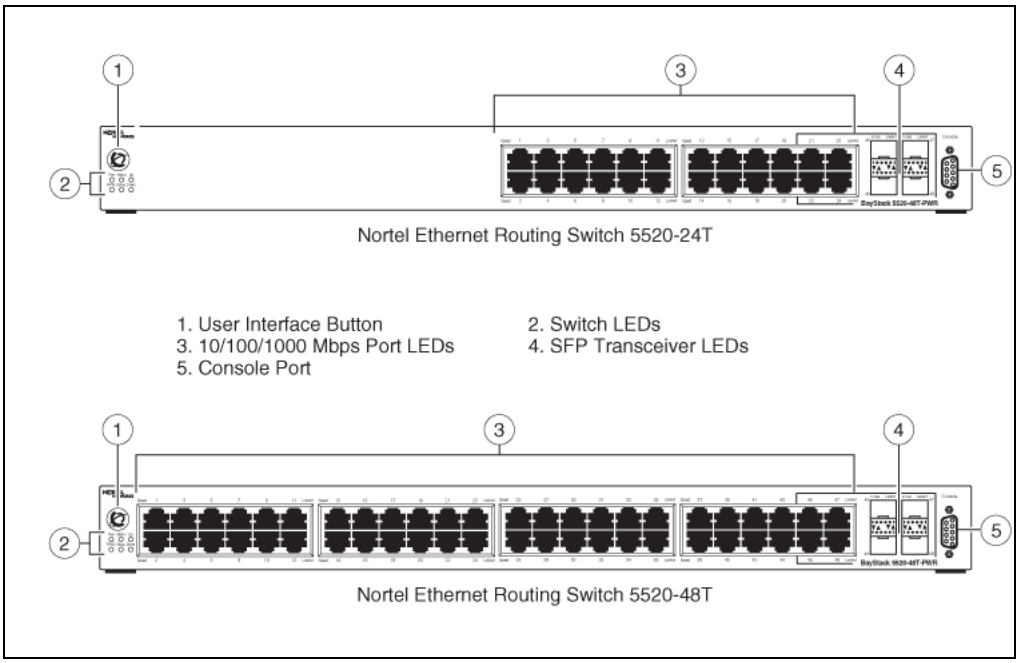
Document title	Document number
Getting Started. Passport 8000 Series Software Release 3.7	313189-D Rev 00
Managing Network Management	315545-C Rev 00
Configuring Network Management	314723-C Rev 00
Configuring QoS and IP Filtering	316433-C Rev 00

Document title	Document number
Configuring IP Routing Operations	314720-D Rev 00
Release Notes for the Passport 8000 Series Switch Software Release 3.7	313177-A Rev 00
System Messaging Platform Reference Guide	315015-C Rev 00
Important Information about the 8000 Series Switch Modules	316340-B Rev 00
Configuring and Managing Security	314724-C Rev 00
Packet Trunking-IP (PT-IP) SN06 Engineering Rules	SEB-02-10-001

Ethernet Routing Switch 5520

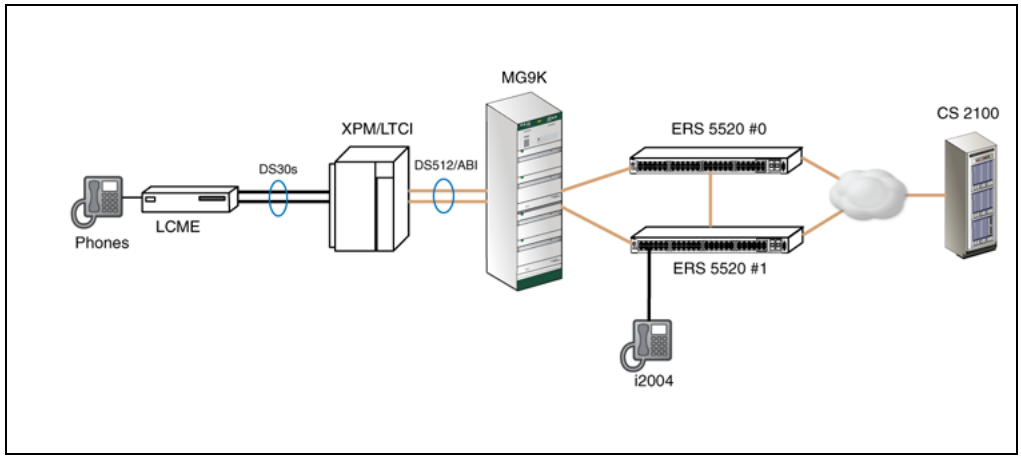
The Ethernet Routing Switch (ERS) 5520 switch provides 10/100/1000 Mbps Ethernet port capability and it allows stacking to expand capacity. There are two models; one model provides 24 ports and the other model provides 48 ports. Each ERS 5520 has four Small Form Pluggable Gigabit Interface Connector (GBIC) ports which can accept packlets to provide uplink capability. "Ethernet Routing Switch 5520 models" (page 134) shows the two models of the ERS 5520.

Ethernet Routing Switch 5520 models



The ERS 5520 is primarily used as an access switch in the Enterprise CS 2100 network to connect remote MG 9000 sites with the CS 2100 host. The ERS 5520 can also host ethernet devices such as IP Phones. "Example of Ethernet Routing Switch 5520 in a CS 2100 network" (page 135)shows an example of the ERS 5520 used as an access switch in the CS 2100 network.

Example of Ethernet Routing Switch 5520 in a CS 2100 network



Power Over Ethernet (POE) is an option with the ERS 5520. To support POE an electrical current is provided by the ERS 5520 to the end device over the Category #5 (CAT5) cable thereby eliminating the need for an AC outlet and power cord. Typical devices that support POE include internet telephones, wireless access points, network cameras, security and lighting devices.

OAMP for Communication Server 2100 networks

This chapter describes how Element Managers and Operations, Administration, Maintenance and Provisioning (OAMP) management applications provide OAMP capabilities for the Communication Server 2100 (CS 2100) and other Network Elements. OAMP for CS 2100 networks falls under the following categories:

Logical OAMP architecture

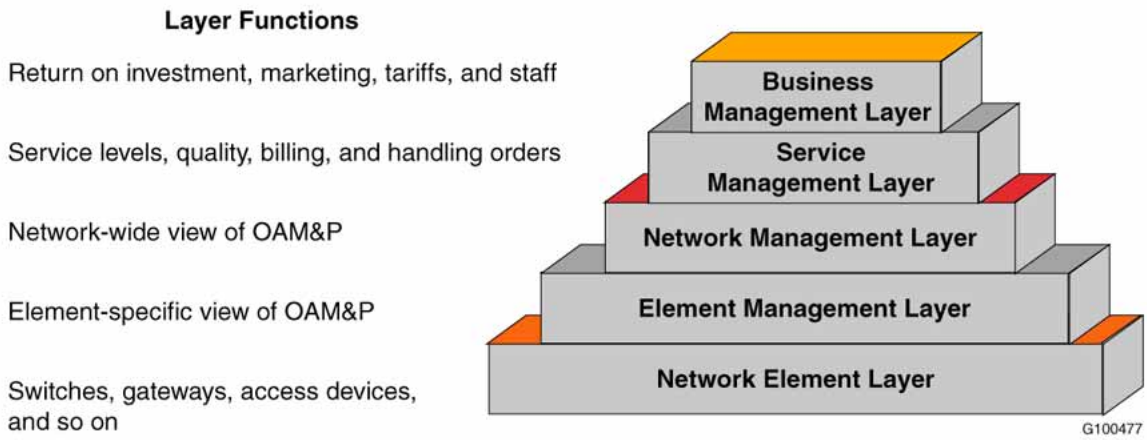
You can think of OAMP applications as belonging to a hierarchy (see "Telecommunications Management Network hierarchy" (page 137)).

Telecommunications Management Network hierarchy

Layer	Description
Network Element Layer (NEL)	At the very lowest level of the Telecommunications Management Network (TMN) hierarchy are the functional Network Elements (NEs) to be managed.

Layer	Description
Element Management Layer (EML)	Above the Network Element Layer, at the lowest management level, an Element Manager (EM) application is available for each type of Network Element or device. Each Element Manager provides management and maintenance capabilities customized for the requirements and characteristics of a specific type of device (for example, Gateway Controllers).
Network Management Layer (NML)	Above the Element Management Layer is the Network Management Layer (NML), which is concerned with the management of the network as a whole, rather than individual functional elements (for example, monitoring overall network performance).
Service Management Layer (SML) and the Business Management Layer (BML)	Above the Network Management Layer are the Service Management Layer (SML) and the Business Management Layer (BML), which build on the Network Management Layer view of the network. The Service Management Layer provides a customer interface to the network (for example, the ability to add new subscribers). At the highest level, the Business Management Layer deals with network planning (for example, monitoring network service agreements).

Telecommunications Management Network hierarchy



Nortel provides Element Managers for CS 2100 components and a number of Network Management Layer applications that are multinode in scope. For other Network Management Layer functions, and for integrated network management at the Service Management Layer and the Business Management Layer levels, such integration is supported by third-party applications and third-party correlation and browsing tools.

The following Element Managers are supported:

- Communication Server 2000 Core Manager

- Communication Server 2000 Gateway Controller Manager
- The Ethernet Routing Switch 8600 Device Manager
- Audio Provisioning Server (APS) Manager for the Media Server 2010 Provisioning Server
- Element managers for each type of trunk gateway (for example, Multiservice Data Manager (MDM) for Media Gateway 15000s)
- Element managers for each type of line media gateway (for example, IPCM Manager)

The following OAMP applications are supported:

- Communication Server 2000 Core Manager applications:
  - SuperNode Billing Application (SBA)
  - Event Reporting (logs)
  - Operational Measurements (OMs)
  - Data Management
- Trunk provisioning and maintenance applications
- Line provisioning and maintenance applications
- Audio Provisioning Server applications for the Media Server 2010
- Management Data Provider (MDP) for Multiservice Data Manager

Physical OAMP architecture

Platforms

SE07 introduced the Integrated Element Management System (IEMS) that provides an integration point for various diverse EMS platforms that make up the CS 2100 management solution. OAMP functions for CS 2100 networks are provided by a range of specialized applications running on a number of different hardware platforms that this section describes. You must understand the basic hardware platforms first to gain better a understanding of the Integrated Element Management System that is described in more detail in "Nortel Integrated Element Management System" (page 147).

- ***SuperNode Data Manager (SDM)***

  Beginning in SE07 the SuperNode Data Manager hardware (in previous releases the SDM is a Motorola PowerPC series FX system running AIX--the IBM version of UNIX), is supported on the SUN Netra 240 and is now called the Core and Billing Manager. The SuperNode Data

Manager supports the following CS 2100 Element Managers and management applications:

— Communication Server 2000 Core Manager, incorporating the following applications:

  – SuperNode Billing Application (SBA)

  – Event Reporting (logs)

  – Operational Measurements (OMs)

  – DMS Data Management System (DDMS)

> ***Note:*** In SE07 the SuperNode Data Manager was replaced by the Core Billing Manager, which incorporated its functions. For more information, see "Nortel Core and Billing Manager" (page 145).

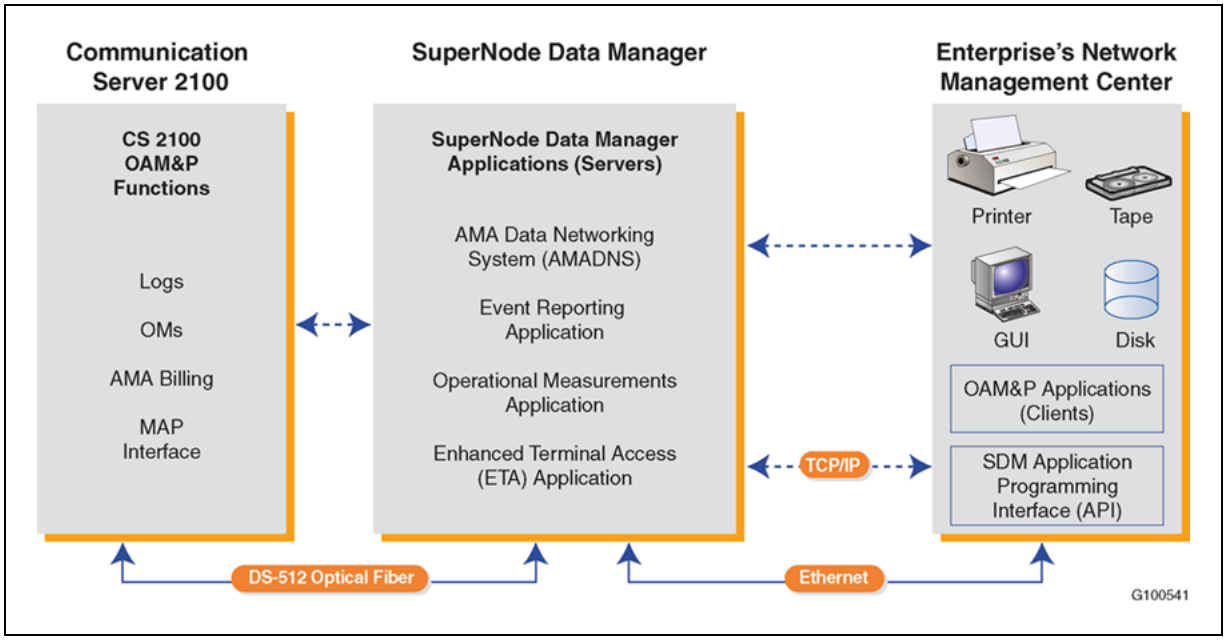
Several SuperNode Data Manager applications are available, each providing support for a different OAMP function. These applications use the client/server model, with the SuperNode Data Manager acting as the server. Application clients run on the organization workstations, which can be centrally located.

Peer-to-peer communication between clients and SuperNode Data Manager applications is supported by the SuperNode Data Manager Application Programming Interface (API), which provides clients with standard mechanisms for controlling SDM operation.

The network connection between the SuperNode Data Manager applications and their clients is provided by the standard TCP/IP protocol over an Ethernet LAN or a direct Ethernet connection. Each SuperNode Data Manager communicates with a central network management site by a managed IP network.

"The role of the SDM and its applications" (page 141) illustrates the role of SuperNode Data Manager applications in standardizing access to CS 2100 OAMP functions.

The role of the SDM and its applications



- ***Sun Netra 240***

  A number of Sun Netra servers can be housed in a single PTE2000 cabinet. Each server can support one or more of the following CS 2100 Element Managers and management applications:

  — Element Managers:

  – Communication Server 2000 Gateway Controller Manager
  – Media Server 2010 Manager
  – Communication Server 2000 SAM21 Manager
  – Audio Provisioning System Manager
  – Multiservice Data Manager (MDM) for Media Gateway 15000s

  — Management applications

  – Trunk provisioning
  – Line provisioning
  – Node provisioning
  – Optional Trunk Management and Maintenance (TMM) application
  – Optional Line Management and Maintenance (LMM) application
  – Line Test Manager (LTM)
  – Network Patch Manager (NPM)

– Audio Provisioning Server (APS) Manager for the Media Server 2010

– Management Data Provider (MDP) for Multiservice Data Manager

"Sun Netra 240" (page 142) shows a line drawing of the Sun Netra 240.

Sun Netra 240

- ***Windows PC***

  The following Element Manager runs on a dedicated Windows PC:

  — IPCM Manager

  — Ethernet Routing Switch 8600 Device Manager

The following additional components are used for OAMP:

- Application client and Graphical User Interfaces (GUIs):

  — Sun workstations supporting X-Windows clients

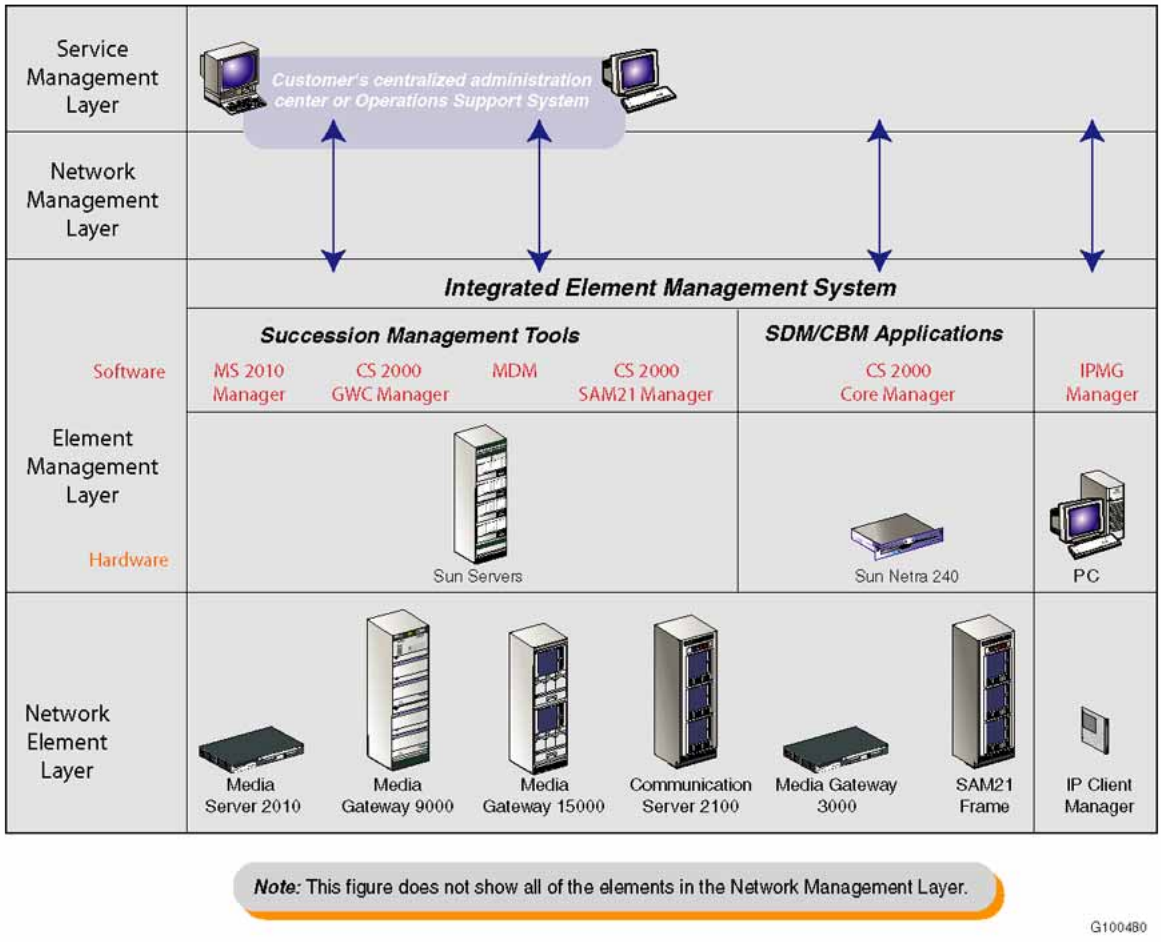
  — Windows PCs supporting Information Element browser clients and application GUIs

- Secure access

  — VPN Router 600, which provides secure remote access to the CS 2100 for Nortel support, using a high-bandwidth TCP/IP connection through the external internet for patching, emergency support, and problem solving.

"Management components and software applications summary" (page 143) maps the physical component and software applications into the Telecommunications Management Network hierarchy.

Management components and software applications summary



Client workstations

"Client platforms" (page 143) lists the platform and method of invocation for each client application.

Client platforms

Name	Invocation	Platform	
		PC	SUN
SAM Clients	Desktop		X
SAM21 Manager	Desktop	X	X
Succession 2000 Management Tools Selector	Browser (HTML)	X	X
Gateway Controller Manager	Browser (JWS)	X	X

Name	Invocation	Platform	
		PC	SUN
Media Server 2010	Browser (JWS)	X	X
Line Maintenance Manager	Browser (JWS)	X	X
Node Provisioning	Browser (JWS)	X	X
Network Patch Manager	Browser (HTML)	X	
Trunk Provisioning	Telnet/STELNET	X	X
Line Provisioning	Telnet/STELNET	X	X
Nodes Provisioning	Telnet/STELNET	X	X
Audio Programming System Manager	Browser	X	
STORM Manager	Browser (Proxy)	X	X
Call Agent Manager	Telnet (Proxy)	X	X
Media Device Manager/Management Data Provider	Desktop (X.11)		X
Device Manager	Desktop (Java)	X	X

References

"Documentation references" (page 144) shows where you can find more information about OAMP.

Documentation references

Document title	Document Number
CS 2000 Core Manager (manages the XA-Core and subtending TDM components of the Communication Server 2100 XA-Core)	
CS 2000 Core Manager Basics	NN10018-111
CS 2000 Core Manager Fault Management	NN10082-911
CS 2000 Core Manager Configuration Management	NN10104-511
CS 2000 Core Manager Accounting Management	NN10126-811
CS 2000 Core Manager Performance Management	NN10148-711
CS 2000 Core Manager Administration and Security	NN10170-611
Upgrading the CS 2000 Core Manager	NN10060-461
Communication Server 2100 Logs (describes logs by component)	
Carrier Voice over IP Fault Management Logs Reference	NN10275-909
Communication Server 2100 OMs (describes OMs by component)	

Document title	Document Number
Carrier Voice over IP Performance Management Operational Measurements Reference	NN10264-709
Backup procedures (describes backups and restorations by component)	
ATM/IP Solution-level Security and Administration	NN10402-600
Upgrade procedures (describes upgrades by component)	
Upgrading the Carrier Voice over IP Network	NN10440-450

Nortel Core and Billing Manager

Introduced in SE07, the Core and Billing Manager (CBM) consolidates Fault, Configuration, Accounting, Performance and Security (FCAPS) for the CS 2100 XA-Core and Compact on a carrier-grade platform. The Core and Billing Manager is a fault-tolerant system that provides a suite of OAMP applications through LAN/WAN Ethernet connectivity.

SuperNode Data Manager applications are extended to the Core Billing Manager. The application and downstream interface are the same as the SuperNode Data Manager.

Benefits

The Core and Billing Manager provides enterprises with the following benefits:

- Conforms to the IEMS consolidation plan using the latest carrier-grade Sun platform, the Netra 240.
- Delivers the same applications as the SuperNode Data Manager suite.
- Provides expansion capability for different applications and call traffic volumes.
- Offers a smaller footprint than legacy SuperNode Data Manager systems (approximately three times smaller).
- Enables many operations, initiatives, and applications, including Billing Stream Filtering, Secure File Transfer, and Operational Measurements.
- Provides central security.
- Maximizes available resources and paves the way for unmanned offices by supporting a remote central location.
- Uses industry-standard operating environments and protocols (for example, UNIX, TCP/IP, and Ethernet).

Functional description

The Core and Billing Manager offers the following capabilities:

- Offloads OAMP responsibilities and processing from the Core.

- Provides secure access to the Core from the operations intranet.
- Provides an end-to-end path from the switch to the operations intranet for the transfer of billing files, logs, and other data.
- Supports electronic software delivery and patching.

The Core and Billing Manager has two Ethernet connections as follows:

- An Ethernet connection to the CS 2100 XA-Core High-capacity Input/Output Processor (HIOP) card or CS 2100 Compact.
- An Ethernet connection to the operations intranet for communications with the Network Management System (GbE IP).

The Core and Billing Manager provides most of the functions offered by the CS 2000 Core Manager and SuperNode Data Manager (SDM) products including the following applications:

- SuperNode Billing Application (SBA)
- Operational Measurement Delivery (OMD)
- Log Delivery

Hardware

The Core and Billing Manager consolidates element managers onto a pair of Sun Netra 240 Servers that results in one platform type and common spares for all OAMP applications. The Sun Netra 240 server is a NEBS-compliant server that offers the following features:

- two Ultra SPARC IIIi processors at 1.28 Ghz
- 2 GB RAM
- three PCI slots
- Digital Video Disk (DVD)-Read/Write (RW) drive (removable)
- four GbE interfaces
- Advanced Lights Out Management (ALOM) function

The Core and Billing Manager servers are part of the Cabinetized Operations Administration and Maintenance (COAM) platform housed in the PTE2000 cabinet. The Core and billing Manager can also be deployed in an existing Miscellaneous Equipment Frame (MIS) frame cabinet.

User interface

The Core and Billing Manager uses local MAP-based interfaces for Core-based OAMP functions. Some Core and Billing Manager applications, such as the SuperNode Billing Application, have unique user interfaces.

Capacity and limitations

The SuperNode Billing Application has scalable storage capacity providing up to 300,000 records per hour of sustained billing throughput (100 bytes per record).

References

"Documentation references" (page 147) shows where you can find more information about the Core and Billing Manager.

Documentation references

Document title	Document Number
CS 2000 Core Manager Basics	NN10018-111
CS 2000 Core Manager Security and Administration	NN10170-611
CS 2000 Core Manager Fault Management	NN10082-911
CS 2000 Core Manager Configuration Management	NN10104-511
CS 2000 Core Manager Performance Management	NN10148-711
Upgrading the CS 2000 Core Manager	NN10060-461
CS 2000 Core Manager Accounting	NN10126-811

Nortel Integrated Element Management System

Overview

Nortel delivers the next generation "super-EMS" known as the Integrated Element Management System (IEMS). This single point of integration and management reduces the maintenance component of large enterprises long-term operating costs by eliminating the need to handle multiple northbound feeds for different Network Elements flowing into Network Management Systems. Instead IEMS consolidates performance, fault, and security functions for the entire VoIP network to reduce cost and integration complexity. Element Manager configuration modules and the billing management module are easily accessed using IEMS. The strategic vision for IEMS includes unification of the configuration user interfaces further simplifying management of VoIP Network Elements.

IEMS improves the simplicity of VoIP network management by aggregating the Element Management function on as small a footprint as possible.

Introduced in SE07, the IEMS Client Interface is a powerful human interface to CS 2100 OAMP components. IEMS presents complex enterprise management information in clear and easily understandable Graphical User Interfaces (GUIs). Acting as a central integration point, IEMS provides access to the following items of the management solution:

- Element Management System platforms
- Element Managers (EMs)

- Management Applications
- Network Elements (NEs)

IEMS provides a central location to view, normalize, and forward faults, and a common maintenance interface launch point to access the various devices in a CS 2100 network.

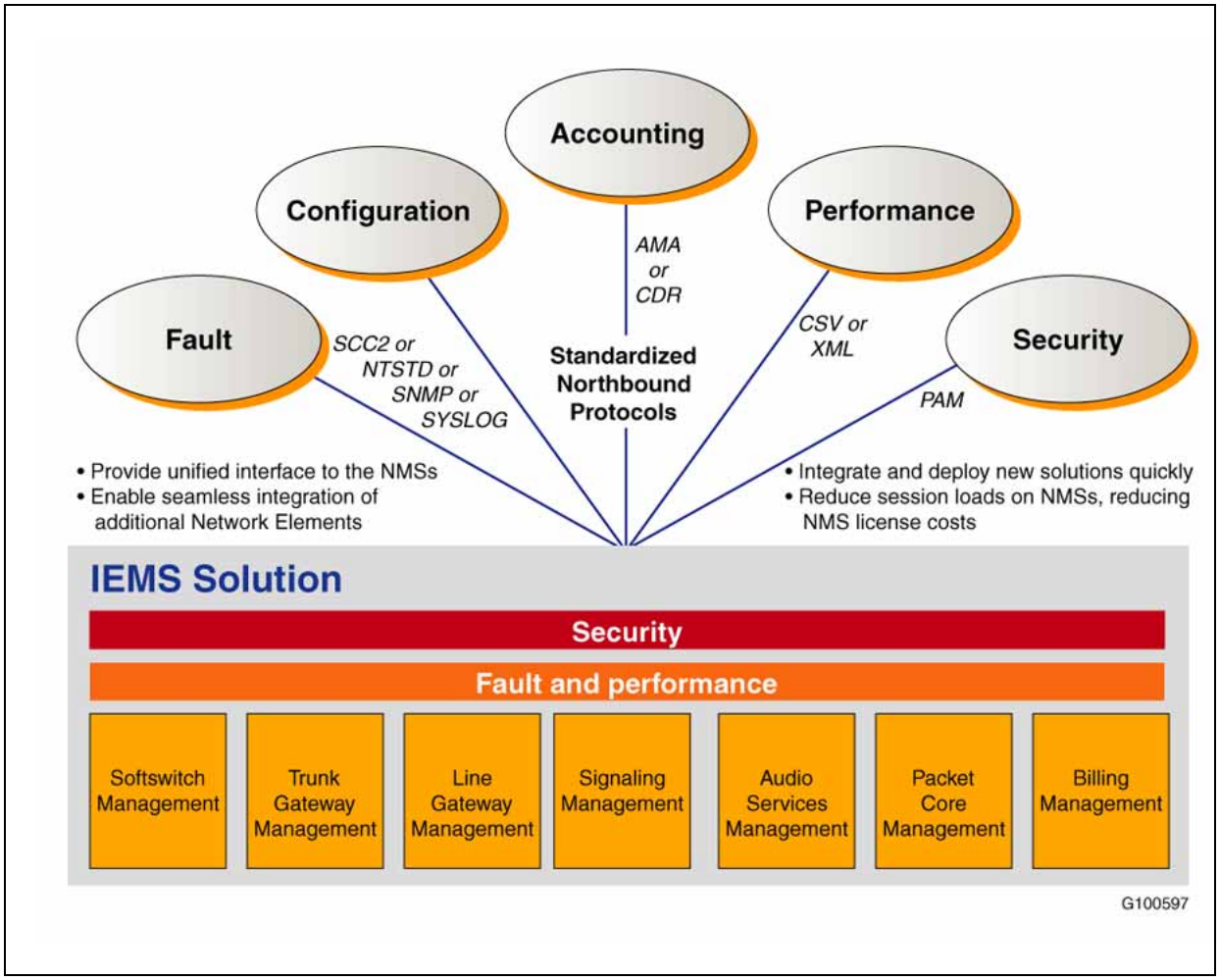
The high-level functional capabilities of IEMS include the following:

- An integrated managed device viewing area.
- An integrated maintenance interface launch point.
- An integrated network event viewing browser.
- An integrated network alarm viewing area.
- Alarm and event mediation from the diverse fault interfaces and standard event interfaces.
- Integrated audit and security log browsers.
- Local security and administration interfaces.

Benefits

"Integrated Element Management System benefits" (page 149) summarizes the benefits that the Integrated Element Management System provides.

Integrated Element Management System benefits



In response to the feedback from the marketplace, requesting solutions requiring less integration and to provide simplicity, IEMS operates as follows:

- Reduce Network Management System (NMS) integration complexity and resource requirement.
- Construct a framework to consolidate Element Managers and, in the process, reduce the footprint, reduce management complexity, and provide a common user interface.
- Deliver security solution enhancements to address multiple strategies to protect data and access to Network Elements.
- Provide a means to quickly manage new Nortel or third-party Network Elements.
- Manage changes in the Network Elements release over release.

IEMS consolidates EMS functions, including configuration and toolsets from the individual EMS modules and in the process drives simplification.

"IEMS initial interface" (page 150) shows the initial interface that appears when launching IEMS.

IEMS initial interface

Client access modes

A technician can access IEMS client through either the full-featured Java Web Start (JWS) interface or a light-weight HTML client. Depending on the circumstances, each access mode has its advantages. While the Java Web Start client provides more functions, it imposes greater resource demands on the client platform and requires more launch time. The HTML interface is well-suited for low-speed client connections.

Java Web Start Client interface

"Java Web Start Client GUI panel items" (page 151) describes the primary functional panels available with the Java Web Start Client.

Java Web Start Client GUI panel items

Item	Description
Menu bar	The menu bar contains the labels for attached menus. A separator is a horizontal line drawn on a menu and is used to separate one set of operations from another. The menu bar contains menus including File, Custom Views, Edit, View, Actions, Tools, Look And Feel, Window, and Help. The menus appearing in the menu bar are context-sensitive to the object selected in the IEMS Java Web Start Client. The menus and menu items appear or disappear dynamically according to the object selected in the IEMS Java Web Start Client.
Toolbar	The toolbar displays a collection of actions, commands, or control functions. Toolbars provide quick access to frequently used components. The default position for the toolbar is below the menu bar. The system provides a tool tip for each button, to indicate the operations performed by them. Tool buttons include Go Back to Previous, Go Forward to Next, Save, Print, Refresh, Delete, Stop, and Help. The toolbar can be moved and floated. Buttons appearing on the toolbar are context-sensitive to the object selected in the IEMS Java Web Start Client. Buttons appear or disappear dynamically according to the object selected in the IEMS Java Web Start Client.
Tree	The system uses a tree to display a set of IEMS applications with their hierarchical data relationships. The fundamental object in a tree is called a node, which represents a data item in the given hierarchical set. Thus, a tree comprises one or more nodes. The root node is the top node of the hierarchical data. Nodes inside root nodes are called child nodes. Nodes that contain no child nodes are called leaf nodes. By selecting a particular node, the corresponding panel is displayed in the right-side frame.
Alarm count panel	The alarm panel count shows the alarm category of each severity (that is, Critical, Major, Minor, Warning, and Clears) for each alarm category. The Alarm panel appears below the IEMS tree. Double-clicking the count displayed in the alarm panel causes the alarms of the specific severity to display in the corresponding alarm panel. The system updates this panel automatically and the counts can be seen continuously, regardless of the functional view (that is, whether maps or events are selected). The tool tip and cursor shape change when the cursor is pointed to alarm counts. By selecting the counts in the alarm count panel, they system displays the respective alarms in the right-side panel.
Status bar	The status bar appears at the bottom of the screen. Messages indicate the status of the current process. The status bar displays "Done" when all the contents are loaded or displays "loading..." if the process is still active. The status bar changes from dark blue to green when a product is loaded.
Display panel	The display panel appears on the right-hand side as a frame within the main window. The panel shows the frame that corresponds to the selection made on the tree.

HTML Web Client interface

"HTML Web GUI panel items" (page 152) describes the primary functional panels available with the HTML Web Client.

HTML Web GUI panel items

Item	Description
Module tabs	Module tabs provide easy navigation of various features in a module of IEMS. The following items are the various modules in the IEMS HTML Web Client: • Topologies • Fault Management • Performance • Inventory • Admin Click each tab to display the respective module view on the right-side frame of the Web Client.
Module tree	A tree appears on the left side of the HTML Web Client that contains various nodes. This tree differs from one module to another. Click each tree node to get the related information on the right-side frame of the HTML Web Client. For example, in the Topologies view, click the Element Managers node on the tree to display the Element Managers in the network.
Module menus	Menus are available as a drop-down box, links, and icons. The drop-down box and links are available only in the Fault Management and Network Database views. The drop-down box contains a set of commands that are useful when you need to perform an operation over multiple elements in a view. For example, in the Inventory view, click the icon to view options to perform an operation, such as Delete Object and Traces over a single Network Element. In the same view, when you need to perform the same operation over more than one Network Element, select the check boxes of those Network Elements, and then select the option in the menu.
Alarm count panel	The alarm panel count shows the alarm category of each severity (that is, Critical, Major, Minor, and Information) for each alarm category. The Alarm panel appears below the IEMS tree. Clicking the count displayed in the alarm panel causes the alarms of the specific severity to display in the corresponding alarm panel.

Launching applications from IEMS

You can launch applications, Element Managers, or commands from the topology GUI in IEMS depending on the object selected. This section summarizes the items that can be launched from the central IEMS platform.

Launching applications for Element Managers

"Element Managers with corresponding application launched" (page 153) lists the Element Managers with corresponding launch applications based on the Command Line User Interface or GUI applications.

Element Managers with corresponding application launched

For Element Manager	Device version	Application or command name	Menu item in object-specific menu or right-click menu of object in topology
Command Line through IEMS Server			
MultiService Data Manager (MDM)	6.2	Command Line	Command Line
IPCM Manager	9.0	Command Line	Launch Command Line
IPCM Manager node	9.0	Command Line	Launch Command Line
GUI applications			
Audio Provisioning Server	6.2/7.0	APS Manager	APS Manager
CS 2000 Core (manages Call Agent Core and XA Core NEs)	9.0	Core Manager Maintenance MAPCI	Launch Core Mgr Maintenance Launch MAPCI Session
Gateway Controller (GWC)	9.0	GWC Manager (CS 2000 Management Tools) GWC Manager Network View	GWC Mgr (CMT) GWC Mgr Network View
SAM21	9.0	SAM21 Manager	SAM21 Mgr GUI
Media Gateway 9000 (MG 9000)	9.0	MG 9000 Manager	MG9K Manager MG9K Manager
MDM (manages Media Gateway 15000)	6.2/7.0	MDM Manager GUI	MDM Mgr GUI
Media Server 2010	6.2/7.0	Media Server 2010 Manager (CS 2000 Management Tools)	MS 2010 Mgr (CMT)
IP Client Manager	9.0	IPCM Manager	Launch CICM Manager

Launching applications for platforms

"Platforms with corresponding application launched" (page 154) lists the platforms with corresponding launch applications based on the Command Line User Interface or GUI applications.

Platforms with corresponding application launched

For Platform	Device version	Application or command name	Menu item in object-specific menu or right-click menu of object in topology
Command Line through Integrated EMS Server			
Multiservice Data Manager	15.3	Command Line	Command Line
Server Platforms Foundation Software (SPFS)	9.0	Command Line Restart SPFS Restart SPFS	Command Line Restart IEMS Restart IEMS
SPFS unit	9.0	Command Line Restart SPFS	Command Line Restart SPFS
SuperNode Data Manager (SDM)	9.0	Command Line	Command Line
GUI applications			
SPFS	9.0	Servman Application Status SWACT Cluster	Servman Application Status SWACT Cluster
SPFS Unit	9.0	Servman Application Status SWACT Cluster	Servman Application Status SWACT Cluster

Launching applications for EMS applications

"EMS applications with corresponding application launched" (page 154) lists the EMS applications with corresponding launch applications based on the Command Line User Interface or GUI applications.

EMS applications with corresponding application launched

For EMS application	Device version	Application or command name	Menu item in object-specific menu or right-click menu of object in topology
Command Line through Integrated EMS Server			
OSSGate	9.0	BPT Command Line	Launch BPT CLUI

For EMS application	Device version	Application or command name	Menu item in object-specific menu or right-click menu of object in topology
QoS Collector Application	9.0	Command Line	Launch Command Line
GUI applications			
Line Maintenance Manager	9.0	Line Maintenance Manager	Line Maintenance Manager (LMM)
Trunk Maintenance Manager	9.0	Trunk Maintenance Manager	Trunk Maintenance Manager (TMM)
OSSGate	9.0	OSSGate BPT Servlet	Launch OSSGate Launch BPT Servlet
Network Patch Manager	9.0	Network Patch Manager	Network Patch Manager (NPM)
Audio Provisioning Server	11.0	APS Manager (CS 2000 Management Tools) APS Audio Configuration Tool	APS Manager (CMT) APS Audio Configuration Tool
Device Manager	5.8.2.1	Device Manager	Device Manager

Launching applications for Network Elements

"NES with corresponding application launched" (page 155) lists the NEs with corresponding launch applications based on the Command Line User Interface or GUI applications.

NES with corresponding application launched

For NE	Device version	Application or command name	Menu item in object-specific menu or right-click menu of object in topology
Command Line through Integrated EMS Server			
ERS 8600	3.7.2.2	Command Line	Command Line
STORM	6.0	Command Line	Launch Command Line
Media Server 2010	4.6	Command Line	Command Line
Call Agent Core managed by Core Manager	9.0	Command Line	Call Agent Platform Command Line
Call Agent Platform managed by Core Manager	9.0	Command Line	Call Agent Platform Command Line

For NE	Device version	Application or command name	Menu item in object-specific menu or right-click menu of object in topology
GWC NE managed by GWC Manager	9.0	Command Line	Launch Command Line
Media Server 2010	4.6	Command Line	Command Line
Session Server	9.0	Command Line	Command Line
Session Server unit	9.0	Command Line	Command Line
IPCM NE	9.0	Command Line	Launch Command Line
IPCM NE node	9.0	Command Line	Launch Command Line
GUI applications			
ERS 8600	3.7.2.2	ERS 8600 Device Manager	ERS 8600 Device Manager
STORM	6.0	STORM Manager	STORM Manager
Call Agent Core managed by Core Manager	9.0	MAPCI Session	Launch MAPCI Session
Call Agent Platform managed by Core Manager	9.0	MAPCI Session	Launch MAPCI Session
Audio Provisioning Server NE managed APS application	11.0	APS Manager (CS Management Tools) APS Audio Configuration Tool	APS Mgr (CMT) APS Audio Configuration Tool
GWC NE managed by GWC Manager	9.0	GWC Unit Manager Line Maintenance Manager Trunk Maintenance Manager Network Patch Manager Launch NPM	GWC Unit Mgr Launch LMM Launch TMM CS Tools Launch CS2K Tools
XA-Core managed by CS 2000 Core Manager	9.0	MAPCI Session	Launch MAPCI Session
Session Server NE	9.0	Session Server	Launch Session Server
Session Server Unit	9.0	Session Server	Launch Session Server
IPCM NE managed	9.0	IPCM Manager	Launch CICM Manager

For NE	Device version	Application or command name	Menu item in object-specific menu or right-click menu of object in topology
IPCM NE node managed IPCM Manager	9.0	IPCM Manager	Launch CICM Manager
SAM21 NE managed by SAM21 Manager	9.0	SCU Subnet SCU Manager	Launch SCU Subnet Launch SCU Manager
Media Gateway 3200	9.0	IPSec and IKE Configuration tool	IPSec and IKE Configuration tool

References

"Documentation references" (page 157) shows where you can find more information about IEMS.

Documentation references

Document title	Document Number
IEMS Basics	NN10329-111
IEMS Security and Administration	NN10336-611
IEMS Fault Management	NN10334-911
IEMS Configuration Management	NN10330-511
IEMS Performance Management	NN10327-711
Communication Server 2100 Commercial Systems Service Order Reference Manual	555-4031-808, 297-8021-808P1 and 297-8021-808P1 (DMS versions)
OSSGate User's Guide	NE10004-512
CS 2000 Core Manager Security and Administration	NN10172-611

Fault management

Three aspects to CS 2100 support for fault management are as follows:

- Fault reporting using logs:
  - — Supported for the CS 2100 Core and SAM21 card cages. Logs are generated in Nortel standard format by the Core and then converted into Switching Control Center 2 (SCC2) format. Switching Control Center 2 is a Bellcore standard for integrating logs generated by different vendor equipment in a multivendor network.
  - — Supported by the Multiservice Data Manager (MDM) used to manage Media Gateway 15000s. The system maps alarm and

status reports provided by Multiservice Data Manager onto logs and converts them into Switching Control Center 2 format through the SuperNode Data Manager Log Generation (SLG) Application Programming Interface (API).

If your organization network uses more than one CS 2100 softswitch, the system optionally sends logs to a Network Management System (NMS).

- Other fault reporting mechanisms

  Network Elements that do not generate logs need to provide notification of alarm and status changes.

  "Additional reporting mechanisms" (page 158) summarizes the mechanisms used.

Additional reporting mechanisms

Network element	Reporting mechanism		Notes
	From element to Element Manager	To present information to Network Management Layer	
Gateway Controller	SNMP	Common Object Request Broker Architecture (CORBA)	In addition to reporting Gateway Controller faults, Gateway Controllers controlling Media Gateway 15000s provide gateway state reports.
ERS 8600	SNMP	SNMP	--
Media Server 2010	SNMP	CORBA	Typically, the Media Server 2010 Server runs on the same server as the Audio Provisioning Server and the Gateway Controller Element Manager, and information is presented to the Network Management Layer on behalf of all three in a single merged stream of CORBA changes.
Media Gateway 15000	Media Gateway 15000s use American Standard Code for Information Exchange (ASCII) over TCP to provide the Multiservice Data	CORBA	Media Gateway 15000 state changes are reported through their Gateway Controllers.

Network element	Reporting mechanism		Notes
	From element to Element Manager	To present information to Network Management Layer	
	Manager with the information used to create logs.		

- Fault isolation and correction:
  - Fault isolation and correction is carried out through the Element Manager for the Network Element in question (for example, the Core Manager or the Gateway Controller Element Manager).
  - In addition, the CS 2100 supports the following two optional management applications for trunk and line maintenance through the Core:
    - Trunk Management and Maintenance
    - Line Management and Maintenance

Access Care

Nortel Access Care provides a comprehensive trouble management application that delivers unified management and diagnostics for packet and TDM networks. Access Care delivers multidomain customer service ticketing, automated testing and diagnostics, sophisticated workforce management, and an integrated network ticket solution. The Access Care application is a multivendor, multitechnology system with industry-standard open interfaces for seamless integration with existing OSS, test equipment, and network elements.

Line or loop testing

Access Care automates testing and diagnostic processes for both the local loop and deployed network. Access tests and diagnoses to efficiently isolate troubles, testing inward toward the network and outward to the customer's PC and modem. Access Care offers testing solutions for POTS, DSL, and special services.

Nortel Access Care external test system has direct access to test heads collocated with the MG 9000, or a Maintenance Trunk Module, for line testing. Access Care communicates with the Line Test Manager through an ethernet port. The manager software provides the line test management application to convert the Access Care parameters into commands that

can be forwarded and processed in the MG 9000. Using the GUI the user specifies the test heads for Access Care use when testing a specified line circuit.

Using Access Care, you can set up a connection for Metallic Test Access (MTA) to a line card by entering a Directory Number (DN). Loop qualification predicts if the loop can deliver the service, including the accurate predictions of upstream and downstream data speeds. The loop qualification results are stored in the customer record as the loop footprint. The footprint can be used later for comparing or tracking changes in the loop performance.

References

"Documentation references" (page 160) shows where you can find more information about Access Care.

Documentation references

Document title	Document number
Access Care documentation (ships with the product)	N/A
ATM/IP Solution-level Fault Management	NN10408-900
MG 9000 Fault Management	NN10074-911

Configuration management

Hardware commissioning

The following items relate to hardware provisioning:

- Commissioning of hardware units for installation is achieved through the local interface and Element Manager for the unit. This applies to the following:
  - CS 2100 Core
  - Gateway Controllers
  - SAM21 card cages
  - IP Client Manager
  - Media Gateway 9000
  - ERS 8600s
  - Media Server 2010
  - Media Gateway 15000s
- CS 2100 Core configuration through the Communication Server 2000 Manager using ASCII over TCP.
- Gateway Controller configuration through the Gateway Controller Element Manager using SNMP.

- ERS 8600 configuration through the ERS 8600 Device Manager using SNMP.
- Media Server 2010:
  - Media Server 2010 audio service configuration through the Audio Provisioning Server using SNMP
  - Automatic discovery of Media Server 2010 hardware to the Media Server 2010 Element Manager
- Media Gateway 15000 configuration and provisioning through the Multiservice Data Manager GUI using ASCII over a TCP interface.
- Primary Trivial File Transfer Protocol (TFTP) server configured on the CS LAN to support load retrieval for Gateway Controllers and SAM21 Shelf Controllers.

Trunk provisioning

Trunk provisioning requires you to update data stored by some or all of the following components:

- CS 2100 Core
- Gateway Controllers
- Trunk media gateways

The following two applications provide help to ensure that these separate updates are coordinated:

- Trunk provisioning application
- Node provisioning application

These applications run on a provisioning server. The server hosts a database that provides an integrated view of the network as a whole, combining the separate views of different network nodes. The server can also host the optional Trunk Maintenance Manager (TMM) application to provide maintenance capabilities.

The trunk provisioning and node provisioning applications both provide Extensible Markup Language (XML) input to generate the following types of information:

- ASCII over TCP, which is provided to the Communication Server 2000 Manager on the SuperNode Data Manager and is used by it to update CS 2100 Core datafill.
- CORBA data, which is provided to the Gateway Controller Element Manager and is used by it to update Gateway Controller data.

Line provisioning

Line provisioning requires you to make updates to the data stored by some or all of the following components:

- CS 2100 Core
- Gateway Controllers
- Line media gateways

The following two applications provide help to ensure that these separate updates are coordinated:

- Line provisioning applications
- Node provisioning application (also used in trunk provisioning)

These applications run on a provisioning server. This server also hosts a database that provides an integrated view of the network as a whole, combining separate views of different nodes. The server can also host the optional Line Maintenance Manager (LMM) application.

The line-provisioning and node-provisioning applications support different interfaces for handling provisioning data as follows:

- The line provisioning application supports the Nortel proprietary Service Order (SERVORD) interface.
- The node provisioning application supports an XML interface.

Each application uses line-provisioning input to generate the following two types of output:

- ASCII over TCP, which is provided to the CS 2000 Manager on the SuperNode Data Manager and is used by it to update the Communication Server 2100 datafill.
- CORBA data, which is provided to the Gateway Controller Element Manager and is used by it to update the Gateway Controller data.

Application Programming Interface (API) in IEMS

The Integrated Element Management System provides an Application Programming Interface that uses Enhanced SERVORD (SERVORD+) commands. These new commands apply to components in a CS 2100 network (for example, gateways). With SERVORD+ commands, the media gateway name (MGName) and Termination Point (TPName) generally replace the LEN for CS 2100 lines. LEN continues to be used in SERVORD commands for TDM lines.

The SERVORD+ commands are NEW, EST, ADD, DEL, OUT, CDN, and CHDN as follows:

- NEW, EST and ADD - add the termination point, Directory Number and indicated Line Class Code
- DEL and OUT - delete the termination point
- CDN and CHDN - change the Directory Number

Accounting

The CS 2100 supports billing by automatically generating call records to capture information such as call start time, call duration, and calling party number. These records are periodically downloaded to a central administrative center for processing. The records provide the organization with all the information necessary to bill individual subscribers or departments for calls made.

The system supports the following call-recording formats:

- Automatic Message Accounting (AMA)
- Station Message Detail Recording (SMDR)

Automatic Message Accounting

The CS 2100 uses a flexible variant of Extended Bellcore Automatic Message Accounting Format (EBAF) AMA records for AMA billing. This variant, Universal AMA, uses a subset of the standard EBAF structures, modified to support open numbering plans. The CS 2100 creates Automatic Message Accounting records, which the system then downloads and processes externally to produce subscriber bills.

Dates and times in Automatic Message Accounting records are based on the CS 2100 Core Time-of-Day (TOD) clock.

Bellcore Automatic Message Accounting record types and generation

An Automatic Message Accounting billing record consists of a fixed-length base record, to which the system can append a number of variable length modules to record additional information about a call.

The main types of record that Bellcore Automatic Message Accounting typically generates are as follows:

- ***Records generated as a result of call handling***

  Translating and routing a call triggers the generation of these records. This type of record must provide the following information for the charges incurred for a call to be calculated:

  — Originating subscriber name

— Terminating number of digits

— Time and date of origination

— Duration (conversation time) of call

- ***Records generated as a result of administrative activity***

  The system typically produces these types of records to inform the downstream processor of events and measurements occurring on the CS 2100 when recording occurs. The following events typically result in Automatic Message Accounting record generation:

  — Closing an active recording file

  — Opening a new active recording file

Automatic Message Accounting base record supported structures

The CS 2100 supports the generation of five different Automatic Message Accounting record types for logging call events. The system distinguishes these record types by the following factors:

- The maximum number of called party digits that can be stored, which can be 18 or 30 digits.
- Whether the record includes an additional field that indicates which of the following type of call completion was encountered:

  — Normal answer

  — Call abandoned (tear down during ringing)

  — Busy treatment

  — Any other treatment

  — Abnormal or unknown completion (any other reason)

- Whether the record includes carrier selection information.

Modules appended to provide further information

In some cases, billing requires more information about a call type than can be provided by the base structure. In this event, the system can append modules or data to the base record. Automatic Message Accounting identifies each module by a unique Module Code, with a Module Code of 000 terminating the Module Code list appended to the record.

Automatic Message Accounting records for long calls

Long calls can generate of more than one Automatic Message Accounting record.

The long-call audit process runs at regular intervals to check whether long calls are in progress. The audit interval typically corresponds to the long-call threshold value. The audit process also generates a partial billing record for each active long call.

Note: It is important to distinguish between long calls, in which both agents are still active, and hung calls, in which one of the trunk agents involved remains connected after call clearing because of some technical problem. The CCBHNG maintenance tool runs at predefined intervals to check for hung calls and to provide notification of them so that the appropriate action can be taken.

Station Message Detail Recording

In a Virtual Private Network (VPN), customers may wish to collect additional information about calls, as well as the information required for billing (for example, to build a profile of calls made and received for a customer group). The Station Message Detail Recording system can record details of billable and non-billable calls for each call leg. The Station Message Detail Recording system uses the Automatic Message Accounting subsystem to collect the call data and record it on a data storage device for subsequent downloading.

Note: The system uses Station Message Detail Recording primarily to collect information about how individual subscribers use features, but it can also be used to collect information at the customer group level.

File transfer to billing records

The Automatic Message Accounting subsystem of the CS 2100 Core generates Automatic Message Accounting records during call processing. The system immediately transfers the records to the Core Manager SuperNode Billing Application (SBA) on the SuperNode Data Manager to be stored, which means that it is not necessary for this to be done on the CS 2100.

Note: Although billing information is usually routed directly to the SuperNode Data Manager, you must configure backup volumes on the CS 2100 to hold this information if a problem with the CS 2100 to SuperNode Data Manager link occurs.

Core Manager SuperNode Billing Application support for billing

All Automatic Message Accounting records that the CS 2100 Core generates are immediately transferred to the Core Manager SuperNode Billing Application for formatting and storage. This means that these tasks

need not be performed on the CS 2100. The system can use either of the following two formats for storing Automatic Message Accounting records and files on the SuperNode Data Manager:

- SuperNode Data Manager Automatic Message Accounting Data Networking System (AMADNS) format.
- Device Independent Recording Package (DIRP) format, as previously used in legacy Meridian SL-100 switches for the local storage of Automatic Message Accounting records.

Performance management

Each network node collects performance data in the form of Operational Measurements (OMs) or Performance Measurements (PMs). The system provides these Operational Measurements and Performance Measurements to an enterprise administrative center, or Network Management System, through Element Managers or some other intermediary.

Operational Measurements are standard measurements originally defined by Bellcore for collecting performance data in circuit-based telephony networks, many of which are also applicable to packet networks supporting IP telephony. Performance Measurements are used to collect data for packet networks nodes and the set of Performance Measurements collected for a given node tends to be node-specific. The CS 2100 uses Operational Measurements and Performance Measurements as follows:

- The system supports performance monitoring through Operational Measurements for all of the CS 2100 Network Elements. It can be complemented by using selected Automatic Message Accounting records to monitor performance.
  - The CS 2100 Core collects Operational Measurements and provides them to the Communication Server 2000 Core Manager running on the SuperNode Data Manager using ASCII over TCP. The Core Manager provides Operational Measurements to the Network Management Layer in the following two formats:
    - Standard subsets of Operational Measurements are sent at predefined intervals using the standard Bellcore-defined TR740 and TR746 interfaces.
    - Operational Measurements are assembled into files in Comma-Separated Value (CSV) format and are transferred using FTP.
  - Billing records to be used in performance monitoring are presented to the Network Management Layer using ASCII over TCP.
- Performance monitoring using Performance Measurements

"Performance Measurement presentation to the Network Management Layer" (page 167) summarizes the way in which the CS 2100 Network Elements, other than the CS 2100, collect Performance Measurements for presentation to the Network Management Layer.

Performance Measurement presentation to the Network Management Layer

Network element	Reporting mechanism		
	From element to intermediary	Intermediary	To present information to Network Management Layer
Gateway Controller	SNMP	Performance Measurement Poller running on the same server as Gateway Controller Element Manager, Media Server 2010 Element Manager, and Audio Provisioning Server	Aggregated Performance Measurements in CSV format using FTP
SAM21	SNMP		
Media Server 2010	SNMP		
ERS 8600	SNMP	ERS 8600 Device Manager	Performance Measurements in CSV format using FTP
Media Gateway 15000	SNMP	Poller task (for example, on an Element Manager)	CORBA

In SE09, Nortel does not offer standard applications for integrated handling of performance reporting and management for a CS 2100 at the Network Management Layer. Instead, such integration is supported by third-party fault collectors and third-party tools for reporting, analysis, and management.

OAMP security

This section describes the security mechanisms used for the OAMP applications. For more information about security for the entire CS 2100 network, see"Communication Server 2100 network security" (page 171).

Introduction

General OAMP security requirements

The following are some of the basic requirements for OAMP security:

- Operation System hardening
- No IP forwarding/IP routing

- No root accounts
- Login security with password changes
- Client is firewall-compatible
- Northbound traffic is not anonymous FTP and uses Secure Shell (SSH)

Mechanisms

This section describes the security mechanisms that are used to protect the OAMP applications. Security in OAMP covers a wide range of requirements, interfaces, and platforms as follows:

- Interfaces
  - — Identification or access control level (authentication)
  - — Authorization or access control level (authorization)
  - — Data integrity
  - — Data confidentiality (privacy)
  - — Auditing
  - — Security administration
  - — Monitoring
  - — Visibility
- Environment
  - — LAN paritioning (VLAN)
  - — Firewall
  - — Platform hardening
  - — Network Elements, Element Management System servers, Element Management System clients, and Network Management System interfaces

Nortel recognizes that OAMP security is a critical requirement for CS 2100 networks. As such, ongoing security developments that include the following improvements:

- Central authentication (Pluggable Authentication Module [PAM]) for GWC Manager, Media Server 2010 Manager, APS Manager, OSSGate, LMM, TMM, NPM, SAM21 Manager, SPFS Platform, MDM, and SDM.
- Common user groups for GWC Manager, Media Server 2010 Manager, APS Manager, OSSGate, LMM, TMM, NPM, SAM21 Manager, and SPFS Platform.
- MAPCI, OSSGate and SPFS platform access through Telnet and Secure Shell (SSH) login.

- Core and SPFS FTP access through FTP using SFFTP (SSH).
- Secure login to web-based applications.
- Removal of Distributed Computing Environment (DCE) dependencies (DCE is optional).
- User login and passwords required for all user interfaces.
- Formal VLAN partitioning rules.
- For CMT, IEMS, and MG 9000 Element Manager, the system provides a user inactivity timer that terminates login when the time is exceeded.
- Ability to notify the administrator of user IDs not used for a specifiable period of time.
- Ability to control access based on time of day and end user system address.
- Ability to track changes in security profiles, configurations, and attributes.
- SDM can be configured for login-only through IEMS.
- All Command Line User Interfaces (CLUI) are accessible from a restricted shell environment.
- Central management and tracking of accounts used for the SDM/CBM portion of MAPCI Passthrough.
- IPSec host to host tunnels for all northbound OSS connections.

Name Service Switch

The Name Service Switch (nsswitch) is used for central authorization or user profile management (for example, groups, home directory, and default shell). Name Service Switch allows a third-party product to supply a Lightweight Directory Access Protocol (LDAP) service (or service compatible with the nsswitch interface) to provide a centralized administration for this data.

The nsswitch capability is compatible with PAM which is used for central authentication (that is, userid/password).

Pluggable Authentication Module

Pluggable Authentication Module (PAM) provides a generic interface for authentication (that is, userid/password). PAM can plug into RADIUS, LDAP, SecureID (uses secure tokens), Oracle, and Passwerks nsswitch (on UNIX) to act as an authentication mechanism.

IEMS API security

The security solution for the IEMS Application Programming Interface centers around the following:

- PAM for authentication

- nsswitch for authorization
- a Single Sign On (SSO) key generation or verification module

On the interfaces side, a given application, or Network Element, can rely on the underlying UNIX PAM/nsswitch or can implement its own RADIUS or Hypertext Transmission Protocol, Secure (HTTPS) interface to interact with the authentication or authorization interfaces.

The Single Sign On key generation interface is available over HTTPS.

Communication Server 2100 network security

This chapter describes the mechanisms used to control access to the Network Elements and applications that comprise Communication Server 2100 (CS 2100)solutions. The system implements security functions in the following ways:

- The functional Network Elements involved in call processing and service provision for end users.
- Element Managers.
- Integrated Management applications.

The objective of these security mechanisms is to protect the CS 2100 Network Elements from unauthorized viewing or data modification, and from denial-of-service attacks.

Specific mechanisms to provide enhanced security include the following items:

- encryption of network management traffic
- standardized secure logs
- robust password management
- firewall protection
- operating system hardening
- virus-free software
- secure remote access
- intrusion detection

Nortel commitment to secure solutions

Nortel provides a common set of product safety requirements including the following items:

- Secure Sockets Layer (SSL) Guideline

- Secure Shell (SSH) Guideline
- IPsec Software Requirements
- Solaris Operating System Hardening Guide
- HP-UX Operating System Hardening Guide
- Microsoft NT 4.0 Operating System Hardening Guide
- Secure Logs Content Security Requirement
- Secure Logs Format Security Requirement
- RADIUS/PAM Guideline
- Firewall Placement Document
- Password Standard for Nortel Products
- Intrusion Detection Security Requirement
- SNMPv3 Guideline Document
- GR815 Guideline Document
- Secure Remote Access Guideline Document
- Single Sign On/Access Control Security Requirement

Network architecture for access control

Appropriate configuration of the CS 2100 LAN/IP network infrastructure is an important part of the solution for providing secure access to OAMP functions.

ATTENTION

See the *Packet Trunking-IP (PT-IP) SN06 Engineering Guidelines*, SEB-02-10-001, for guidelines for configuring the CS LAN security.

To configure the LAN setup for a CS 2100 network, the following items are required:

- ERS 8600 (or comparable router), duplicated for redundancy, provides filtering and routing between the LANs (for more information, see"Ethernet Routing Switches" (page 125)).
- Alteon or comparable firewall.

A Network Element or application can talk to others only by going through the ERS 8600. In addition, a Network Element or application uses separate interfaces and ports to talk to each applicable VLAN. No multiuse ports is available for multiple VLANS.

To enhance security, the network for a CS 2100 solution is partitioned into a number of subnets enforced using VLANs, which can be referred to as the internal CS-LAN subnet structure (see "CS LAN Ethernet Routing Switch 8600 VLAN configuration" (page 128) for a sample depiction of this LAN configuration).

Note: The following is an example only; customer's configurations of private and public IP addresses can vary according to their individual IP network configuration.

The VLANS can be summarized as follows:

- The signaling VLAN (also referred to as the call processing or CallP VLAN) interconnects the functional CS 2100 Network Elements involved in call processing and service provisioning for end users.

  The signaling VLAN uses private IP addresses from within the CS 2100 IP domain. VLAN protects functional CS 2100 Network Elements from access, except access from other Network Elements on the same VLAN. The signaling VLAN is protected from all direct external access.

- The OAMP VLAN interconnects the Element Management System servers supporting the Element Managers for functional Network Elements.

  The OAMP VLAN uses public IP addresses. Access to the Element Management System servers on this VLAN is by appropriately authenticated entities on the enterprise Network Management Systems LAN (for example, desktop clients and Higher-Level Management application servers). Other users can access CS 2100 Network Elements only through Element Management System interfaces. Other users have no direct IP route to the CS 2100 Network Elements. No extension of the OAMP VLAN to other servers or services is permitted, to prevent a compromise to compromise the security of the CS 2100 Network Elements.

- An Access LAN that connects to the Network Elements (for example, Media Gateway 15000s). Access LANs are located on the other side of the ERS 8600s.

- A Media (and bearer) VLAN is configured to handle Media Server 2010 bearer traffic on the CS LAN.

- A Network Management Systems LAN is an external OAMP LAN to the various Network Management Systems.

Since the CS-LAN switches provide a common interface to the Access/Aggregation Network, the packet filtering rules enforced by them allow only valid call signaling, media, and OAMP traffic to reach the appropriate servers that it processes. All traffic between CS 2100 network

components is isolated from the traffic between external devices and the servers. This limits the types of traffic to which key servers are exposed and minimizes the potential for a malicious attack.

The internal CS-LAN subnet structure enforced by VLAN separation provides further access restrictions for different types of devices. For example, direct access to the call processing and media device is not permitted from the Network Management System. All access must be proxied by the Element Management Systems through secure, authenticated interfaces. To protect the critical call processing function from being affected by internal attacks originating in the Network Management System.

In addition to the firewall, the BCP 7000 series provides additional protection for media components hosted on the CS-LAN. It filters and proxies media traffic by the CS 2100 to the appropriate media gateway in the Media subnet.

Network segregation aimed at protecting the CS 2100 network does not end with the CS-LAN. Only valid VoIP protocols and corresponding OAMP traffic is allowed on the Core network. Nortel recommends using virtual separation of VoIP traffic into a virtual CS 2100 Core network containing all non-CPE components. This can be achieved using means such as IP Virtual Private Networks (VPNs) or Multiprotocol Label Switching (MPLS) tunnels.

In a VPN configuration, Nortel recommends an internal firewall such as the Alteon Switched Firewall (ASF) be used to protect the servers and inspect bearer streams. Alteon Switched Firewall creates a Secure Voice Zone (SVZ). The ASF firewalls and enterprise infrastructure routing switching (for example, ERS 8600) protect the CS 2100. In addition, extensive use can be made of the VPN Router Secure IP Services Gateway (SISG) platform to provide encrypted VPN tunnels across the corporate WAN (and/or MAN).

The firewall also plays a key role in mitigating Denial of Service attacks by throttling various types of traffic preventing them from exceeding nominal levels or blocking them altogether. Finally, the firewall can provide Network Intrusion Detection functionality to help identify malicious traffic sent towards the Core network.

Security and administration management

Security management includes the authentication and authorization of end users and applications. Security management includes the following tasks:

- creating, deleting, and controlling security services and mechanisms
- distributing security information
- recording and reporting security related events

Functional summary

Nortel recognizes that security is a key to any organization move to IP telephony. As such, SE09 supports the following security management functions:

- Network Element security provisioning through respective Element Managers.
- Operating systems provide security for access to the Gateway Controller Manager, Media Server 2010 Manager and Multiservice Data Manager.
- Single login and central user administration support for the Network Patch Manager, Line Maintenance Manager, Trunk Maintenance Manager, Gateway Controller Manager, Media Server 2010 Manager, Line Test Manager, and Multiservice Data Manager through the Pluggable Authentication Module (PAM) implementation of user access management.
- FTP, bootp, SSH, and Telnet proxy support for embedded management systems, such as Call Agent and STORM.
- Support for Sun and PC clients for the Gateway Controller Manager, Line Maintenance Manager, Trunk Maintenance Manager, Network Patch Manager, and SAM21 Manager.
- Context-sensitive GUI launching for the Gateway Controller Manager and SAM21 Manager.
- User-level access support for the Gateway Controller Manager, Media Server 2010 Manager, Line Test Manager, Trunk Maintenance Manager, Network Patch Manager, Multiservice Data Manager, and Device Manager.
- User activity audit logging for the Gateway Controller Manager.
- Ability to notify the administrator of user IDs not used for a specifiable period of time.
- Ability to control access based on time of day and end user system address.
- Ability to track changes in security profiles, configurations, and attributes.
- SDM can be configured for login-only through IEMS.
- All Command Line User Interfaces (CLUI) are accessible from a restricted shell environment.
- Central management and tracking of accounts used to the SDM/CBM portion of MAPCI Passthrough.
- IPSec host to host tunnels for all northbound OSS connections.
- IPSec between the Multiservice Data Manager and Media Gateway 15000.

- IPSec log reporting from the Gateway Controller.

User management

User types

The CS 2100 supports the following two types of users:

- The administrative class consists of the root user.
- The maintenance class consists of the maintenance user by default, you can add maintenance class users.

"User class profiles" (page 176) lists the capabilities available to each class of user.

User class profiles

Class	Responsibilities	Capabilities
Administration	System administration	• User and group administration — adding and removing users — assigning and restricting user access — password administration • System image backup and restore • Unrestricted command access • Local console access from LAN • Setting the time zone and the date and time • All maintenance user capabilities
Maintenance	Maintenance	• Using maintenance commands (for example, busy, return to service, and off line) • Monitoring system performance • Restricted command access • Changing system alarm thresholds • Updating passwords • Configuring application-specific tools

Password administration

The root user can change any password on the system at any time. Maintenance class users can change only their own passwords. The following conditions apply to user passwords:

- The maximum duration for passwords is four weeks for root users and nine weeks for maintenance class users.
- The system issues warnings seven days before the password expires and repeats the warning at each login until the password is changed.
- A user cannot reuse a password for 26 weeks after its assignment.
- If a maintenance class user password expires, the user has up to two weeks after the expiration date to change the password. During this period, the user must enter a new password to log in. If the user does not change the password by the end of the two-week period, the root user must reset the password before the maintenance user can log in.
- The minimum length of password is six characters. The password must contain a minimum of one alphabetic character and a minimum of one numeric or special character. Although users can enter more than eight characters for a password, the system considers only the first eight characters.

  Note: Although passwords beginning with a number are valid, they cannot currently be accepted following the SMDRLogin command.

Idle logins

The system automatically logs out all users if no activity occurs for ten minutes.

For CMT, IEMS, and MG 9000 Element Manager, the system provides a user inactivity timer that terminates login when exceeded.

Authentication mechanisms

The CS 2100 configuration uses the following mechanisms to manage user authentication:

- Pluggable Authentication Module (PAM) is the default mechanism.
- Component Element Management Systems
- Component operating systems

Pluggable Authentication Module

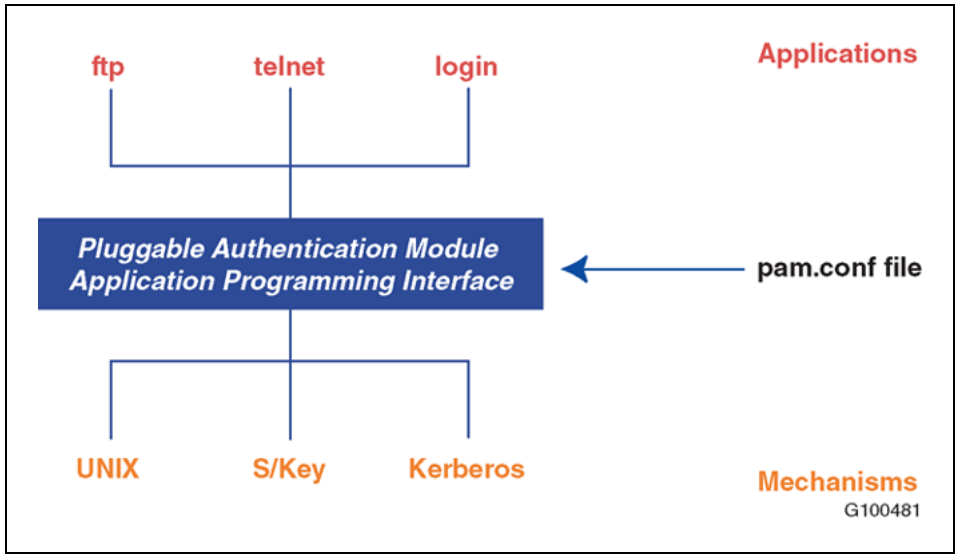
With the Pluggable Authentication Module framework, multiple authentication technologies can be added without changing any of the log in services, thereby preserving existing system environments. The Pluggable Authentication Module integrates login services with different technologies.

The core components of the Pluggable Authentication Module framework include the following:

- authentication library Application Programming Interface (API)
- authentication mechanism-specific modules

"Basic Pluggable Authentication Module architecture" (page 178) shows the Pluggable Authentication Module architecture.

Basic Pluggable Authentication Module architecture



When an application calls the Pluggable Authentication Module Application Programming Interface, it loads the appropriate authentication module, as determined by the configuration file pam.conf. The system forwards the request to the underlying authentication module to perform the specified operation. The Pluggable Authentication Module is partitioned into the following functional areas:

- Authentication Management includes the pma_authenticate function to authenticate the user and the pam_setcred interface to set, refresh, or remove the user credentials.
- Account Management includes the pam_acct_mgmt function to check whether users should receive access to their accounts. This function can implement account expiration and access-hour restrictions.
- Session Management includes the pam_open_session and pam_close_session functions for session management and accounting.
- Password Management includes the pam_chauthtok function to change the password.

Element Management Systems

User authentication for some components is controlled by the component Element Management System, which controls access through individual user account databases with the Element Management System.

Operating systems

Operating systems provide security for the all components used in the CS 2100 network. The operating systems of the components are "hardened" to provide additional security diligence.

References

"Documentation references" (page 179) shows where you can find more information about the CS 2100 security for large enterprises.

Documentation references

Document title	Document number
ATM/IP Solution-level Security and Administration	NN10402-600
Communication Server 2000 Security and Administration	NN10171-611
CICM Security and Administration	NN10252-611
IEMS Security and Administration	NN10336-611
STORM Security and Administration	NN10176-611
Media Server 2000 Series Security and Administration	NN10337-611
IW SPM-IP Security and Administration	NN10166-611
MG 9000 Security and Administration	NN10162-611
Securing the Enterprise Network Document Library	A wide range of articles, positioning papers, white papers, and solution and application overviews are available on Nortel.com

Appendix A
Technical specifications

Operating environment

Ceiling height

A minimum clear ceiling height of 3 m (10 feet) is required for the Communication Server 2100 (CS 2100) cabinets and frames. The recommended clear ceiling height is 3.4 m (11 feet).

Floor loading

The floor loading of fully-equipped CS 2100 bays, including frame supporting cabling, averages 3.38 kilonewtons per square meter (80 pounds per square foot). You should include an allowance of 0.423 kilonewtons per square meter (10 pounds per square foot) for ceiling-supported cabling of the floor below in multifloor buildings. Add a further allowance of 0.423 kilonewtons per square meter (10 pounds per square foot) for personnel and transient loads. The total loading in a multifloor building is, therefore, 4.2 kilonewtons per square meter (100 pounds per square foot).

Environmental specifications

CS 2100 equipment remains functional and operates as expected under the environmental conditions that "Environmental conditions" (page 181) shows.

Environmental conditions

Condition	Value
Ambient temperature	In the range of 10°C to 30°C (with short-term variations in the range of 5°C to 49°C) (see note)
Relative humidity	In the range of 22% to 55% (with short-term variations in the range of 20% to 80%) (see note)
Note: Short-term means not more than 72 consecutive hours and no more than 15 days in one year.	

Condition	Value
Atmospheric pressure	423 mmHg (69.2 KPa), corresponding to 3,048 m (10,000 feet) of altitude.
Ambient air	With cleanliness ≤ class 100,000 (number of particles ≥ 0.5 microns per cubic foot)
Note: Short-term means not more than 72 consecutive hours and no more than 15 days in one year.	

Temperature and humidity should be measured 1.254 m (5 feet) above floor level and 381 mm (15 inches) in front of the equipment. Rate of temperature change must not exceed 6.7°C (15°F) per hour.

The heat dissipation of a CS 2100 configuration averaged over the equipment room floor and over 24 hours should not exceed 861 watts per square meter (80 watts per square foot).

Maximum sound levels produced by equipment to be located in power rooms, or in special sound-tested areas, should not exceed 85 dBA. Maximum sound levels for all other equipment should not exceed 75 dBA.

Storage and shipping conditions

General storage conditions are in accordance with ISO R14. Transportation and intermediate storage conditions are in accordance with ISO O22. You can ship the CS 2100 by truck, rail, sea, or air when it is packed for transportation. "Storage and shipping conditions" (page 182) shows the environmental conditions that should not be exceeded during transportation.

Storage and shipping conditions

Condition	Value
Ambient temperature	-40°C to 71°C (-40°F to 160°F)
Humidity	10% to 95% maximum water vapor pressure not to exceed 25 mmHg
Vibration	Up to 3.5 g at 5 Hz to 500 Hz
Shock	Equivalent to a 152-mm (6-inch) drop for a 454 Kg (1000 lb) equipped bay

You can store CS 2100 equipment in a sheltered environment under the same ambient temperature and humidity conditions detailed for transportation.

Compliance with standards

CS 2100 equipment complies the following North American softswitch standards for telecommunication equipment:

- FCC part 15, Class A
- UL 1950/CSA 950
- Telcordia NEBS Level 3 criteria (GR-63-CORE, GR-1089-CORE)

The inherent strength and stability of the CS 2100 cabinets provide Zone 4 earthquake protection without additional bracing. The CS 2100 cabinets meet industry isolated grounding and requirements and feature connectors to facilitate testing.

Communication Server 2100 cabinets and frames

The following two types of CS 2100 configurations are supported:

- CS 2100 XA-Core
- CS 2100 Compact

Both types of configuration support the same range of call-processing agents, protocols and telephony features. The main differences are that the CS 2100 Compact uses a different processor complex, has a significantly smaller footprint, and delivers reduced call-processing capacity.

"Communication Server 2100 cabinet summary" (page 183) describes the cabinets that can house the CS 2100 components.

Communication Server 2100 cabinet summary

Cabinet	Dimensions	Used to house
C42 equipment cabinet	107 cm wide x 183 cm high x 71 cm deep (42 inches x 72 inches x 28 inches)	• XA-Core • Message Switch • ENET

Cabinet	Dimensions	Used to house
C28 equipment cabinet	71 cm wide x 183 cm high x 71 cm deep (28 inches x 72 inches x 28 inches)	• SuperNode Data Manager • Integrated Service Module/Input/Output Module
PTE2000 equipment cabinet	61 cm wide x 213 cm high x 61 cm deep (24 inches x 84 inches x 24 inches)	• SAM21 shelves with Call Agent, Network File System and Gateway Controllers • Sun Netra servers for Device Managers and OAMP applications ***Note:*** In CS 2100 Compact configurations, the main PTE cabinet houses two SAM21 shelves. A second PTE2000 frame is required to house Element Managers for CS 2100 Compact components.

Each cabinet, or frame, contains equipment shelves that provide slots for installing circuit cards and/or space to house specialized units that, in turn, contain circuit cards.

CS 2100 cabinets meet industry requirements for isolated grounding and feature connectors to facilitate testing. The cabinets provide greater physical and electrostatic discharge damage protection for the enclosed equipment than open frames. They also comply with electromagnetic compatibility requirements and provide Zone 4 earthquake protection without additional bracing.

Power consumption examples

"Power consumption examples" (page 185) provides examples of the power requirements for CS 2100 cabinets.

Note: Power consumptions vary depending on the actual components housed in each cabinet.

Power consumption examples

Item	Call Control Frame	OAMP cabinet	SuperNode Data Manager cabinet
Power	2500 watts 8,540 BTU/hour	1650 watts 5,640 BTU/hour	870 watts 3980 BTU/hour
Current drain	56.2A	32.5A	17.2A
Nominal voltage	-50.25 V	-50.25 V	-50.25 V

Appendix B Peripheral support

"Supported Meridian SL-100 peripherals" (page 187) lists the Meridian SL-100 peripherals that are supported on the TDM side of the Communication Server 2100 (CS 2100) hybrid.

Supported Meridian SL-100 peripherals

Peripheral	Abbreviation
Series I	
Conference Trunk Module	CTM
Digital Trunk Module	DTM
Input/Output Controller	IOC
Input/Output Module	IOM
Integrated Services Module	ISM
Intelligent Peripheral Equipment	IPE
Maintenance Trunk Module	MTM
Packaged Trunk Module	PTM
Remote Maintenance Module	RMM
Service Trunk Module	STM
Trunk Module, 8-Wire	TM8
Series II	
Digital Trunk Controller	DTC
Digital Trunk Controller-ISDN	DTC(I)
Enhanced D-channel Handler	EDCH
Enhanced Line Concentrating Module	ELCM
Line Concentrating Module	LCM
Line Concentrating Module-Enhanced	LCME
Line Group Controller	LGC

Peripheral	Abbreviation
Line Group Controller-ISDN	LGC-I
Line Trunk Controller	LTC
Line Trunk Controller-ISDN	LTC-I
Remote Cluster Controller	RCC
Remote Cluster Controller 2	RCC2
Remote Line Concentrating Module	RLCM
Subscriber Carrier Module-100 Access	SMA
Subscriber Carrier Module-100 Access, Second Version	SMA2
Series III	
SS7 Link Interface Unit (requires 32M processor)	LIU7
Ethernet Interface Unit ***Note:*** Not supported on the CS 2100 Compact.	EIU
Enhanced Network	ENET
Link Peripheral Processor	LPP
Message Switch	MS
Spectrum Peripheral Module	SPM

ATTENTION

Refer to the *Communication Server 2100 Peripheral Module Release Document RELDOC* (555-4001-599) for detailed information about Meridian SL-100 Peripheral Modules.

List of terms

3WC
Three-Way Calling

AAL5
ATM Adaption Layer for lightweight VBR real-time traffic.

ABI
Access Bridging Interface

AC
alternating current

AC
Access Point

ACD
Automatic Call Distribution

ACF
Active Call Failover

ADSL
Asymmetrical Digital Subscriber Loop

AEM
Accessory Expansion Module

AG
Application Gateway

ALOM
Advanced Lights Out Management

ALT
Automatic Line Test

AMA
Automatic Message Accounting

AMADNS
Automatic Message Accounting Data Networking System

AMATEST
Automatic Message Accounting Test Call Capability

APD
Address and Port Discovery

API
Application Programming Interface

APS
Audio Provisioning Server

ASCII
American Standard Code for Information Interchange

ASF
Alteon Switched Firewall

ASIC
Application-Specific Integrated Circuit

ASM
Application Master Server

ASU
Application Specific Unit

ATC
Automatic Time and Charges

ATM
Autovon Trunk Module

ATM
Asynchronous Transport Mode

ATMF UNI
ATM Forum Unidirectional

ATT
Automatic Trunk Test

AUI
Application Unit Interface

B8ZS
Bipolar with 8 Zeros Substitution

BCP
Border Control Point

BCT
Bearer Channel Tandeming

BHCA
Busy Hour Call Attempts

BIC
Bus Interface Card

BIP
Breaker Interface Panel

BML
Business Management Layer

bootp
Bootstrap Protocol

BRI
Basic Rate Interface

BRISC
BNR Reduced Instruction Set Computing

CA
Call Agent

CAC
Call Admission Control

CALEA
Communications Assistance for Law Enforcement Act

CallP
Call Processing

CAT5
Category #5

CBM
Core and Billing Manager

CCA
Compact Call Agent

CCF
Call Control Frame

CCS
Centi-Call Seconds

CDN
Called Party Number

CE
Customer Edge

CFB
Call Forward Busy

CFD
Call Forward Do Not Answer

CFNA
Call Forward No Answer

CFP
Channel Frame Processor

CFU
Call Forward Universal

CICM
Centrex IP Client Manager

CLAN
Customer Local Area Network

CLASS
Custom Local Area Signaling Service

CLI
Command Line Interface

CLI or CLID
Calling Line Identification

CM
Computing Module

CNF
Station Controlled Conference

COAM
Cabinetized Operations Administration and Maintenance

COI
Community of Interest

CONF
Preset Conference

CORBA
Common Object Request Broker Architecture

CoS
Class of Service

CP
Control Processor

cPCI
compact Peripheral Component Interconnect

CPE
Customer Premises Equipment

CPU
Central Processing Unit

CPU
Call Pickup

CR
Centralized Replicator

CS
Communication Server

CS 2100
Communication Server 2100

CS LAN
Communication Server LAN

C-side
Core-side

CSM
Channel Supervision Message

CSV
Comma-Separated Value

CTI
Computer Telephony Integration

CTM
Conference Trunk Module

CTR
Continuity Tone Detector

CWT
Call Waiting

CXR
Call Transfer

DAT
Digital Audio Tape

DC
direct current

DCC
Digroup Control Card

DCC
Data Control Card

DCE
Distributed Computing Environment

DCM
Digital Carrier Module

DCPK
Directed Call Park

DCPU
Directed Call Pickup

DHCP
Dynamic Host Configuration Protocol

DiffServ
Differentiated Services

DIRP
Device Independent Recording Package

DLC
Data Link Controller

DLC
Digital Loop Carrier

DLM
Digital Line Module

DMS
Digital Multiplex System

DN
Directory Number

DNS
Domain Name System

DPT
Dynamic Packet Trunk

DRAM
Digital Recorded Announcement Machine

DS0
Digital Signal, Level 0

DS1
Digital Signaling Level 1

DS3
Digital Signaling Level 3

DSN
Defence Switched Network

DSP
Digital Signaling Processor

DTC
Digital Trunk Controller

DTC(I)
Digital Trunk Controller-ISDN

DTC7
SS7 Digital Trunk Controller

DTE
Data Terminating Equipment

DTM
Digital Trunk Module

DTMF
Dual-tone Multifrequency

DVD
Digital Video Disk

DWDM
Dense Wave Division Multiplexing

EBAF
Extended Bellcore Automatic Message Accounting Format

EBIP
Electrical Breaker Interface Panel

EBS
Electronic Business Set

ECAN
Echo Cancellation

EDC
Extended Distance Capability

EDRAM
Enhanced Digital Recorded Announcement Machine

EIA
Electronic Industries Association

EIC
Ethernet Interface Card

EIP
Ethernet Interface Paddleboard

EIPE
Enhanced Intelligent Peripheral Equipment

EISP
Enhanced ISDN Signaling Preprocessor

EIU
Ethernet Interface Unit

ELCM
Enhanced Line Concentrating Module

EM
Element Manager

EMC
Electromagnetic Compatibility

EMI
Electromagnetic Interference

EML
Element Management Layer

EMS
Element Management System

EMW
Network Executive Message Waiting

ENET
Enhanced Network

ENUM
E.164 Numbering

ERS
Ethernet Routing Switch

ESA
Emergency Stand Alone

ESD
Electrostatic Discharge

ESF
Extended Super Frame

ESMA
Expanded Subscriber Carrier Module Access

ETS
Electronic Telephone Sets

ETSI
European Telecommunications Standards Institute

FCAPS
Fault, Configuration, Accounting, Performance and Security

FCC
Federal Communications Commission (United States)

FE
far end

FP
Function Processor

FRIU
Frame Relay Interface Unit

FTP
File Transfer Protocol

FX
Foreign Exchange

FXS
Foreign Exchange Service

GbE
Gigabit Ethernet

GBIC
Gigabit Interface Converter

GEM
Gig Ethernet Resource Module

GbE
Gigabit Ethernet

GoS
Grade of Service

GPS
Global Positioning System

GPS
Global Product Support

GTR
Global Tone Receiver

GTT
Global Title Translation

GUI
Graphical User Interface

GWC
Gateway Controller

HDLC
High-Level Data Link Control protocol

HIE
Host Interface Equipment

HIOP
High-capacity Input/Output Processor

HLM
High-Level Management

HSC
Hot Swap Controller

HSDU
High-Speed Data Unit

HSM
Hitless Software Migration

HTTP
Hyper-Text Transfer Protocol

HVAC
Heating, Ventilation and Air Conditioning

IAD
Integrated Access Device

IBIP
Intelligent Bay Interface Panel

ICM
Intelligent Call Management

IE
Information Element

IEEE
Institute of Electrical and Electronic Engineers

IEMS
Integrated Element Management System

IETF
Internet Engineering Task Force

IGW
Integrated Gateway Access (Generation 1 IP-enabled is supported from an LTCI)

IP
Internet Protocol

IPCM
IP Client Manager

IPCM EM
IP Client Manager Element Manager

IPDR
Internet Protocol Detail Recording

IPE
Intelligent Peripheral Equipment

IPEC
Intelligent Peripheral Equipment column

IPF
Integrated Processor FBus card

IPSec
IP Security Protocol

IS
In Service

ISA
Integrated Services Access

ISDN
Integrated Services Digital Network

ISM
Integrated Services Module. A replacement for the Maintenance Trunk Module (MTM).

ISUP
Integrated Services Digital Network User Part

IT
Information Technology

ITP
Internet Telephony Processor

ITU
International Telecommunications Union

ITX
Internet Telephony Extender

IU
Interface Unit

IVR
Interactive Voice Response

IW SPM-IP
Interworking Spectrum Peripheral Module Internet Protocol

JWS
Java Web Start

kbps
Kilobits per second

KEM
Key Expansion Module

LAN
Local Area Network. A network that connects computers to share data storage devices and printers.

LBL
Limited Bandwidth Link

LCAP
Local Craft Access Panel

LCC
Line Class Code

LCD
Liquid Crystal Display

LCM
Line Concentrating Module

LCME
Line Concentrating Module-Enhanced

LDAP
Lightweight Directory Access Protocol

LEA
Law Enforcement Agency

LED
Light Emitting Diode

LEN
Line Equipment Number

LGC
Line Group Controller

LGC(I)
Line Group Controller ISDN

LIU7
SS7 Link Interface Unit (requires 32M processor)

LM
Line Module

LMM
Line Maintenance Manager

LMM
Line Management and Maintenance

LMS
Local Message Switch

LNR
Last Number Redial

LPP
Link Peripheral Processor

LSDU
Low-Speed Data Unit

LSSGR
LATA Switching System Generic Requirement

LTC
Line Trunk Controller

LTC(I)
Line Trunk Controller ISDN

LTI
Line Side T1 IPE Interface

LTM
Line Test Manager

LTP
Line Test Position

M3UA
MTP3 User Adaptation Layer

MADN (MCA)
Multiple Appearance Directory Number (MADN) Multiple Call Arrangement (MCA)

MADN (SCA)
Multiple Appearance Directory Number (MADN) Single Call Arrangement (SCA)

MAN
Metropolitan Area Network

MAP
Maintenance and Administration Position

MAPCI
Maintenance and Administration Position Command Interpreter

MAU
Media Access Unit

Mbps
Megabits per second

MCNI
Meridian Cabinet Network Interface

MCS 5100
Multimedia Communications Server 5100

MDM
MultiService Data Manager

MDP
Management Data Provider

MF
Multi Frequency

MFIO
Multi-Function Input/Output

MG 9000
Media Gateway 9000

MGC
Media Gateway Controller

MGCP
Media Gateway Control Protocol

MGCP+
Enhanced Media Gateway Control Protocol

MIB
Management Information Base

MLT
MultiLink Trunking

MPLS
Multiprotocol Label Switching

ms
micro-second

MS
Message Switch

MS 2010
Media Server 2010

MSB
Make Set Busy

MSR
Message Storage and Retrieval

MSS
Management for Succession Solutions

MTBF
Mean Time Between Failures

MTM
Maintenance Trunk Module

MTM OAU
Maintenance Trunk Module Office Alarm Unit

MTP
Message Transfer Part

MWI
Message Waiting Indication

MWT
Message Waiting

NACD
Network Automatic Call Distribution

NAPT
Network Address and Port Translator

NAT
Network Address Translation

NE
Network Element

NE
near end

NEBS
Network Equipment Building Standard

NEL
Network Element Layer

NEMW
Network Executive Message Waiting

NFS
Network File System

NI-1
National ISDN 1 (also known as NTNA)

NI-2
National ISDN 2

NIC
Network Interface Card

NIU
Network Interface Unit

NM
Network Module

NML
Network Management Layer

NMS
Network Management System

NMWI
Network Message Waiting Indicator

NPM
Network Patch Manager

NRAG
Network Ring Again

NSF
Network Specific Facilities

nsswitch
Name Service Switch

NWM
Network Management

OAMP
Operations, Administration, Maintenance, and Provisioning

OAU
Office Alarm Unit

OC-3
Optical Carrier Level 3: the SONET transmission rate of 155.52 Mbps.

OM
Operational Measurement

OMD
Operational Measurement Delivery

ONP
One Night Process

OOS
Out of Service

OPAC
Outside Plant Access Cabinet

OPM
Outside Plant Module

OSS
Operations Support System. Carrier equivalent of Network Management System.

PAM
Pluggable Authentication Module

P-Bus
Processor Bus

PBX
Private Branch Exchange

PC
Personal Computer

PCI
Peripheral Component Interconnect

PCL
Product Computing-module Load

PCM
Pulse Code Modulation

PDP
Power Distribution Panel

PDS
Persistent Data Storage

PDTC
PCM-30 Digital Trunk Controller

PE
Processor Element

PEEL
Protel Environment Emulation Layer

PIM
Personal Information Manager

PIU
Port Interface Unit

PLC
Packet Loss Concealment

PM
Performance Management

PM
Peripheral Module

PMC
Peripheral Message Controller

POE
Power over Ethernet

POTS
Plain Ordinary Telephone Service

PP
Peripheral Processor

PPVM
Peripheral Processor Virtual Machine

PRI
Primary Rate Interface

PRK
Call Park

PRL
Peripheral/Remote Loader

PRL
Privacy Release

P-side
Peripheral-side

PSTN
Public Switched Telephone Network

PTE2000
Packet Telephony Equipment 2000

PTM
Packaged Trunk Module

PVC
Permanent Virtual Connection

PVG
Packet Voice Gateway

QoS
Quality of Service

RADIUS
Remote Authentication Dial-In User Service

RAG
Ring Again

RAID
Redundant Array of Inexpensive Disks

RCC
Remote Cluster Controller

RCC2
Remote Cluster Controller 2

REX
Periodic Routine Testing

RDT
Remote Digital Terminal

RLCM
Remote Line Concentration Module

RLM
Remote Line Module

RLT
Release Link Trunk

RM
Resource Module

RMM
Remote Maintenance Module

RND
Redirecting Number Delivery

RSC
Remote Switching Center

RSC-S
Remote Switching Center-Second series

RTCP
Real-time Control Protocol

RTOS
Real Time Operating System

RTP
Real-time Transport Protocol

RTU
Right-To-Use

RW
Read/Write

SAM16
Service Application Module 16

SAM21
Service Application Module 21

SAM21 EM
SAM21 Element Manager

SAN
Storage Area Network

SBA
SuperNode Billing Application

SBC
Single Board Computer

SC
Shelf Controller

SCCP
Signaling Connection Control Part

SCOCS
Selective Class of Call Screening

SCP
Service Control Point

SCSI
Small Computer System Interface

SCTP
Stream Control Transmission Protocol

SCU
Speed Calling User

SDM
SuperNode Data Manager

SDN
Synchronous Digital Network

SDP
Session Description Protocol

SERVORD
Service Order

SESM
Succession Element and Subnetwork Manager

SID
Silence ID

SigTran
Signaling Transport

SIM
Serial Interface Module

SIMRING
Simultaneous Ringing

SISG
Secure IP Services Gateway

SLG
SuperNode Data Manager Log Generation

SLM
System Load Module

SM
Shared Memory

SMA2
Subscriber Carrier Module-100 Access, Second Version

SMDR
Station Message Detail Recording

SML
Service Management Layer

SMS-R
Subscriber Carrier Module Remote

SMTP
Simple Mail Transfer Protocol

SNMP
Simple Network Management Protocol

SNPA
Serving Numbering Plan Area

SNSE
SuperNode Size Enhanced

SNTP
Simple Network Time Protocol

SP
Signaling Point

SPCS
Stored Program Control Switch

SPFS
Server Platforms Foundation Software

SPM
Spectrum Peripheral Module

SPVC
Switched Permanent Virtual Connection

SS7
Signaling System #7

SSH
Secure Shell

SSL
Secure Sockets Layer

SSLPP
Single-Shelf Link Peripheral Processor

SSO
Single Sign On

SSP
Service Switching Point

STM
Service Trunk Module

STM-1
Synchronous Transport Mode 1

STORM
Storage Management

STP
Signal Transfer Point

SVC
Secure Voice Zone

SVP
SpectraLink Voice Priority protocol

SWACT
Switch Activity

TAPI
Telephony Application Programming Interface

T-Bus
Transaction Bus

TCP
Transmission Control Protocol

TDM
Time Division Multiplexing

TFTP
Trivial File Transfer Protocol

TM
Transition Module

TM8
Trunk Module, 8-Wire

TMM
Trunk Maintenance Manager

TMM
Trunk Management and Maintenance

TMN
Telecommunications Management Network

TOD
Time of Day

TP
TrunkPack

TSP
TAPI Service Provider

TTP
Trunk Test Position

UA
User Agent

UDP
User Datagram Protocol

UNIStim
Unified Network Stimulus protocol

UPS
Uninterruptible Power Supply

UPSR
Unidirectional Path-Switched Ring

USB
Universal Serial Bus

USP
Universal Signaling Point

UTR
Universal Tone Receiver

V
volt(s)

VCAC
Virtual Call Admission Control

VLAN
Virtual Local Area Network

VMG
Virtual Media Gateway

VoIP
Voice over IP

VoP
Voice over Packet

VPN
Virtual Private Network

VRRP
Virtual Router Redundancy Protocol

VRU
Voice Response Unit

VSP
Voice Service Processor

WAN
Wide Area Network

Wi-Fi
Wireless Fidelity

WLAN
Wireless LAN

XA-Core
Extended Architecture Core

XAI
Extended Architecture Interconnect

XLIU
Enhanced Link Interface Unit

XML
Extensible Markup Language

XPM
Extended Peripheral Module

XTS
Extreme Thin Server

Communication Server 2100

Product Guide

Publication: 555-4001-806
Document status: Standard
Document version: 04.04
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.