555-4001-806

Nortel Communication Server 2100

Product Guide

SE08 Standard 03.06 February 2006

NORTEL

Nortel Communication Server 2100

Product Guide

Publication number: 555-4001-806
Product release: SE08
Document release: Standard 03.06
Date: February 2006

Publication history

February 2006

Version 03.06, SE08, Standard. Document updated to remove references to Global Line 32 card.

September 2005

Version 03.05, SE08, Standard. Document updated to include description of Nortel's Access Care external test system.

May 2005

Version 03.04, SE08, Standard. This is the third standard issue of the document.

September 2004

Version 02.04, SE07, Standard. This is the second standard issue of the document.

March 2004

Version 01.06, SE06, Standard. This is the first standard issue of the document.

Contents

About this document

Purpose and audience

The SE08 software release builds on the Meridian SL-100 migration to packet-based, IP telephony, that began in SE06. This document describes the hardware platform required for the Meridian SL-100 move to IP telephony, which is called the Communication Server 2100.

This guide is a companion to the *Meridian SL-100/Communication Server 2100 Application Planning Guide*, which describes the applications and services that operate on the two hardware platforms. The *Meridian SL-100/Communication Server 2100 Application Planning Guide* also contains packaging and ordering information.

This document's audience is service provisioning, administrative and network management and planning personnel.

How to check the version and issue of this document

The version and issue of the document are indicated by numbers (for example, 01.01). For example, the first release of a document is 01.01. In the next software release cycle, the first release of the same document is 02.01.

The first two digits indicate the version. The version number increases each time the document is updated to support a new software release.The second two digits indicate the issue. The issue number increases each time the document is revised, but re-released in the same software release cycle. For example, the second release of a document in the same software release cycle is 01.02.

FOR MORE INFORMATION

To determine whether you have the latest version of this document, check the release information in the *Meridian SL-100 Master Index of Publications*.

References in this document

This guide provides an overview of the hardware components that make up the Meridian SL-100 and those that make up the Communication Server 2100. The document is designed to act as a road map to help you find the hardware information related to your specific network configuration. As such, at the end of many of the sections in this guide, there are tables that list references to more detailed information about the component described.

Note: Reference documents may contain Nortel product names used in the carrier market.

What's new in SE08

New hardware elements and applications

The following new elements and features being introduced in SE08 to the Communication Server 2100 network are described in this document:

- Nortel Media Gateway 15000 (replaces the 7480 Packet Voice Gateway) – see "Nortel Media Gateway 15000" on page 77
- Nortel Media Gateway 3500 – see "Nortel Media Gateway 3000 Series" on page 84
- IP Client Manager Active Call Failover – see "Active Call Failover" on page 96
- Media Gateway 9000 Enhancements – see "MG 9000 enhancements in SE08" on page 102
- "Call Admission Control" on page 131
- "Access Care" on page 176

The following features being introduced in SE08 to the Communication Server 2100 network are described in other documents:

- Session Initiation Protocol Trunks – see *Communication Server 2100 Session Initiation Protocol Service Implementation Guide*.
- H.323 features – see *Communication Server 2100 H.323 Service Implementation Guide*.
- Geographic Survivability Enhancements – see *Communication Server 2100 Geographic Survivability Planning Guide*.

Note 1: New SE08 applications are described in the SE08 version of the *Meridian SL-100/Communication Server 2100 Application Planning Guide*.

Note 2: New SE08 DSN elements and applications are described in the *Meridian SL-100/Communication Server 2100 DSN General Description*.

Beginning in SE08, the Mediatrix products have moved to the Nortel Select Product Program (SPP). The distributor will be the primary interface to the customer when Mediatrix products are required to be included in a Communication Server 2100 configuration.

Access more information at:
http://www.nortel.com/prd/select/mediatrix.html

New Nortel Branding

Nortel has undergone a major rebranding initiative to make our product names easier for customers to understand. The SE08 version of the *Communication Server 2100 Product Guide* reflects these changes in product names.

Introduction

Meridian SL-100 evolution

The Meridian SL-100 is tailored for the large enterprise network of 4,000 plus lines and has been for over two decades. Advances in Internet telephony technology are changing the way in which Private Branch Exchanges (PBXs) provide communication services to enterprises around the world. SE08 uses this growing technology to offer businesses unprecedented choices in 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 delivers the same rich features of today's Meridian SL-100, while also paving the way for a new suite of services that result from the converging of telephony and data networks.

Software release SE08 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 Nortel's IP product portfolio. Previous Meridian SL-100 software releases have now been migrated to the SE software stream.

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

The Communication Server 2100 solution is based on the use of a single packet backbone network. This use of 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
- by allowing bandwidth to be used with maximum efficiency, because there is no longer any need for circuit-switched connections

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

The Communication Server 2100 enables the transition from a Time Division Multiplexing (TDM) to packet architecture to be seamless, with existing services remaining fully operational throughout the upgrade process. It is even possible for traditional circuit-switched TDM and packet capabilities to be supported in parallel by the same software load, with the Interworking Spectrum Peripheral Module IP (IW SPM-IP) being used to provide connections between the TDM and packet environments. This offers medium to large enterprise customers a second layer of flexibility when deciding what is the best way, and the best time, to reap the benefits of IP switching. The Communication Server 2100 uses the term "hybrid" to describe that this Communication Server can deliver both IP and traditional TDM telephony services.

Available configurations

To provide Meridian SL-100 customers maximum flexible in any upgrade to IP telephony, Nortel is introducing the following two base platforms, both of which deliver carrier-grade reliability:

- **Communication Server 2100 XA-Core (CS 2100 XA-Core)** – provides packet switching by leveraging current investment through the use of the Nortel's 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" on page 71.

  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" on page 61.

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

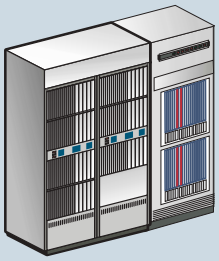
Both configurations support the same range of call processing agents, protocols and telephony features. The main differences between them are that the Communication Server 2100 Compact uses a different processor complex, has a significantly smaller system footprint and delivers reduced call processing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

The Communication Server 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 there are differences between the standard and compact configurations in terms of hardware components used to implement certain functions. See "Communication Server 2100 hardware" on page 29 for further information.

Figure 1 on page 18 summarizes the basic differences in hardware components between the two systems.

Figure 1
Summary of processing differences between the two configurations

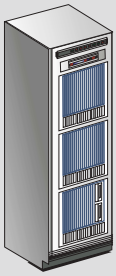
Communication Server 2100 (XA-Core)



XA-Core – Extended Architecture Core. Multi-processor Core (n + 1 sparing is used to support load sharing). Can be housed in SuperNode cabinet along with MS, or in SNSE cabinet along with MS, ENET and LPP shelf.

MS – Message Switch. System bus for proprietary intra-switch messaging. MS also provides Time Of Day (TOD) clock for XA-Core and clock synchronization of legacy Meridian SL-100 peripherals in a hybrid configuration.

Communication Server 2100 (Compact)



Call Agent – Dual-processor Motorola Core. Housed in SAM21 card cage along with Gateway Controllers (GWCs). No links with MS in non-hybrid configuration.

STORM – Storage Manager provides mass storage for the Call Agent card. STORM SAM-XTS uses dual twin-unit rackmount servers installed below the Breaker Interface Panel (BIP) in the Call Control Frame (CCF) for communicating with the Call Agent through the Ethernet Routing Switch 8600s.

G100466

Features and services

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

FOR MORE INFORMATION

This document focuses on the base platform of the Communication Server 2100. See the *SE08 Meridian SL-100/Communication Server 2100 Application Planning Guide* for a comprehensive description of features and services that the Communication Server 2100 supports.

Capacity

In Table 1 all figures quoted are general, and are subject to variation depending on the network call model and capacity requirements. Network-specific estimates should be determined in consultation with Nortel Sales Engineering.

Table 1
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 165,000 clients (not including trunks) • Maximum 56,000 simultaneous calls	• Maximum 1.3 million Busy Hour Call Attempts (BHCAs) • Maximum of 60,000 clients (not including trunks) • Maximum 32,000 simultaneous calls
Trunks and/or endpoints	Overall maximum of 165,000 trunk and/or endpoints. Within this, the limits that apply to different endpoint types are • 48,000 Primary Rate Interface (PRI/H.323) trunks • 130,000 analog subscriber lines	

Network topology

This chapter contains the following sections:

IP network architecture

The network architecture for the Communication Server 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 functionality 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 providing any required format conversion while maintaining content integrity).
- **Signaling gateway** – provides an interface for signaling connections. It terminates legacy network signaling on one side and packet network signaling on the other, and supports all necessary interpretation and conversion between the two.

These are logical functions, not node types. A given node can provide media gateway functionality, signaling gateway functionality, or both. Similarly, gateway functionality can be provided by a combination of nodes, rather than a single node. For more information about the supported gateways, see “Gateways” on page 75.

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).

The control and coordination of packet network gateways to support applications such as IP telephony is the responsibility of a Media Gateway Controller (MGC). As with gateways, a Media Gateway Controller is a logical function, not a node type. Media Gateway Controller functionality can be provided by a combination of nodes, rather than a single node. It is also possible for a given node to provide server functionality, as well as Media Gateway Controller functionality.

Communication Server 2100 implementation of IP architecture

In terms of IP network architecture, the Communication Server 2100 is a Communication Server providing call processing capabilities. It also provides Media Gateway Controller functionality. Together with various types of gateway and server, it supports IP telephony. Specifically, Communication Server 2100 capabilities include the following:

- **Basic connectivity and Network Element control**
  - — Control over the media gateways that provide the bearer connection interface between the packet network environment and other TDM or access networks. In SE08, the Communication Server 2100 provides the following three types of access using gateways:
    - – Access to/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 supporting capabilities such as announcements and conferencing over the packet network.
  - — Originations and terminations for inter-Communication Server signaling across the packet network to/from other Communication Server 2100s and 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.

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

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

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

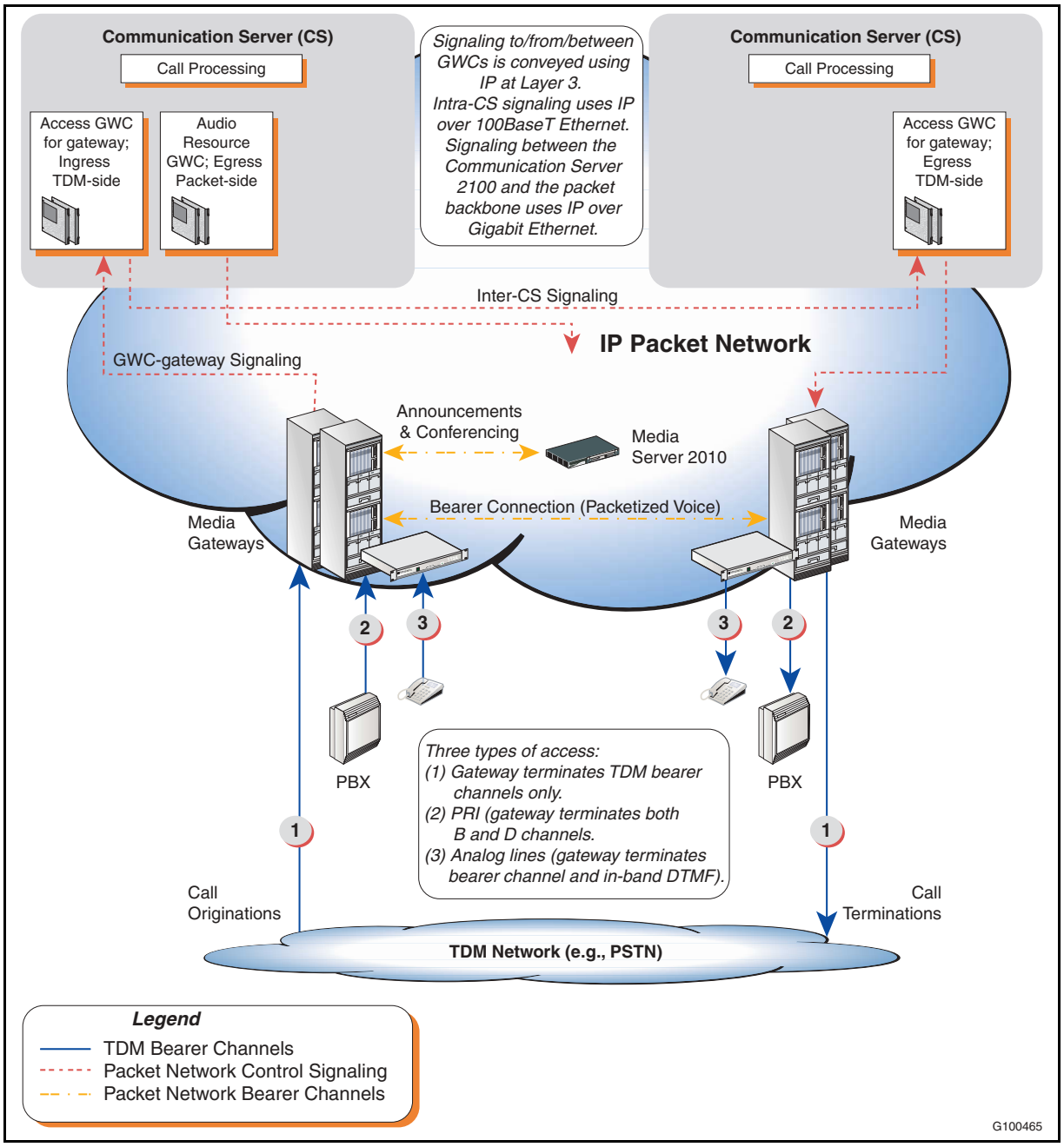
- To support communication between peer Communication Servers for the handling of networked calls. This is accomplished through inter-Communication Server signaling, also based on packet network protocols.

In the Communication Server 2100 architecture, you configure Gateway Controllers as Communication Server 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 has been developed for different types of communication involving Gateway Controllers.

Figure 2 shows a functional overview of the Communication Server 2100 network architecture for IP telephony. It focuses on the roles of the different Gateway Controller types. For simplicity, Operations, Administration, Maintenance and Provisioning (OAM&P) components are not shown (these are described in "OAM&P for Communication Server 2100 networks" on page 151).

Figure 2
Communication Server network architecture for IP telephony



Communication Server 2100 support for network architecture

Hardware support

Components

Communication Server functionality is allocated to the Communication Server 2100 as follows:

- Call processing is supported by the Communication Server 2100 processor complex (Core).
- Different types of Gateway Controller functionality 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. Similarly, an access Gateway Controller can control either trunk gateways or line gateways, but not both.
  - Audio Gateway Controller for the Media Server 2010 which supports announcements and conferencing.

Gateways

SE08 supports the use of the following gateway types:

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

Software support

Because the Communication Server 2100 is a distributed system, it is necessary to consider the support for protocols that are internal to the network, as well as the PSTN interfaces it supports externally. The SE08 software delivers protocol stacks which support three types of IP signaling that are 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 that allows 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.

SE08 software load

SE08 is the third Communication Server 2100 release for the Meridian SL-100. The SE08 software load provides all of the required software functionality for packet-based signaling. In addition, SE08 can be installed on legacy Meridian SL-100 hardware platforms in which case it is referred to as SE08 (TDM). You can install the SE08 software load in a hybrid configuration that comprises circuit-switched and packet-switched capabilities simultaneously.

The backbone packet network

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

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

When this document refers to an IP backbone packet network, it denotes the bearer network, not the control network. The control network uses IP at Layer 3.

Note: SE08 does not support Asynchronous Transport Mode (ATM) as the backbone network.

Communication Server 2100 hardware

Overview

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

The Communication Server 2100 is based on a distributed modular architecture that provides inherent scalability, allowing the capacity of each Communication Server 2100 to 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, ensuring that optimum use is made of Core capacity.

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

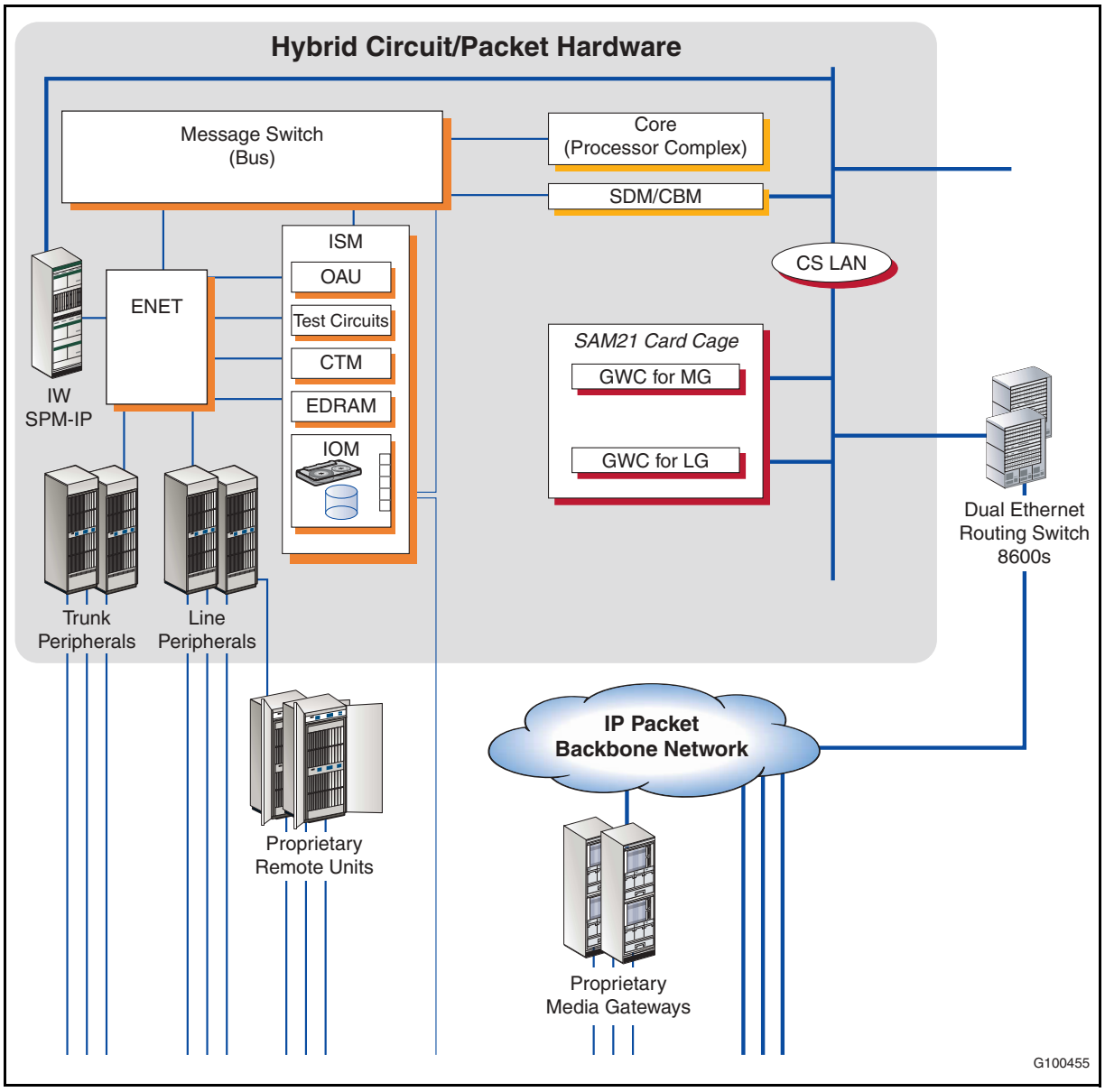
To meet the divergent needs of large enterprise customers, SE08 supports the following two hardware configurations:

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

A Communication Server 2100 Communication Server is a distributed system comprising a number of different functional elements. Figure 3 on page 30 provides a high-level logical view of the interaction between the main functional elements, which are common to both types of configurations. Some functions are, however, provided by different hardware components in XA-Core and Compact configurations.

Figure 3 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 Communication Server 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 be able to survive the failure of one of its constituent hardware units.

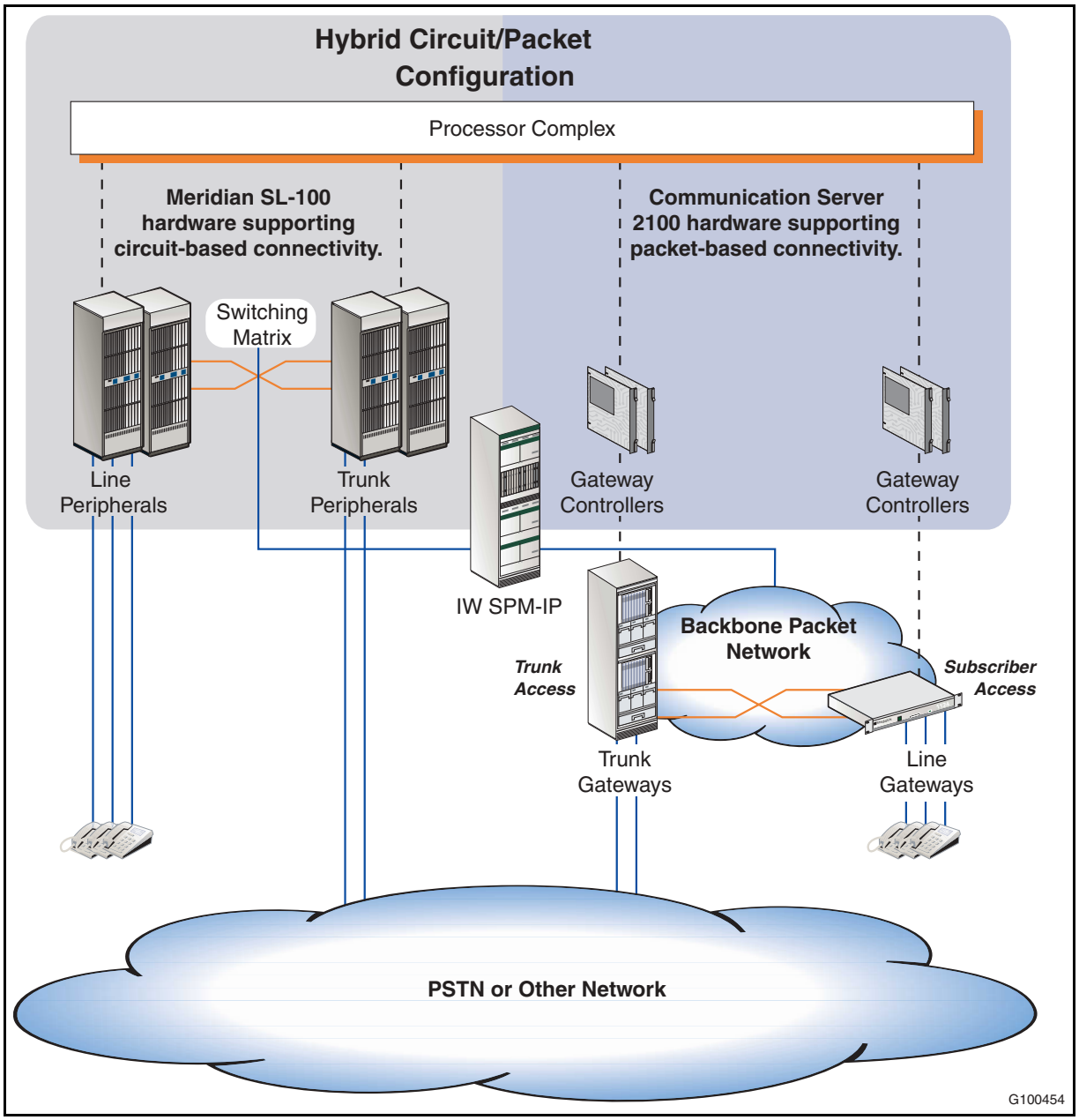
Figure 3
Functional overview of the Communication Server 2100 hardware and CS LAN



Hybrid support

Figure 4 breaks out Figure 3 on page 30 to provide a simplified functional view of the different roles the Communication Server 2100 and legacy Meridian SL-100 switches. The figure shows how these units can be combined in a hybrid configuration to support both circuit-switched and packet-switched capabilities.

Figure 4
Functional view of hybrid circuit/packet configuration



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

Chapter format

This chapter focuses on describing the internal hardware components of the Communication Server 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)**
- **Internal communication (Communication Server LAN and Message Switch)**
- **Gateway Controllers**
- **Interworking Spectrum Peripheral Module IP**

OAM&P platforms are described in a separate chapter (see “OAM&P for Communication Server 2100 networks” on page 151). In addition, to clearly distinguish between the two types of Communication Server 2100 hardware configurations, this chapter includes the following sections:

- **Communication Server 2100 Compact**
- **Communication Server 2100 XA-Core**

Processor complex (Core)

The processor complex, or Core, is the central computing engine of a Communication Server 2100. This 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, it is the centrally-located Product Computing-module Load that supports call processing agents for telephony interfaces, translations and routing, and service logic for the delivery of 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 type of configuration, the Communication Server 2100 supports two different Cores as follows:

- The Extended Architecture Core (XA-Core), as described in "XA-Core" below, provides processing power for Communication Server 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)" on page 38, provides processing power for Communication Server 2100 Compact configurations.

XA-Core

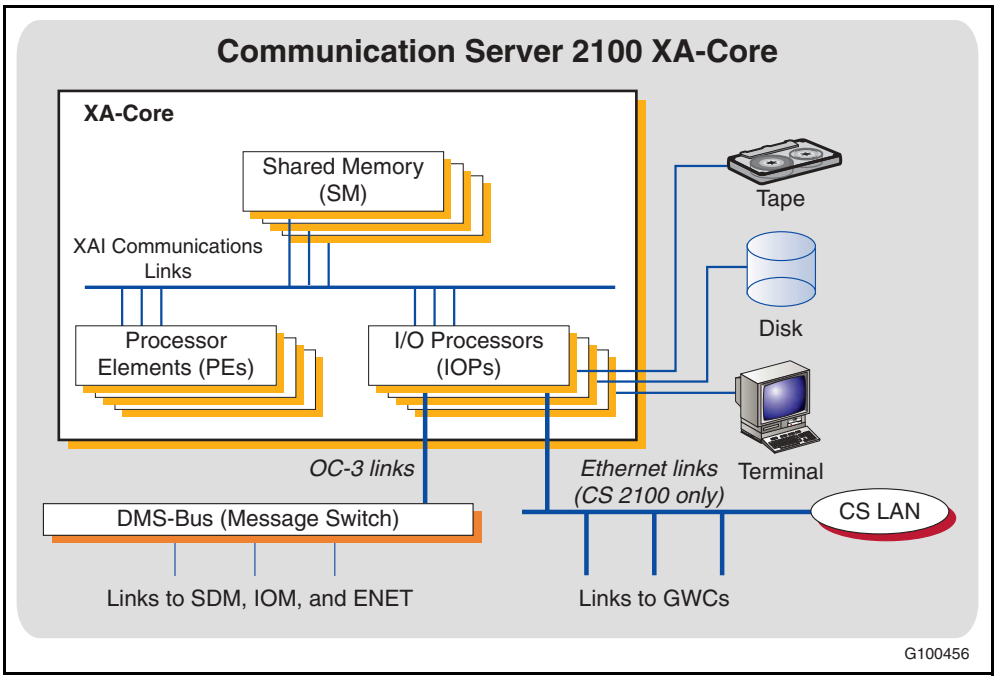
The XA-Core is the call processing platform for the Communication Server 2100 XA-Core. The XA-Core provides an OC-3c network connection provisioned for two Permanent Virtual Connections between each trunk gateway for signaling data and a 10BaseT interface to the CS LAN for OAM&P data. The XA-Core connects 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 running off 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:

- 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). Figure 5 illustrates XA-Core architecture at the logical level.

Figure 5
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 these circuit cards. A SuperNode C42 cabinet houses the XA-Core shelf.

The XA-Core shelf can be packaged in a cabinet along with the Message Switch and Enhanced Network (ENET) in separate cabinets. Alternatively, the XA-Core can be packaged 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 Mbytes 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, thus theoretically leaving one spare). This gives the system the ability to handle a full workload, even in the event of a Processor Element failure.

Shared memory

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

Mated pairs of 32-Mybte memory blocks located 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 a given 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 Communication Server 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 of 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 8600s through 100BaseT full duplex links. During normal operation, both HIOPs are active and operate in load-balancing mode.
- An interface to the Communication Server 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 Gybtes.
- Tape storage (DAT) with capacity of 1.3, 2 or 4 Gybtes.

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. These processes include 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, 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.

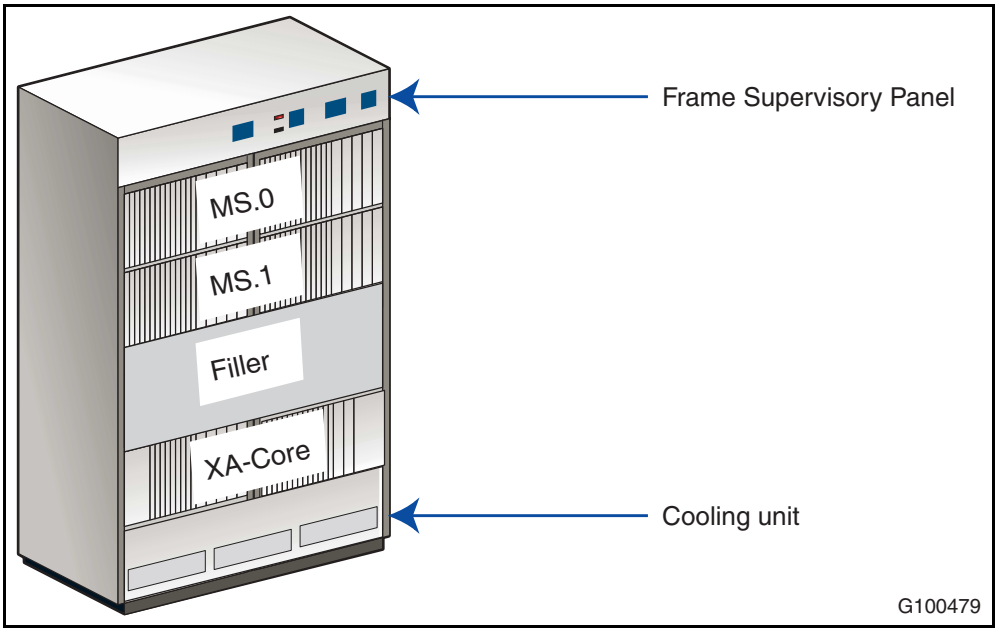
Together these circuit cards form a high-performance, multiprocessing compute engine that is completely scalable in terms of processing, memory and I/O capability. Adjusting system capacity, or adding another interface, is as simple as plugging in a new card.

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.

Figure 6 on page 37 shows the cabinet configuration when the XA-Core and Message Switch shelves are in the same cabinet.

Figure 6
XA-Core frame layout



For additional information about XA-Core-based systems, see “Communication Server 2100 XA-Core” on page 71.

References

Table 2 shows where you can find more detailed information about the hardware components used with the Communication Server 2100 XA-Core.

Table 2
Documentation references (Sheet 1 of 2)

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

Table 2
Documentation references (Sheet 2 of 2)

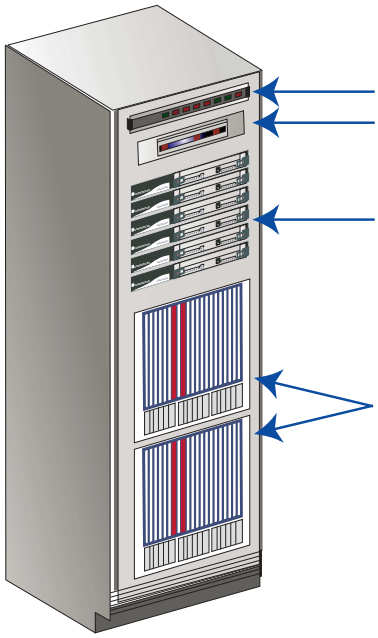
Document title	Document Number
XA-Core	
Communication Server 2000 Basics ***Note:*** Due to the commonality between the two systems, these documents also apply to the CS 2100.	NN10286-111
Communication Server 2000 Fault Management	NN10083-911
Communication Server 2000 Configuration Management *IAW & IAC Configuration Management*	NN10193-511 NN10188-511
Globalized Solution-Level Accounting	NN10400-800
Communication Server 2000 Performance Management	NN10149-711
Communication Server 2000 Administration and Security	NN10171-611
Upgrading the Communication Server 2000 *IP Solutions Upgrades*	NN10061-461 NN10444-450

Processor complex for Communication Server 2100 Compact (Call Agent)

The processor complex for the Communication Server 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 cards, also known as blades. The Call Agent supports call processing and service logic by means of the SE08 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 (24” x 84” x 24”) walled frame with a door. Figure 7 on page 39 illustrates the Call Control Frame and its contents.

Figure 7
Communication Server 2100 Compact Call Control Frame



Power distribution shelf, including Astec Electrical Breaker Interface Panel (EBIP).

Persistent Data Storage shelf housing a pair of SAM-XTS servers with integrated Storage Manager (STORM) using Persistent Data Storage (PDS).

Media Server 2010 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. This area can also be used for the Session Server - Trunk which is a 2U box.

Two SAM21 Call Agent shelves, each housing:
- Call Agent card processor
- Message Switch interface card terminating OC-3 interface with DMS-Bus
- One pair of Shelf Controller cards (in slots 7 and 9)

The remaining slots in each shelf house pairs of Gateway Controller (GWC) cards for controlling media gateways in hybrid configurations that support packet-based, as well as circuit-based capabilities.

Legend

Fiber channel interfaces are used for connections between the Call Agent processor cards on the two Call Agent shelves. Each STORM unit has two 100 MBit Ethernet interfaces that are bound in software into a redundant, single interface. The Ethernet links connect to a router switch on the CS LAN.

G100457

Frame layout

The Communication Server 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 Communication Server 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. RAID-1 allows one of the two drives to fail without loss of data.

In addition to the Call Control Frame, a Communication Server 2100 Compact cabinet lineup includes a cabinet housing a CBM that resides in the COAM, the CS 2000 Manager and a PTE2000 frame housing OAM&P servers for Gateway Controllers and other Communication Server 2100 Compact components (see “Communication Server 2100 Compact” on page 61 for more information).

Shelf layout

Each Communication Server 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/fan modules

Call Agent card

The Call Agent card is easy to insert, remove and replace at the card level. This improves availability and simplifies such things as maintenance and sparing. The shelf supports the hot swapping of cards.

The Call Agent card increases the density of processing within a given space. The Motorola MCPN765 Call Agent card consists of the following:

- 500 MHz PowerPC 7410 processor
- 1.5 Gig ECC RAM
- 2MB L2 cache
- 16MB on-board flash memory
- on-board debug monitor with diagnostics
- dual Ethernet transceiver, 10/100 Mbps
- 32KB NVRAM and time-of-day clock
- four asynchronous serial ports
- four 32-bit timers, one watchdog timer

Nortel designed the Call Agent card with survivability in mind. The two Call Agent units can be distributed on separate shelves. In this situation, they are interconnected through IP for messaging, Fiber Channel for sparing, with a backup serial link, eliminating the need for the two shelves to be collocated.

References

Table 3 shows where you can find more detailed information about the Call Agent.

Table 3
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 Management	NN10110-511
STORM Performance Management	NN10054-711
STORM Administration and Security	NN10176-611
Upgrading the STORM	NN10066-461

Internal communication (Communication Server LAN and Message Switch)

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

- The Communication Server Local Area Network (CS LAN)

  Used primarily to support 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)

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

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

Communication Server Local Area Network

Figure 3 on page 30 depicts how the CS LAN supports communication between Communication Server 2100 components.

Communication Server 2100 components linked by the CS LAN

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

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

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

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

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

    For more detailed information about the Media Server 2010, see “Nortel Media Server 2010” on page 112.
- Sun Netra 240 servers housed in a dedicated PTE2000 OAM&P frame, supporting Device Managers and management applications for Gateway Controllers and non-Communication Server 2100 units such as media gateways.
- Dynamic Host Configuration Protocol (DHCP) server.
- 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 8600. Physically, the CS LAN consists of direct Ethernet cable connections between ports on the Ethernet Routing Switch 8600 and ports on the Communication Server 2100 hardware components.

See “Ethernet Routing Switch 8600” on page 141 for more detailed information about the Ethernet Routing Switch 8600.

To provide redundancy, each CS LAN uses two Ethernet Routing Switch 8600s. A given Communication Server 2100 component, such as a Gateway Controller, connects to both Ethernet Routing Switch 8600s, using one as its 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 Ethernet Routing Switch 8600s serve as a hub for the CS LAN subnetwork providing all the necessary routing functionality for communication across the LAN.

FOR MORE INFORMATION

See the *Packet Trunk-IP Engineering Rules System Engineering Bulletin*, SEB-02-10-001, for comprehensive recommendations for configuring the CS LAN.

The CS LAN not only supports intra-Communication Server 2100 communication, but also provides the interface between the CS LAN and the external managed IP network.

Message Switch (Communication Server 2100 XA-Core bus)

Figure 4 on page 31 depicts how the Message Switch supports communication between Communication Server 2100 components using an OC-3 link (the Message Switch is not used in Communication Server 2100 Compact configurations).

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

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

- 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 Communication Server 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 alarms.

Integrated Services Module

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

In the Communication Server 2100 XA-Core configuration, the Integrated Services Module houses Input/Output Modules. These provide ports for serial input/output, enabling local and remote devices to communicate with the rest of the Communication Server 2100 XA-Core through the Message Switch. Communication Server 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 RS232 links

The system supports X.25 data communications over either V.35 or RS232.

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 Communication Server 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 address (port numbers within the Message Switch) to/from the logical addresses of switch components.
- A port interface subsystem consisting of a a number of Port Interface Units (PIUs), each of which includes the following:
  - An interface card that logically faces towards the Message Switch Transaction Bus and provides Message Switch addressable ports.
  - A paddleboard supporting one or more links to the following other 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. They receive instructions from the XA-Core, or Call Agent, to perform such operations as the following:

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

The software that the Gateway Controllers use 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 Communication Server 2100 to access the packet backbone network. They perform lower-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 Communication Server 2100 softswitches across the packet network.

In SE08, the Communication Server 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” on page 77) or the Nortel Media Gateway 3000 Series (see “Nortel Media Gateway 3000 Series” on page 84). 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
- Gateway Controller for the Media Server 2010.

Note: In terms of the Communication Server 2100 network architecture, the Media Server 2010 subtends the SAM21 and is therefore categorized as a media server, not as a Communication Server 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 co-ordination 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. 16 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).

There are two 10/100 BaseT Ethernet links running 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.

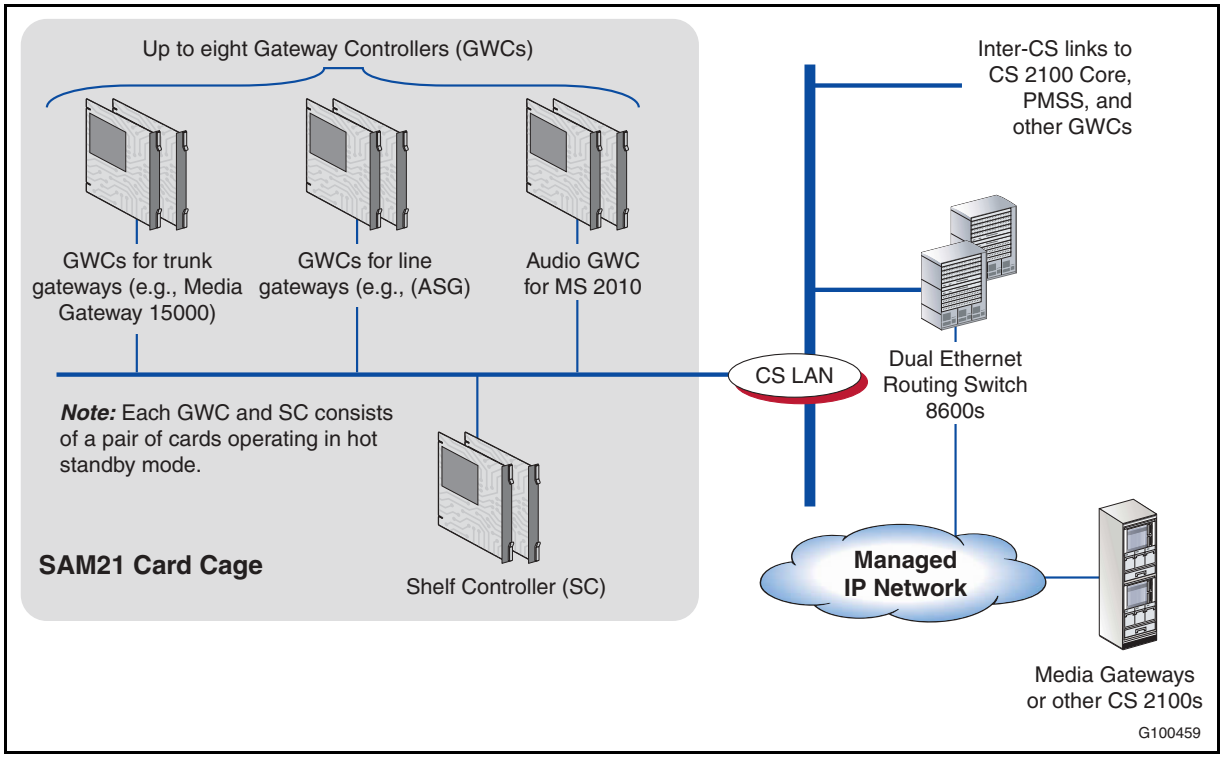
The backplane of the SAM21 card cage provides a compact Peripheral Component Interconnect (cPCI) bus for communication between circuit cards housed in the card cage. Ethernet 10/100BaseT ports on the cards themselves provide access to the Ethernet Routing Switch 8600-based CS LAN. Gateway Controllers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

Figure 8 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 Communication Server 2100 softswitches and packet network components. Communication between the Shelf Controllers and Gateway Controllers through the cPCI bus is not shown.

Figure 8
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 an OC-3c interface for connection to the packet network.

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

In a Communication Server 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 Communication Server 2100 Compact configuration. These shelves not only house Gateway Controllers, but also house the Call Agent processor cards. To increase capacity, a Communication Server 2100 Compact lineup can include a PTE2000 Extension Frame, as well as the Call Control Frame, housing up to three SAM21 shelves with additional Gateway Controllers.

For further information, see Figure 7 on page 39 which depicts the Communication Server 2100 Compact Call Control Frame.

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

- 17 I/O slots and four system slots per chassis
- redundant -48V d.c. 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 to be 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, Media Server 2010) and the call processing and service logic functionality provided by the Core. The Gateway Controller does this by relaying requests and information from the packet network components to the Core and relaying instructions and information from the Core. Gateway Controllers terminate packet network signaling and map this onto proprietary intra-Communication Server 2100 signaling to/from the Core. Gateway Controllers must also provide protocol support for OAM&P access from Device Managers and management applications.

The Communication Server 2100 also supports the Simple Network Management Protocol (SNMP) between Gateway Controllers and the Gateway Controller Manager running on a Sun Netra OAM&P server.

Gateway Controller provisioning and capabilities

Table 4 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.

Table 4
Gateway Controller engineering guidelines (Sheet 1 of 3)

Component	Description
SAM21s/ 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 Communication Server 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 Communication Server 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 given Gateway Controller can support trunk access or line access, but not both.

Table 4
Gateway Controller engineering guidelines (Sheet 2 of 3)

Component	Description
Trunks/ lines/ endpoints	• A Communication Server 2100 can support an overall 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 — 1,225 H.323 endpoints — 130,000 lines • The allocation of the total number of supported trunks between access Gateway Controllers depends on the call model to be supported by the Communication Server 2100.
Trunk access Gateway Controllers	• A trunk access Gateway Controller can support up to 30 media gateways. • A trunk access Gateway Controller can support up to 4,096 TDM-side trunk endpoints terminated on media gateways (up to 2,048 on a given 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.
Line access Gateway Controllers and gateways	• The maximum number of line endpoints that can be supported by a line access Gateway Controller is 6,400. • The maximum BHCA that can be supported by a line access Gateway Controller is 38,000. • CPE LAN line gateway guidelines are as follows: — Lines are assigned to line groups, each consisting of a maximum of 1,024 lines (actually 1,023, as one is reserved for maintenance). All of the lines belonging in a given line group (that is, all the gateways serving those lines) must be supported by one Gateway Controller. — There is a maximum of 2,000 simultaneous calls per line Gateway Controller.
Audio Controller Gateway Controller for Media Server 2010	• A maximum of 720 ports 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. • Provides a maximum of 468 simultaneous announcements for IP. • The maximum BHCA is 40,000 or 60,000 depending on the CPU, with a maximum of 20,000 on one interface card.

Table 4
Gateway Controller engineering guidelines (Sheet 3 of 3)

Component	Description
Audio Controller Gateway Controller for Media Server 2010	• A maximum BHCA of 80,000. • 120 or 240 ports for conferencing and/or monitoring. • 240 ports for announcements.

Supported protocols

Table 5 describes the protocols that Gateway Controllers support.

Table 5
Protocol summary (Sheet 1 of 2)

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.
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)	Is an IETF standard (RFC 1889) for streaming real-time multimedia over IP in packets. It is designed to carry 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 is designed to monitor the Quality of Service (QoS) and to convey information about the participants in an on-going RTP session. The system sends feedback information 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 need to 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 performs the conversion of media signals between circuits and packets, and at least one “signalling gateway”.

Table 5
Protocol summary (Sheet 2 of 2)

Protocol	Description
Session Initiation Protocol (SIP)	Beginning in SE08, 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 is terminated on the Session Server, which extracts the CCS7 signaling and passes it on to the Dynamic Packet Trunk (DPT) Gateway Controller.

References

Table 6 shows where you can find more detailed information about Gateway Controllers and Shelf Controllers.

Table 6
Documentation references

Document title	Document Number
Gateway Controllers (GWCs) (provide the equivalent of XPMs)	
GWC Basics	NN10189-111
GWC Fault Management	NN10202-911
GWC Configuration Management	NN10205-511
GWC Performance Management	NN10208-711
GWC Security and Administration	NN10213-611
Upgrading the GWC	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 Interworking Spectrum Peripheral Module Internet Protocol is a legacy-based, fault-tolerant peripheral with the following network connections:

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

The Interworking Spectrum Peripheral Module Internet Protocol supports the following:

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

Supported call types

The Interworking Spectrum Peripheral Module Internet Protocol 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 Interworking Spectrum Peripheral Module Internet Protocol bridges calls between Nortel's existing 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 1: Non-hybrid configurations do not require an Interworking Spectrum Peripheral Module Internet Protocol.

Note 2: The Interworking Spectrum Peripheral Module Internet Protocol does not support calls to IP Client Manager 6.1 or 6.2.

The Interworking Spectrum Peripheral Module Internet Protocol connects to an ENET over C-side DS-512 fiber links and to the IP network over Gigabit Ethernet on the P-side. In between these two connections are the following:

- 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 Gigabit Ethernet.

The Interworking Spectrum Peripheral Module Internet Protocol provides interworking capability to legacy Meridian SL-100 TDM peripherals. It enables the legacy TDM equipment to access Dynamic Packet Trunks (DPTs) and make connections to far-end nodes. The Interworking Spectrum Peripheral Module Internet Protocol also provides interworking to test trunk services for media gateways.

The Interworking Spectrum Peripheral Module Internet Protocol is required for both the Communication Server 2100 XA-Core and the Communication Server 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, called the Gig Ethernet Resource Module, is easily added to an existing Spectrum Peripheral Module in order to support a Gig interface to the network.

Technicians perform Interworking Spectrum Peripheral Module Internet Protocol maintenance functions, such as 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.

Figure 9 on page 57 shows an example of how the Interworking Spectrum Peripheral Module Internet Protocol is configured in an enterprise network.

Figure 9
IW SPM-IP enterprise network configuration example

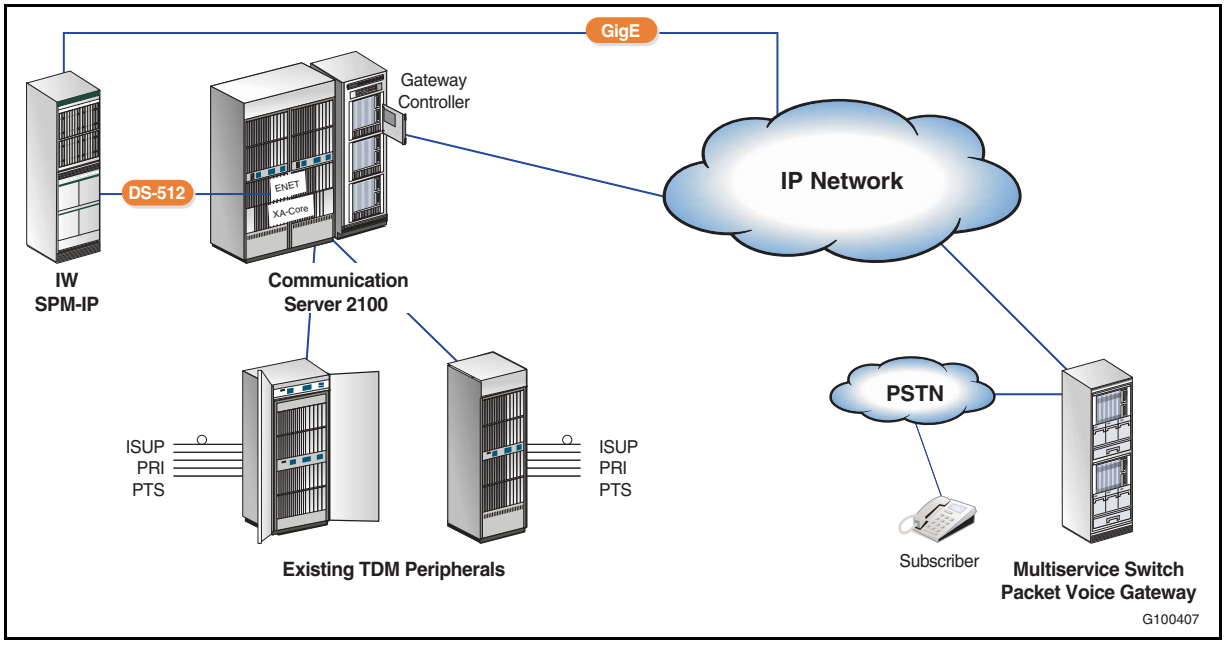
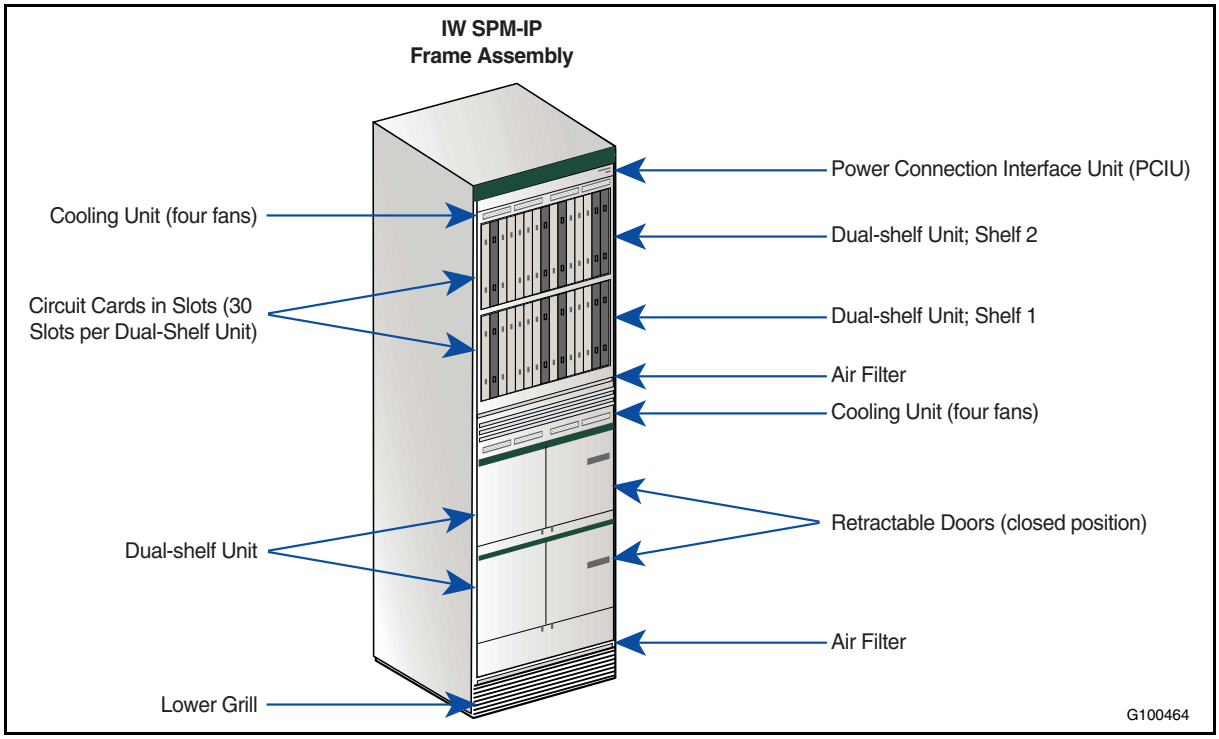


Figure 10 illustrates the layout of an IW SPM-IP cabinet.

Figure 10
Interworking Spectrum Peripheral Module Internet Protocol frame assembly



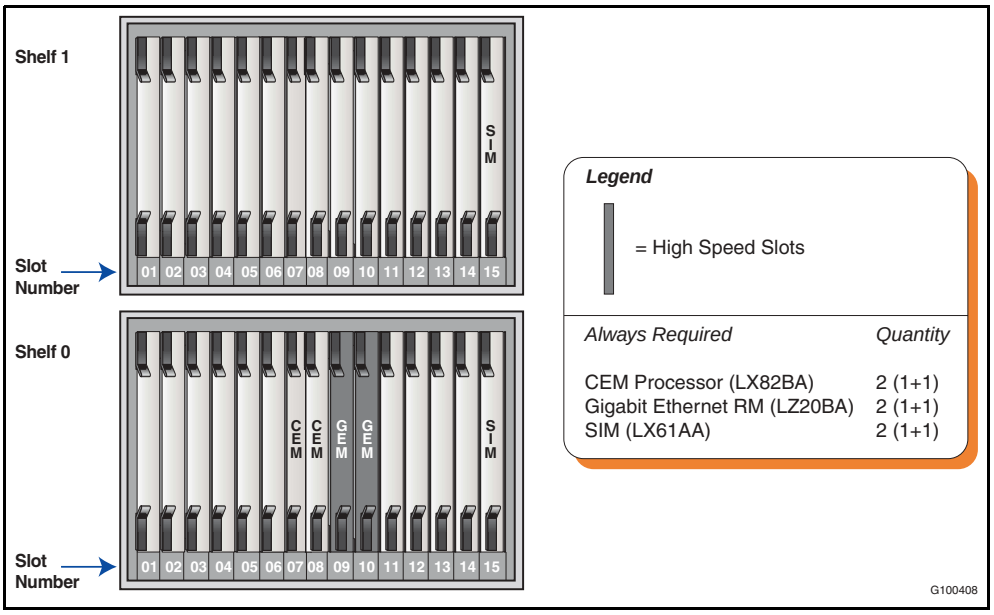
The Interworking Spectrum Peripheral Module Internet Protocol is an ENET-hosted Spectrum Peripheral Module that has four C-side DS-512 links connecting the Common Equipment Module of the Interworking Spectrum Peripheral Module Internet Protocol to the ENET. On the P-side (facing the packet network) the Interworking Spectrum Peripheral Module Internet Protocol has two Gigabit Ethernet links to the Ethernet Routing Switch 8600s in the CS LAN.

The Interworking Spectrum Peripheral Module Internet Protocol uses Peripheral Processor Virtual Machine (PPVM, an internal Communication Server 2100 protocol) for communication with the XA-Core. The Interworking Spectrum Peripheral Module Internet Protocol uses Real Time Protocol (RTP), or Real Time Control Protocol (RTCP) which compliments RTP by monitoring data delivery, for bearer connections to the Media Gateway 15000.

Shelf layout and physical interfaces

Figure 11 shows the recommended card configuration for the Interworking Spectrum Peripheral Module Internet Protocol.

Figure 11
IW SPM-IP shelf layout



The Interworking Spectrum Peripheral Module Internet Protocol 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 Interworking Spectrum Peripheral Module Internet Protocol
    - control of signal processing
    - system clock
    - physical connection to ENET
  - The Gigabit Ethernet Module (GEM) provides the physical connection to the packet network. The Gigabit Ethernet Module transcodes voice signals. Each shelf assembly contains two Gigabit Ethernet Modules.

Operating parameters

The following operating parameters apply to the Interworking Spectrum Peripheral Module Internet Protocol:

- 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
- Fax and modem support using G.723 and G.729

References

Table 7 shows where you can find more detailed information about the Interworking Spectrum Peripheral Module Internet Protocol.

Table 7
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 Monitoring	NN10144-711
IW SPM-IP Administration and Security	NN10166-611
Upgrading the IW SPM-IP	NN10056-461

Communication Server 2100 Compact

Description

The Communication Server 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 Communication Server 2100 Compact call processing.

Enterprise customers have a second core processor option, the Communication Server 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 this flexibility in a standards-based manner.

The off-the-shelf software is the most open software available today, Linux©. But this Linux is not your 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 Communication Server 2100 Compact provides flexible, distributed call and service control across a packet network over an IP backbone. The Communication Server 2100 Compact performs all call control processing functions for your network including translations, routing and centralized service delivery. You can deploy next generation services on a single Communication Server 2100 Compact and make them available to multiple customer groups.

FOR MORE INFORMATION

For more information about the SE08 IP telephony solution, see the *SE08 Meridian SL-100 Application Planning Guide*.

There are two 10/100 BaseT Ethernet interfaces running from the Call Agent on the Communication Server 2100 Compact to the CS LAN. Each Ethernet link connects to a different Ethernet Routing Switch 8600.

Communication Server 2100 Compact hardware

The Communication Server 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 Communication Server 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:

- provides call processing services on line and trunk endpoints
- supports translation and routing for all endpoints served by the Communication Server 2100 Compact
- provides a provisioned view of profiles of
  - subscriber services
  - trunk group services
- collects and formats billing data, before sending the data to the Element Management System (EMS)
- collects log, alarm and Operational Measurement (OM) information for use in downstream network management systems

The Call Agent resides on the Call Agent card in the Communication Server 2100 Compact.

Storage Management (STORM)

Storage Management provides Network File System (NFS) services to applications running on the Communication Server 2100 Compact. A Network File System is a distributed file system that allows applications to access files and directories on remote computers. Storage Management acts as a Network File System 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 do not provide any 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.

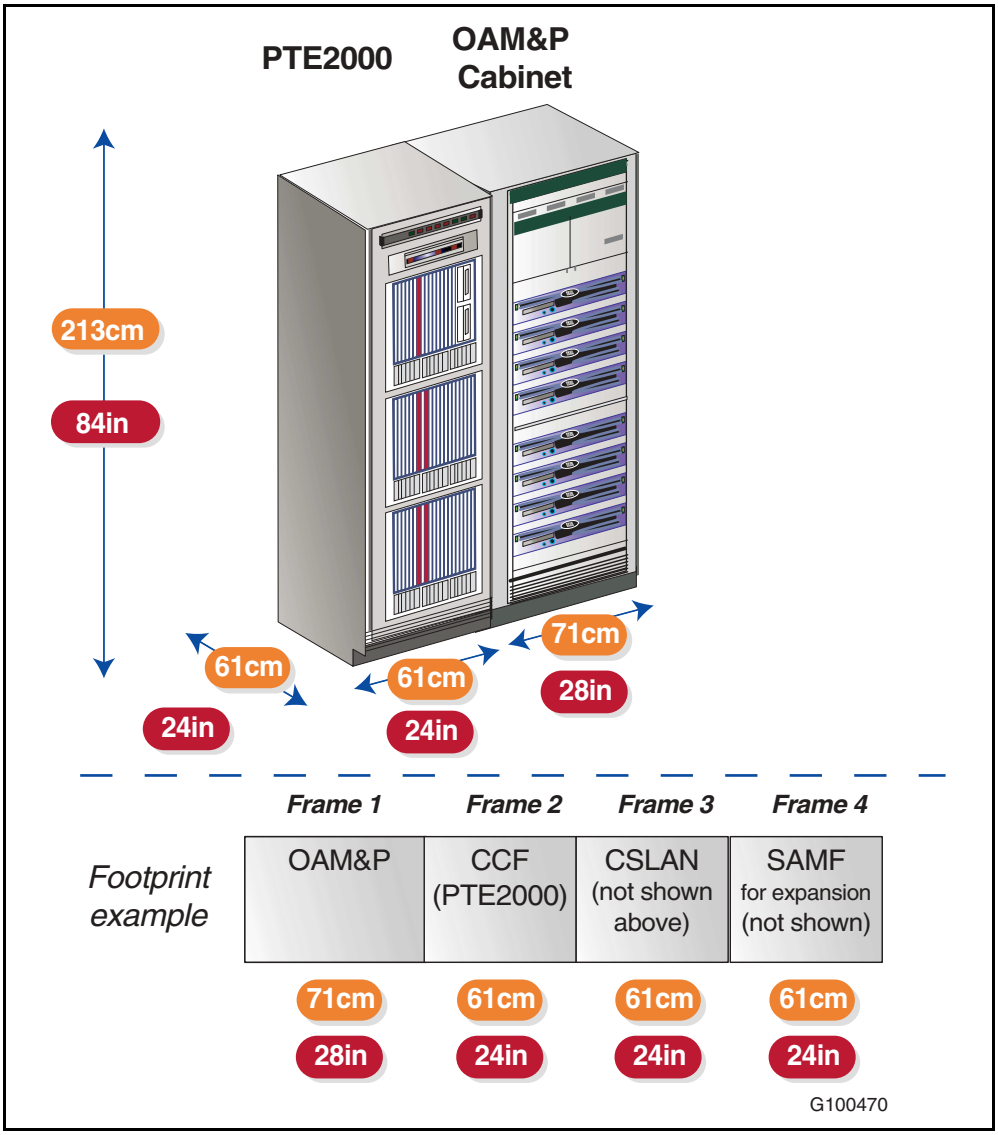
Frame layout

The Communication Server 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

Figure 7 on page 39 shows the Call Control Frame. Figure 12 on page 64 shows a sample cabinet lineup.

Figure 12
Sample Communication Server 2100 Compact cabinet lineup

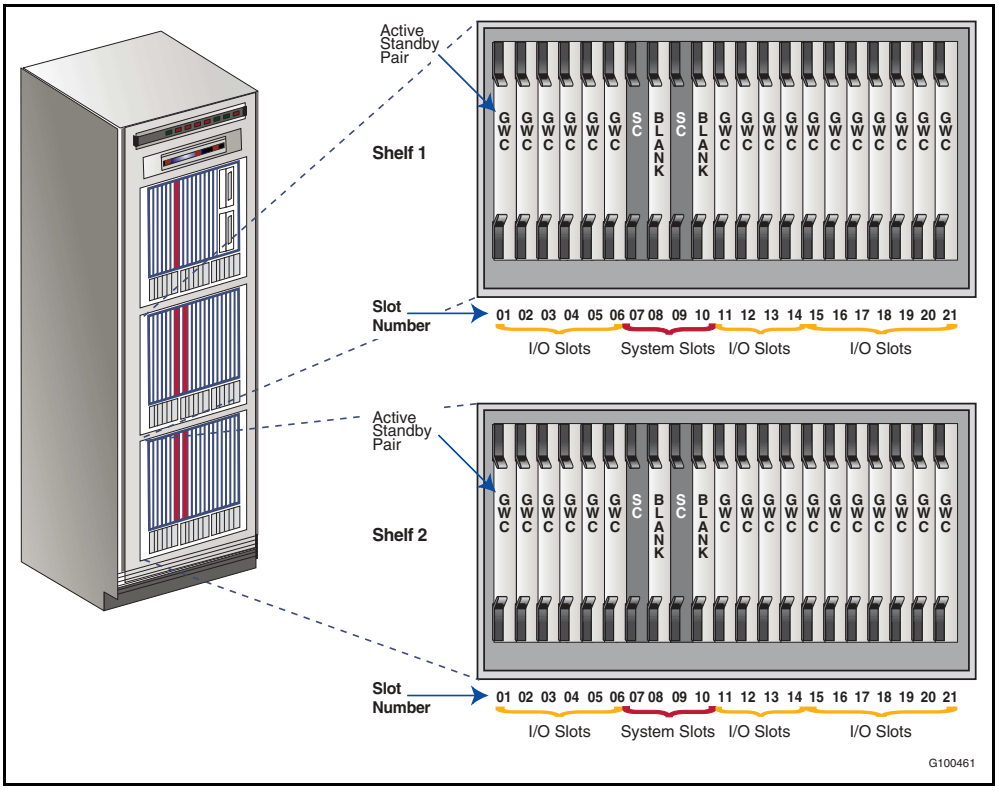


Card configuration

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 Communication Server 2100 Compact with its Media Gateway Controller functionality. Processing capacity is scalable by adding additional Gateway Controller circuit card pairs. There is a maximum of eight Gateway Controller card pairs 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 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 Figure 13, depending on the network requirements of your organization.

Figure 13
Communication Server 2100 sample SAM21 shelf configuration



Geographic survivability

The Geographic Survivability for Communication Server 2100 Compact solution provides redundancy for the Communication Server 2100 Compact by distributing its architecture in different physical locations. This redundant configuration ensures continued operation in the event that the building in which the Communication Server 2100 Compact resides is damaged. To achieve full geographic survivability, the configuration uses Storage Area Network (SAN) communication architecture used within the Communication Server 2100 Compact and uses transport equipment to provide location redundancy on top of traditional redundancy (for example, power, shelf) built into the architecture.

Customers can install each Communication Server in buildings up to 120 kilometers (74.5 miles) apart. In the event of a disaster destroying one of the sites, the second Communication Server takes over call processing to ensure full service and operations. In each location, the maximum distance between the Call Agent and the first optical element is 300 meters (984 feet) (that is, the fiber channel interface on the faceplate of the Call Agent card to the first Ethernet Routing Switch 8600). The configuration uses two Gigabit Ethernet (Gig-E) interfaces to provide link redundancy.

Note: This functionality does not apply to the Communication Server 2100 XA-Core.

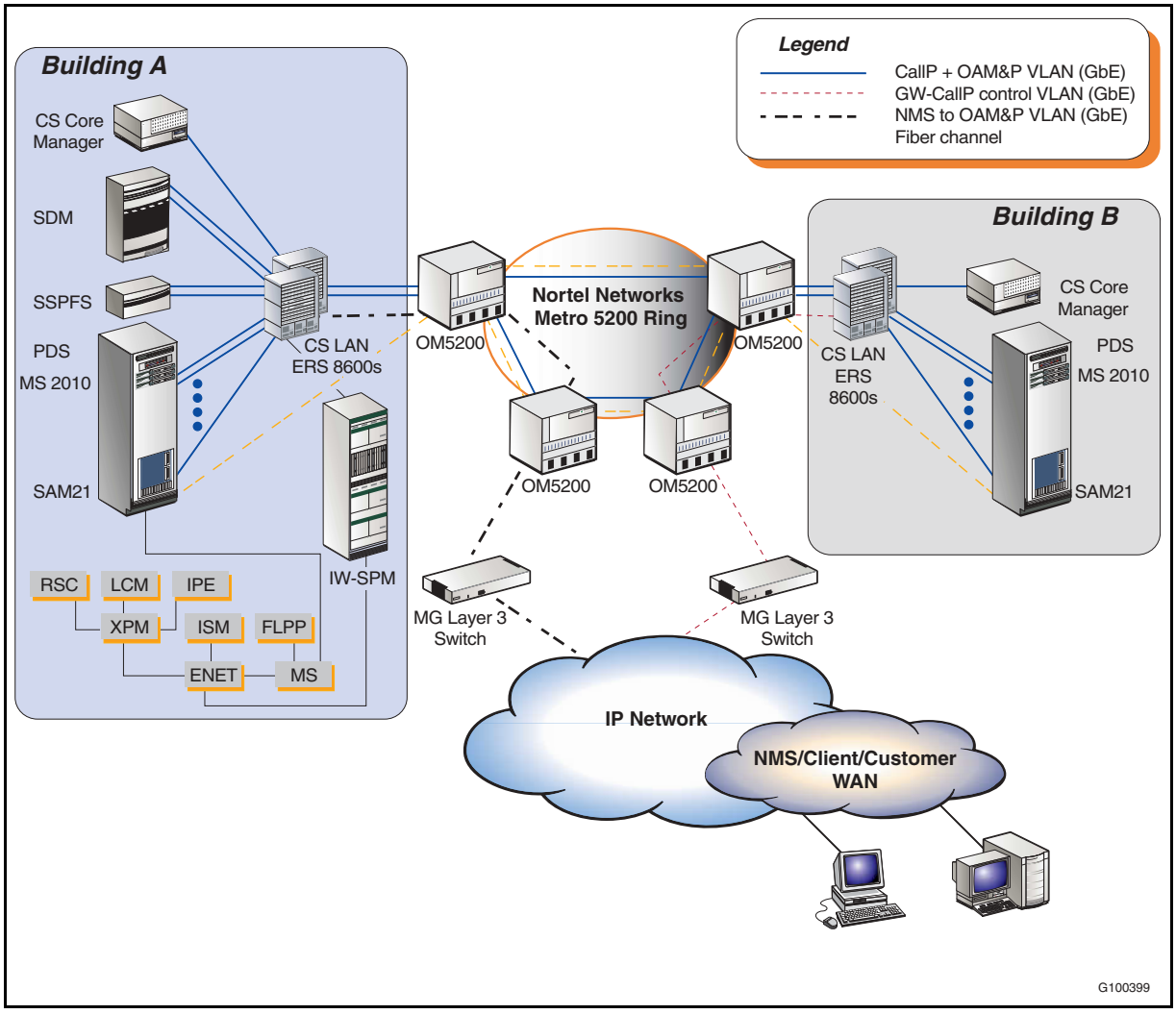
This configuration uses a Dense Wave Division Multiplexing (DWDM) ring to connect the distributed locations (SONET is also supported for Greenfield systems only - it does not apply to hybrid configurations). With the two halves of the Communication Server separated, one in Building A and the second in Building B, when a disaster impacts either building, a Unidirectional Path-Switched Ring (UPSR) maintains service from the gateways on the edges of the ring. The Communication Server performs a warm Switch Activity (SWACT) if necessary between the two geographically dispersed halves maintaining full operation in a non-redundant mode. This is the only impact that this feature has on the Communication Server halves.

To provide additional protection from service degradation during a disaster, the Gateway Controllers are also separated geographically.In addition, SE08 now supports a highly-available configuration of the management servers split between locations. For example, Site A can have an active CMT and a cold standby CBM, while Site B has a cold standby CMT and an active CBM.

A geographically survivable Communication Server 2100 Compact supports Time Division Multiplexing (TDM) interfaces only in non-survivable mode. If a disaster occurs that takes down the building housing the TDM portion of the system, TDM service is lost until that Communication Server half recovers. Therefore, the TDM, or hybrid, portion of the switch is not geographically survivable.

Figure 14 on page 67 shows an example of the geographic survivability configuration of the Communication Server 2100 Compact.

Figure 14
Geographic survivability network configuration



LAN architecture

The LAN architecture does not differ significantly from the base Communication Server 2100 Compact platform; however, additional considerations are implemented to reduce the risk of a gateway having visibility to both halves of the Communication Server, while the two halves cannot see each other. If this occurs, the Communication Server is operating in what is termed as a “split brain” scenario. To prevent this from happening, the gateways cannot reside on the same LAN as the Communication Server. As shown in Figure 14, the gateways must reside outside of the Communication Server LAN. If a gateway can see two active call servers, the gateway will not come into service.

Transport requirements

This section describes the transport requirements for the Communication Server 2100 Compact geographic survivability configuration.The Communication Server and call control network have the following characteristics:

- The configuration supports two Gig-E, and one fiber channel, point-to-point connections between Communication Servers (that is, on the Communication Server LAN).
- The call control path between the gateway and the Communication Server is point-to-two-points.
- The Communication Server LAN and the call control path are over the same network.
- A gateway cannot communicate with both Communication Servers if both Communication Servers cannot communicate with one another.

The bearer path network has the following characteristic:

- The bearer path is point-to-multipoint and can be separate from the Communication Server LAN and call control path.

FOR MORE INFORMATION

See the *Meridian SL-100 Communication Server 2100 Compact Geographic Survivability Planning Guide*, 555-4031-901, for more detailed information about the geographic survivability configuration.

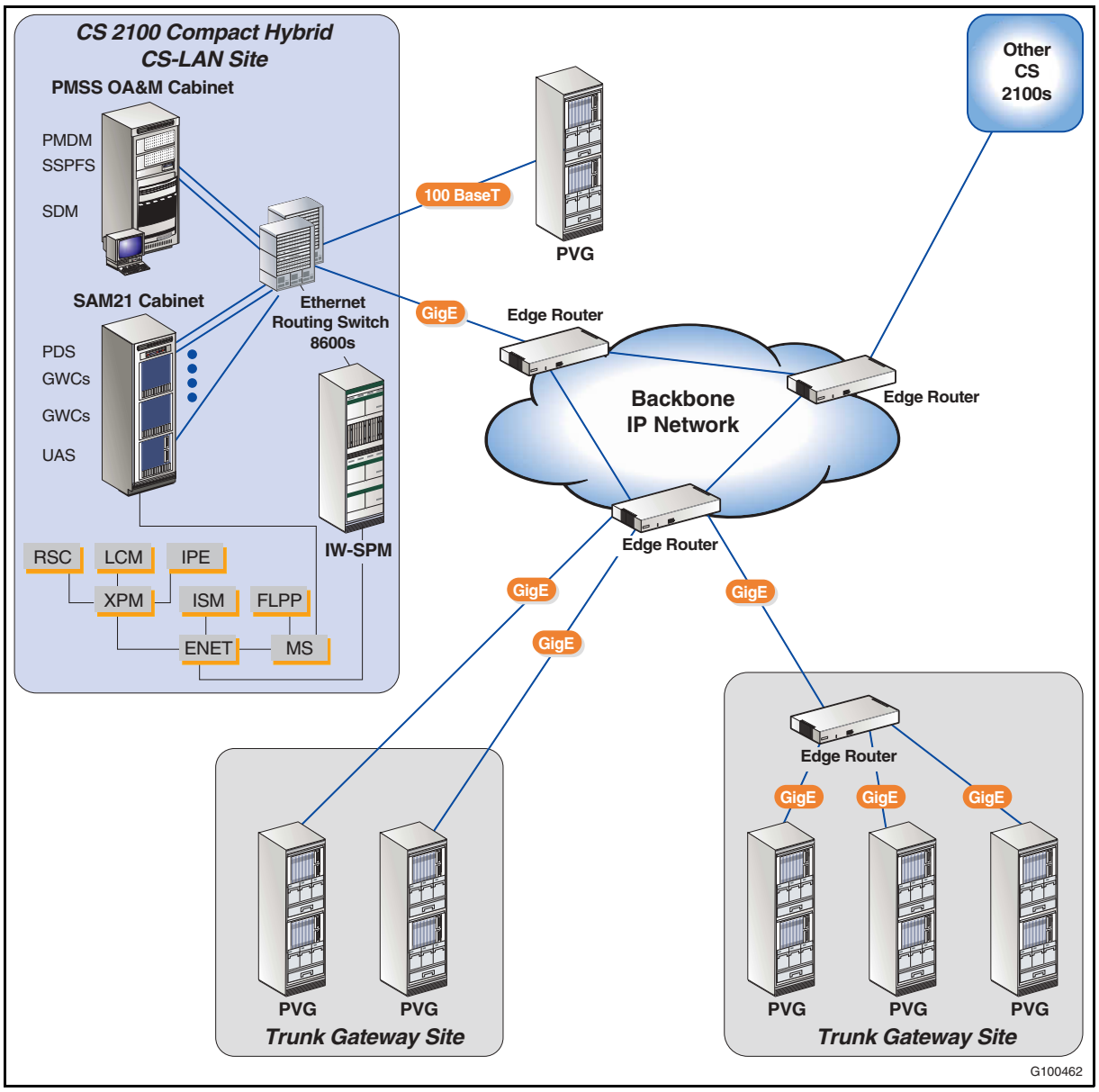
Hybrid support

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

“Appendix B: Peripheral support” on page 205 lists the existing Meridian SL-100 peripherals that are supported on the TDM side of the network in a hybrid configuration.

Figure 15 on page 69 shows the Communication Server 2100 Compact in a hybrid configuration.

Figure 15
Example Communication Server 2100 Compact hybrid configuration



Signaling interfaces

Table 8 shows the telephony protocols to which the packetized portion of this offering can interface.

Table 8
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 (native on Media Gateway 15000)	DS3
Analog line	–

Operating parameters

The following operating parameters apply to the Communication Server 2100 Compact:

- The Media Gateway 15000 does not support Multi frequency (MF) trunks. Signaling System # 7 (SS7) currently is not supported.
- The Communication Server 2100 Compact currently does not support international protocols.
- Communication Servers are limited in capacity in SE08 is as follows:
  - 60,000 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

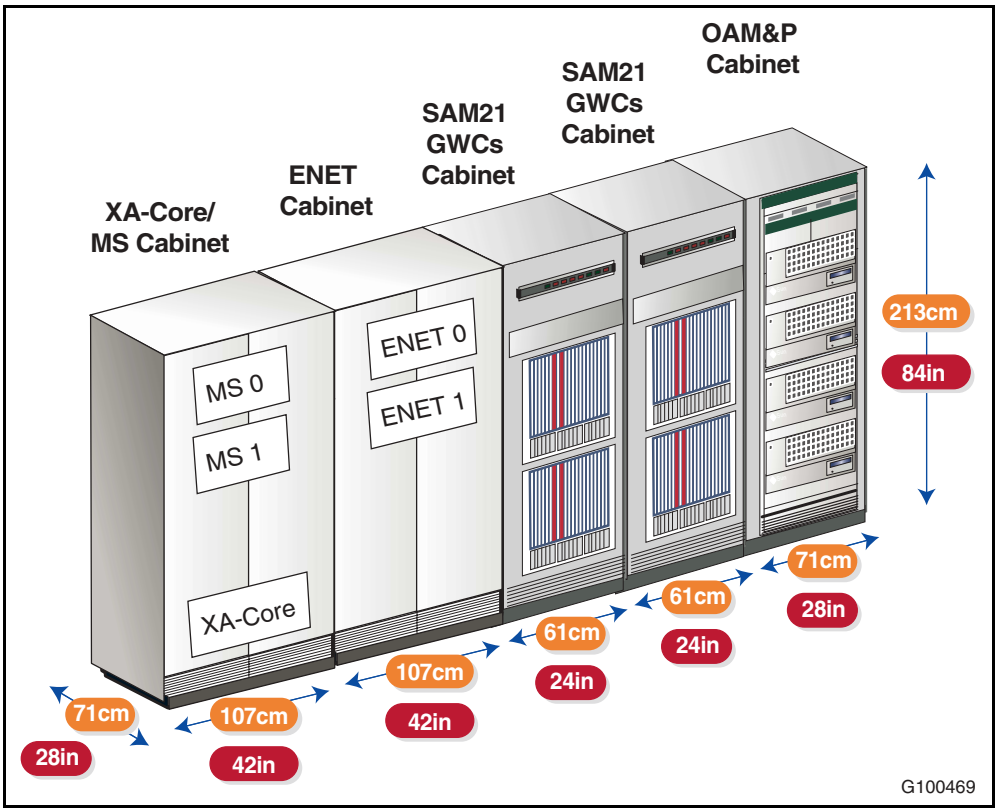
The Communication Server 2100 XA-Core provides the foundation for the IP switching by building on the hardware of existing Meridian SL-100 digital switches. Specifically, it re-uses the XA-Core as its processing engine.

There are two 10/100 BaseT Ethernet links running from the High Performance I/O Processor (HIOP) cards on the Communication Server 2100 XA-Core to the CS LAN. Each Ethernet link connects to a different Ethernet Routing Switch 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.

Figure 16 shows a sample cabinet lineup.

Figure 16
Sample Communication Server 2100 XA-Core cabinet lineup



Hybrid support

The Communication Server 2100 XA-Core provides the ability to support a Time Division Multiplexing and packet softswitch from the same Core. The Communication Server 2100 XA-Core provides hybrid support through the Asynchronous Transport Mode (ATM) 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 Communication Server 2100 XA-Core supports the NTFX32xx based storage media.
- “Appendix B: Peripheral support” on page 205 lists the existing Meridian SL-100 peripherals that are supported on the TDM side of the network in a hybrid configuration.

Signaling interfaces

The Communication Server 2100 XA-Core supports the same telephony protocols as the Communication Server 2100 Compact (see Table 8 on page 70).

Operating parameters

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

- Junctored Network is not supported with the Communication Server 2100 XA-Core.
- The Media Server 2010 is not supported in a hybrid configuration.
- The Input/Output Controller does not support the magnetic Tape Drive for a disk drive supported by a NT1X55xx based disk drive controller.
- Software upgrades from BNR Reduced Instruction Set Computing (BRISC) based TDM systems support conversion only from MSL17 to SE06 and SE06 to SE06.
- The Media Gateway 15000 does not support Multi frequency (MF) trunks. Signaling System No. 7 (SS7) is currently not supported.
- The Communication Server 2100 XA-Core currently does not support international protocols.

- Communication Servers are limited in capacity in SE08 is as follows:
  - 165,000 clients (not including trunks)
  - 1,650,000 Busy Hour Call Attempts (BHCAs)
- NEBS compliant
- In-service upgrades
- 99.999 percent availability

Gateways

Introduction

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

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**
- **Nortel Media Gateway 3000 Series**

Line gateways

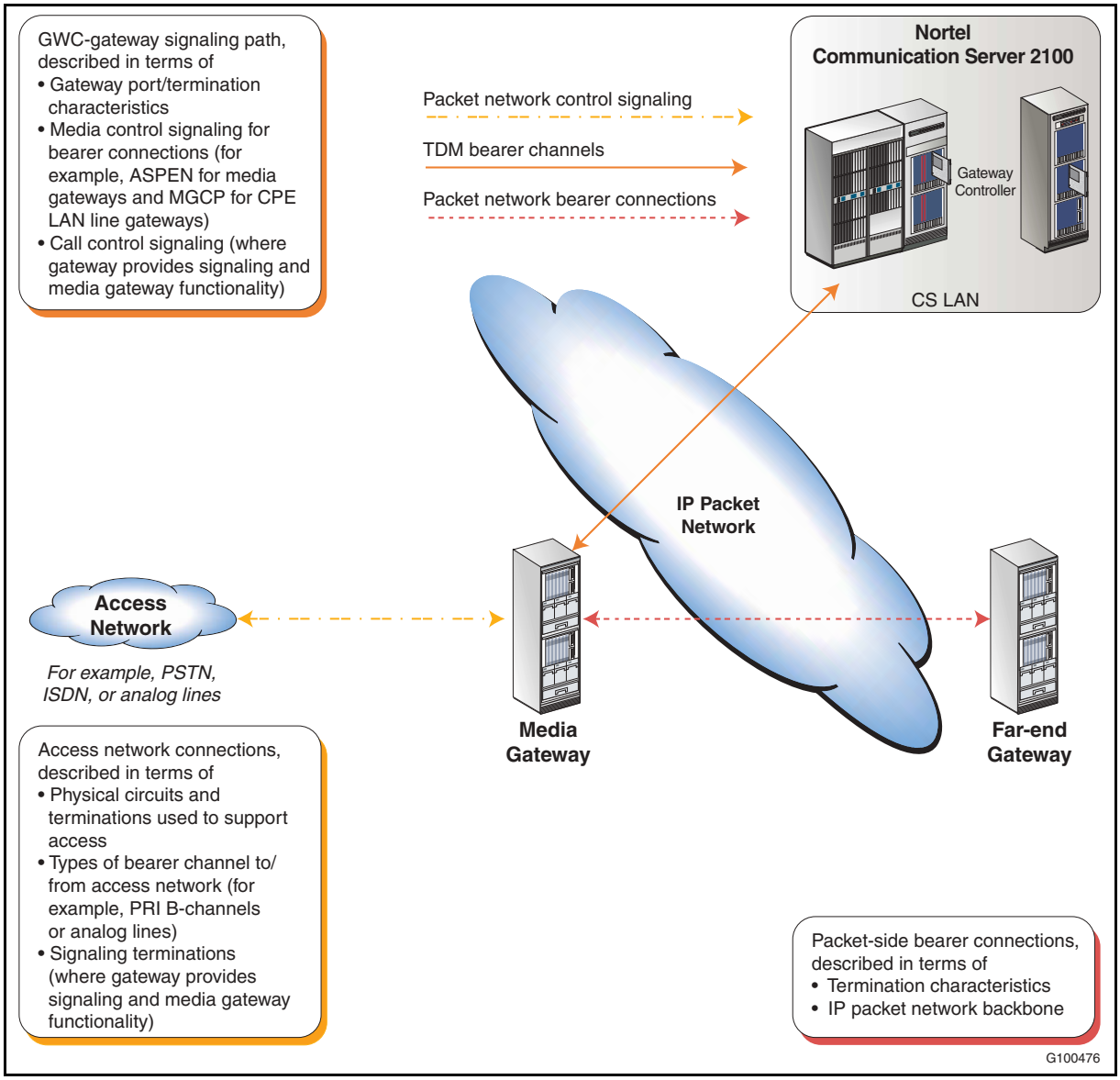
- **Communication Server 2100 IP Client Manager**

Multiservice gateways

- **Nortel Media Gateway 9000**

Figure 17 on page 76 summarizes how gateway capabilities can be categorized.

Figure 17
Media gateway capabilities



New in SE08

Nortel Media Gateway 15000

Description

The Media Gateway 15000 supports Primary Rate Interface (PRI) trunk access to the IP packet backbone network. It 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

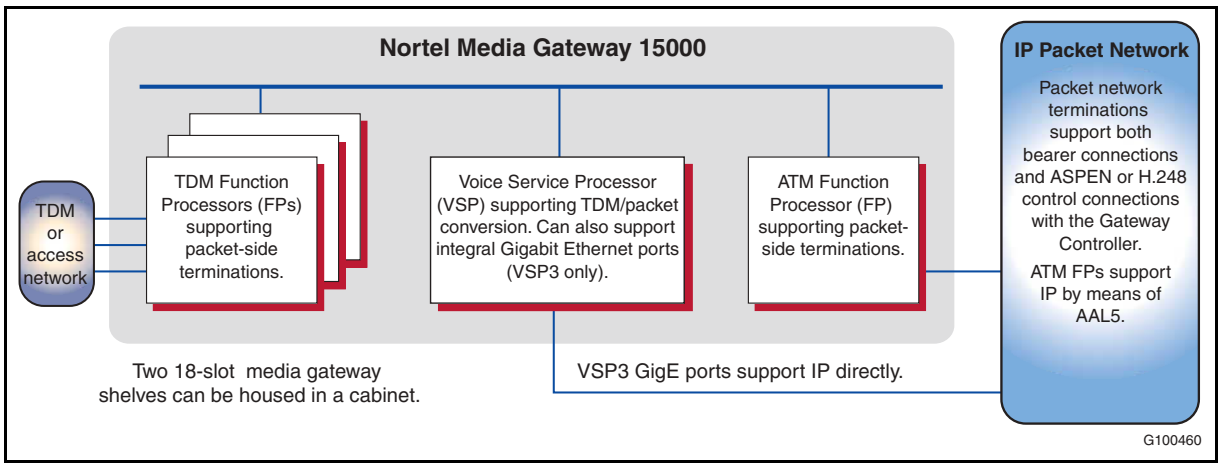
Note: The Media Gateway 15000 was previously called the Passport 15000 Packet Voice Gateway.

The Media Gateway 15000 application is a carrier-grade integrated voice and data interworking service. With the Media Gateway 15000, the Communication Server 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 functionality, as well as media gateway functionality. Media gateway functionality for PRI means mapping ISDN B-channels onto packet network media streams under ASPEN (a proprietary Gateway Controller-gateway device control protocol used for IP telephony) control. Signaling gateway functionality 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 Communication Server 2100.

Figure 18 on page 78 illustrates Media Gateway 15000 components and their functions at a logical level.

Figure 18
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) and supports IP datagram encapsulations using AAL5 and RFC1483. 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 in housed in a Media Gateway 15000 shelf, the Gateway Controller perceives each one as a separate entity. The trunks on a given TDM-side T1 carrier are all assigned to a particular Voice Service Processor and are not available to any other Voice Service Processor. Similarly, each Voice Service Processor uses only one Media Gateway 15000 Function Processor for access to the packet network. Each Voice Service Processor and its associated Function Processor and TDM T1s can, therefore, be regarded as a logical gateway.

There is a native IP interface from the VSP3 or VSP3o card on the Media Gateway 15000. In addition, there is a 10/100 BaseT Ethernet link to the CS LAN.

Physical configuration

The Media Gateway 15000 serves as a media gateway in the Communication Server 2100 network. It 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 can be deployed 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 multi-protocol routing services, intelligent traffic management, and 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 a 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

The Media Gateway 15000 supports the following:

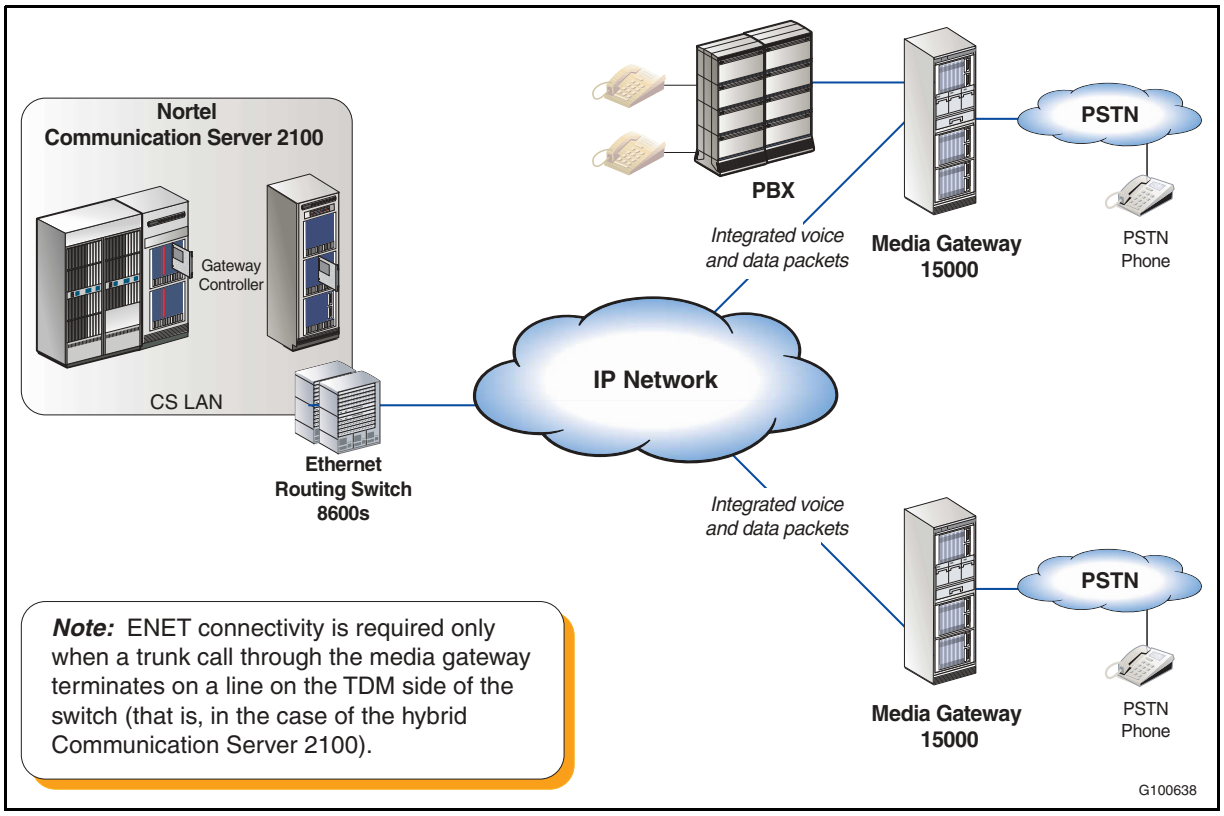
- toll-quality ITU-T G.711 PCM, G.726 PCM, G.726 ADPCM, or G.729 A/B CS-ACELP voice with silence suppression, comfort noise generation and dynamic downspeeding capability for congestion management
- tone generation on the TDM side of the gateway, such as basic service tones, and basic and expanded call progress tones
- Dual-tone Multifrequency (DTMF) digit collection for ANSI/ETSI PRI agencies
- 56/64 kbps clear-channel fax and modem support
- AAL-2 encoding for voice, modem and fax traffic for low-end delay and high-bandwidth efficiency
- 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

Figure 19 shows an example of a Media Gateway 15000 in a Communication Server 2100 network. The IP channels transport voice and voice-band data traffic over virtual connections within the Media Gateway 15000. The virtual connections consist of the following:

- Permanent Virtual Connections (PVCs)
- Switched Permanent Virtual Connections (SPVCs)

Figure 19
Media Gateway 15000 example configuration



Requirements

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

- **Hardware**
  - a Voice Service Processor 2 (VSP2) or VSP3 Function Processor
  - a TDM Function Processor (that is, DS3 for T1)
  - a 100BaseT Ethernet Function Processor (for the native IP configuration)
- **Software**
  - Media Gateway base
  - Packet Voice Gateway

    Note: The Communication Server 2100 only supports AAL5.

  - 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 DS3 or OC-3; mux to deliver DS1.
- Although the Media Gateway 15000 supports additional protocols, the Communication Server 2100 implementation only supports PRI in SE08. Signaling System #7 is not supported.

Media Gateway 150000 physical interfaces depend on the type of Packet Voice Gateway and Voice Services Processor. Table 9 lists the overall maximum number of 64 kbps bearer connections or DS0s that can be supported by various Media Gateway 15000 configurations (the numbers will be less if redundancy is in use).

Table 9
Media Gateway 15000s capacity summary

Media Gateway type	Codec type	Maximum 64 kbps channels/DS0s per VSP
Media Gateway 15000 with VSP3	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
Media Gateway 15000 with VSP2	G.711 (10 ms)	1,120
	G.711 (20 ms)	1,120
	G.729a/b (10 ms + digit collection)	800
	G.729a/b (20 ms + digit collection)	800

References

Table 10 shows where you can find more detailed information about the Media Gateway 15000s.

Table 10
Documentation references (Sheet 1 of 2)

Document title	Document number
Nortel Multiservice Switch 7400/15000/20000 Overview	NN10600-030
Nortel Multiservice Switch 7400/15000/20000 Technology Fundamentals	NN10600-780
Nortel Multiservice Switch 7400/15000/20000 Configuring Switched Service Configuration Management	NN10600-782
Nortel Multiservice Switch 15000/20000 Hardware Description	NN10600-120
Nortel Multiservice Switch 15000/20000 Hardware Installation, Maintenance and Upgrades	NN10600-130

Table 10
Documentation references (Sheet 2 of 2)

Document title	Document number
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 smaller scale alternative to the Media Gateway 15000 traditionally deployed in the carrier market. In the Communication Server 2100 configuration, trunk gateways provide access to the Public Switched Telephone Network. A key strategy of the Meridian SL-100 evolution to the Communication Server 2100 is to provide customers with flexibility. Thus, there is a need to deliver a cost-effective Time Division Multiplexing (TDM) gateway to access the PSTN in the Communication Server 2100 product offering.

Nortel 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 Nortel Media Gateway 3000 Series gateways into the Communication Server 2100 environment.

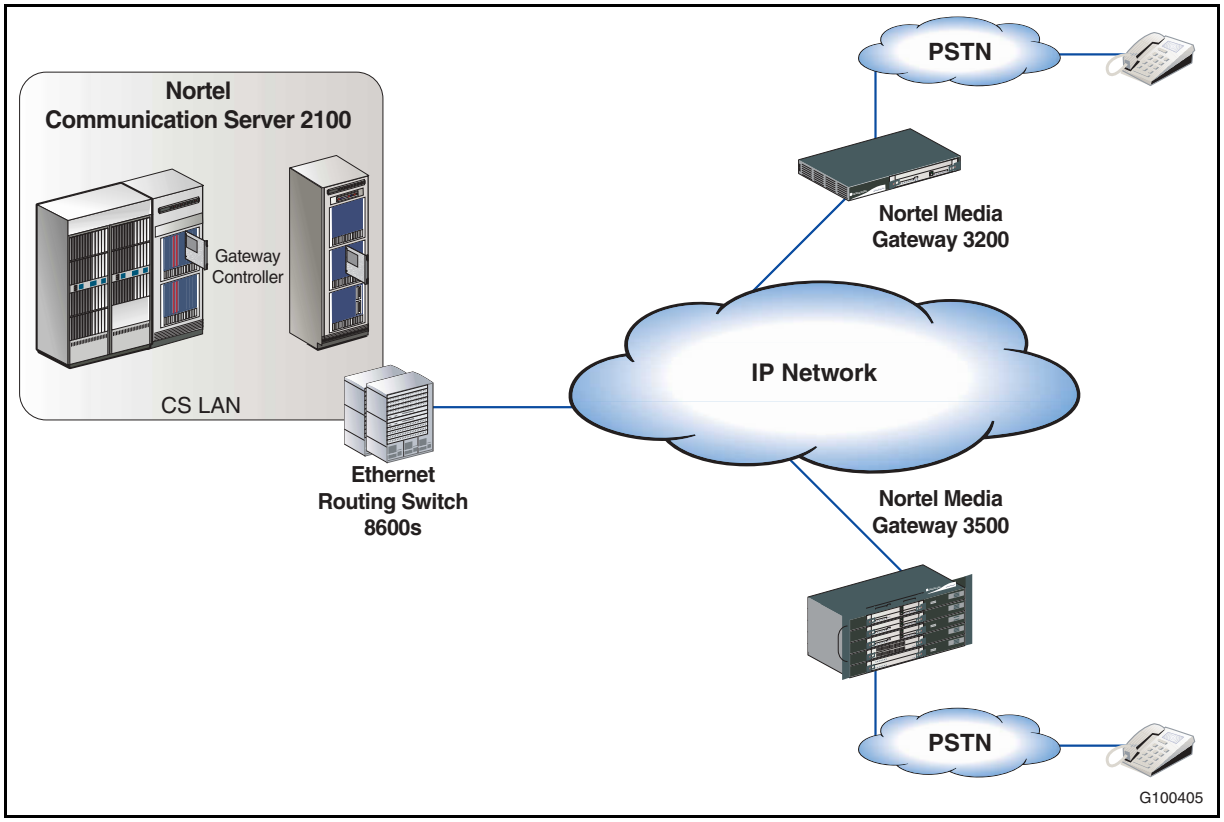
There are two versions of the Nortel Media Gateway 3000 Series as follows:

New in SE08

- The Nortel Media Gateway 3200 provides options for 1, 2, 4, 8, and 16 spans of independent, simultaneous VoP calls. It supports up to 16 T1/E1 spans.
- The Nortel Media Gateway 3500 provides up to 2,880 independent IP to PSTN voice calls. Supports up to 96 non-spared, or 80 spared, T1/E1 spans.

Figure 20 on page 85 shows an example of Nortel Media Gateway 3000 Series in a Communication Server 2100 configuration.

Figure 20
Nortel Media Gateway 3000 Series network configuration



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

User interface

The Nortel Media Gateway 3000 series comes 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.

Feature support

NI-1 Primary Rate Interface (PRI) features

Table 11 describes the NI-1 features supported by the Nortel Media Gateway 3000 Series gateways.

Note: NI1 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.

FOR MORE INFORMATION

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.

Table 11
NI-1 features (Sheet 1 of 3)

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 any 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.
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.

Table 11
NI-1 features (Sheet 2 of 3)

Feature	Description
Network Name CLID	Allows the transport of the calling, redirecting, and called parties' names across the PRI. The service allows an originating node to receive the name of the terminating party and deliver the originator's name to the terminating node. When a call is redirected, the name of the connected party is also delivered.
Network Ring Again (NRAG)	Allows a calling user to be notified 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)	Provides the ability to distribute incoming calls to a set of answering positions (agent positions). These positions can be at a local node or remote nodes, where each node can be served by a similar or like node (for example, Communication Server 2100 to Communication Server 2100). Information exchanged between nodes is used to determine the best routing to evenly distribute calls among the answering positions.
Special Number Services	Enables a PRI user to 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)
10-Digit Local Display	Allows a called party's display phone to display the three-digit area code, along with the seven-digit DN of the calling party 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 are using CLID

Table 11
NI-1 features (Sheet 3 of 3)

Feature	Description
Network Message Service	The following types of Network Message Service are supported: • Network Message Waiting Indicator (NMWI) – Allows a Message Service on one node to activate or deactivate the message waiting indicator of a subscriber located at a different node. • Network Executive Message Waiting (NEMW) – Allows the Executive Message Waiting (EMW) feature on one node to activate the message waiting indicator of a subscriber located at a different node.
Release Link Trunk (RLT) Enhancement	RLT optimizes the use of NTNA PRI trunks and is available on an optional basis. This feature includes the ability to drop PRI trunks between two Communication Server 2100s. It also enables a Communication Server 2100 to receive a call from another Communication Server 2100, transfer the call back to the originating Communication Server 2100, and release the redundant trunk.
Integrated Services Access (ISA)	Permits one PRI interface to replace several dedicated trunk groups, resulting in efficiencies and simplified administration. ISA provides the capability to signal information which 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 which 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. Provides the equivalent of local service at the distant exchange. • 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 which 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

Table 12 describes the NI-2 features supported by the Nortel Media Gateway 3000 Series gateways.

Note: NI2 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.

Table 12
NI-2 features (Sheet 1 of 3)

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	Provides the ability to convey 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
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 Communication Server 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

Table 12
NI-2 features (Sheet 2 of 3)

Feature	Description
Message Service	Allows subscribers to retrieve messages that were 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's 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 has activated 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 have been 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 has deactivated the message-waiting indicator, the SPCS sends an acknowledgement message to the MSR.
PRI administration/maintenance services	
Back-up 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 for more than one DS1 interface). This service provides a procedure for employing a standby D-channel which 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 available as an option on a per ISDN PRI basis.
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 the expiry of timer T309) • after the expiry of timer T308 for a second time, caused by the absence of a response to the RELEASE message • upon data link establishment at the time of a system initialization • when adding or returning B-channels to service from a Maintenance or Out-of-Service state

Table 12
NI-2 features (Sheet 3 of 3)

Feature	Description
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. 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. If a channel carrying a call reaches the OOS state once 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, there are restrictions/limitations 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 *Meridian SL-100/CS 2100 Application Planning Guide*.

Operating parameters

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

- Signaling System #7 (SS7) is not supported in SE08.
- multiple density options (from one T1 to 16 T1s)
- NEBS level 3 complaint
- Packet Telephony standards compliant
- IETF standards compliant
- optional AC power supply redundancy
- hot swappable enabled

References

Table 13 shows where you can find more detailed information about the Nortel Media Gateway 3000 Series. Note: The Nortel Media Gateway 3000 Series gateways were previously called the Audiocodes Mediant gateways.

Table 13
Documentation references

Document title	Document number
Mediant 2000 VoP Media Gateway User's Manual	LTRT-69801
Mediant 2000 Configuration Instructions for Nortel CS2000 and CS2100 H.248/IUA & H.248/ISUP Solutions	LTRT-72901
Mediant™ 2000 Fast Track Installation Guide MGCP, MEGACO, H.323 & SIP	LTRT-70102
IPmedia™ 2000 Media Server Platform User's Manual	LTRT-69701
AudioCodes EMS Users Manual	LTRT-01010
AudioCodes EMS Product Description	LTRT-01040
AudioCodes' EMS Server Installation and Maintenance Manual	LTRT-01041
Detailed hardware specifications are available at www.audiocodes.com.	N/A

Communication Server 2100 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 Communication Server 2100. In SE06, the Communication Server 2100 XA-Core and the Communication Server 2100 Compact both supported the Nortel IP Phone 2000 series and the Nortel Softphone 6350 through the IP Client Manager.

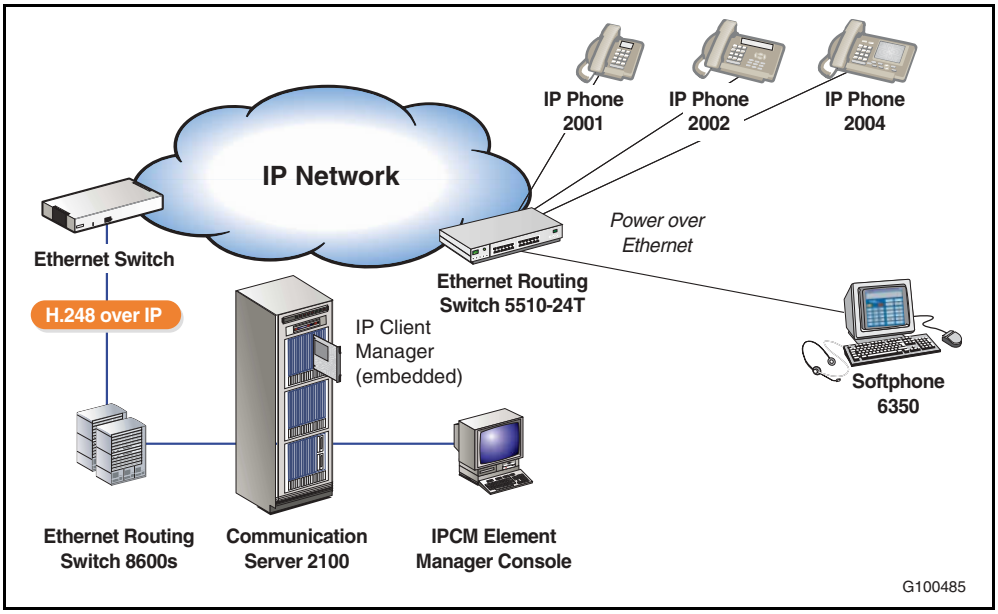
SE07 built on the SE06 release and introduced the support of the IP Client Manager 7.0 in the Communication Server 2100 network. A pair of IP Client Manager Element Managers (IPCM-EMs) can manage up to 100 IP Client Managers. They provide the OAM&P interface.

There are two possible configurations for IP Client Manager as follows:

- The first configuration is the same as the IPCM 6.12 IP configuration.
- The second configuration was introduced in IPCM 7.0 in which the IP Client Manager, including the Element Manager, reside in a SAM21 chassis (on Motorola 5385 CPUs).

Figure 21 shows how the IP Client Manager now resides in a SAM 21.

Figure 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 Communication Server 2100 IP solution are routed directly between media endpoints. The IP Client Manager terminals (for example, the IP Phone 2004) are media endpoints. Other endpoints in a Communication Server 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 off 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).
- Base OS evolution (upgrading from Windows NT Embedded to Windows XP Embedded).
- Support of the IP Phone 2001.
- Support of the Phase 2 IP Phones 2002 and 2004.
- Support for the IP Softphone 6350 PC-based telephone.
- Support for the Key Expansion Module.
- Support for the IP Conference Phone 2033.
- UNIStim security (gateway to 200x).
- UNIStim security (gateway to soft client).
- Alignment of the Element Manager with Communication Server 2100 Integrated Element Management System (IEMS) (see “Nortel Integrated Element Management System” on page 162).
- 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” on page 65)
- Support of the a wide range of IP Phone features described in *CICM Product and Technology Fundamentals*, NN10044-111. Contact your Nortel representative for a complete list of features supported on the IP Phones and IP Softphone, many of which were developed explicitly for Meridian SL-100 customers, but now operate off the Communication Server 2100.

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, there was no indication 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 have the ability to “hot-desk” from IPCM phone to IPCM phone. However, hot-desking may not occur that frequently and there may be a phone that is 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

FOR MORE INFORMATION

See the *Meridian SL-100 Feature Description Manual,* 555-4031-801 for information about how to configure and administer the Line Option for IPCM Phones feature.

New in SE08

Active Call Failover

Prior to SE08, IP terminals could connect to either node of a IP Client Manager for service. Should a node fail, all terminals hosted by the defunct node would experience an outage (possibly losing one or more calls) while they rebooted and reconnected to the mate node. The Active Call Failover (ACF) functionality 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. Should the master node fail, the mate assumes the role of master node, takes over this floating IP address and begins the recovery of terminals while maintaining active calls.

A Switch of Activity (SWACT) occurs when the role of master is transitioned from one node to another. Figure 22 on page 98 shows the IP Client Manager architecture when configured for Active Call Failover. From this figure, this implies 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.

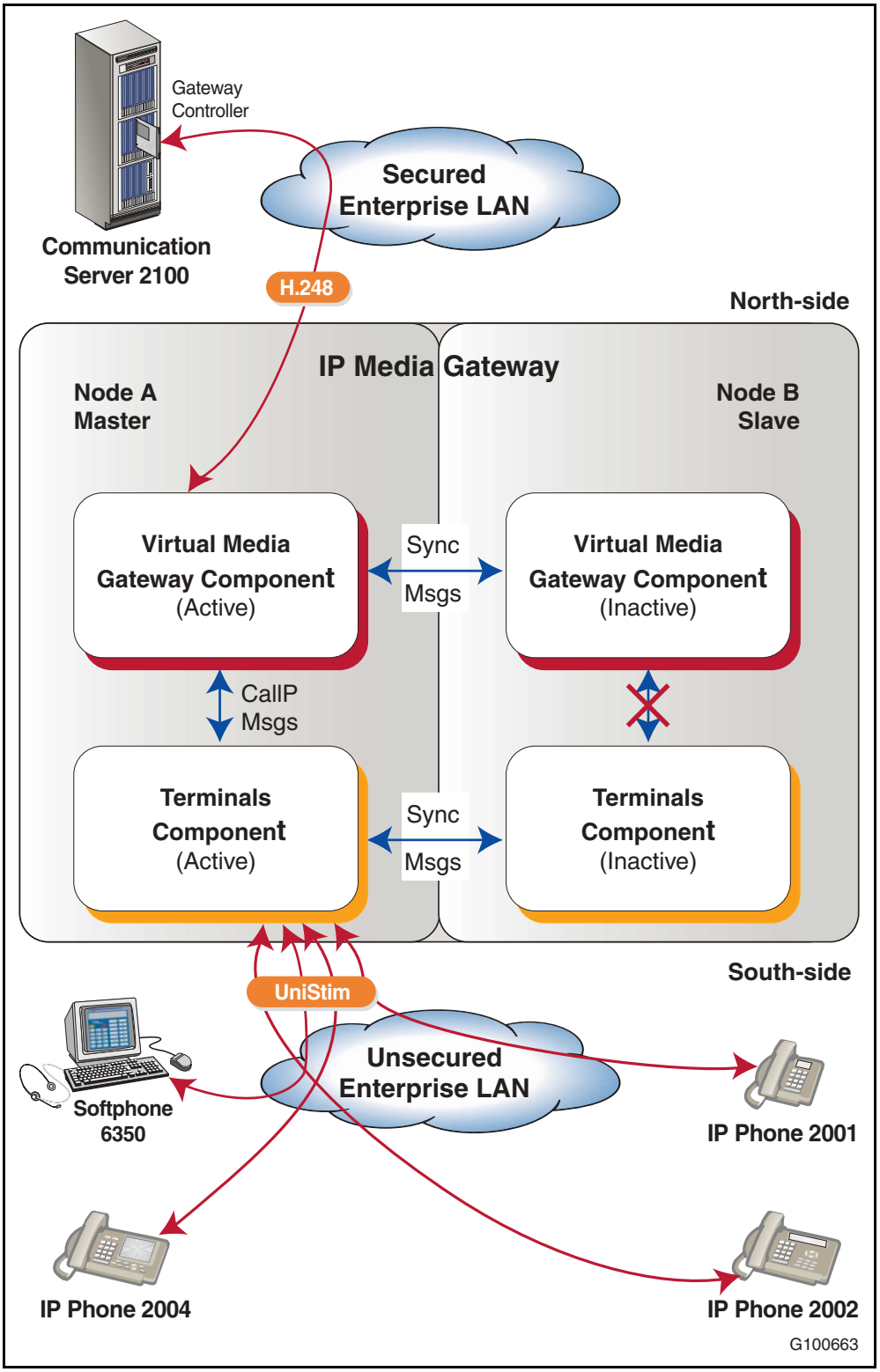
As shown, the north-side of the IP Client Manager continues to communicate with the Gateway Controller using the H.248 protocol over a single interface. However, Active Call Failover changes the architecture of the IP Client Manager so that the south-side now also presents a single, but unique interface. Terminals no longer have an option to connect to one or the other nodes as in SE07. Instead, terminals are now only aware 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’s interface. Each component shown in Figure 22 on page 98 is responsible for managing its floating IP address and for ensuring 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 these components on both nodes of the IP Client Manager illustrates this. This configuration is necessary to ensure that both nodes have an accurate view of 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 in-active component.

Figure 22
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 is 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 IP Softphone firmware. However, enhancements have been made to both the firmware and IP Softphone 6350 software in order to minimize the impact on the user during a SWACT. Nortel therefore recommends that the IP Phones/ Softphones be upgraded to the latest versions that ship as part of the IP Client Manager release.

References

Table 14 shows where you can find more detailed information about the IP Client Manager.

Table 14
Documentation references (Sheet 1 of 2)

Document	Order number
CICM Etherset Installation Guide and User Manual ***Note:*** Centrex IP Client Manager (CICM) is the carrier name for the IP Client Manager.	NN10027-113
CICM m6350 SoftClient Branding Kit	NN10183-114
CICM m6350 Installation Guide	NN10182-113
CICM Series 8.0 CICM Basics	NN10044-111
CICM Upgrades (describes how to upgrade from IPCM 2.5 and IPCM 6.12 to IPCM 7.0)	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
Meridian SL-100 Feature Description Manual (refer to the Line Option for IP Phones feature description)	555-4031-801
Meridian SL-100 Service Order Reference Manual (refer to the IPCLIENT – IP Client section)	555-4031-808

Table 14
Documentation references (Sheet 2 of 2)

Document	Order number
Meridian SL-100 Data Schema Reference Guide (refer to the KSETFEAT Feature IP Client section)	555-4031-851
m6350 TAPI Service Provider Installation and Troubleshooting Guide	*Magnetic North Software Limited*

Nortel Media Gateway 9000

Description

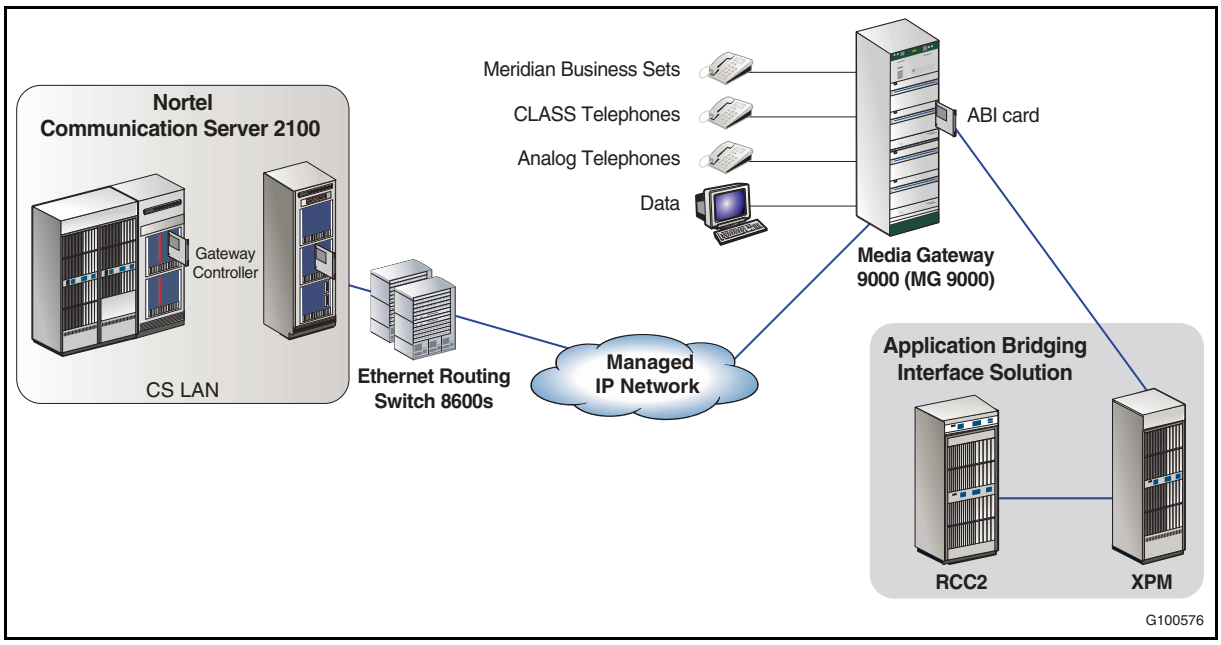
The Nortel Media Gateway 9000 (MG 9000) is a multi-service media gateway that enables large enterprises to use a single access platform for a wide-range of services. Positioned at the edge of an IP network, the Media Gateway 9000 combines voice and data services into a single access gateway, with a single 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 and Digital Subscriber Loop services.
- Connects subscriber interfaces directly to packet backbone networks.
- Supports the following data connections and services in the master shelf:
  - Full-rate Asymmetrical Digital Subscriber Loop (ADSL) supported on ATM networks. It is not supported on a Gig-E interface.
  - Digital Signal Level 0 (DS0) Specials.
- 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 (OAM&P), and data traffic.

Figure 23 on page 102 shows an example of a Media Gateway 9000 network configuration.

Figure 23
MG 9000 example configuration



MG 9000 enhancements in SE08

The SE08 release introduces the following enhancement to the MG 9000:

- Defense Switched Network support in normal operation.

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 functionality 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 of these applications 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 helps facilitate 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 will migrate to the MG 9000 Access Bridging Interface for call control through the Communication Server 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 quicker 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, 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 Equipement (IPE)
  - Line Concentrating Module Enhanced (LMCE)
  - Remote Switching Center (RSC)
  - Remote Switching Center SONET (RSC-S)

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

The ABI functionality also adds support for hosting a Remote Maintenance Module (RMM) off of ABI-based XPMs, specifically the LTC, LTCI, LGC, LGCI and Subscriber Carrier Module-100 Access, Second Version (SMA2). A subset of line diagnostics are provided for ABI lines, when the switching platform is configured as pure IP.

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.

The “network-side” ABI card is responsible for controlling the MIB data, handling connection setup 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 Communication Server 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 there is a failure on the call control link back to the Communication Server 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 GigE interfaces to the enterprise’s 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, which contains the common equipment cards for the node. This 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. Figure 24 on page 105 shows a Media Gateway 9000 frame.

Figure 24
NTNY01BB Media Gateway 9000 frame

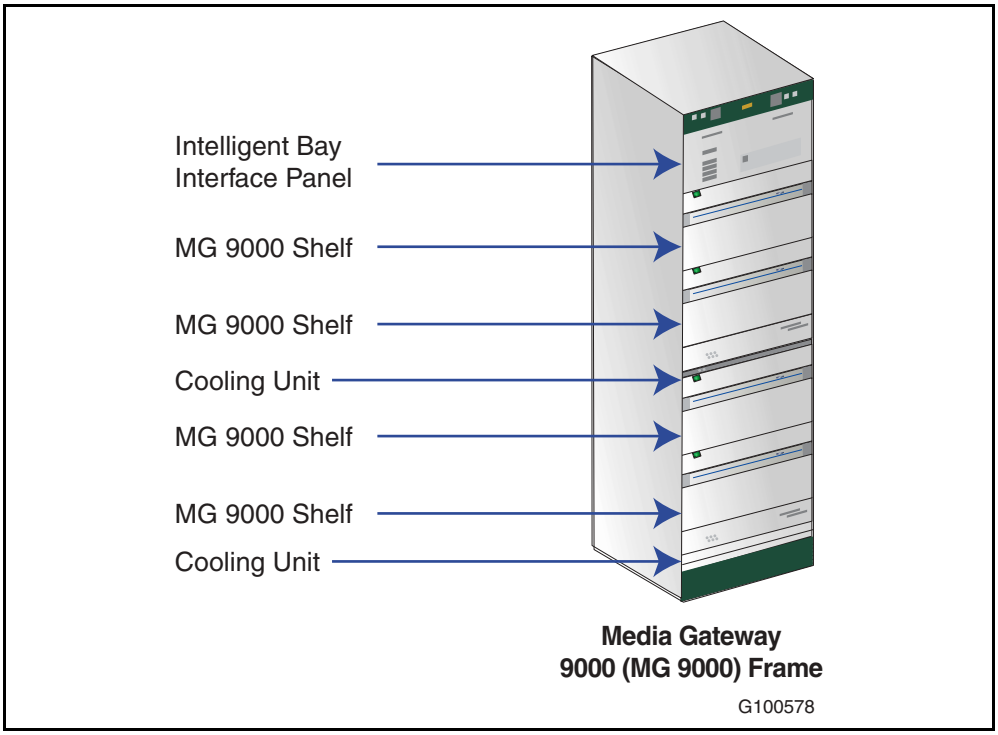


Table 15 describes the components that reside in a Media Gateway 9000 frame.

Table 15
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 dc loads 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. • 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 the following application: • switched lines

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

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. Figure 25 on page 107 shows an example of a Media Gateway 9000 shelf. The Media Gateway 9000 contains up to 16 service slots in each shelf.

Figure 25
Media Gateway 9000 shelf

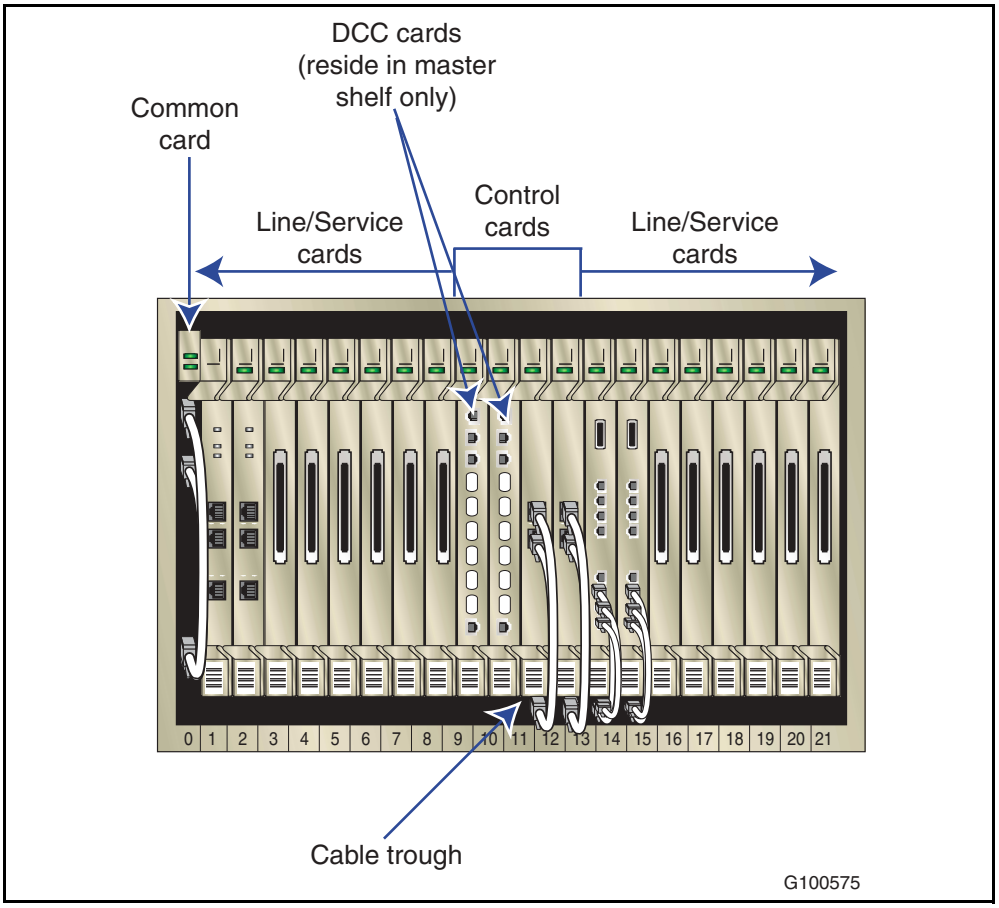


Table 16 describes the shelves in a Media Gateway 9000 frame.

Table 16
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, which prevents traffic conditions in one domain from degrading the operating capacity in the other domain.
NTNY15AA	Air filter assembly.
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, middle cooling unit).

Table 17 lists the Media Gateway 9000 line/service cards that are supported in a Communication Server 2100 network.

Table 17
Media Gateway 9000 line/service cards

Card	Description
POTS 32	Traditional telephone service cards with 32 ports.

Emergency Stand Alone

Emergency Stand Alone 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). Emergency Stand Alone also provides basic emergency service access, such as 911, 411 and 611. In an IP configuration, six- to 13-digit dialing plan lengths are supported.

As mentioned previously, Emergency Stand Alone is also supported with the Access Bridging Interface functionality, in which case the subtending peripherals maintain service (except the RSC which maintains its own ESA mode). SE08 expands the Emergency Standalone mode to provide the ability to make ESA calls between MG 9000 nodes (Internodal ESA).

Protocol support

Table 18 lists the industry-standard protocols that are applicable to the Media Gateway 9000.

Table 18
Media Gateway 9000 protocols

Function	Standard	Description
Call control	ITU H.248	The ITU H.248 media gateway control messaging is used between the Communication Server 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 SE08.
- The Universal Access AALI multi-service ATM network solution is not supported in a Communication Server 2100 network.
- The DS1 private lines application is not supported in a Communication Server 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

Table 19 shows where you can find more detailed information about the Media Gateway 9000.

Table 19
Documentation references

Document title	Document number
MG 9000 Basics	NN10011-111
MG 9000 Upgrades	NN10048-461
MG 9000 Operational Configuration	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 centralized resource for the delivery, management and manipulation of packet-based media streams and services over the backbone network. In SE08, the Communication Server 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 Communication Server 2100.
- Conference circuits for multi-party calls across the packet network.

This chapter contains the following section:

- **Nortel Media Server 2010**

Nortel Media Server 2010

The Nortel Media Server 2010 (MS 2010) offers advanced IP packet audio and conferencing services in a Communication Server 2100 enterprise network. It replaces 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 Communication Server 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.

Figure 26 on page 113 shows the Media Server 2100.

Figure 26
Media Server 2010

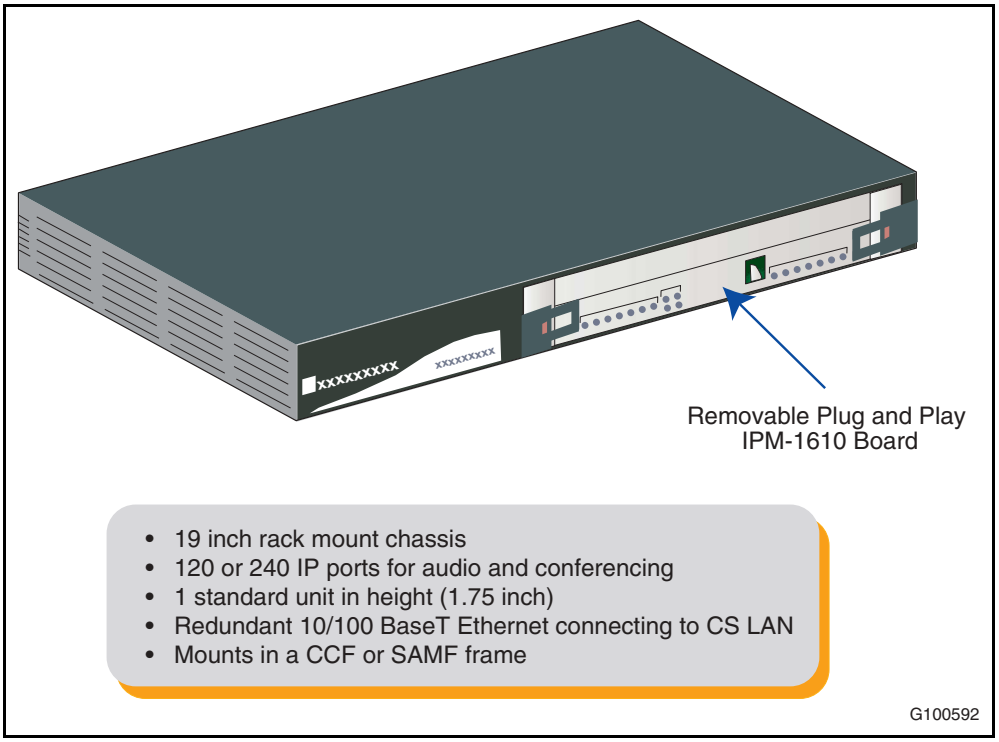


Table 20 describes the features offered by the Media Server 2010.

Table 20
Media Server 2010 features (Sheet 1 of 2)

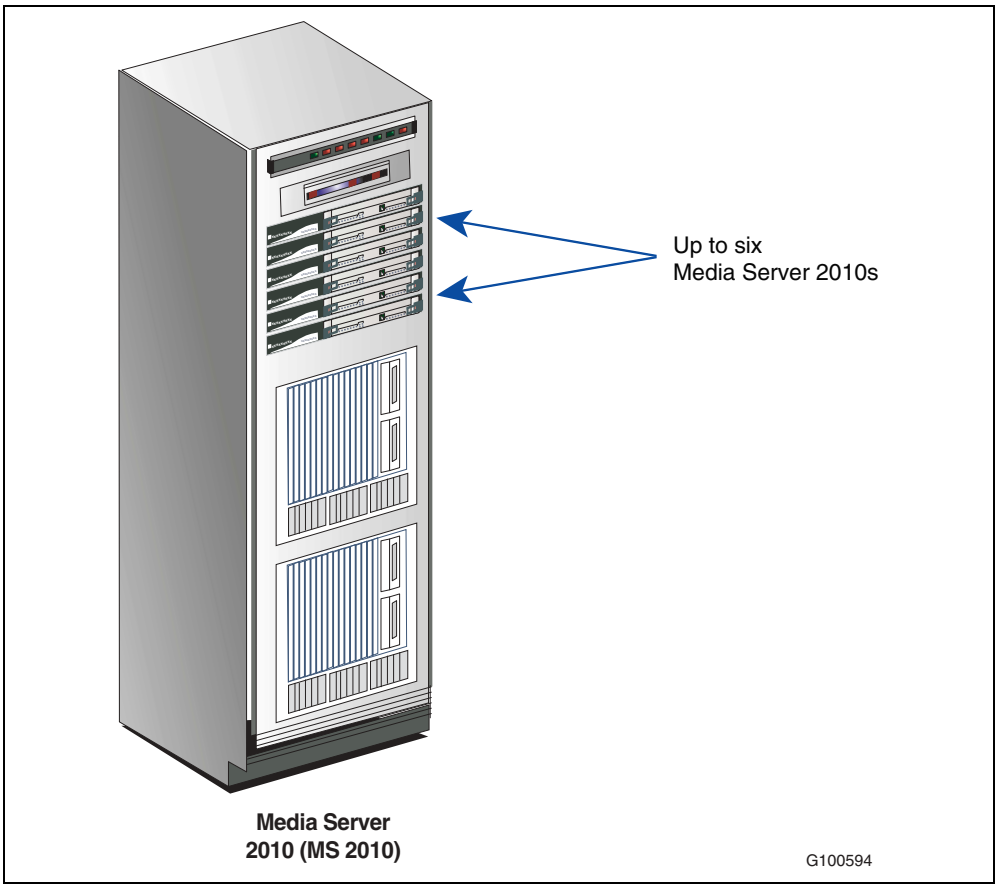
Feature	Description
Announcements	Play, Play Collect and Play Record.
Conferencing	Conferencing, Optional Deletion of Last Port, Play to Conference, Record from Conference and Monitor only Conference.
Flexible, Centralized Audio Management and Provisioning	Together with the Audio Provisioning Server (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.

Table 20
Media Server 2010 features (Sheet 2 of 2)

Feature	Description
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, etc.).
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 OA&M messaging – Audio files are transferred using FTP – IP connectivity is 10/100BaseT

Figure 27 illustrates Media Server 2010s in a SAMF Frame.

Figure 27
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 Communication Server 2100 enterprise network:

- Communication Server 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. T.38 Fax is also supported.
  - 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.

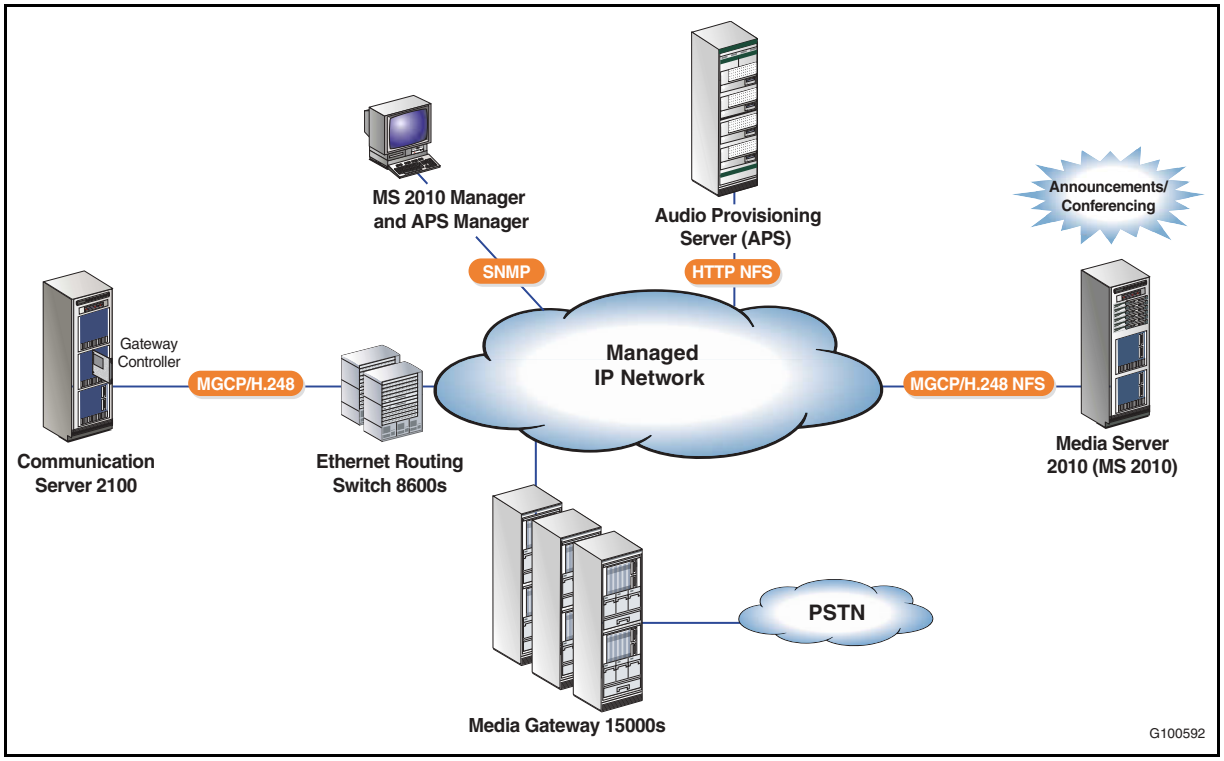
- The Audio Provisioning Server (APS) hardware and software. The APS has the following features:
  - — Provides a database to store all recorded audio segments. It can store over 100 hours of audio information.
  - — Uses a web-based interface to easily configure and assemble audio announcements for 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.

Figure 28 on page 117 illustrates a typical Communication Server 2100 network configuration with Media Server 2010s. The Communication Server 2100 directs the Media Server 2010 to play audio or provide conferencing resources. The Media Server 2010 interprets the messages sent by the Communication Server 2100 and retrieves the audio or initiates the conferencing request.

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 start-up of a node or on a periodic basis.

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

Figure 28
Media Server 2010s in a typical Communication Server 2100 configuration



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 the Media Server 2010's centralized audio management tool, the Audio Provisioning Server (APS). 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 functionality 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, 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 Communication Server 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

Table 21 lists documentation references for the Media Server 2010.

Table 21
Document references for the Media Server 2010

Document title	Document number
MS 2000 Series Basics	NN10323-111
MS 2000 Series Fault Management	NN10328-911
MS 2000 Series Configuration Management	NN10340-511
MS 2000 Series Performance Management	NN10331-711
MS 2000 Series Administration and Security	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. It 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 functionality and NAT traversal in generic terms. The second section describes the capabilities of the RTP Media Portal, which is the media proxy implementation supported by the Communication Server 2100 beginning in SE07.

This chapter contains the following sections:

- **Network Address Translation (NAT) functionality**
- **Nortel Real-time Transport Protocol 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's 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 in handling a typical call, each presenting an interface to one of the endpoints involved in the call. There is a connection 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 it 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 located 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 will otherwise be unable to 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). During call establishment, each gateway uses device/media control signaling to inform its GWC of the bearer capabilities it can support (for example, codecs and packetization rates). It 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 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 by means of 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's 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. And RTP/RTCP provides no address discovery mechanism that can be used to set up a two-way connection between media gateways.

Hence the need for a media proxy 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 Communication Server 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 middlebox(es), 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 functionality. In particular, it does not require gateways to be aware of network topology and middlebox 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 "Call Admission Control" on page 131.

Nortel Real-time Transport Protocol Media Portal

Overview

The Nortel Real-time Transport Protocol (RTP) Media Portal is a Gateway Controller-controlled media proxy. Its primary purpose is to support public address discovery for media streams that have been routed using a NAT. The media portal 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 Communication Server 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:

- It 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).
- It can act as a firewall to control the traversal of media streams into the private VoIP address domain used for the Communication Server 2100 CS LAN and large carrier-located gateways.

The RTP Media Portal is built on the SAM16 hardware platform and is controlled by Communication Server 2100 Gateway Controllers using the MGCP+ device/media control protocol.

The RTP Media Portal enables elements in the private network to securely communicate with elements in the public network in both directions. It 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.

Figure 29 on page 124 illustrates the network role of the RTP Media Portal in supporting NAT traversal between two media gateways located in private networks behind NAT devices.

Figure 29
RTP Media Portal and NAT traversal

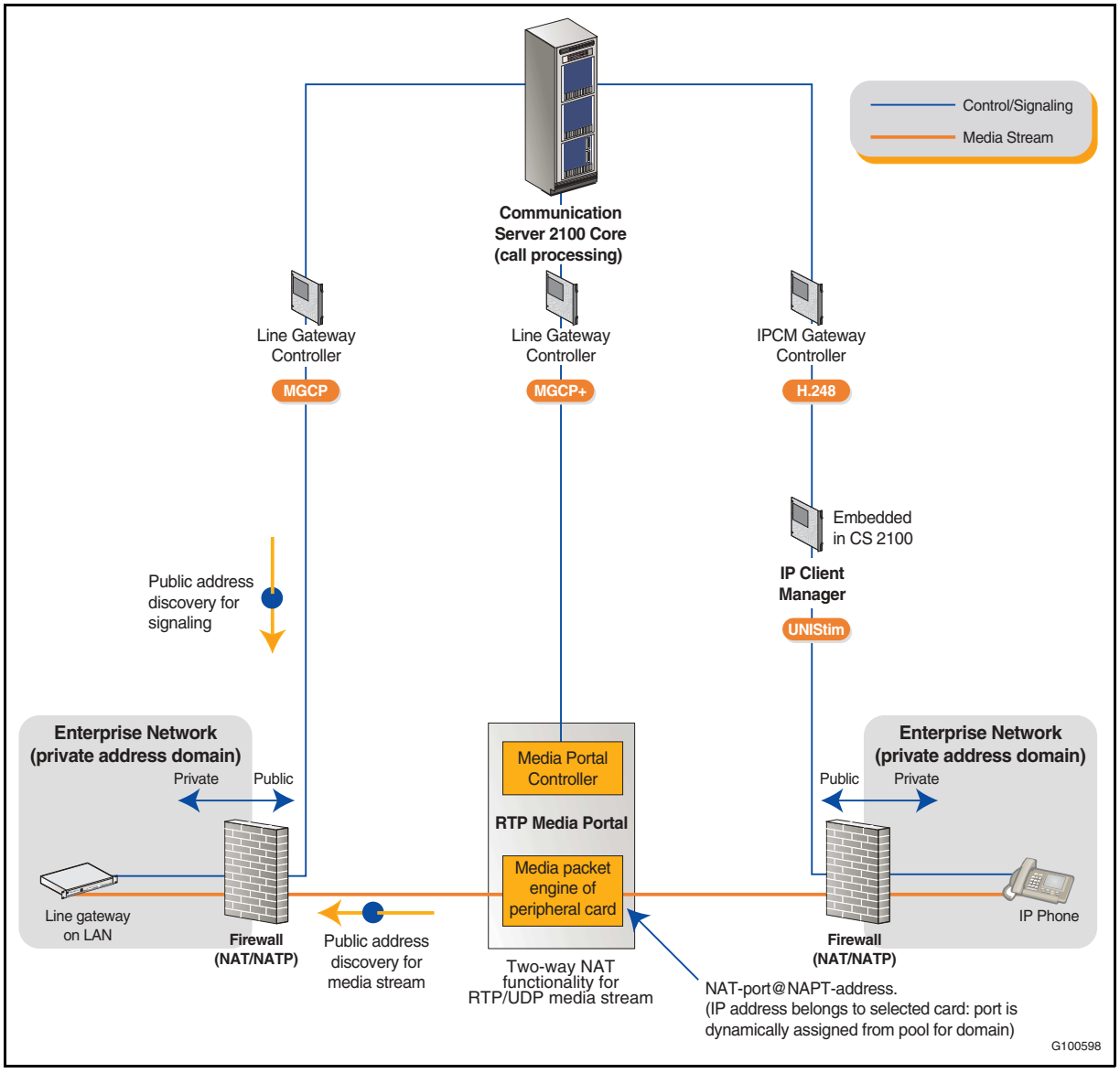
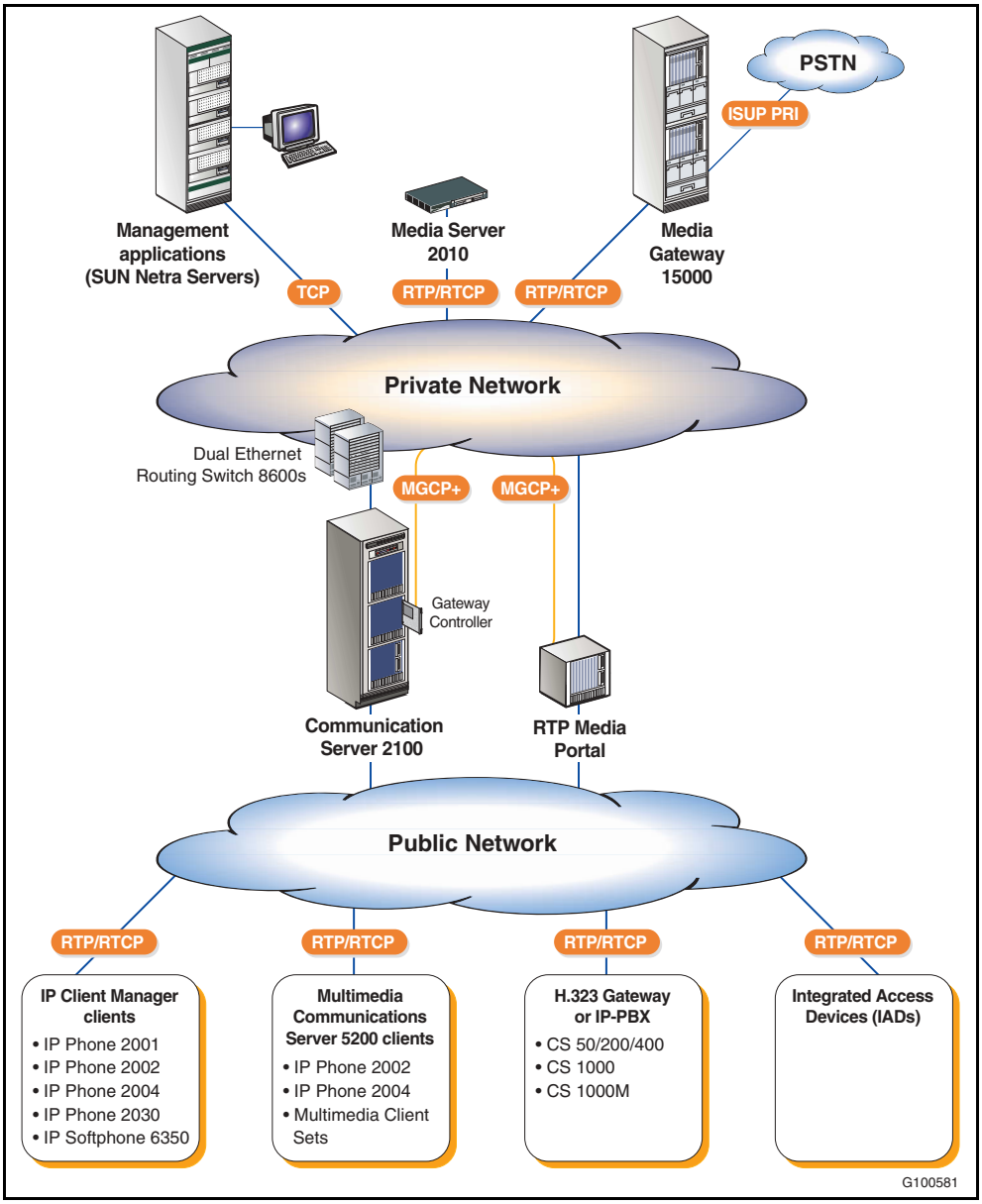


Figure 30 on page 125 shows an example of a RTP Media Portal network configuration.

Figure 30
RTP Media Portal in a Communication Server 2100 network



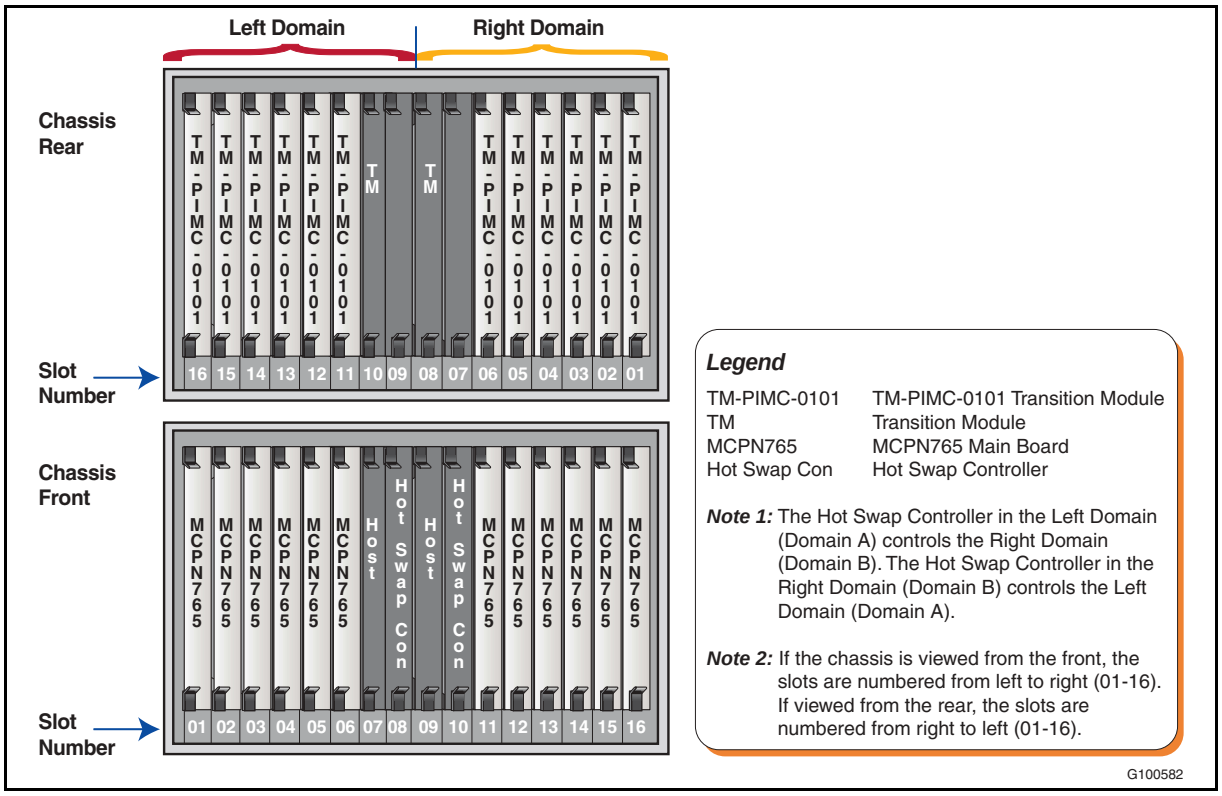
Note: In Figure 30, the public and private networks should not be confused with public and private IP addressing. In addition, the list of clients and gateways is not conclusive.

The clouds in the illustration represent two distinct networks. The “Private Network cloud” interacts with the “Public Network cloud” through the various edge components. In addition to extending service reach to obscured multimedia clients attached to the public network, the RTP Media Portal provides media-layer functionality for the RTP, RTCP and UDP transmissions that traverse between the public network and the private network.

Physical description

The RTP Media Portal resides on a Motorola CPX8216T platform which is a compact Peripheral Component Interconnect (cPCI) chassis design. The chassis provides the basic operating environment, such as power, cooling and mounting slots, required to house cPCI-based single-board computers. The CPX8216T partitions the chassis into two separate logical operating domains, dividing the chassis shelf into two half-shelves consisting of eight-slots each. An RTP Media Portal occupies a single chassis domain (side) on the CPX8216T. Therefore, a single CPX8216T can host two RTP Media Portal components (that is, one in chassis Domain A, the other in chassis Domain B). Figure 31 shows a typical card configuration used for the RTP Media Portal domains.

Figure 31
Card slots for the two different domains



The PCX8216T dual eight-slot architecture further refines the domain definition so that each chassis domain is dedicated to a host card (with an associated Transition Module in the rear), another slot is dedicated to the Motorola Hot Swap Controller (HSC) and the remaining six slots can be populated with what is commonly referred to as media blades (that is, Input/Output cards with an associated Transition Module in the rear).

Each chassis half shelf, and therefore each RTP Media Portal, 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:

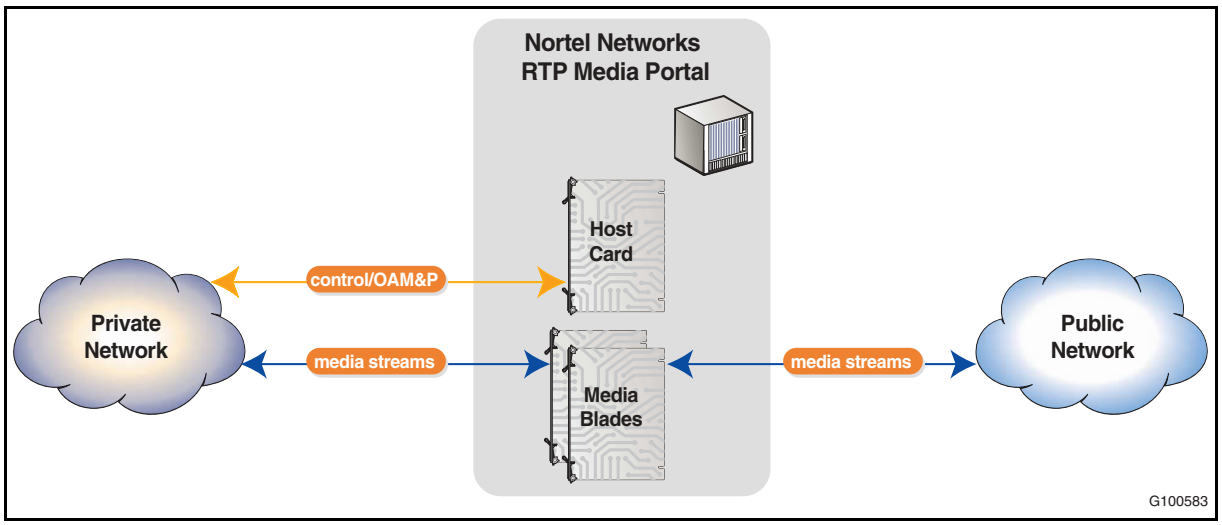
- mouse
- keyboard
- monitor

Network interfaces

The host card provides the MGCP+ control signaling and OAM&P data interface to/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 RTP Media Portal host card connects to the private network. The RTP Media Portal is an edge component that is dual-homed to the public network and the enterprise's private network. It is the media blades that span these two distinct networks (see Figure 32 on page 128).

Figure 32
RTP Media Portal interfaces



Cards

Table 22 describes the cards that are used in the RTP Media Portal.

Table 22
RTP Media Portal card summary (Sheet 1 of 2)

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 which provide connectivity to the private network. The connection carries control signaling and OAM&P 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 configuring the RTP Media Portal. The Ethernet connections provide the following: • MCGP+ control signaling to communicate with the Communication Server 2100. • OAM&P data to the Management Module over TCP.

Table 22
RTP Media Portal card summary (Sheet 2 of 2)

Card	Description
Media blades	Network interfaces on each of the media blades (MCPN765) in the RTP Media Portal provide a path for media streams to/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:*** These I/O cards must always be deployed in pairs. There is a 1:1 relationship 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 obscured 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.

OAM&P strategy

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

For more information about system management, see “OAM&P for Communication Server 2100 networks” on page 151.

References

Table 23 shows where you can find more detailed information about the RTP Media Portal.

Table 23
Documentation references

Document title	Document number
Carrier Voice over IP RTP Media Portal Basics that contains the following modules: • Overview • Upgrades • Fault management • Configuration management • Accounting management • Performance management • Security and administration	NN10367-111
Carrier Voice over IP System Management Console User Guide – describes the centralized location for OAM&P management of the RTP Media Portal.	NN10370-111

Call Admission Control

New in SE08

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 are unable to seize trunk circuits. Accepting that some new calls will not be 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. It 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 newly set up calls. Accepting some degradation in voice quality is the price of placing no restrictions on the setting up of 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 or not a new call being set up will degrade 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 would encounter bandwidth restrictions and should, therefore, not be set up in the first place.

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. For the purposes of this document, it is assumed that bandwidth in the core network is effectively unlimited. Typically, however, there will be access and enterprise networks connected to the core network. It is not the responsibility of the network operator to engineer 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 to support Virtual Call Admission Control (VCAC):

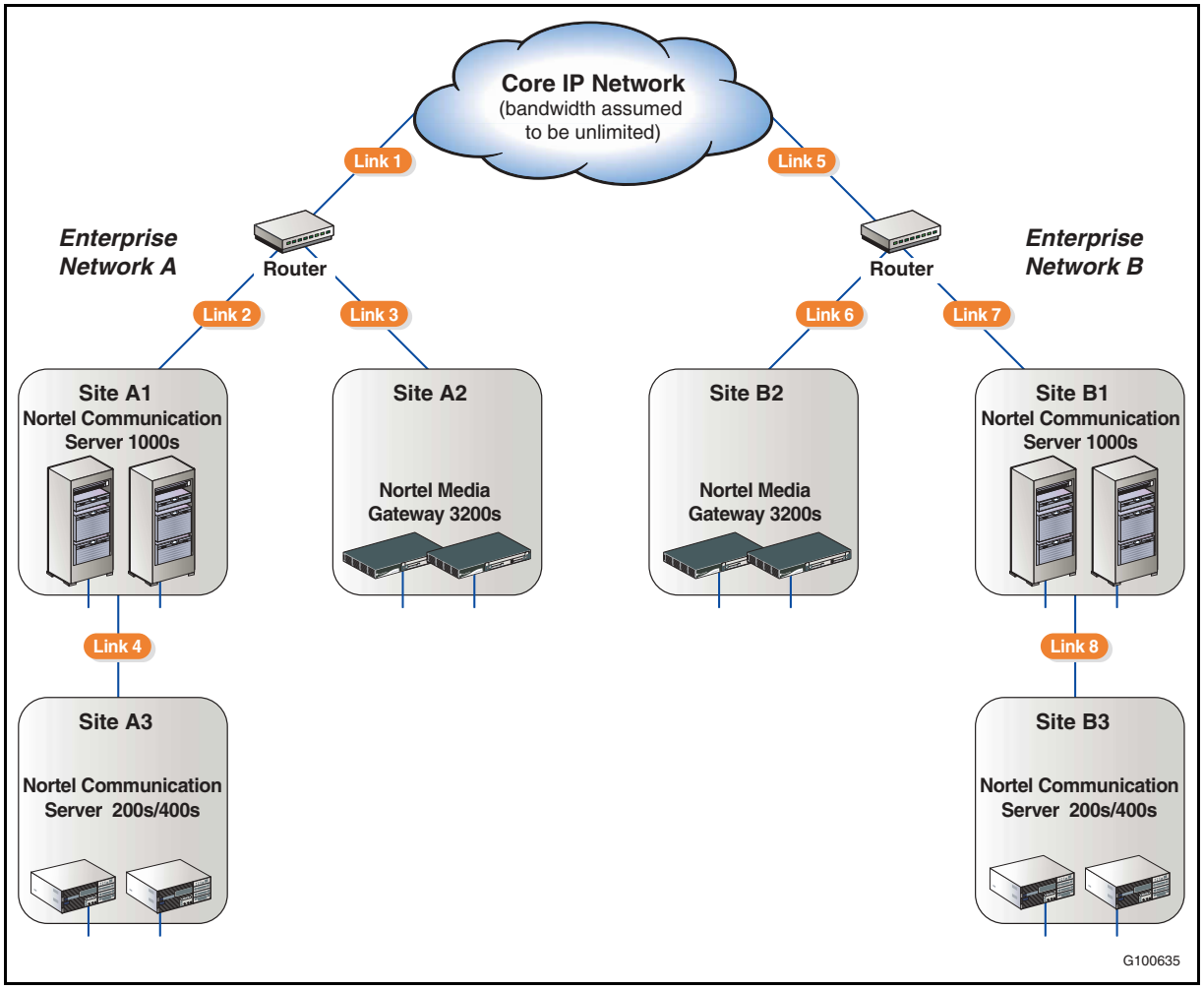
- A logical model of the overall network structure identifying which Limited Bandwidth Links (LBLs), if any, must be traversed to reach a given media gateway endpoint.
- A mechanism for capturing this network structure information in a standardized way and making it available to the Communication Server 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 Communication Server 2100 to cancel post-dial, pre-ringing calls that would overload a segment of the packet network.

Logical network model

Access and enterprise networks can be viewed 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 Figure 33 on page 133).

Figure 33
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 Figure 33, 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 has purchased 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:

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

Gateways can be added to any Limited Bandwidth Link in the logical model. A Limited Bandwidth Link can have any number of gateways hanging off it. This is usually 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/finish in the core network.

Once a call is made, the Communication Server 2100 identifies the Limited Bandwidth Links and Network Address Translations along the speechpath between the two endpoints and calculates if there are sufficient resources 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 *GWC Configuration Management*, NN10205-511.

Take, for example, a call between a gateway on Site A3 and a gateway on Site A2. This call will use 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 Link(s), if any, need to be traversed to reach a given gateway. To enable Communication Server 2100 Gateway Controllers to determine whether bandwidth limitations mean that Call Admission Control should be applied for a call attempt, each Gateway Controller stores the following data:

- Information about all the Limited Bandwidth Links in the network.
- Information about which Limited Bandwidth Links(s), 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. It examines the negotiated codec and processing time (ptime) for the call and checks that each Limited Bandwidth Link in the path has sufficient resources for the call to be set up. If there are sufficient resources, the call proceeds as normal. If there are insufficient resources 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 has not reached 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/decrease the value away from the real “bits on the wire” value. This also allows a customer to simply 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 it 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 will 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 easier for technicians to provision Virtual Call Admission Control:

- The creation of a provisioning capability on Succession Element and Subnetwork Manager (SESM) for the Virtual Call Admission Control functionality: 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 regarding the provisioning of Limited Bandwidth Link middleboxes:

- Provides (CORBA) interfaces and a GUI panel to allow the user to change, delete the Limited Bandwidth Link middleboxes.
- Provides an interface that allows the user to navigate through 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 regarding the provisioning of Resource Usage:

- Creates a new table in the database for Resource Usage table data.
- Provides (CORBA) interfaces and a GUI panel to allow the user to add, change and delete the Resource Usage table data.
- 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/display Resource Usage table data as appropriate (for example, select Resource Usage table entries required by a given Gateway Controller).

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 look-up table for use at Internet transparency call set-up 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 have been added:

- add/change/delete/query operations for Network Address Translation middleboxes
- add/change/delete/query operations for Limited Bandwidth Link middleboxes
- add/change/delete/query operations for media proxies
- add/change/delete/query operations for the Resource Usage look-up 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, this causes a problem, 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 being behind one internet transparency middlebox to another. To complicate matters, an IP Client Manager can also serve multiple enterprises; this 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 this 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.

This feature enhances the Virtual Call Admission Control provisioning functionality 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 Communication Server 2100 XA-Core and Compact systems.

References

Table 24 shows where you can find more detailed information about Virtual Call Admission Control.

Table 24
Documentation references

Document title	Document number
GWC Basics	NN10189-111
GWC Configuration Management	NN10205-511
OSSGate Users Guide	NE10004512
For more information about the CS 2000 Management Tools GUI and the Gateway Controller Element Manager, see “OAM&P for Communication Server 2100 networks” on page 151.	N/A

Ethernet Routing Switch 8600

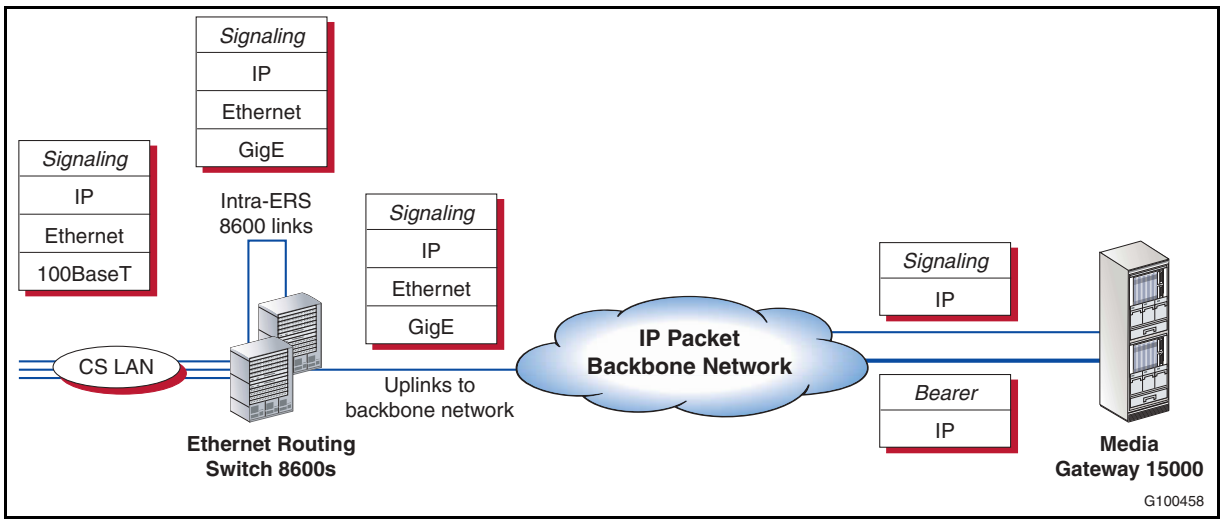
Description

The Ethernet Routing Switch 8600s (that is, the 8606 and 8610) described in this chapter are used in the SE08 Communication Server 2100 network. Although the Ethernet Routing Switch 8600 is a product in its own right rather than a Communication Server 2100 component, the Ethernet Routing Switch 8600 is an integral part of the Communication Server 2100 Communication Server Local Area Network (CS LAN). It is therefore described in this document as if it were a Communication Server 2100 component.

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

The CS LAN not only supports intra-Communication Server 2100 communication, but also provides the interface between the CS LAN and the external managed IP network (see Figure 34 on page 142).

Figure 34
Connectivity for an IP backbone network



The Ethernet Routing Switch 8600 passes signaling and management messages between the Network Elements. It provides control messages between the Communication Server 2100 and gateways through the Gateway Controller and other components. It supports the following interfaces:

- Gigabit Ethernet
- Multiport 10/100BaseT

The Ethernet Routing Switch 8600 also supports a redundant configuration to connect the following components:

- Communication Server 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)
  - Preside Multiservice Data Manager (PMDM)
  - SuperNode Data Manager (SDM)/Core and Billing Manager (CBM)
  - Preside Management Solutions (PMS)
- Optivity

Note: Two Ethernet Routing Switch elements are required. Deployment of the two Ethernet Routing Switch 8600 elements in separate frames is NEBS compliant, or you can select to deploy both elements in a single frame as a low-risk, non-NEBS tested alternative.

In order to provide secure access to different functions, the Ethernet Routing Switch 8600 is used to configure the CS LAN as a number of Virtual LANs (VLANs) as shown in Figure 35 on page 144. The CS LAN Ethernet Routing Switch 8600s support three trusted VLANs:

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

The Ethernet Routing Switch 8600s also provide access to two types of external communication:

- Intranet connectivity such as access from separate (untrusted) LANs for OAM&P clients such as a Network Management System (NMS).
- Backbone network connectivity through the Access LAN in the form of GigE uplinks to the backbone packet network. This is used for signaling between Communication Server 2100 Gateway Controllers and their remote media gateways, and for peer-to-peer signaling between Communication Server 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). This is useful in preventing IP traffic from lesser trusted nodes/networks from reaching critical CS LAN elements.

Figure 35 on page 144 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 OAM&P and CallP VLANs.

Figure 35
CS LAN Ethernet Routing Switch 8600 VLAN configuration

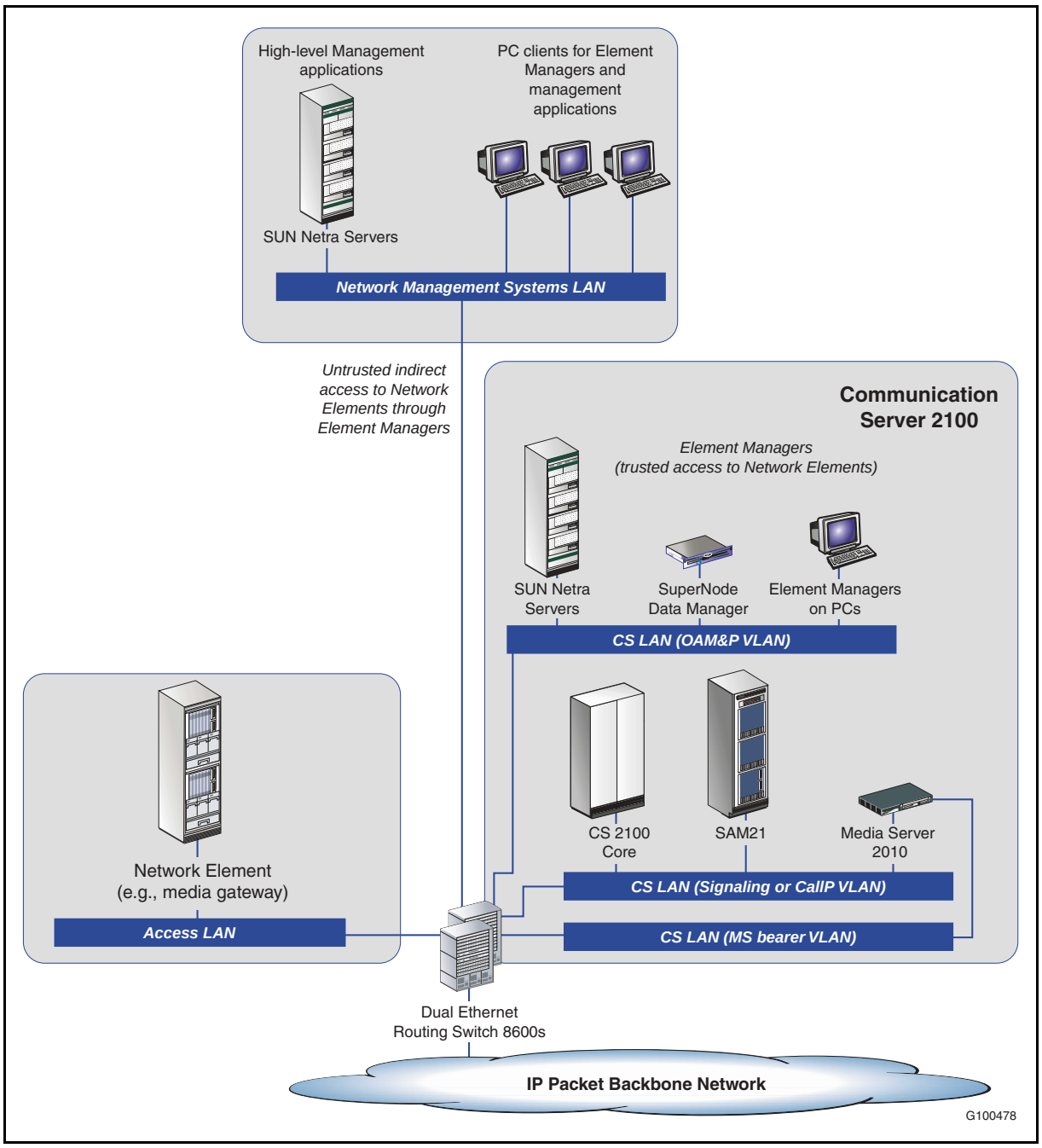
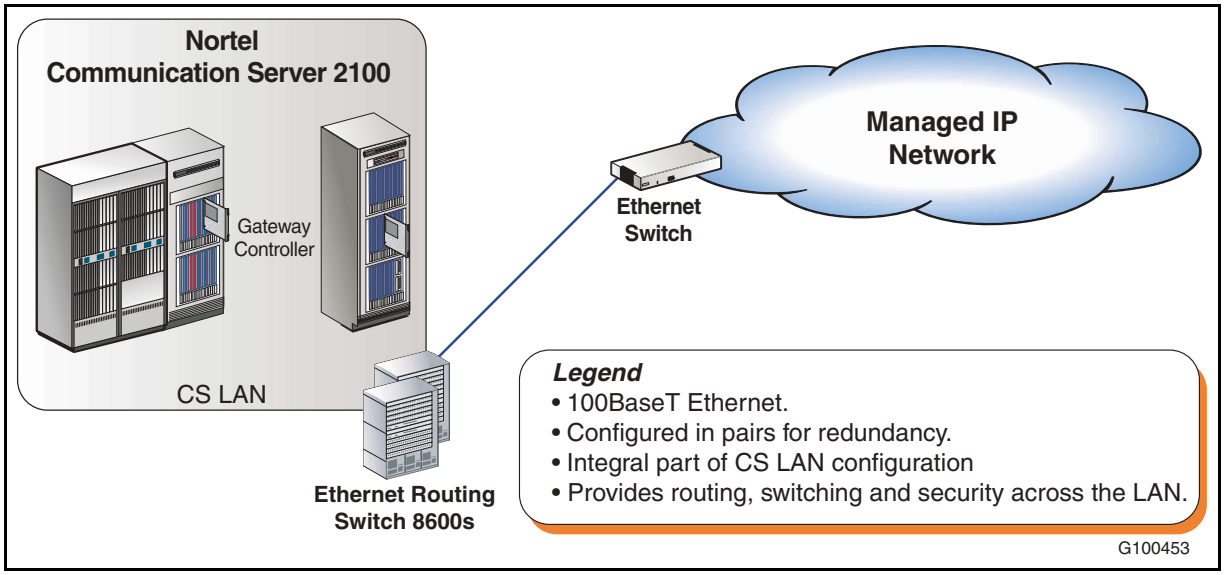


Figure 36 on page 145 shows an example of the Ethernet Routing Switch 8600 in a network configuration.

Figure 36
CS LAN Ethernet Routing Switch 8600 network configuration



IP addressing

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

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

Each Ethernet Routing Switch 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 Ethernet Routing Switch 8600, along with other Ethernet Routing Switch 8000 series switches, provides filtering capabilities that allow the switch to filter out non-call related traffic to prevent that traffic from interfering with Communication Server 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 Ethernet Routing Switch 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 Ethernet Routing Switch 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 DiffServe network, IP filtering allows you to assign QOS levels that can be based on a range of filtering conditions.

CS LAN connections for Communication Server 2100 components

Within a Communication Server 2100 CS LAN, communication is based on IP over 100BaseT Ethernet. Table 25 summarizes how the 100BaseT Ethernet ports provided by the dual Ethernet Routing Switch 8600s are used to support CS LAN connections with other components.

Table 25
CS LAN connections supported by dual Ethernet Routing Switch 8600s (Sheet 1 of 3)

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 Ethernet Routing Switch 8600, but not to the other. During normal operation, both High-capacity Input/Output Processors are active and operate in load-balancing mode.

Table 25
CS LAN connections supported by dual Ethernet Routing Switch 8600s (Sheet 2 of 3)

Component	100BaseT terminations provided by	Connection characteristics
Call Agent	Two Ethernet ports on NTRX51G2 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 Ethernet Routing Switch 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 Ethernet Routing Switch 8600s.
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 Ethernet Routing Switch 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 Ethernet Routing Switch 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 Ethernet Routing Switch 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 Ethernet Routing Switch 8600s, but not the other.
OAM&P 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 Ethernet Routing Switch 8600s, but not the other.

Table 25
CS LAN connections supported by dual Ethernet Routing Switch 8600s (Sheet 3 of 3)

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 Ethernet Routing Switch 8600s, but not the other.
Preside Multi-service 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 Ethernet Routing Switch 8600s, but not the other.

Requirements

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

Each CS LAN is based on two complementary Ethernet Routing Switch 8600s housed in a single cabinet, each in a separate shelf/chassis and provisioned as summarized in Table 26.

Table 26
Ethernet Routing Switch 8600 hardware (Sheet 1 of 2)

Unit	Function	Provisioning
8010co chassis	Provides 10 slots for housing Ethernet Routing Switch 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	Ethernet Routing Switch 8600 Central Processing Unit (CPU) and switching fabric.	One per chassis.

Table 26
Ethernet Routing Switch 8600 hardware (Sheet 2 of 2)

Unit	Function	Provisioning
8632TXE	Supports: • 32 Ethernet 100BaseT ports • two Gigabit Ethernet ports	Two per chassis, supporting a minimum total of eight GigE ports for the CS LAN, allocated as follows: • Four GigE ports are used for fully redundant inter-chassis communication using at least two GigE links. • For IP telephony, at least two GigE 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 GigE 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 Ethernet Routing Switch 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 Ethernet Routing Switch 8600:

- Supports DS1 using demux.
- Supports DS3.

References

Table 27 shows where you can find more detailed information about the Ethernet Routing Switch 8600.

Table 27
Documentation references (Sheet 1 of 2)

Document title	Document number
Getting Started Ethernet Routing Switch 8000 Series Software Release 3.7	313189-D Rev 00
Managing Platform Operations and Using Diagnostic Tools Ethernet Routing Switch 8000 Series Software Release 3.7	315545-C Rev 00

Table 27
Documentation references (Sheet 2 of 2)

Document title	Document number
Configuring Network Management Ethernet Routing Switch 8000 Series Software Release 3.7	314723-C Rev 00
Configuring QoS and IP Filtering Ethernet Routing Switch 8000 Series Software Release 3.7	316433-C Rev 00
Configuring IP Routing Operations Ethernet Routing Switch 8000 Series Software Release 3.7	314720-D Rev 00
Release Notes for the Ethernet Routing Switch 8000 Series Switch Software Release 3.7	313177-A Rev 00
System Messaging Platform Reference Guide Ethernet Routing Switch 8000 Series Software Release 3.7	315015-C Rev 00
Important Information about the 8600 Series Switch Modules	316340-B Rev 00
Configuring and Managing Security Ethernet Routing Switch 8600 Software Release 3.7	314724-C Rev 00
Packet Trunk-IP (PT-IP) Engineering Rules	SEB-02-10-001

OAM&P for Communication Server 2100 networks

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

- **Logical OAM&P architecture**
- **Physical OAM&P architecture**
- **Nortel Core and Billing Manager**
- **Nortel Integrated Element Management System**
- **Fault management**
- **Configuration management**
- **Accounting**
- **Performance management**
- **OAM&P security**

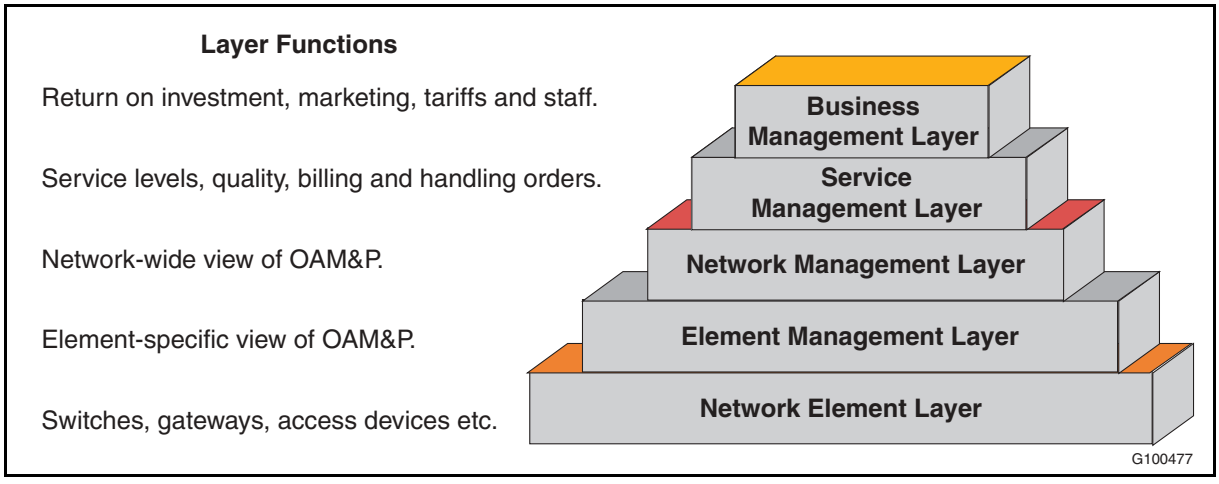
Logical OAM&P architecture

OAM&P applications can be thought of as belonging to a hierarchy (see Table 28).

Table 28
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.
Element Management Layer (EML)	Above the Network Element Layer, at the lowest management level, there is an Element Manager (EM) application 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).

Figure 37
Telecommunications Management Network hierarchy



Nortel provides Element Managers for Communication Server 2100 components and a number of Network Management Layer applications that are multi-node 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.

SE08 supports the following Element Managers:

- 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, Preside Multi-service Data Manager (PMDM) for Media Gateway 15000s)
- Element managers for each type of line media gateway (for example, IPCM Manager)

SE08 supports the following OAM&P applications:

- 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 Preside Multi-service Data Manager

Physical OAM&P architecture

Platforms

SE07 introduced the Integrated Element Management System (IEMS) that provides an integration point for various diverse EMS platforms that comprise the Nortel Communication Server 2100 management solution. OAM&P functionality for Communication Server 2100 networks is provided by a range of specialized applications running on a number of different hardware platforms that this section describes. It is important to 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” on page 162.

- ***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 Communication Server 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 functionality. For more information, see “Nortel Core and Billing Manager” on page 159.

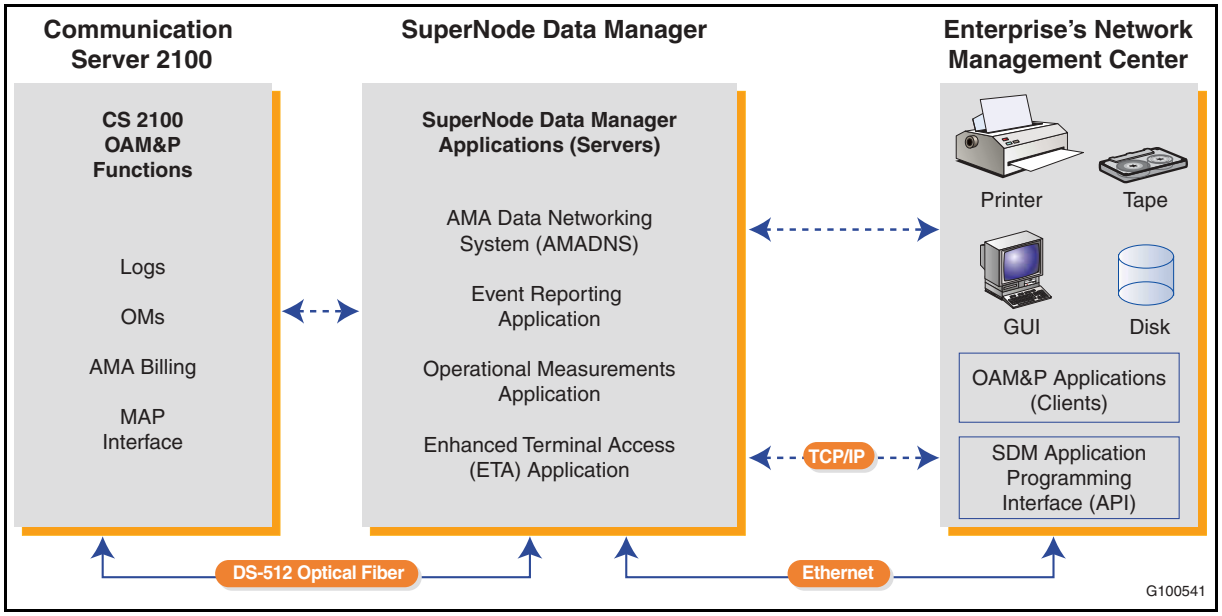
  There are several SuperNode Data Manager applications, each providing support for a different OAM&P function. These applications use the client/server model, with the SuperNode Data Manager acting as the server. Application clients run on the organization’s workstations, which can be centrally located.

  Peer-to-peer communication between clients and SuperNode Data Manager applications is supported by means of 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 means of a managed IP network.

Figure 38 illustrates the role of SuperNode Data Manager applications in standardizing access to Communication Server 2100 OAM&P functions.

Figure 38
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 Communication Server 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

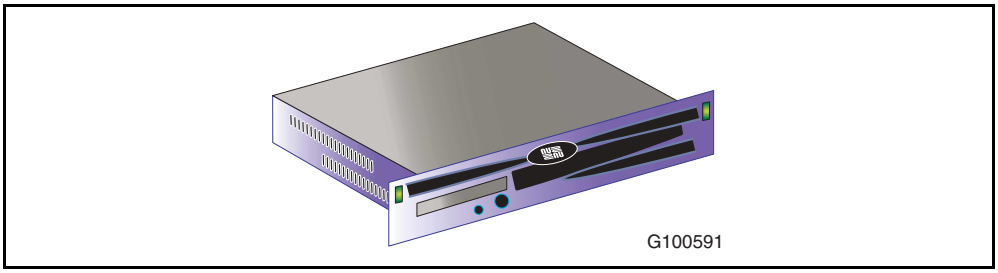
- Preside Multi-service Data Manager (PMDM) for Media Gateway 15000s

— 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 Preside Multi-service Data Manager

Figure 39 shows a line drawing of the Sun Netra 240.

Figure 39
Sun Netra 240



- ***Windows PC***

The following Element Manager runs on a dedicated Windows PC:

— IPCM Manager

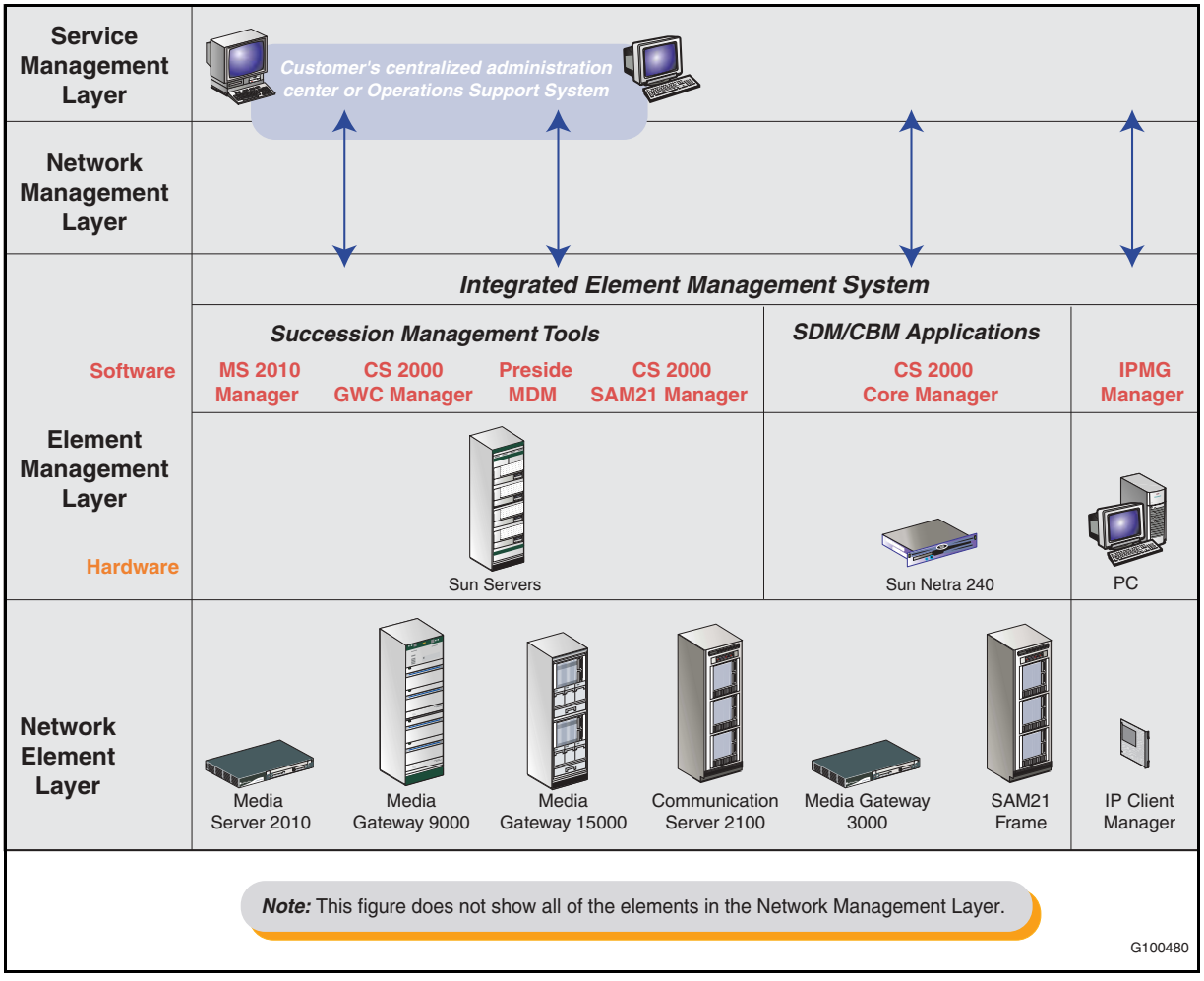
— Ethernet Routing Switch 8600 Device Manager

The following additional components are used for OAM&P:

- 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 Communication Server 2100 for Nortel support, using a high-bandwidth TCP/IP connection through the external internet for patching, emergency support and problem solving.

Figure 40 maps the physical component and software applications into the Telecommunications Management Network hierarchy.

Figure 40
Management components and software applications summary



Client workstations

Table 29 lists the platform and method of invocation for each client application.

Table 29
Client platforms

Name	Invocation	Platform	
		PC	SUN
SAM Clients	Desktop		☆
SAM21 Manager	Desktop	☆	☆
Succession 2000 Management Tools Selector	Browser (HTML)	☆	☆
Gateway Controller Manager	Browser (JWS)	☆	☆
Media Server 2010	Browser (JWS)	☆	☆
Line Maintenance Manager	Browser (JWS)	☆	☆
Node Provisioning	Browser (JWS)	☆	☆
Network Patch Manager	Browser (HTML)	☆	
Trunk Provisioning	Telnet/STELNET	☆	☆
Line Provisioning	Telnet/STELNET	☆	☆
Nodes Provisioning	Telnet/STELNET	☆	☆
Audio Programming System Manager	Browser	☆	
STORM Manager	Browser (Proxy)	☆	☆
Call Agent Manager	Telnet (Proxy)	☆	☆
Media Device Manager/Management Data Provider	Desktop (X.11)		☆
Device Manager	Desktop (Java)	☆	☆

References

Table 30 shows where you can find more detailed information about OAM&P.

Table 30
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)	
Succession Fault Management Logs Reference	NN10275-909
Communication Server 2100 OMs (describes OMs by component)	
Succession Performance Management Operational Measurements Reference	NN10264-709
Backup procedures (describes backups and restorations by component)	
ATM/IP Security and Administration	NN10402-600
Upgrade procedures (describes upgrades by component)	
IP Solutions Upgrades	NN10344-450

Nortel Core and Billing Manager

Introduced in SE07, the Core and Billing Manager (CBM) consolidates Fault, Configuration, Accounting, Performance and Security (FCAPS) for the Communication Server 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 OAM&P applications through LAN/WAN Ethernet connectivity.

SuperNode Data Manager applications have been 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 Integrated Element Management System consolidation plan using the latest carrier-grade Sun platform, the Netra 240.
- Delivers the same applications as the SuperNode Data Manager suite.
- Provides the ability to be expandable 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 centralized security.
- Maximizes available resources and paves the way for unmanned offices by supporting a remote centralized 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 OAM&P 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 Communication Server 2100 XA-Core High-capacity Input/Output Processor (HIOP) card or Communication Server 2100 Compact.
- An Ethernet connection to the operations intranet for communications with the Network Management System (GigE IP).

The Core and Billing Manager provides most of the functionality 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 which results in one platform type and common spares for all OAM&P 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 gigabytes RAM
- three PCI slots
- Digital Video Disk (DVD)-Read/Write (RW) drive (removable)
- four GigE 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. It 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 OAM&P 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. It can provide up to 300,000 records per hour of sustained billing throughput (100 bytes per record).

References

Table 31 shows where you can find more detailed information about the Core and Billing Manager.

Table 31
Documentation references

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

Nortel Integrated Element Management System

Overview

Nortel is delivering 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 the Integrated Element Management System consolidates performance, fault and security functions for the entire VoIP network which reduces cost and integration complexity. Element Manager configuration modules and the billing management module are easily accessed using the Integrated Element Management System. The strategic vision for the Integrated Element Management System includes unification of the configuration user interfaces further simplifying management of VoIP Network Elements.

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

Introduced in SE07, the Integrated Element Management System Client Interface is a powerful human interface to Communication Server 2100 OAM&P components. The Integrated Element Management System presents complex enterprise management information in clear and easily understandable Graphical User Interfaces (GUIs). Acting as a central integration point, the Integrated Element Management System provides access to the following items of the management solution:

- Element Management System platforms
- Element Managers (EMs)
- Management Applications
- Network Elements (NEs)

The Integrated Element Management System provides a centralized location to view, normalize and forward faults, and a common maintenance interface launch point to access the various devices in a Communication Server 2100 network.

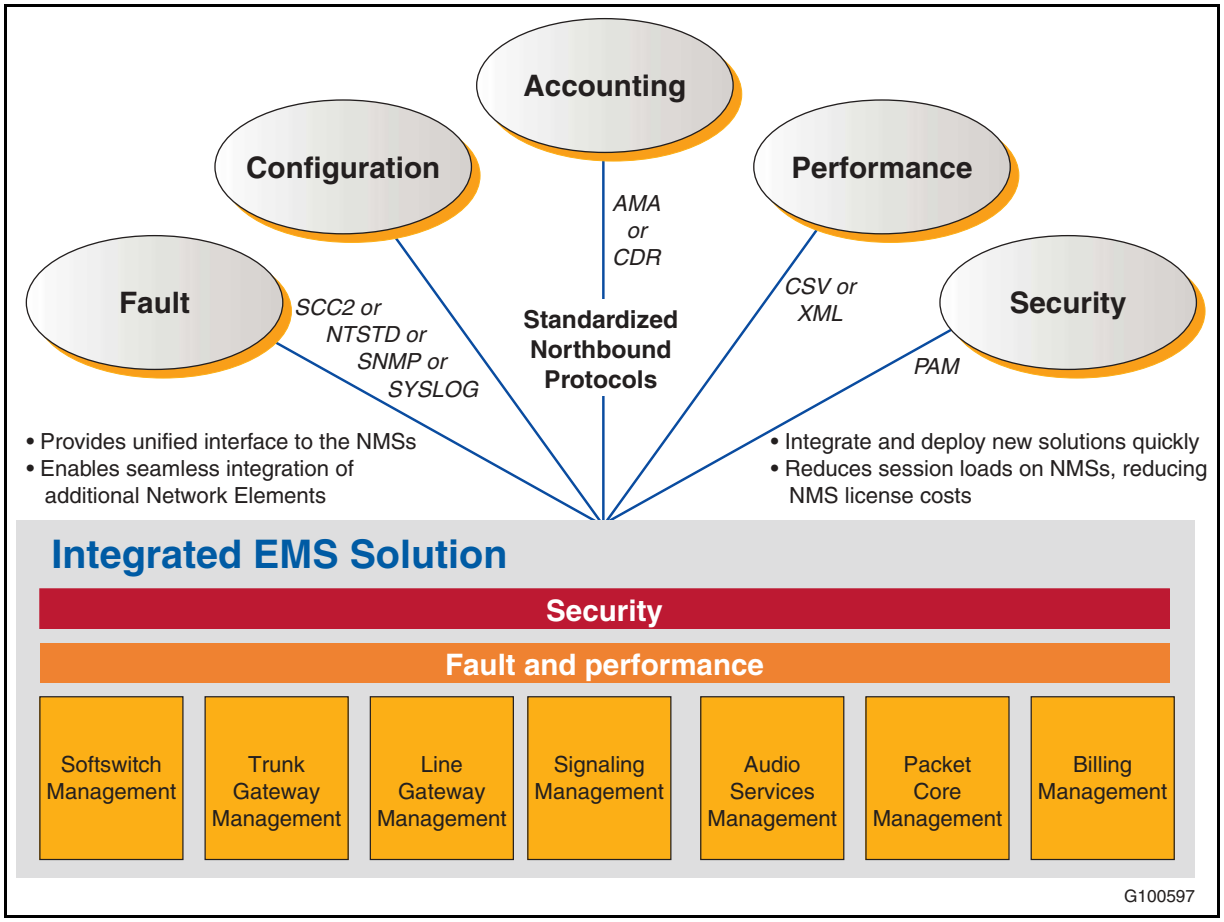
The high-level functional capabilities of the Integrated Element Management System include the following:

- 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

Figure 41 on page 164 summarizes the benefits that the Integrated Element Management System provides.

Figure 41
Integrated Element Management System benefits



In response to the feedback from the marketplace, requesting solutions requiring less integration and to drive more simplicity, the Integrated EMS is designed to operate as follows:

- Reduce Network Management System (NMS) integration complexity and resource requirement.
- Construct a framework to consolidate Element Managers and in the process reduce footprint, 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.

The Integrated Element Management System consolidates EMS functions, including configuration and toolsets from the individual EMS modules, and in the process drives simplification.

Figure 42 shows the initial interface that appears when launching the Integrated Element Management System.

Figure 42
IEMS initial interface

Client access modes

A technician can access the Integrated Element Management System client through either the full-featured Java Web Start (JWS) interface or a lighter-weight HTML client. Depending on the circumstances, each of these access modes has its advantages. While the Java Web Start client provides greater functionality, it does impose greater resource demands on the client platform and also requires more launch time. The HTML interface is better suited for lower-speed client connections.

Java Web Start Client interface

Table 32 on page 166 describes the primary functional panels available with the Java Web Start Client.

Table 32
Java Web Start Client GUI panel items

Item	Description
Menu bar	The menu bar contains the labels of drop-down menus that are attached to it. A separator is a horizontal line drawn on a menu. Separators are used to separate one set of operations from another. The menu bar contains drop-down 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 Integrated Element Management System Java Web Start Client. The menus and menu items appear or disappear dynamically according to the object selected in the Integrated Element Management System 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, which indicates 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 is moveable and floatable. Buttons appearing on the toolbar are context sensitive to the object selected in the Integrated Element Management System Java Web Start Client. They appear or disappear dynamically according to the object selected in the Integrated Element Management System Java Web Start Client.
Tree	The system uses a tree to display a set of the Integrated Element Management System 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 is composed of 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 Integrated Element Management System 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 mouse pointer is pointed on 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. It indicates 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 during the loading of the product.
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

Table 33 describes the primary functional panels available with the HTML Web Client.

Table 33
HTML Web GUI panel items

Item	Description
Module tabs	Module tabs provide easy navigation of various features in a module of the Integrated Element Management System. The following items are the various modules in the Integrated Element Management System 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 which 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 which are useful when you need to perform an operation over multiple elements in a view. For example, in the Inventory view, use options on clicking the icon 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 drop-down 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 Integrated Element Management System 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 the Integrated Element Management System

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

Launching applications for Element Managers

Table 34 lists the Element Managers with corresponding launch applications based on the Command Line User Interface or GUI applications.

Table 34
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 Integrated EMS Server			
Preside Multi-Service Data Manager (MDM)	6.2	Command Line	Command Line
IPCM Manager	6.2/7.0	Command Line	Launch Command Line
IPCM Manager node	6.2/7.0	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)	6.2/7.0	Core Manager Maintenance MAPCI	Launch Core Mgr Maintenance Launch MAPCI Session
Gateway Controller (GWC)	6.2/7.0	GWC Manager (CS 2000 Management Tools) GWC Manager Network View	GWC Mgr (CMT) GWC Mgr Network View
SAM21	6.2/7.0	SAM21 Manager	SAM21 Mgr GUI
Media Gateway 9000 (MG 9000)	6.2 7.0	MG 9000 Manager 6.2 MG 9000 Manager 7.0	MG9k Manager MG9K Manager
Preside 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	6.2/7.0	IPCM Manager	Launch CICM Manager

Launching applications for platforms

Table 35 lists the platforms with corresponding launch applications based on the Command Line User Interface or GUI applications.

Table 35
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			
Multi-service Data Manager	6.2/7.0	Command Line	Command Line
Succession Server Platforms Foundation Software (SSPFS)	6.2/7.0	Command Line Restart SSPFS Restart IEMS	Command Line Restart SSPFS Restart IEMS
SSPFS unit	6.2/7.0	Command Line Restart SSPFS	Command Line Restart SSPFS
SuperNode Data Manager (SDM)	6.2/7.0	Command Line	Command Line
GUI applications			
SSPFS	6.2/7.0	Servman Application Status SWACT Cluster	Servman Application Status SWACT Cluster
SSPFS Unit	6.2/7.0	Servman Application Status SWACT Cluster	Servman Application Status SWACT Cluster

Launching applications for EMS applications

Table 36 lists the EMS applications with corresponding launch applications based on the Command Line User Interface or GUI applications.

Table 36
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	6.2/7.0	BPT Command Line	Launch BPT CLUI
QoS Collector Application	6.2/7.0	Command Line	Launch Command Line
GUI applications			
Line Maintenance Manager	6.2/7.0	Line Maintenance Manager	Line Maintenance Manager (LMM)
Trunk Maintenance Manager	6.2/7.0	Trunk Maintenance Manager	Trunk Maintenance Manager (TMM)
OSSGate	6.2/7.0	OSSGate BPT Servlet	Launch OSSGate Launch BPT Servlet
Network Patch Manager	6.2/7.0	Network Patch Manager	Network Patch Manager (NPM)
Audio Provisioning Server	6.2/7.0	APS Manager (CS 2000 Management Tools) APS Audio Configuration Tool	APS Manager (CMT) APS Audio Configuration Tool

Launching applications for Network Elements

Table 37 lists the NEs with corresponding launch applications based on the Command Line User Interface or GUI applications.

Table 37
NES with corresponding application launched (Sheet 1 of 2)

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			
Ethernet Routing Switch 8600	6.2/7.0	Command Line	Command Line
STORM	6.2/7.0	Command Line	Launch Command Line
Media Server 2010	6.2/7.0	Command Line	Command Line
Call Agent Core managed by Core Manager	6.2/7.0	Command Line	Call Agent Platform Command Line
Call Agent Platform managed by Core Manager	6.2/7.0	Command Line	Call Agent Platform Command Line
GWC NE managed by GWC Manager	6.2/7.0	Command Line	Launch Command Line
Media Server 2010	6.2/7.0	Command Line	Command Line
Session Server	6.2/7.0	Command Line	Command Line
Session Server unit	7.0	Command Line	Command Line
IPCM NE	6.2/7.0	Command Line	Launch Command Line
IPCM NE node	6.2/7.0	Command Line	Launch Command Line
GUI applications			
Ethernet Routing Switch 8600	6.2	Ethernet Routing Switch 8600 Device Manager	Ethernet Routing Switch 8600 Device Manager
STORM	6.2/7.0	STORM Manager	STORM Manager
Call Agent Core managed by Core Manager	6.2/7.0	MAPCI Session	Launch MAPCI Session
Call Agent Platform managed by Core Manager	6.2/7.0	MAPCI Session	Launch MAPCI Session

Table 37
NES with corresponding application launched (Sheet 2 of 2)

For NE	Device version	Application or command name	Menu item in object-specific menu or right-click menu of object in topology
Audio Provisioning Server NE managed APS application	6.2/7.0	APS Manager (CS Management Tools) APS Audio Configuration Tool	APS Mgr (CMT) APS Audio Configuration Tool
GWC NE managed by GWC Manager	6.2/7.0	GWC Unit Manager Line Maintenance Manager Trunk Maintenance Manager Network Patch Manager CS Tools	GWC Unit Mgr Launch LMM Launch TMM Launch NPM Launch CS2K Tools
XA-Core managed by CS 2000 Core Manager	6.2 7.0	MAPCI Session MAPCI Session	Launch MAPCI Session Launch MAPCI Session
Session Server NE	6.2/7.0	Session Server	Launch Session Server
Session Server Unit	7.0	Session Server	Launch Session Server
IPCM NE managed	6.2/7.0	IPCM Manager	Launch CICM Manager
IPCM NE node managed IPCM Manager	6.2/7.0	IPCM Manager	Launch CICM Manager
SAM21 NE managed by SAM21 Manager	6.2/7.0	SCU Subnet SCU Manager	Launch SCU Subnet Launch SCU Manager

References

Table 38 shows where you can find more detailed information about the Integrated Element Management System.

Table 38
Documentation references

Document title	Document Number
Integrated EMS Basics	NN10329-111
Integrated EMS Security and Administration	NN10336-611
Integrated EMS Fault Management	NN10334-911
Integrated EMS Configuration Management	NN10330-511
Integrated EMS Performance Management	NN10327-711
Meridian SL-100 Service Order Reference Manual	555-4031-808, 297-8021-808P1 and 297-8021-808P1 (DMS versions)
OSSGate User Guide	NE10004512
CS 2000 Management Tools Administration and Security	NN10172-611

Fault management

There are three aspects to Communication Server 2100 support for fault management as follows:

- Fault reporting using logs:
  - — Supported for the Communication Server 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's equipment in a multi-vendor network.
  - — Supported by the Preside Multi-service Data Manager (PMDM) used to manage Media Gateway 15000s. The system maps alarm and status reports provided by Preside Multi-service 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's network uses more than one Communication Server 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.

  Table 39 on page 175 summarizes the mechanisms used.

Table 39
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.
Ethernet Routing Switch 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 Preside Multi-service Data Manager with the information used to create logs.	CORBA	Media Gateway 15000 state changes are also reported through their Gateway Controllers.

- 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 Communication Server 2100 supports the following two optional management applications for trunk and line maintenance through the Core:
    - – Trunk Management and Maintenance
    - – Line Management and Maintenance

New in SE08

Access Care

Nortel's Access Care provides a comprehensive trouble management application that delivers unified management and diagnostics for packet and TDM networks. It delivers multi-domain customer service ticketing, automated testing and diagnostics, sophisticated workforce management and an integrated network ticket solution. The Access Care application is a multivendor, multi-technology system designed with industry-standard open interfaces to enable 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. It enables testing and diagnostics 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's 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. The GUI specifies the test heads for Access Care use when testing a specified line circuit.

Using Access Care, a connection for Metallic Test Access (MTA) to a line card can be set up by entering a Directory Number (DN). Loop qualification predicts if the loop has the ability to 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's footprint. The footprint can be used later for comparing or tracking changes in the loop's performance.

References

Table 40 shows where you can find more information about Access Care.

Table 40
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:
  - Communication Server 2100 Core
  - Gateway Controllers
  - SAM21 card cages
  - IP Client Manager
  - Media Gateway 9000
  - Ethernet Routing Switch 8600s
  - Media Server 2010
  - Media Gateway 15000s
- Communication Server 2100 Core configuration through the Communication Server 2000 Manager using ASCII over TCP.
- Gateway Controller configuration through the Gateway Controller Element Manager using SNMP.
- Ethernet Routing Switch 8600 configuration through the Ethernet Routing Switch 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 Preside Multi-service 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:

- Communication Server 2100 Core
- Gateway Controllers
- Trunk media gateways

The following two applications provide help to ensure that these separate updates are co-ordinated:

- 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. It can also host the optional Trunk Maintenance Manager (TMM) application, which provides 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 Communication Server 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:

- Communication Server 2100 Core
- Gateway Controllers
- Line media gateways

The following two applications provide help to ensure that these separate updates are co-ordinated:

- 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. It 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 Nortel Network's 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 Communication Server 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 Communication Server 2100 network (for example, gateways). With SERVORD+ commands, the media gateway name (MGName) and Termination Point (TPName) generally replace the LEN for Communication Server 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 Communication Server 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 centralized administrative center for processing. They 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 Communication Server 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 Communication Server 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 Communication Server 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***

  Generation of these records is triggered in the course of translating and routing a call. This type of record must provide the following information in order to allow 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 Communication Server 2100 at the time the recording is taking place. 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 Communication Server 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 onto the record.

Automatic Message Accounting records for long calls

Long calls result in the generation of more than one Automatic Message Accounting record.

The long call audit process runs at regular intervals to check whether there are long calls 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 has remained 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 up a profile of calls made and received per 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 individual subscriber feature usage, 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 Communication Server 2100 Core generates Automatic Message Accounting records during the course of 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 Communication Server 2100.

Note: Although billing information is usually routed directly to the SuperNode Data Manager, you must configure backup volumes on the Communication Server 2100 to hold this information in the event of a problem with the Communication Server 2100 to SuperNode Data Manager link.

Core Manager SuperNode Billing Application support for billing

All Automatic Message Accounting records that the Communication Server 2100 Core generates are immediately transferred to the Core Manager's SuperNode Billing Application for formatting and storage. This means that it is not necessary for these tasks to be performed on the Communication Server 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's administrative center, or Network Management System, through Element Managers or some other intermediary.

Operational Measurements are standard measurements originally defined by Bellcore for the collection of 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 Communication Server 2100 uses Operational Measurements and Performance Measurements as follows:

- The system supports performance monitoring through Operational Measurements for all of the Communication Server 2100 Network Elements. It can be complemented by the use of selected Automatic Message Accounting records to monitor performance.
  - The Communication Server 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

  Table 41 summarizes the way in which the Communication Server 2100 Network Elements, other than the Communication Server 2100, collect Performance Measurements for presentation to the Network Management Layer.

Table 41
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 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		
Ethernet Routing Switch 8600	SNMP	Ethernet Routing Switch 8600 Device Manager	Performance Measurements in CSV format using FTP
Media Gateway 15000	SNMP	Poller task (for example, on an Element Manager)	CORBA

In SE08, Nortel does not offer standard applications for integrated handling of performance reporting and management for a Communication Server 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.

OAM&P security

This section describes the security mechanisms used for the OAM&P applications. For more information about security for the entire Communication Server 2100 network, see"Communication Server 2100 network security" on page 189.

Introduction

General OAM&P security requirements

The following are some of the basic requirements for OAM&P 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 OAM&P applications. Security in OAM&P covers a wide range of requirements, interfaces and platforms as follows:

- Interfaces
  - Identification/access control level (authentication)
  - Authorization/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 OAM&P security is a critical requirement for Communication Server 2100 networks. As such ongoing security developments have resulted in improvements that include the following items:

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

Name Service Switch

The Name Service Switch (nsswitch) is used for centralized authorization/user profile management (for example, groups, home directory and default shell). This 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 centralized 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, Passwerks nsswitch (on Unix) to act as an authentication mechanism.

Integrated Element Management System API security

The security solution for the Integrated Element Management System Application Programming Interface centers around the following:

- PAM for authentication
- nsswitch for authorization
- a Single Sign On (SSO) key generation/verification module

On the interfaces side, a given application, or Network Element, can choose to 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 solutions. The system implements security functionality 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 Communication Server 2100 Network Elements from unauthorized viewing and/or modification of data, 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's commitment to secure solutions

Nortel has developed 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 Communication Server 2100 LAN/IP network infrastructure is an important part of the solution for providing secure access to OAM&P functionality.

FOR MORE INFORMATION

See the *Packet Trunk-IP Engineering Rules System Engineering Bulletin*, SEB-02-10-001, for guidelines for configuring the CS LAN security.

In order to configure the LAN setup for a Communication Server 2100 network, the following items are required:

- Ethernet Routing Switch 8600 (or comparable router), duplicated for redundancy, provides filtering and routing between the LANs (for more information, see "Ethernet Routing Switch 8600" on page 141).
- Alteon or comparable firewall.

A Network Element or application can talk to others only by going through the Ethernet Routing Switch 8600. In addition, a Network Element or application uses separate interfaces/ports to talk to each of the applicable VLANs. There is no multi-use of ports for multiple VLANS.

To enhance security, the network for a Communication Server 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 Figure 35 on page 144 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 Communication Server 2100 Network Elements involved in call processing and service provisioning for end users.

  The signaling VLAN uses private IP addresses from within the Communication Server 2100 IP domain. It protects functional Communication Server 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 OAM&P VLAN interconnects the Element Management System servers supporting the Element Managers for functional Network Elements.

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

- An Access LAN which connects to the Network Elements (for example, Media Gateway 15000s). It is located on the other side of the Ethernet Routing Switch 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 OAM&P 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/OAM&P traffic to reach the appropriate servers that it processes. All traffic between Communication Server 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. This protects the critical call processing funtionality from being affected by internal attacks originating in the Network Management System.

In addition to the firewall, the RTP Media Portal provides additional protection for any media components hosted off the CS-LAN. It filters and proxies media traffic by the Communication Server 2100 to the appropriate media gateway in the Media subnet.

Network segregation aimed at protecting the Communication Server 2100 network does not end with the CS-LAN. Only valid VoIP protocols and corresponding OAM&P traffic is allowed on the Core network. Nortel recommends using virtual separation of VoIP traffic into a virtual Communication Server 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, Ethernet Routing Switch 8600) protect the Communication Server 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's move to IP telephony. As such, SE08 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 Preside Multi-service Data Manager.
- Single login and centralized 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 Preside Multi-service 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, Preside Multi-service Data Manager and Device Manager.
- User activity audit logging for the Gateway Controller Manager.

- IPSec between the Preside Multi-service Data Manager and Media Gateway 15000.
- IPSec log reporting from the Gateway Controller.

User management

User types

The Communication Server 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, but additional maintenance class users can be added.

Table 42 lists the capabilities available to each class of user.

Table 42
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	• Maintenance commands (for example, busy, return to service and off-line) • Monitoring system performance • Restricted command access • Changing system alarm thresholds • Password update • Application-specific configuration tools

Password administration

The root user can change any password on the system at any time. Maintenance class users can only change 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's 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 there is no activity for ten minutes.

Authentication mechanisms

The Communication Server 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

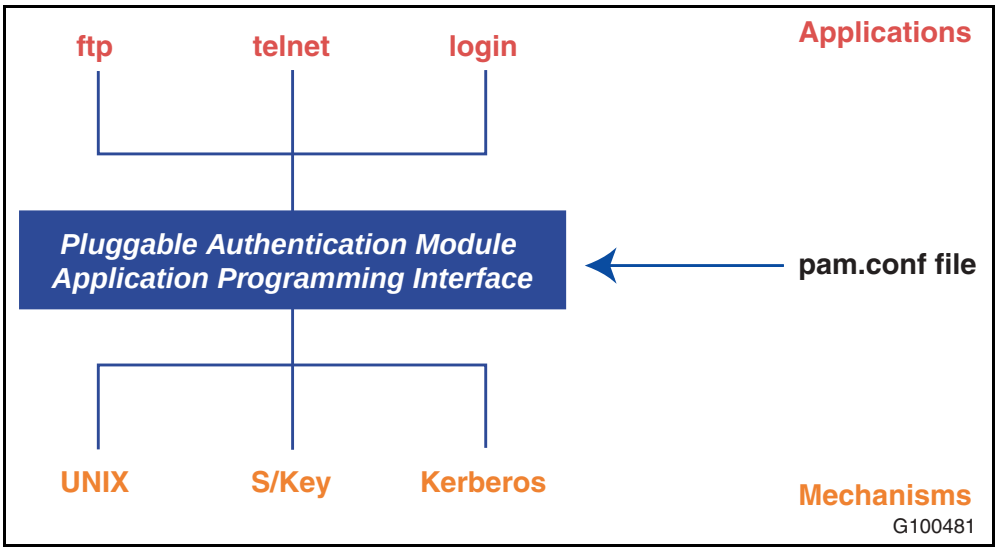
With the Pluggable Authentication Module framework, multiple authentication technologies can be added without changing any of the login services, therefore preserving existing system environments. The Pluggable Authentication Module integrates login services with different technologies.

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

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

Figure 43 shows the Pluggable Authentication Module architecture.

Figure 43
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's 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 the components used in the Communication Server 2100 network. The operating systems of the components are "hardened" to provide additional security diligence.

References

Table 43 shows where you can find more detailed information about the Communication Server 2100 security for large enterprises.

Table 43
Documentation references (Sheet 1 of 2)

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
Integrated EMS Security and Administration	NN10336-611
STORM Security and Administration	NN10176-611
MS 2000 Series Administration and Security	NN10337-611
IW SPM-IP Security and Administration	NN10166-611
MG 9000 Security and Administration	NN10162-611

Table 43
Documentation references (Sheet 2 of 2)

Document title	Document number
Securing the Enterprise Network Document Library	A wide range of articles, positioning papers, white papers and solution/application overviews are available on Nortel.com
Secure VoIP for Enterprise SR&S Corporation Case Study Version No. 1.0	TD-0S03-113-2003

Appendix A: Technical specifications

Operating environment

Ceiling height

A minimum clear ceiling height of 3m (10 feet) is required for the Communication Server 2100 cabinets and frames. The recommended clear ceiling height is 3.4m (11 feet).

Floor loading

The floor loading of fully-equipped Communication Server 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 multi-floor 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 multi-floor building is, therefore, 4.2 kilonewtons per square meter (100 pounds per square foot).

Environmental specifications

Communication Server 2100 equipment will remain functional and operate as expected under the environmental conditions that Table 44 shows.

Table 44
Environmental conditions (Sheet 1 of 2)

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)
Atmospheric pressure	423mmHg (69.2KPa), corresponding to 3,048m (10,000 feet) of altitude.

Table 44
Environmental conditions (Sheet 2 of 2)

Condition	Value
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 1.254m (5 feet) above floor level and 381mm (15 inches) in front of the equipment. Rate of temperature change must not exceed 6.7ºC (15ºF) per hour.

The heat dissipation of a Communication Server 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 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 Communication Server 2100 by truck, rail, sea or air when packed for transportation. Table 45 shows the environmental conditions that should not be exceeded during transportation.

Table 45
Storage and shipping conditions

Condition	Value
Ambient temperature	-40ºC to 71ºC (-40ºF to 160ºF)
Humidity	10% to 95%; maximum water vapor pressure not to exceed 25 mmHg
Vibration	Up to 3.5g at 5Hz to 500Hz
Shock	Equivalent to a 152mm (six inch) drop for a 454Kg (1000lb) equipped bay

You can store Communication Server 2100 equipment in a sheltered environment under the same ambient temperature and humidity conditions detailed for transportation.

Compliance with standards

Communication Server 2100 equipment is compliant with 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 Communication Server 2100 cabinets provide Zone 4 earthquake protection without additional bracing. They meet industry isolated grounding and requirements and feature connectors to facilitate testing.

Communication Server 2100 cabinets and frames

SE08 supports the following two types of Communication Server 2100 configurations:

- Communication Server 2100 XA-Core
- Communication Server 2100 Compact

Both types of configuration support the same range of call processing agents, protocols and telephony features. The main differences between them are that the Communication Server 2100 Compact uses a different processor complex, has a significantly smaller footprint and delivers reduced call processing capacity.

Table 46 describes the cabinets that can house the Communication Server 2100 components.

Table 46
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
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 OAM&P applications ***Note:*** In Communication Server 2100 Compact configurations, the main PTE cabinet houses two SAM21 shelves. A second PTE2000 frame is required to house Element Managers for Communication Server 2100 Compact components.

Each cabinet, or frame, contains equipment shelves that provide slots for the installation of circuit cards and/or space to house specialized units that, in turn, contain circuit cards.

Communication Server 2100 cabinets meet industry requirements for isolated grounding and feature connectors to facilitate testing. They provide greater physical and electrostatic discharge damage protection for the enclosed equipment than open frames. They also are compliant with electromagnetic compatibility requirements and provide Zone 4 earthquake protection without additional bracing.

Power consumption examples

Table 47 provides examples of the power requirements for Communication Server 2100 cabinets.

Note: Power consumptions vary depending on the actual components housed in each cabinet.

Table 47
Power consumption examples

Item	Call Control Frame	OAM&P 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	-50.25V	-50.25V	-50.25V

Appendix B: Peripheral support

Table 48 lists the Meridian SL-100 peripherals that are supported on the TDM side of the Communication Server 2100 hybrid.

Table 48
Supported Meridian SL-100 peripherals (Sheet 1 of 2)

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

Table 48
Supported Meridian SL-100 peripherals (Sheet 2 of 2)

Peripheral	Abbreviation
Line Concentrating Module	LCM
Line Concentrating Module-Enhanced	LCME
Line Group Controller	LGC
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

FOR MORE INFORMATION

Refer to the *Peripheral Module Release Document (PM 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
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
CBM	Core and Billing Manager
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
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
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 8600	Ethernet Routing Switch 8600
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
GBIC	Gigabit Interface Converter
GEM	Gig Ethernet Resource Module
Gig-E	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	Multi-Service 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
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
OAM&P	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
PMDM	Preside Multi-service Data Manager
POTS	Plain Ordinary Telephone Service
PP	Peripheral Processor
PPVM	Peripheral Processor Virtual Machine
Preside MSS	Preside Management for Succession Solutions
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
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
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
SSPFS	Succession Server Platforms Foundation Software
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

Nortel Communication Server 2100

Product Guide

Publication number: 555-4001-806
Product release: SE08
Document release: Standard 03.06
Date: February 2006
Printed in the United States of America.

NORTEL