Nortel Communication Server 1000

Nortel Communication Server 1000 Release 4.5

Communication Server 1000E

Planning and Engineering

Document Number: 553-3041-120
Document Release: Standard 6.00
Date: December 2006

Produced in Canada

Revision history

December 2006

Standard 6.00. This document is up-issued to revise Signaling Server memory requirements.

July 2006

Standard 5.00. This document is up-issued to include corrections for CR Q001324850.

February 2006

Standard 4.00. This document is up–issued to include SIP CTI / TR 87 information from the new Nortel Converged Office Implementation Guide (553-3001-025).

January 2006

Standard 3.00. This document is up-issued with editing corrections related to CS 1000 Release 4.5 content.

August 2005

Standard 2.00. This document is up-issued to support Communication Server 1000 Release 4.5. New material relating to data networking planning for VoIP has been added.

September 2004

Standard 1.00. This document is issued for Communication Server 1000 Release 4.0.

Contents

List of procedures

Finding the latest updates on the Nortel web site

The content of this documentation was current at the time the product was released. To check for updates to the latest documentation and software for CS 1000E, click one of the links below.

Latest Software	Takes you directly to the Nortel page for CS 1000E software.
Latest Documentation	Takes you directly to the Nortel page for CS 1000E documentation.

How to get help

This section explains how to get help for Nortel products and services.

Getting help from the Nortel Web site

The best way to get technical support for Nortel products is from the Nortel Technical Support Web site:

www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. More specifically, the site enables you to:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting help over the telephone from a Nortel Solutions Center

If you don't find the information you require on the Nortel Technical Support Web site, and have a Nortel support contract, you can also get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following Web site to obtain the phone number for your region:

www.nortel.com/callus

Getting help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

www.nortel.com/erc

Getting help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller.

About this document

This document is a global document. Contact your system supplier or your Nortel representative to verify that the hardware and software described are supported in your area.

Subject

WARNING

Before a CS 1000E system can be installed, a network assessment **must** be performed and the network must be VoIP-ready.

If the minimum VoIP network requirements are not met, the system will not operate properly.

For information on the minimum VoIP network requirements and converging a data network with VoIP, refer to *Converging the Data Network with VoIP* (553-3001-160).

This document provides the information necessary to properly engineer a Communication Server 1000E (CS 1000E) system. There are two major purposes for using this document: to engineer an entirely new system, and to evaluate a system upgrade.

The NNEC provides an alternative to the manual processes given in this document. It is beyond the scope of this document to describe the NNEC process.

Note on legacy products and releases

This NTP contains information about systems, components, and features that are compatible with Nortel Communication Server 1000 Release 4.5 software. For more information on legacy products and releases, click the **Technical Documentation** link under **Support & Training** on the Nortel home page:

www.nortel.com

Applicable systems

This document applies to the Communication Server 1000E (CS 1000E) system.

> ***Note:*** When upgrading software, memory upgrades may be required on the Signaling Server, the Call Server, or both.

Intended audience

This document is intended for system engineers responsible for engineering the switch and the Nortel Technical Assistance Support personnel who support them. Engineers can be employees of the end user, third-party consultants, or distributors.

The engineer responsible for system implementation should have several years of experience with Nortel PBX systems.

Others who may be interested in this information, or find it useful, are Sales and Marketing, Service Managers, Account Managers, and Field Support.

Conventions

In this document, the CS 1000E system is referred to generically as “system.”

Related information

This section lists information sources that relate to this document.

NTPs

The following NTPs are referenced in this document:

- *Converging the Data Network with VoIP* (553-3001-160)
- *Dialing Plans: Description* (553-3001-183)
- *Circuit Card: Description and Installation* (553-3001-211)
- *IP Peer Networking: Installation and Configuration* (553-3001-213)
- *Branch Office: Installation and Configuration* (553-3001-214)
- *System Security Management* (553-3001-302)
- *Software Input/Output: Administration* (553-3001-311)
- *Element Manager: System Administration* (553-3001-332)
- *IP Line: Description, Installation, and Operation* (553-3001-365)
- *Telephones and Consoles: Description, Installation, and Operation* (553-3001-367)
- *IP Phones: Description, Installation, and Operation* (553-3001-368)
- *Traffic Measurement: Formats and Output* (553-3001-450)
- *Communication Server 1000S: Overview* (553-3031-010)
- *Communication Server 1000E: Installation and Configuration* (553-3041-210)
- *CallPilot Planning and Engineering* (553-7101-101)

Online

To access Nortel documentation online, click the **Technical Documentation** link under **Support & Training** on the Nortel home page:

www.nortel.com

CD-ROM

To obtain Nortel documentation on CD-ROM, contact your Nortel customer representative.

Overview of the engineering process

Contents

This section contains information on the following topics:

Introduction

WARNING

Before a CS 1000E system can be installed, a network assessment **must** be performed and the network must be VoIP-ready.

If the minimum VoIP network requirements are not met, the system will not operate properly.

For information on the minimum VoIP network requirements and converging a data network with VoIP, refer to *Converging the Data Network with VoIP* (553-3001-160).

A switch must be engineered upon initial installation, during upgrades, and when traffic loads change significantly or increase beyond the bounds anticipated when the switch was last engineered. A properly engineered switch is one in which all components work within their capacity limits during the busy hour.

This document is not intended to provide a theoretical background for engineering principles, except to the extent required to make sense of the information. Furthermore, in order to control complexity, technical details and data are sometimes omitted when the impact is sufficiently small.

This document does not address the engineering or functionality of major features, such as Automatic Call Distribution (ACD) or Network Automatic Call Distribution (NACD), and of auxiliary processors and their applications, such as Symposium and CallPilot. Guidelines for feature and auxiliary platform engineering are given in documents relating to the specific applications involved. This document provides sufficient information to determine and account for the impact of such features and applications upon the capacities of the system itself.

Engineering a new system

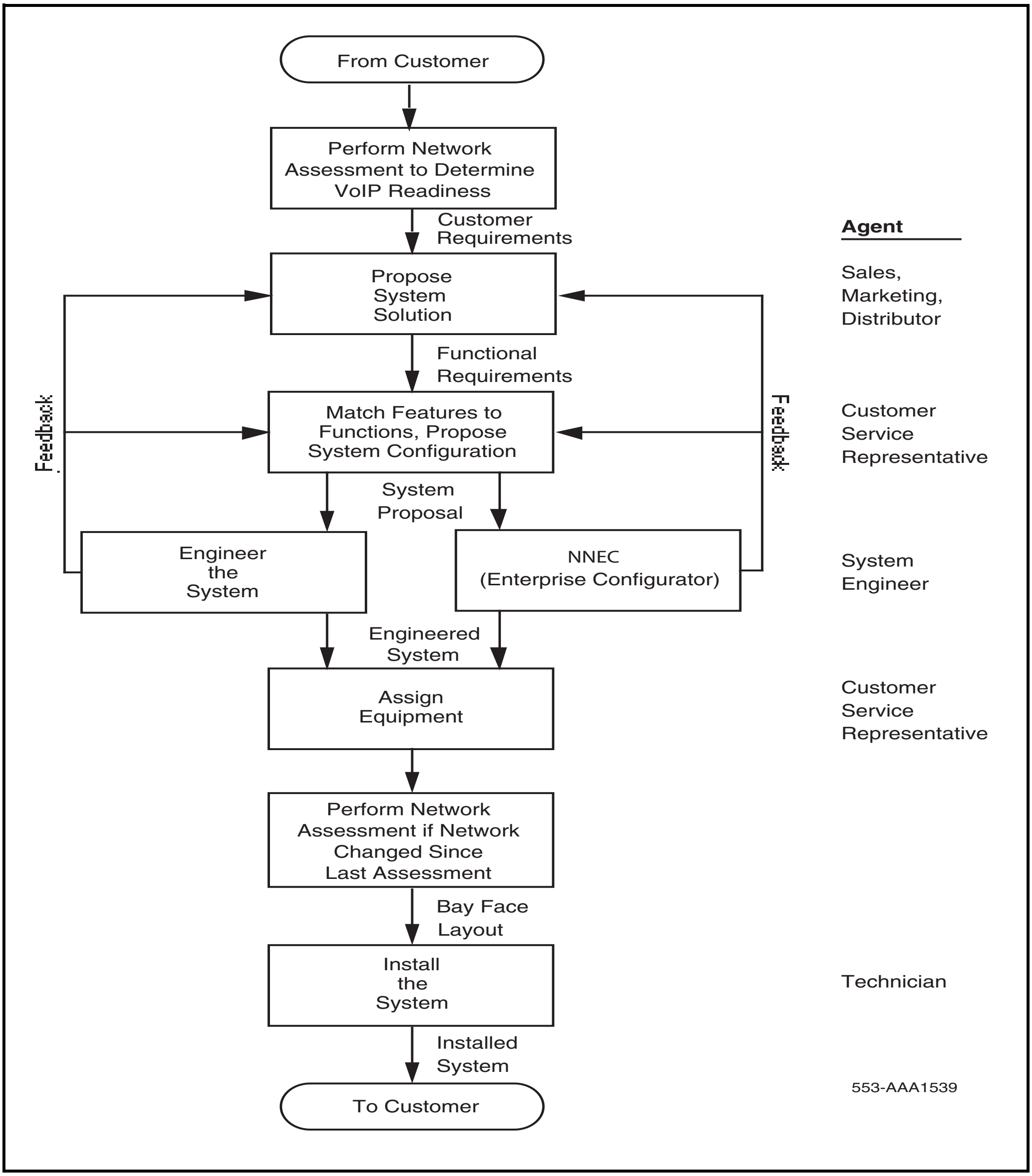
Figure 1 on page 27 illustrates a typical process for installing a new system. The agent expected to perform each step of the process is listed to the right of the block. The highlighted block is the subject of this document.

Engineering a system upgrade

In cases of major upgrades or if current resource usage levels are not known, Nortel recommends following the complete engineering process, as described for engineering a new system.

If minor changes are being made, calculate the incremental capacity impacts and add them to the current resource usage levels. Then compare the resulting values with the system capacities to determine whether the corresponding capacity has been exceeded.

Figure 1
Engineering a new system



NNEC

The NNEC is a global engineering and quotation tool to assist the site engineer, sales person, or customer in engineering the switch. It is available in both stand-alone and web-based versions. For users in North America and the Caribbean and Latin America (CALA), it replaces Meridian Configurator and 1-Up. For users in Europe, Middle East, and Africa (EMEA) countries, it replaces NetPrice.

The NNEC provides a simple “needs-based” provisioning model that allows for easy configuring and quoting. The NNEC supports CS 1000E new system sales and upgrades by analyzing input specifications for a digital PBX to produce a full range of pricing, engineering reports, and graphics. These reports include equipment lists, cabling reports, software matrix, engineering capacities, and pricing for currently available CS 1000E configurations. Graphics depict the engineered platform, card slot allocations as well as loop assignments.

The NNEC runs on the user’s Windows-based or MacOS personal computer. It uses standard browser and Microsoft Office applications. For details on computer system requirements and for user instructions, refer to the Nortel web site.

NNEC implements the algorithms specified in this document for real time, memory, and physical capacities. It is the official tool for determining whether a proposed configuration will meet the customer’s capacity requirements.

Where applicable, in this document, references are made to the NNEC inputs that correspond to parameters being described.

Data network planning for VoIP

Contents

This section contains information on the following topics:

Introduction

WARNING

Before a CS 1000E system can be installed, a network assessment **must** be performed and the network must be VoIP-ready.

If the minimum VoIP network requirements are not met, the system will not operate properly.

For information on the minimum VoIP network requirements and converging a data network with VoIP, refer to *Converging the Data Network with VoIP* (553-3001-160).

The data network's infrastructure, engineering, and configuration are critical to achieve satisfactory IP Telephony voice quality. A technical understanding of data networking and Voice over IP (VoIP) is essential for optimal performance of the CS 1000E system.

Refer to *Converging the Data Network with VoIP* (553-3001-160) for detailed information about network requirements. These requirements are critical to the system Quality of Service (QOS).

Data network planning for VoIP

Consider the following when planning the network:

- system network requirements (for ELAN and TLAN subnets)
- basic data network requirements for Call Server to Media Gateway connections, including the following:
  - jitter
  - delay
  - bandwidth
  - LAN recommendations
- basic data network requirements for IP Phones
  - bandwidth
- power requirements for IP Phones

Evaluating the existing data infrastructure

Evaluate the existing data infrastructures (LAN and WAN) to confirm their suitability for VoIP deployment. In some cases, VoIP deployment requires additional bandwidth, improved performance and QOS, and greater availability.

To evaluate voice performance requirements, review such things as device inventory, network design, and baseline information. Links and devices must have sufficient capacity to support additional voice traffic. It may be necessary to upgrade links that have high peak or busy hour utilization.

When assessing the environment, target devices with the following characteristics:

- high CPU utilization
- high backplane utilization
- high memory utilization
- queuing drops
- buffer misses for additional inspection
- potential upgrade

Peak utilization characteristics in the baseline are valuable in determining potential voice quality issues.

To evaluate requirements for the VoIP network, review network topology, feature capabilities, and protocol implementations. Measure redundancy capabilities of the network against availability goals with the network design recommended for VoIP.

Evaluate the overall network capacity to ensure that the network meets overall capacity requirements. Overall capacity requirements must not impact existing network and application requirements. Evaluate the network baseline in terms of the impact on VoIP requirements.

To ensure that both VoIP and existing network requirements are met, it may be necessary to add one or more of the following:

- memory
- bandwidth
- features

Planning deployment of a CS 1000E system on a data network

To deploy the CS 1000E system on a data network, consider the following data networking details and refer to *Converging the Data Network with VoIP* (553-3001-160):

- VoIP technology
  - H.323 protocols
  - VoIP concepts and protocols
  - RTP
  - Codecs including G.711 and G.729
- data network architecture
  - TCP/IP
  - IP subnetting
  - routing protocols including EIGRP, OSPF, RIP, and BGP
- data services and peripherals
  - DNS
  - DHCP
  - TFTP
  - Web server
  - QOS

QOS planning

An IP network must be engineered and provisioned to achieve high voice quality performance. It is necessary to implement QOS policies network-wide to ensure that voice packets receive consistent and proper treatment as they travel across the network.

IP networks that treat all packets identically are called “best-effort networks”. In a best-effort network, traffic can experience varying amounts of delay, jitter, and loss at any time. This can produce speech breakup, speech clipping, pops and clicks, and echo. A best-effort network does not guarantee that bandwidth is available at any given time. Use QOS mechanisms to ensure bandwidth is available at all times, and to maintain consistent, acceptable levels of loss, delay, and jitter.

For planning details for QOS, see *Converging the Data Network with VoIP* (553-3001-160).

Core network planning

There are three networks in the CS 1000E IP Telephony network design:

1 Call Server to Media Gateway network

2 ELAN (Management LAN) subnet

3 TLAN (Voice LAN) subnet

> ***Note:*** The ELAN (Embedded LAN) subnet, isolates critical telephony signaling between the Call Server and the other components. The TLAN (Telephony LAN) subnet, carries telephony, voice, and signaling traffic, and connects to the customer network and the rest of the world.

100BaseTx IP connectivity

Between the Call Server and Media Gateway, the CS 1000E supports 100BaseTx IP point-to-point connectivity or campus data network connectivity. Campus data network connectivity is provided through IP daughterboards in the Call Server and the Media Gateway.

To satisfy voice quality requirements, adhere to applicable engineering guidelines. Refer to *Converging the Data Network with VoIP* (553-3001-160) for details. Contact the local Data Administrator to obtain specific IP information.

Campus network system requirements

The following campus network system requirements are necessary:

- The ELAN subnet and the TLAN subnet must be separate.

- ELAN subnet applications must be on the same subnet. This includes the Voice Gateway Media Cards, which must be on the same ELAN subnet.
- Voice Gateway Media Cards in the same node must be on the same TLAN subnet.
- Use of the VLAN concept is a practical way to maintain the same subnet for remote locations.

Refer to *Converging the Data Network with VoIP* (553-3001-160) for information on basic data network and LAN requirements for Call Server to Media Gateway connections, including the following:

- Packet Delay Variation (PDV) jitter buffer
- bandwidth planning
- LAN recommendations for Excellent Voice Quality
- monitoring IP link voice quality of service
- basic data network requirements for IP Phones
  — bandwidth requirements
  — bandwidth planning

Media conversion devices

Third-party media conversion devices can extend the range of the 100BaseTx and convert it to fiber. Use caution when extending the length of cable used in the point-to-point configuration. Do not exceed the specified round-trip delay parameters.

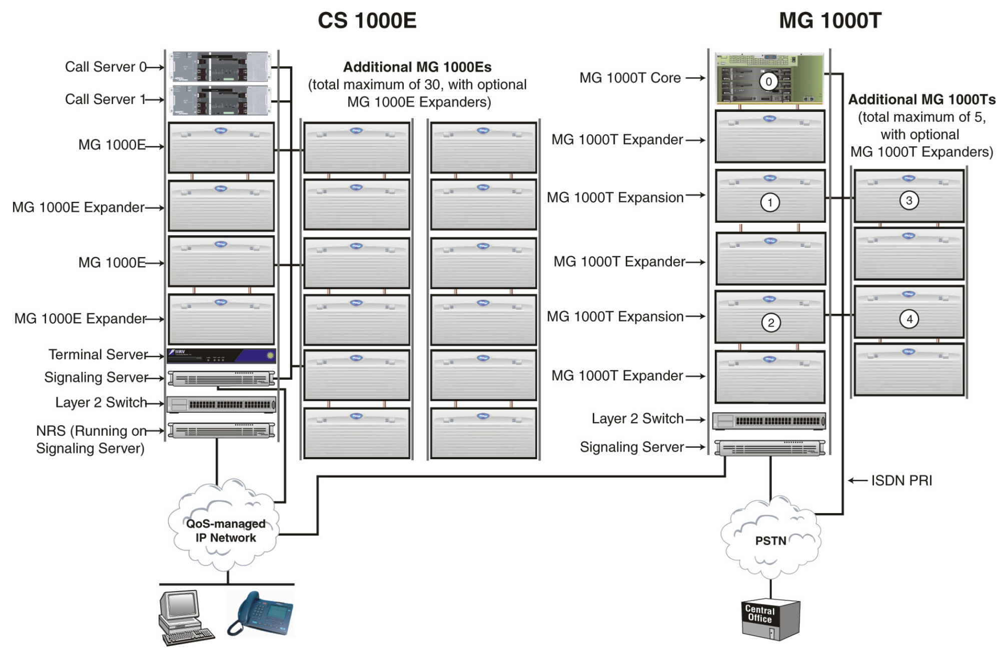
System architecture

Contents

Main components

Figure 2 shows the main components of a typical CS 1000E solution. The remainder of this chapter discusses each component in further detail.

Figure 2
Basic CS 1000E solution



A typical CS 1000E solution is comprised of a Communication Server 1000E (CS 1000E) system and a Media Gateway 1000T (MG 1000T) platform.

- The **CS 1000E** system provides core processing capability and IP functionality. It includes:
  - — dual CS 1000E Core Call Servers (0 and 1) (see page 38)
  - — 1 to 30 Media Gateway 1000Es (MG 1000E) and optional MG 1000E Expanders (see page 52)
  - — Signaling Servers (total number required depends on capacity and survivability levels) (see page 58)

— an MRV Terminal Server (see page 61)

— Layer 2 switches (see page 71)

The CS 1000E system software is based on the core software of the CS 1000M Large Systems. Each Core Call Server in the CS 1000E has two circuit cards: a CP PIV Call Processor card, and a System Utility card — a set similar to that used in CS 1000M Large Systems.

Another key element in the CS 1000E is the Network Routing Service (NRS), a software application that provides network-based routing capability. The NRS runs on a Signaling Server, with other applications or as a stand-alone component.

- The **MG 1000T** platform provides the CS 1000E system with digital trunk and PRI access to the PSTN and to other PBX systems. It includes:

— an MG 1000T Core (MG 1000T 0) and optional MG 1000T Expander (see page 63)

— an additional 1 to 4 MG 1000T Expansions and optional MG 1000T Expanders that are controlled by the MG 1000T Core (see page 63)

— Signaling Servers (total number required depends on capacity and survivability levels) (see page 58)

— Layer 2 switches (see page 71)

The MG 1000T software is based on the core software of the CS 1000S systems. The main controller in the MG 1000T Core is the Small System Controller (SSC) card, the same card used in CS 1000M Small Systems and CS 1000S systems.

Software on the MG 1000T supports a Clock Controller; software on the CS 1000E does not. This means that only the MG 1000T can support the following features (because they use a Clock Controller):

— ISDN PRI and BRI applications (D-channel functionality)

— DECT

As well, given its main role as a trunking gateway, the MG 1000T cannot be provisioned with User Licenses (with the exception of DECT User Licenses).

CS 1000E Core Call Server

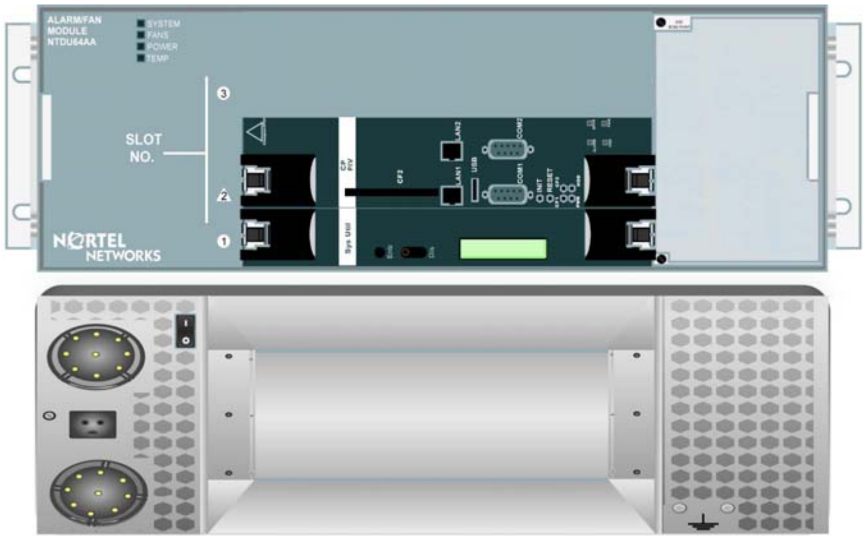
Main role

The CS 1000E Core Call Servers serve as the core processors for the CS 1000E system, including the MG 1000Es.

Physical description

Figure 3 shows the front (without cover) and rear of one Call Server.

Figure 3
CS 1000E Core Call Server (front and rear)



Hardware components

Similar to the set of core circuit cards used in CS 1000M Large Systems, each Call Server contains the following:

- CP PIV Call Processor card
- System Utility card

In addition, each Call Server is equipped with the following modules:

- Power supply module
- Alarm/fan module

CP PIV Call Processor card

The CP PIV Call Processor card (NT4N39AA) is the main processor for the Call Server, controlling all call processing and telephony services. It also provides the system memory required to store operating software and customer data.

The CP PIV Call Processor card provides the following connectors:

- The **Com 1 port** connects to an IP-based Terminal Server, which provides standard serial ports for system maintenance and third-party applications (for more information, see "Terminal Server" on page 61). The Com 1 port can also be directly connected to a system terminal for system access.
- The **Com 2 port** can be used as an additional RS-232 port (for system maintenance only).
- The **LAN 1 Ethernet port** connects the Call Server to the Embedded LAN (ELAN) subnet through an ELAN Layer 2 switch to provide IP connections between the Call Server, Signaling Servers, and MG 1000Es. The port is a 10/100/1000MB auto-negotiate port.
- The **LAN 2 Ethernet port** connects Call Server 0 to Call Server 1 over a 1 Gbps auto negotiating high speed pipe to provide communication and database synchronization.
- The **USB port** is not supported by the CS 1000E system and cannot be used.

System Utility card

The System Utility card (NT4N48) provides auxiliary functions for the Call Server.

> ***Note:*** The minimum vintage for the System Utility card with CS 1000E is NT4N48BA.

System Utility card functions include:

- LCD display for system diagnostics
- interface to the Call Server alarm monitor functions
- Core-selection DIP switches to specify Call Server 0 or Call Server 1

- software security device holder

  Note: The software security device enables the activation of features assigned to the CS 1000E system. The security device for a CS 1000E Core Call Server is similar to the one used on a CS 1000M Large System.

Filler Blank

The filler blank covers over the disk carrier slot used in the older CP PII-based system. The blank supports the blue LEDs that illuminate the Nortel Logo.

Power supply module

The AC power supply module (NTDU65) is the main power source for the Call Server and is field-replaceable.

Alarm/fan module

The alarm/fan module (NTDU64) provides fans for cooling the Call Server and provides status LEDs indicating the status of Call Server components. The alarm/fan module is field-replaceable.

Functional description

The Call Servers provide the following functionality:

- provide main source of call processing
- process all voice and data connections
- control telephony services
- control circuit cards installed in MG 1000Es
- provide resources for system administration and user database maintenance

Operating parameters

The CS 1000E has dual Call Servers (0 and 1) to provide a fully redundant system.

Call Servers 0 and 1 operate in redundant mode: one runs the system while the other runs in a "warm standby" mode, ready to take over system control if the active Call Server fails.

The system configuration and user database are synchronized between the active and inactive Call Servers. This allows the inactive Call Server to assume call processing in the event of failure of the active Call Server.

The Call Server uses a proprietary protocol to control the MG 1000Es. This proprietary protocol is similar to industry-standard Media Gateway Control Protocol (MGCP) or H.248 Gateways.

The Call Servers can control up to 30 MG 1000Es.

> ***Note:*** The Call Servers provide connectivity to telephony devices using IP signaling through MG 1000Es rather than by direct physical connections.

Media Gateway

Main role

The Media Gateway houses circuit cards and connectors to support the functionality of an MG 1000E or MG 1000T. The ultimate role of any Media Gateway is determined by its use as either an MG 1000E or MG 1000T (see "Media Gateway 1000E" on page 52 and "Media Gateway 1000T" on page 63 for details).

> ***Note:*** The MG 1000B and MG 1000S also use the same base Media Gateway hardware as the MG 1000E and MG 1000T. (For more information, see *Branch Office: Installation and Configuration* (553-3001-214) and *Communication Server 1000S: Overview* (553-3031-010).)

Physical description

Figure 4 shows the Media Gateway (NTDU14).

Figure 4
Media Gateway

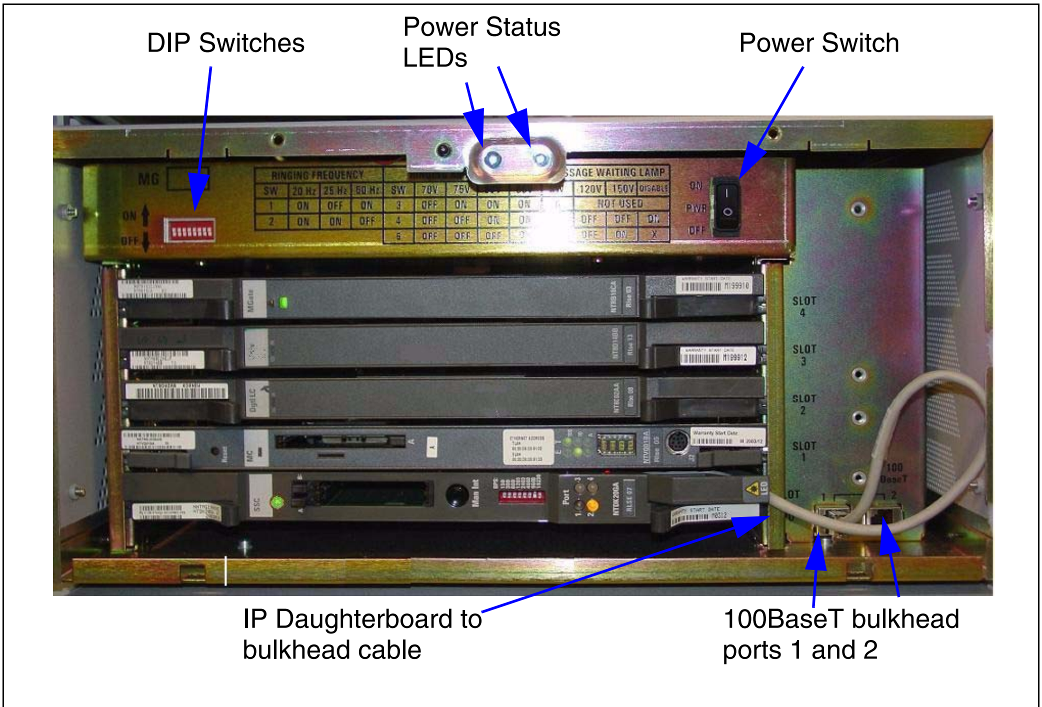
Hardware components

Front components

Figure 5 shows the Media Gateway with the front cover removed. Note the following:

- The DIP switches set ringing voltages, ringing frequencies, and message waiting voltages.
- The 100BaseT bulkhead ports 1 and 2 provide SSC daughterboard ports with connections to rear bulkhead ports.

Figure 5
Front components in the Media Gateway (NTDU14)



Rear components

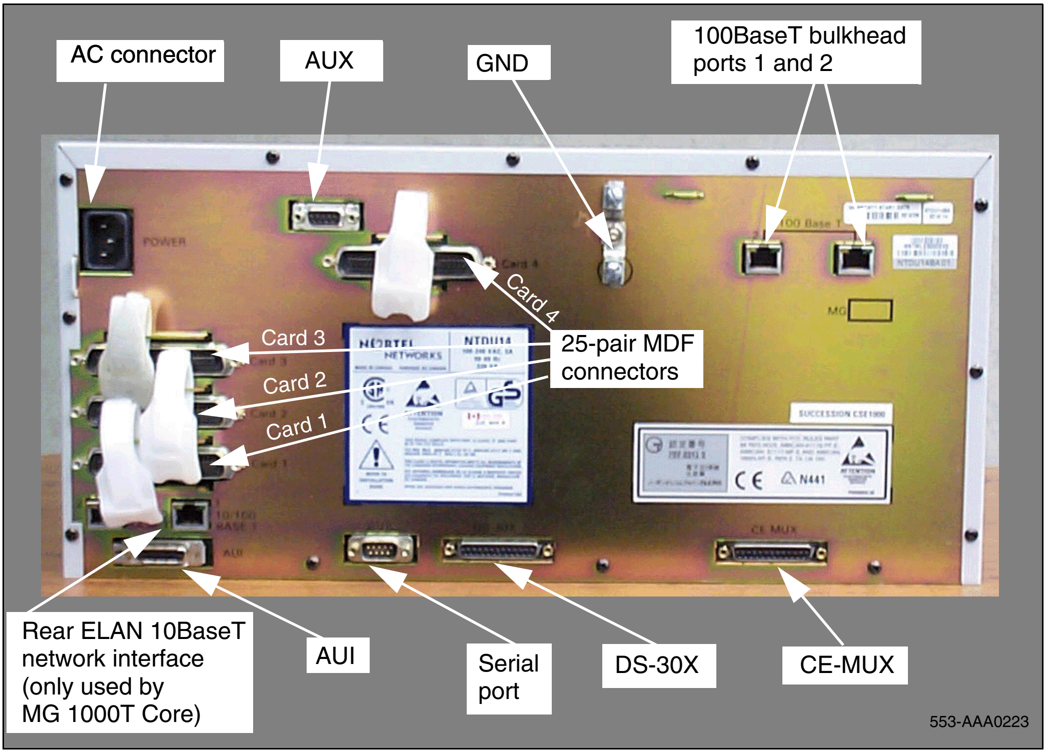
Figure 6 on page 46 shows the rear components on the Media Gateway. Note the following:

- The AC power cord connector provides AC connection to the Media Gateway.
- AUX extends Power Failure Transfer Unit (PFTU) signals to the Main Distribution Frame (MDF).
- GND is used for ground cable termination.
- 100BaseT bulkhead ports 1 and 2 provide connections from IP daughterboard ports on the SSC card to other system components as follows:

- On MG 1000Es, these ports provide connections to the Call Server ELAN through a Layer 2 or a Layer 3 switch.
- On MG 1000T Expansions, these ports provide direct connections to the MG 1000T Core.

- The rear ELAN network interface (10BaseT) provides communication between the MG 1000T Core SSC card and the ELAN subnet (this network interface is not used with MG 1000Es).
- The Attachment Unit Interface (AUI) is used with SSC cards that require a Media Access Unit (MAU).
- The serial port connects to maintenance terminals.
- DS-30X and CE-MUX interconnect the Media Gateway to the Media Gateway Expander.
- 25-pair connectors extend the IPE card data to the MDF.

Figure 6
Rear components in the Media Gateway



Circuit cards

Each Media Gateway can house the following circuit cards:

- SSC card (not used in the Expander)
- Media Card and Voice Gateway Media Card
- Intelligent Peripheral Equipment (IPE) cards (see “Media Gateway 1000E” on page 52 and “Media Gateway 1000T” on page 63 for specific cards supported on each Media Gateway type)

Small System Controller (SSC) card

The SSC card (NTDK20) contains software that controls interface cards and application cards in the Media Gateway. The SSC card hardware resources provide 32 channels of conferencing and 60 channels of tone generation.

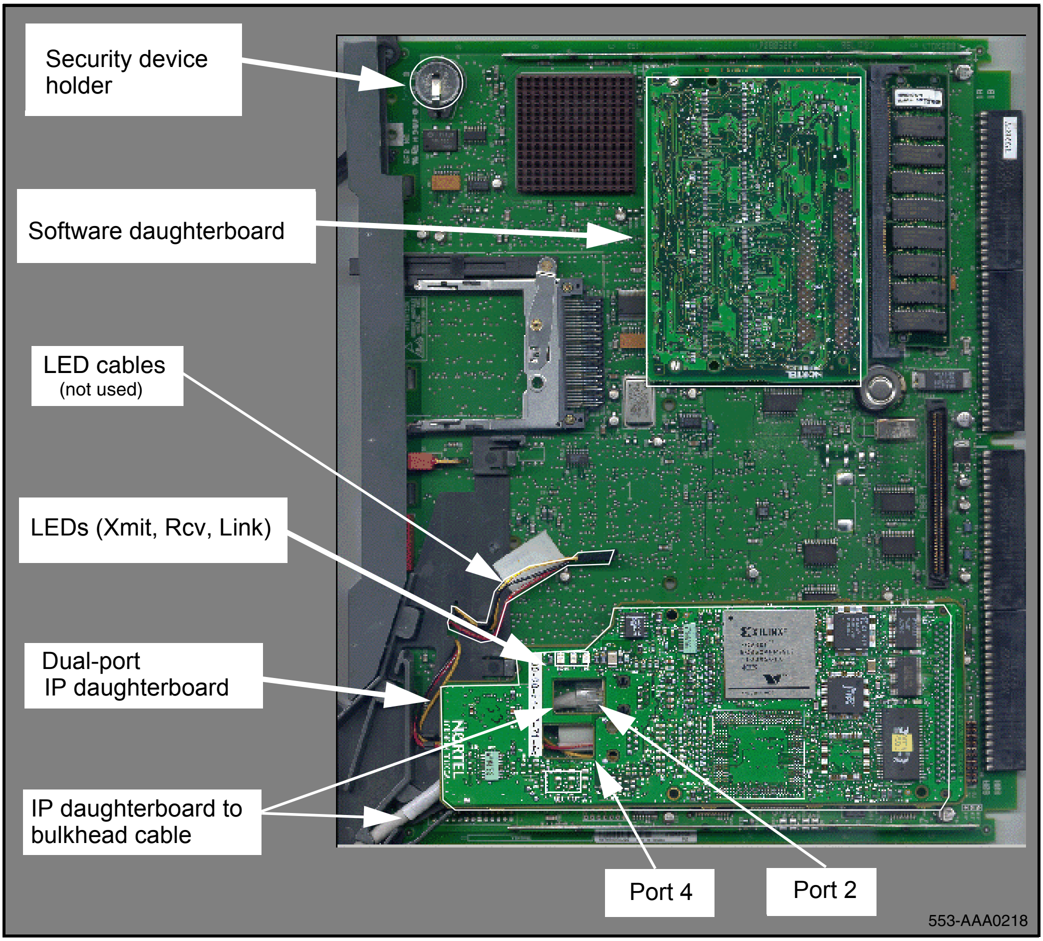
The SSC card is also equipped with IP daughterboards that provide 100BaseT IP interfaces to the ELAN subnet. Each IP daughterboard connected to the SSC also provides an additional 16 conference channels per port (16 channels with each single-port daughterboard and 32 channels with each dual-port daughterboard).

The SSC card also houses the software security device for the Media Gateway.

> ***Note:*** A specific type of security device is required for each type of Media Gateway: MG 1000E, MG 1000T Core, or MG 1000T Expansion. For details, see "Media Gateway 1000E" on page 52 and "Media Gateway 1000T" on page 63.

Figure 7 on page 48 shows the components in the SSC card.

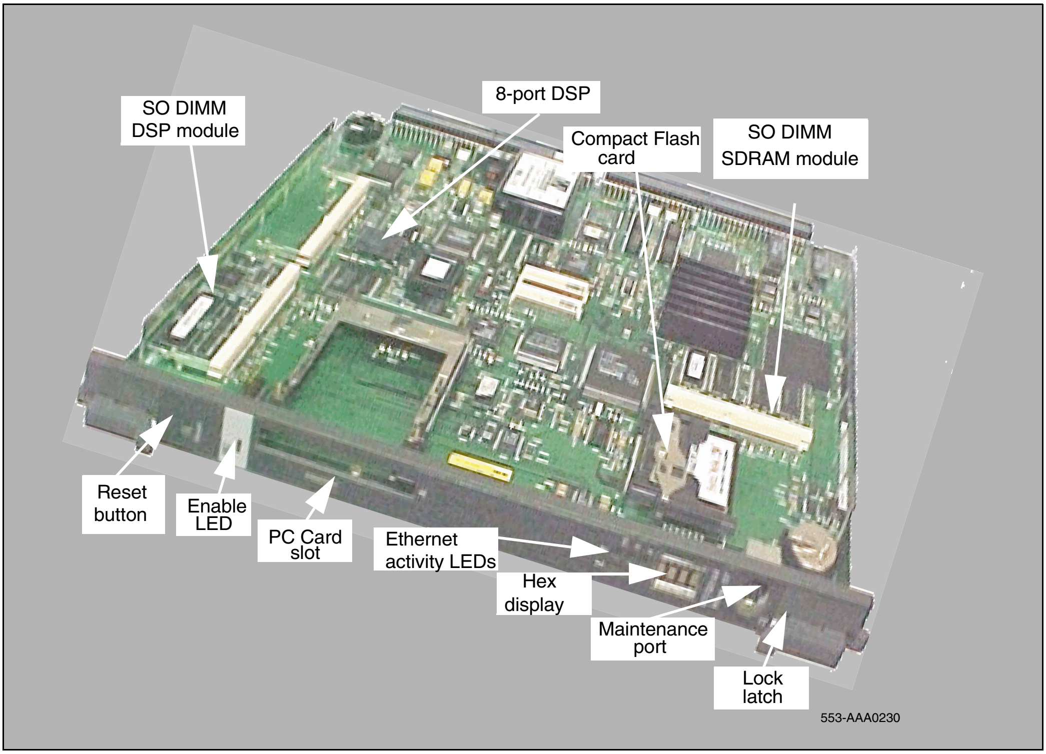
Figure 7
Small System Controller card (NTDK20)



Media Card

The Media Card provides interfaces that connect to the Telephony Local Area Network (TLAN) and Embedded Local Area Network (ELAN) subnets. The Media Card can also run various applications. Figure 8 on page 49 shows faceplate connectors and indicators on the Media Card. For more information on Media Card features, refer to *IP Line: Description, Installation, and Operation* (553-3001-365).

Figure 8
Media Card



Voice Gateway Media Card

A Voice Gateway Media Card is any Media Card that runs the IP Line application. A Voice Gateway Media Card provides Digital Signal Processor (DSP) ports to translate between IP and TDM. Each Voice Gateway Media Card provides 32 DSP ports. For additional information on the IP Line application, see *IP Line: Description, Installation, and Operation* (553-3001-365).

Media Gateway Expander

Main role

The Media Gateway Expander supports up to four circuit cards. It does not house an SSC card and does not support Clock Controller cards. The SSC card in the corresponding MG 1000E or MG 1000T controls each card in an Expander.

> ***Note:*** The CS 1000E system supports lineside T1 (NT5D14) and lineside E1 (NT5D34) cards. For further information about T1/E1 lineside cards, refer to *Circuit Card: Description and Installation* (553-3001-211).

Physical description

Figure 9 shows the Media Gateway Expander (NTDU15).

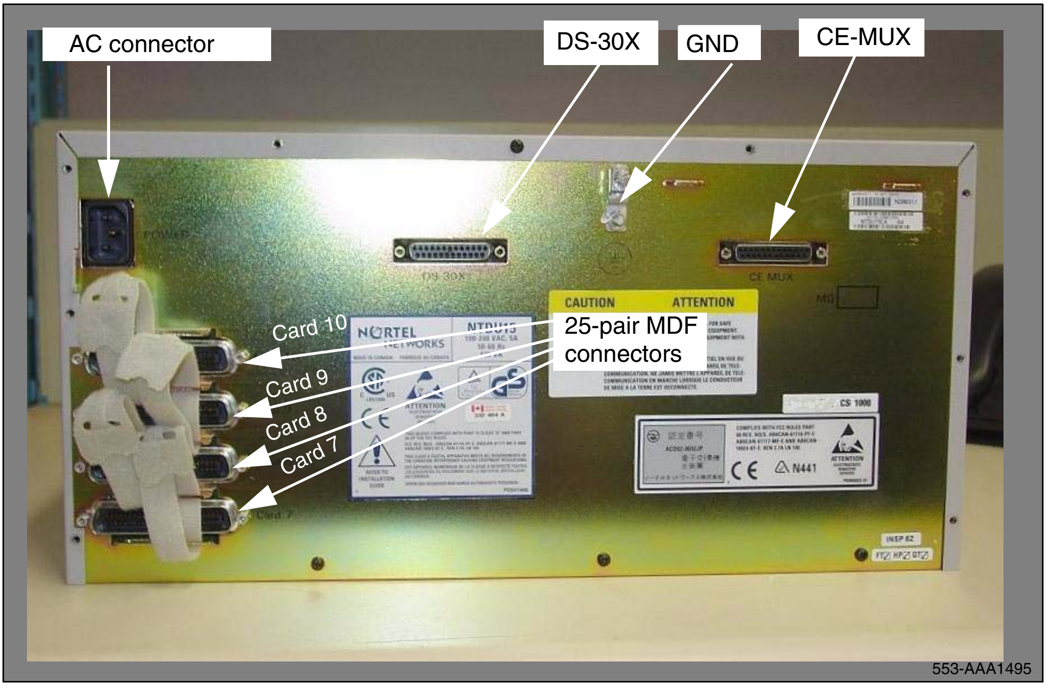
Figure 9
Media Gateway Expander (NTDU15)

Rear components

Figure 10 shows the rear components in the Expander. Note the following:

- The AC power cord connector provides an AC connection to the Expander.
- GND is used for ground cable termination.
- DS-30X and CE-MUX are used to interconnect the Media Gateway and the Expander.
- 25-pair connectors are used to extend IPE card data to the MDF.

Figure 10
Rear components in the Media Gateway Expander



Operating parameters

Each Media Gateway supports one optional Expander.

Media Gateway 1000E

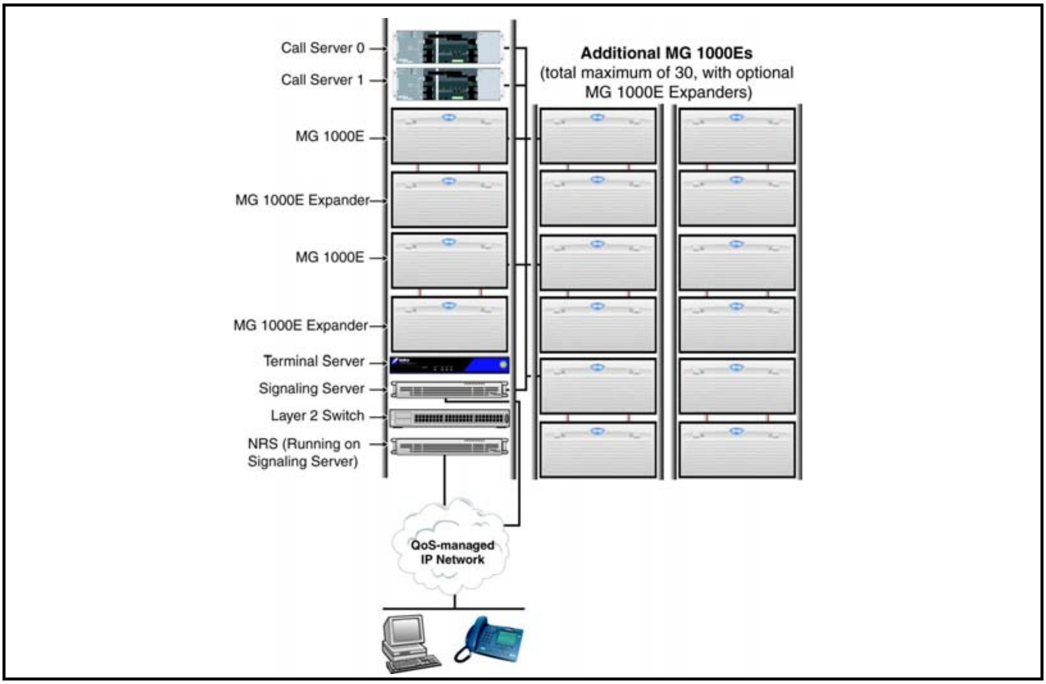
Main role

The Media Gateway 1000E (MG 1000E) provides basic telephony media services, including tone detection and generation and conference, to CS 1000E telephones. The MG 1000E also supports Nortel Integrated Applications, including Integrated Recorded Announcer. It can also provide connectivity for digital and analog (500/2500-type) telephones as well as analog trunks for telephone and fax.

Physical description

Figure 11 shows the MG 1000Es controlled by the Core CS 1000E Call Servers and connected to the IP network.

Figure 11
Media Gateway 1000Es



Hardware components

The MG 1000E houses an SSC card and contains four slots for IPE cards. Each MG 1000E supports an optional MG 1000E Expander through copper connections. For more details, see "Media Gateway" on page 42 and "Media Gateway Expander" on page 50.

Security device

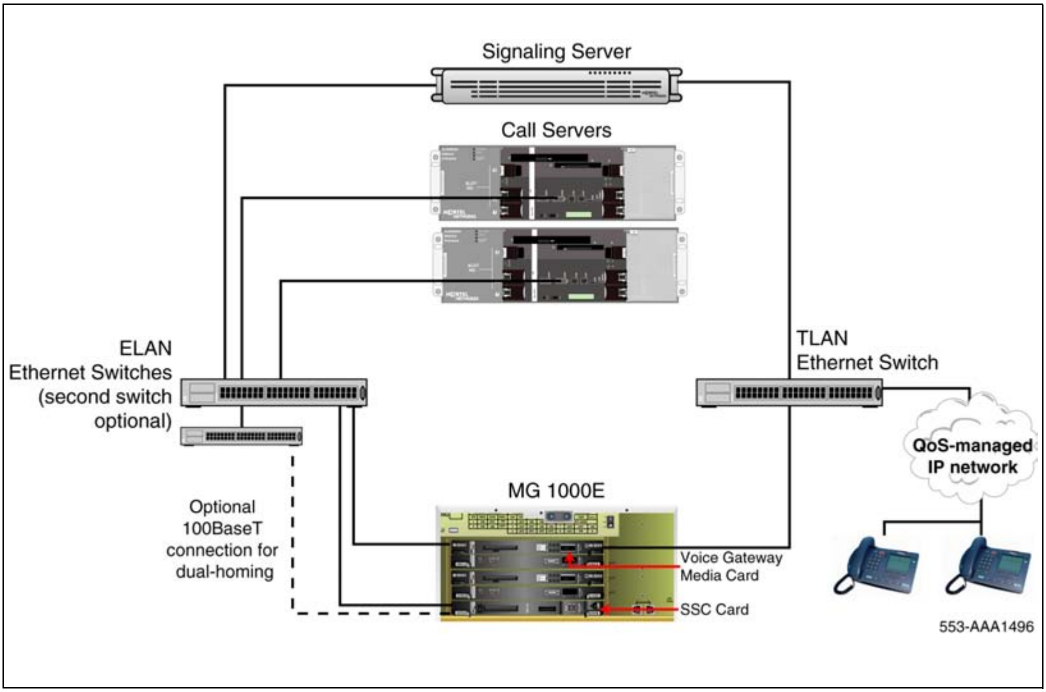
The security device on the MG 1000E SSC card is a generic security device that allows the MG 1000Es to register with the CS 1000E Core Call Servers.

Control for the activation of features assigned to the CS 1000E system, including MG 1000Es, is provided by the security device on the System Utility card in the Call Servers.

Network connections

Figure 12 shows a schematic representation of the typical network connections for one MG 1000E.

Figure 12
Network connections on MG 1000E



Note: The ELAN of the MG1000E may reside in a separate layer 3 subnet from that of the Call Server ELAN.

The separate LAN subnets that connect the MG 1000E and the Call Server to the customer IP network are as follows:

- **ELAN subnet**. The ELAN subnet (100BaseT, full-duplex) is used to manage signaling traffic between the Call Server, Signaling Server, and MG 1000Es. The ELAN subnet isolates critical telephony signaling between the Call Servers and the other components.
- **TLAN subnet**. The TLAN subnet (100BaseT, full-duplex) is used to manage voice and signaling traffic. It connects the Signaling Server and Voice Gateway Media Cards to the Customer LAN. It also isolates the IP Telephony node interface from broadcast traffic.

The dual-port IP daughterboard on the SSC card in the MG 1000E provides two 100BaseT ports for communication with the Call Server. In the basic configuration, Port 2 must connect to the ELAN through a Layer 2 or Layer 3 switch.

When connecting the MG 1000E to the ELAN through a Layer 3 switch, it must meet the following pararmeters: the connection from the Call Server to the MG 1000E must have a round trip delay of less than 20 msec and have a packet loss of less than 0.5 %.

To provide additional redundancy for the MG 1000E, the 100BaseT Port 4 should read port 1 switch to provide a dual-homed connection to the ELAN subnet. This allows the MG 1000E to remain operational if the Port 2 connection fails.

Functional description

The MG 1000E provides the following functionality:

- tones, conference, and digital media services (for example, Music and Recorded Announcement) to all phones
- support for CallPilot and Nortel Integrated Applications
- direct physical connections for analog (500/2500-type) phones, digital phones, and fax machines
- direct physical connections for analog trunks

Operating parameters

The MG 1000E operates under the direct control of the Call Server. Up to 30 MG 1000Es can be configured on the Call Server.

To allow IP Phones to access digital media services, the MG 1000Es must be equipped with Voice Gateway Media Cards.

The MG 1000E supports the following circuit cards and applications:

- Voice Gateway Media Cards: transcode between the IP network and digital circuit cards
- Service cards: provide services such as Music or Recorded Announcements (RAN)
- Analog interfaces to lines and trunks: support analog (500/2500-type) phones and fax, analog PSTN trunks, and external Music or RAN sources
- Digital line cards: support digital terminals, such as attendant consoles, M2000/M3900 series digital phones, and external systems that use digital line emulation, such as CallPilot Mini
- CLASS Modem card (XCMC)
- Nortel Integrated Applications, including:
  - Integrated Conference Bridge
  - Integrated Call Assistant
  - Integrated Call Director
  - Integrated Recorded Announcer
  - Hospitality Integrated Voice Services

- MGate cards for CallPilot
- CallPilot IPE

> **IMPORTANT!**
>
> The MG 1000E does not support digital trunks or PRI. Digital trunk and PRI access to the PSTN and other PBXs is provided by the MG 1000T.
>
> The MG 1000E does not support cards and applications that require a clock controller and a T1/E1 interface. This includes DECT Mobility cards, the Nortel Remote Gateway 9150 application, and the 802.11 Wireless IP Gateway.

Signaling Server

Main role

The Signaling Server provides SIP/H.323 signaling between components in a CS 1000E system.

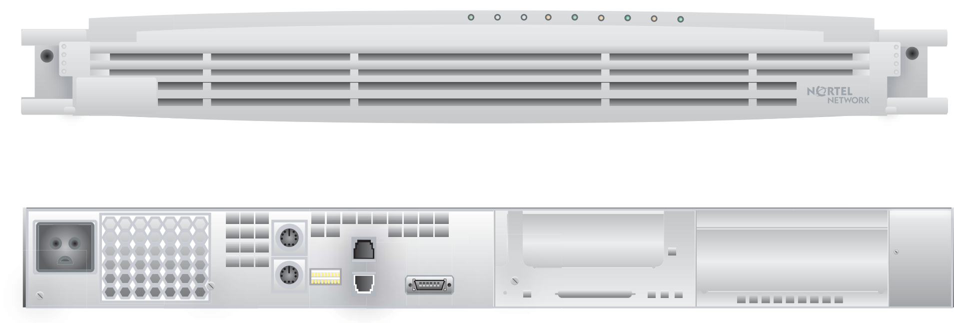
The Signaling Server is a standard hardware platform used to run multiple applications, including:

- SIP/H.323 Signaling Gateways
- Terminal Proxy Server (TPS)
- Network Routing Service (NRS)
- Element Manager
- Application Server for Personal Directory, Callers List, and Redial List for UNIStim IP Phones

Physical description

Figure 13 shows the Signaling Server.

Figure 13
Signaling Server front and rear



Hardware components

The front of the Signaling Server has the following components:

- A CD-ROM drive to load software files for the Signaling Server, Voice Gateway Media Cards, and IP Phones.
- A floppy disk drive if the CD-ROM is not bootable.
- A Maintenance port for a login session for Command Line Interface (CLI) management. (It does not provide system messages.)

  Note: Maintenance ports are on the front and back of the Signaling Server. Do not use both ports at once. The rear port is the recommended primary maintenance port.

The rear of the Signaling Server has the following components:

- The AC power cord connector provides an AC connection to the Signaling Server.

- The 100BaseT TLAN network interface is used for telephony signaling traffic.
- The 100BaseT ELAN network interface connects the Signaling Server to the Call Server and to the other CS 1000E components on the ELAN subnet.
- The rear maintenance port is the primary port for maintenance and administration terminals.
- The remaining ports are not used for any system functions. Do not plug any device into these ports.

Software applications

The following software components operate on the Signaling Server:

- Terminal Proxy Server (TPS)
- SIP Gateway (Virtual Trunk)
- H.323 Gateway (Virtual Trunk)
- Network Routing Service
  - H.323 Gatekeeper
  - SIP Redirect Server
  - Network Connection Server (NCS)
- CS 1000 Element Manager
- Application Server for the Personal Directory, Callers List, and Redial List features

All the software elements can coexist on one Signaling Server or reside individually on separate Signaling Servers, depending on traffic and redundancy requirements for each element.

For descriptions of each element's function and engineering requirements, see Table 30 on page 183. For detailed Signaling Server engineering rules and guidelines, see "Signaling Server algorithm" on page 218. For more information about H.323 and SIP Trunking, refer to *IP Peer Networking: Installation and Configuration* (553-3001-213).

Functional description

The Signaling Server provides the following functionality:

- provides IP signaling between system components on the LAN
- enables the Call Server to communicate with IP Phones and MG 1000Ts
- supports key software components (see "Software applications" on page 60)

Operating parameters

The Signaling Server provides signaling interfaces to the IP network using software components that run on the VxWorks operating system.

The Signaling Server can be installed in a load-sharing, survivable configuration.

The total number of Signaling Servers that you require depends on the capacity and redundancy level that you require (see "Signaling Server algorithm" on page 218).

Terminal Server

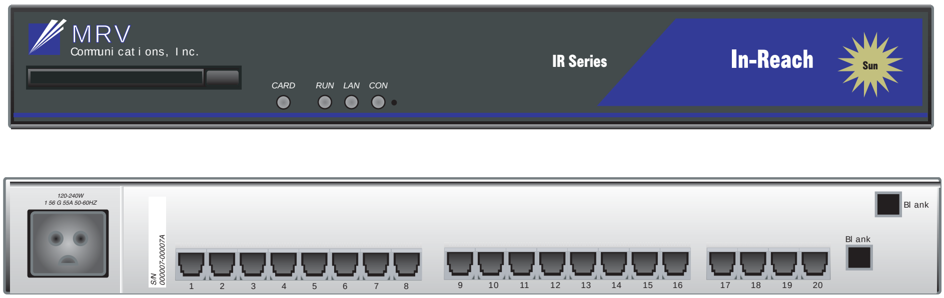
Main role

The MRV IR-8020M IP-based Terminal Server provides the Call Server with standard serial ports for applications and maintenance.

Physical description

Figure 14 shows the Terminal Server.

Figure 14
Terminal Server



Hardware components

The MRV Terminal Server provides 20 console ports for modular RJ-45 connectors. It is also equipped with one RJ-45 10BaseT connection for network interface to the ELAN subnet and an internal modem to provide remote access.

Operating parameters

Traditionally, serial ports are used to connect terminals and modems to a system for system maintenance. As well, many third-party applications require serial port interfaces to connect to a PBX. Because the Call Server provides only two local serial ports for maintenance purposes, an IP-based Terminal Server is required to provide the necessary serial ports.

The Terminal Server provides standard serial ports for applications. These applications include billing systems that analyze Call Detail Recording (CDR) records, Site Event Buffers (SEB) that track fault conditions, and various legacy applications such as Property Management System (PMS) Interface and Intercept Computer applications. In addition, serial ports are used to connect system terminals for maintenance, modems for support staff, and printers for system output.

The Terminal Server is configured to automatically log in to the active Call Server at start-up. For this reason, each Call Server pair requires only one Terminal Server. Customers can configure up to 16 TTY ports for each Call Server pair.

The Terminal Server can be located anywhere on the ELAN subnet. However, if the Terminal Server is used to provide local connections to a Com port on the Call Server, it must be collocated with the system.

The Terminal Server can also be used as a central point to access and manage several devices through their serial ports.

IMPORTANT!

Currently, the CS 1000E only supports the MRV IR-8020M commercial Terminal Server.

Media Gateway 1000T

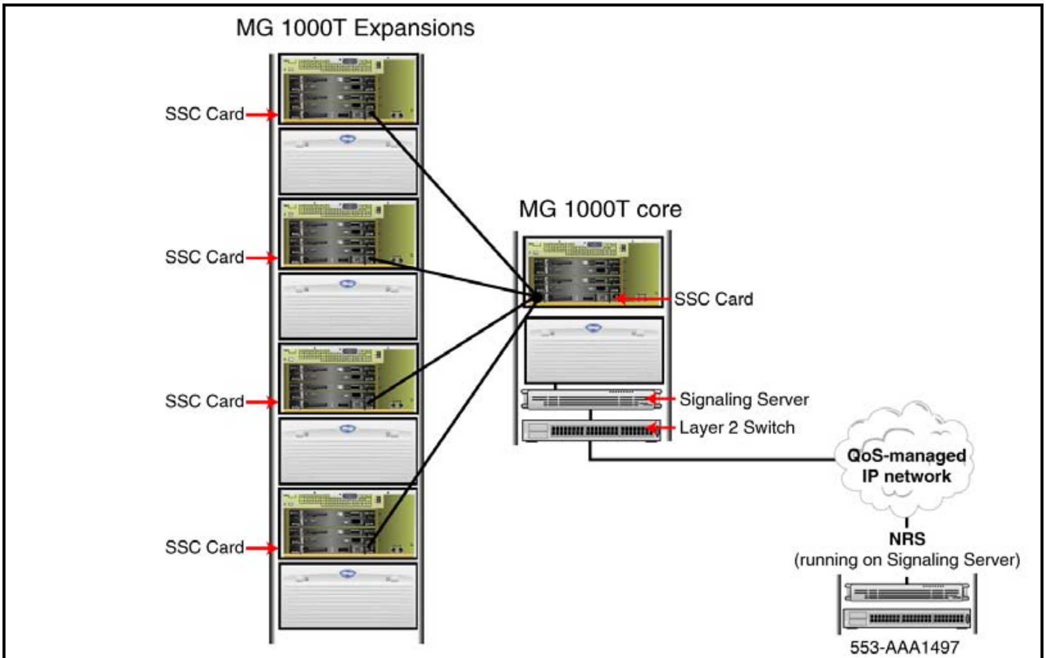
Main role

The Media Gateway 1000T (MG 1000T) platform provides the CS 1000E with digital trunk and PRI access to the PSTN and to other PBX systems. It functions as an independent resource on the network and is therefore accessible by any peer node on the network using the NRS. Given its main role as a trunking gateway, the MG 1000T cannot be provisioned with User Licenses (with the exception of DECT User Licenses).

Physical description

Figure 15 shows the MG 1000T Core controlling the MG 1000T Expansions through connections to the SSC cards.

Figure 15
Media Gateway 1000T



Hardware components

The MG 1000T Core and Expansions each house an SSC card and contain four slots for IPE cards. They also each support an optional MG 1000T Expander through copper connections.

The MG 1000T Core and Expansions use the same base hardware as the MG 1000E. For more information, see "Media Gateway" on page 42.

MG 1000T Core

Unlike the MG 1000Es, the MG 1000T platform does not operate under the direct control of the CS 1000E Core Call Servers. Instead, the MG 1000T Core (MG 1000T 0) provides the primary processing for the MG 1000T platform. The MG 1000T Core SSC card controls the circuit cards in the MG 1000T Core and all cards in up to four MG 1000T Expansions.

The MG 1000T Core SSC card can be equipped with two dual-port IP daughterboards, providing a total of four IP ports for connections to the SSC cards on the MG 1000T Expansions. As a result, each MG 1000T Core can support up to four MG 1000T Expansions with optional MG 1000T Expanders.

Figure 16 shows the MG 1000T Core SSC card components. The 100BaseT cables connect the dual-port IP daughterboard ports 1, 3, 2, and 4 to the MG 1000T Expansion SSC cards.

Figure 16
MG 1000T Core SSC card components

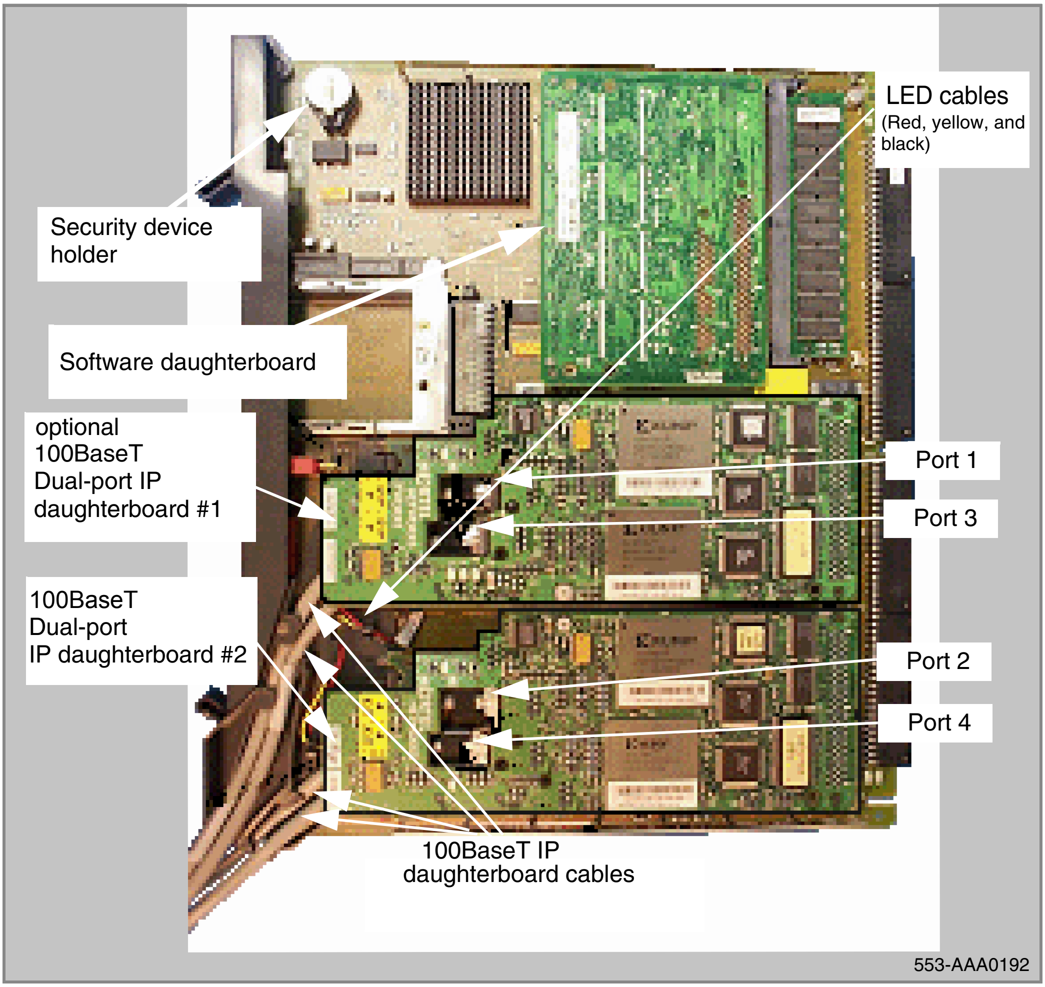
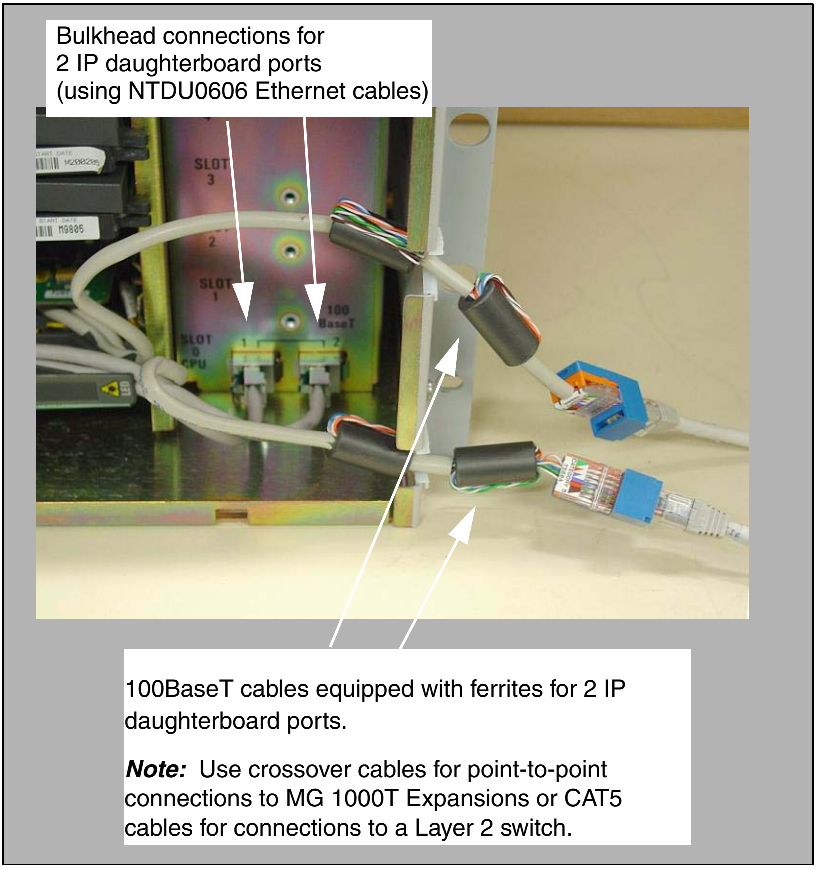


Figure 17 shows the cabling from the SSC card on the MG 1000T Core.

Figure 17
MG 1000T Core cabling



Two IP daughterboard ports on the MG 1000T Core SSC connect to the bulkhead, providing rear bulkhead connections to two MG 1000T Expansions. The other two IP daughterboard ports on the SSC connect directly to the remaining two MG 1000T Expansions.

> *Note:* SSC cards on the four MG 1000T Expansions are equipped with single-port IP daughterboards.

Connections between the MG 1000T Core and the MG 1000T Expansions can be made through directly connected 100BaseT crossover cable or through a Layer 2 switch.

Security devices

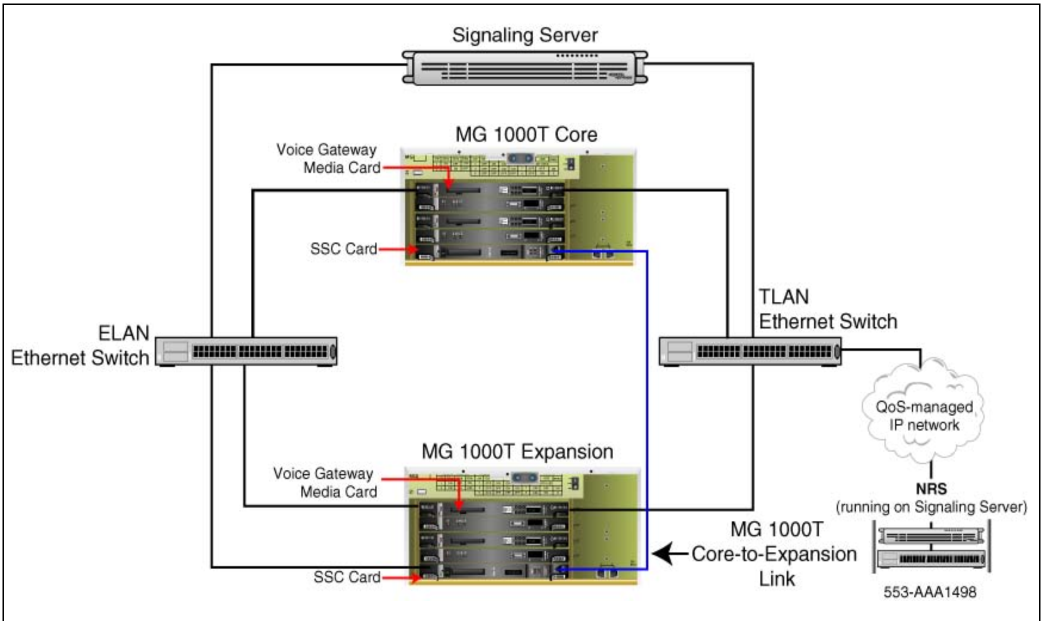
The security device on the MG 1000T Core SSC card enables the activation of the software and features assigned to the MG 1000T.

The security device on the MG 1000T Expansion SSC cards are directly associated with the MG 1000T Core security device.

Network connections

Figure 18 shows a detailed view of typical network connections between the MG 1000T Core, an MG 1000T Expansion, and the QOS-managed IP network.

Figure 18
Network connections on MG 1000T



The separate LAN subnets that connect the MG 1000T to the customer IP network are as follows:

- **Core-to-Expansion Link (SLAN subnet)**. Each MG 1000T Expansion directly connects to the MG 1000T Core through a special IP link (point-to-point or through a Layer 2 switch). This IP link carries signaling and telephony traffic.
- **ELAN subnet**. The ELAN subnet (10/100BaseT, full-duplex) can belong to, or be separate from, the main CS 1000E ELAN subnet. The ELAN subnet provides management and signaling functions for MG 1000T components.
- **TLAN subnet**. The TLAN subnet (100BaseT, full-duplex) provides voice and signaling traffic and isolates the IP Telephony node from broadcast traffic.

The MG 1000T communicates with the CS 1000E using IP Peer Networking with Signaling Servers. The Signaling Servers run SIP and H.323 Signaling Gateway software.

As a result, the MG 1000T platform can be separated from the CS 1000E across the network to provide PSTN access wherever needed. With IP Peer Networking, any CS 1000E system in the network can access the MG 1000T using the NRS for numbering plan resolution and least cost routing.

The MG 1000T can be collocated with the CS 1000E system to provide a configuration that is similar to that of a traditional PBX.

Functional description

The MG 1000T provides the following functionality:

- provides digital trunks to the PSTN and trunking to other PBX systems using E1, T1, and ISDN BRI circuit cards
- supports analog trunks
- supports Voice Gateway Media Cards for transcoding between IP and TDM
- supports the DECT application

Operating parameters

The MG 1000T functions as an independent resource on the network. It is therefore accessible by any peer node on the network in addition to the CS 1000E.

To provide IP Phones with access to digital trunking, the MG 1000T must use Voice Gateway Media Cards. The Voice Gateway Media Cards provide DSP ports to translate between IP and TDM.

The MG 1000T uses a Signaling Server to communicate with the Call Server across the IP network. The Signaling Server runs SIP/H.323 Signaling Gateway software. Signaling between the Call Server and the MG 1000T uses the SIP protocol or the H.323 protocol, with MCDN extensions to provide more complete feature transparency.

The MG 1000T supports the following circuit cards:

- Media Cards: transcode between the RTP media streams on the IP network and the interface cards within the gateways
- Digital PSTN Interface Cards, including E1, T1, and ISDN Basic Rate interfaces: provide access to PSTN
- Analog trunk cards
- Service cards: provide services such as Music or Recorded Announcements (RAN)
- DECT Mobility cards

Note: As an alternative to installing an MG 1000T, the CS 1000E can obtain PSTN access by using IP Peer Networking with other systems in the network, such as a pre-existing CS 1000M Large System, a CS 1000S, or an MG 1000B.

Layer 2 switch

Main role

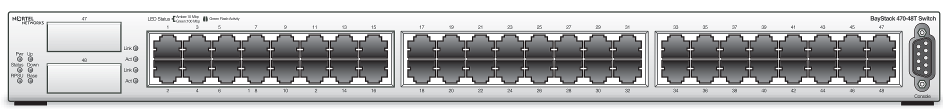
The Layer 2 switch transmits data packets to devices interconnected by Ethernet to the ELAN or TLAN subnets. The switch only directs data to the target device, rather than to all attached devices.

Physical description

ELAN Layer 2 switch

Figure 19 shows an example of an ELAN Layer 2 switch.

Figure 19
ELAN Layer 2 switch (BayStack 470-48T)



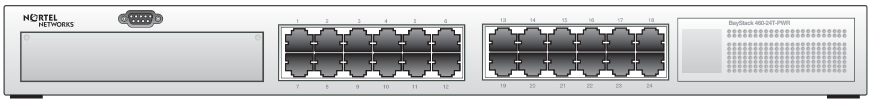
TLAN Layer 2 switch

To provide Layer 2 connections on the TLAN subnet, Nortel recommends the BayStack 460 Ethernet switch, which has embedded Power-over-LAN capabilities for powering IP Phones.

Optionally, other Power-over-LAN units can also be used to provide power to IP Phones.

Figure 20 shows the BayStack 460 Layer 2 switch.

Figure 20
TLAN Layer 2 switch (BayStack 460)



Operating parameters

These components must be supplied by the customer. See *Converging the Data Network with VoIP* (553-3001-160) for further details.

Component dimensions

All components fit in 19-inch racks. Table 1 lists the height of each component.

Table 1
Height dimension of CS 1000E components

Component	Height
NTDU62 Core Call Server	3 U
Signaling Server	1 U
NTDU14 Media Gateway	< 5 U
NTDU15 Media Gateway Expander	< 5 U
MRV Terminal Server	1 U
BayStack 460	< 2 U
BayStack 470	1 U
Note: 1 U = 4.4 cm (1-3/4 in.)	

The clearance in front of rack-mounted equipment is the same for all major components. For the Core Call Servers, Media Gateways, and Media Gateway Expanders, the distance from the mounting rails of the rack to the front of the bezel/door is 7.6 cm (3 in.).

Configuration options

Contents

Introduction

The IP-distributed architecture of the CS 1000E enables flexibility when it comes to component location. Given this flexibility, the CS 1000E offers many configuration options to support increased system redundancy.

The CS 1000E can be deployed in many ways in LAN and WAN environments. Although many different installations are possible, most fall into one of the following categories:

- Multiple buildings in a campus
  - Campus-distributed MG 1000Es
  - Campus Redundancy
- Multiple sites
  - Central Call Server with Branch Office
  - Geographic Redundancy

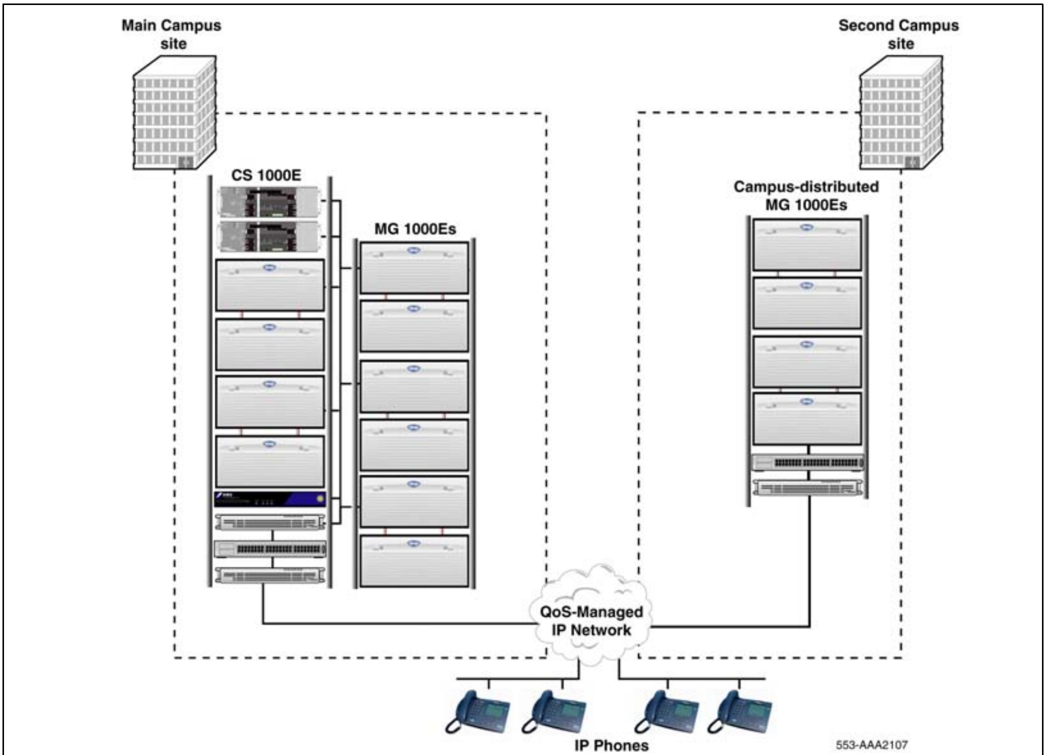
The following sections describe each of these configuration options.

Note: These configurations provide CS 1000E systems with many options for redundancy and reliability. Careful planning is required to determine which configuration is right for your needs.

Option 1: Campus-distributed MG 1000Es

With multiple buildings in a campus, you can distribute MG 1000Es across a campus IP network. Figure 21 shows MG 1000Es distributed across multiple buildings in a campus setting.

Figure 21
Campus-distributed MG 1000Es



In this configuration, a CS 1000E system is installed at the main site, and additional MG 1000Es and an optional Signaling Server are installed at a second campus site. All IP Phones are configured and managed centrally from the main site.

> ***Note:*** For details on the specific operating and network parameters for the MG1000E, see "Media Gateway 1000E" on page 52.

Modem traffic

The CS 1000E supports modem traffic in a campus-distributed network with the following characteristics:

- Media Card configuration:
  - G.711 codec
  - 20 msec packet size
- one-way delay less than 5 msec
- low packet loss

> ***Note:*** Performance degrades significantly with packet loss.

IMPORTANT!

Nortel has conducted extensive but not exhaustive tests of modem-to-modem calls, data transfers, and file transfers between a CS 1000E and MG 1000T, using Virtual Trunks and PRI tandem trunks. While all tests have been successful, Nortel cannot guarantee that all modem brands will operate properly over all G.711 Voice over IP (VoIP) networks. Before deploying modems, test the modem brand within the network to verify reliable operation. Contact your system supplier or your Nortel representative for more information.

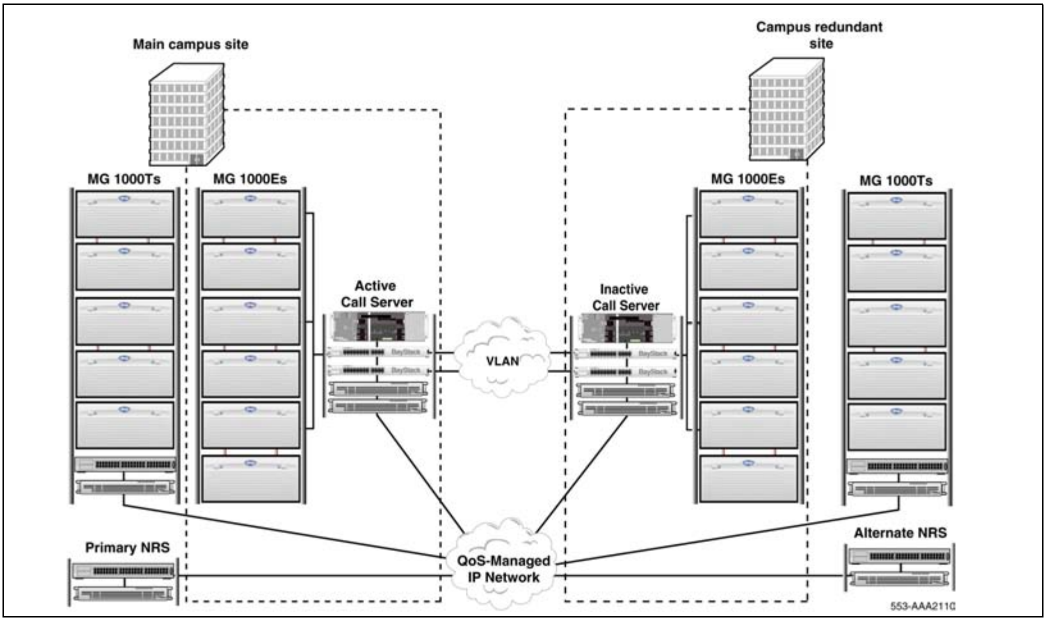
Option 2: Campus Redundancy

With Campus Redundancy, customers can separate the Call Server pair across a campus IP network (the distance depends upon network parameter limitations specified in *Communication Server 1000: System Redundancy*

(553-3001-307)). This provides additional system redundancy within a local configuration. The Call Servers function normally and the inactive Call Server assumes control of call processing if the active Call Server fails.

To do this, the ELAN subnet and the subnet of the High Speed Pipe (HSP) are extended between the two Call Servers using a dedicated Layer 2 Virtual LAN configured to meet specified network parameters. Figure 22 shows a CS 1000E system in a Campus Redundancy configuration. For more information, refer to *Communication Server 1000: System Redundancy* (553-3001-307).

Figure 22
Campus Redundancy configuration

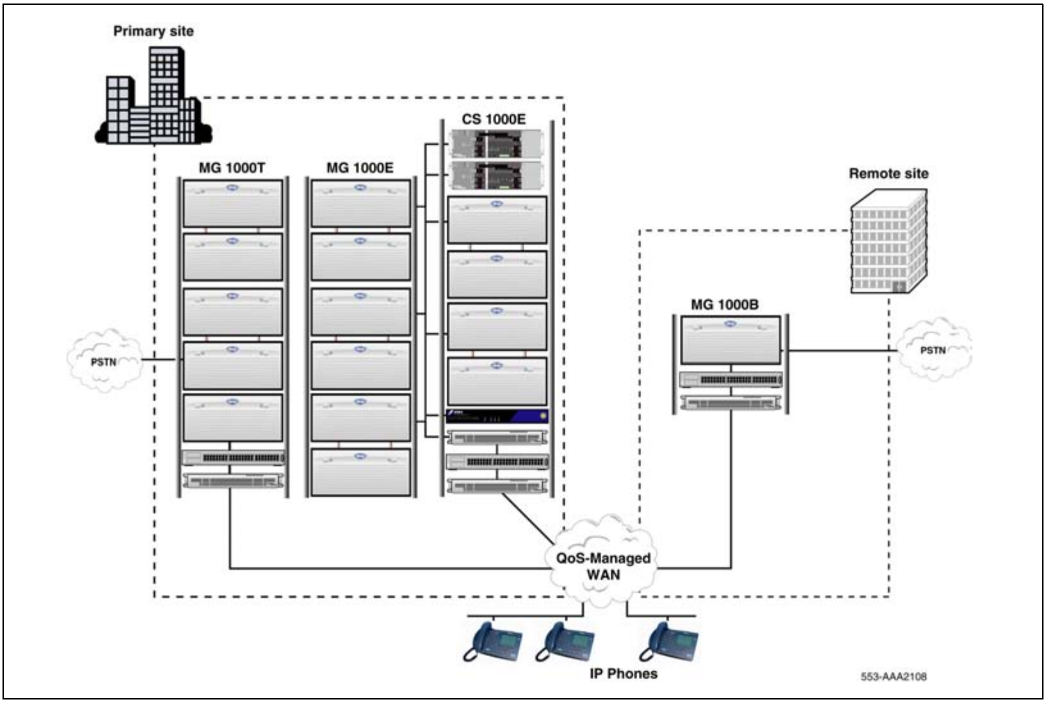


For more information on Campus Redundancy, see *Communication Server 1000: System Redundancy* (553-3001-307).

Option 3: Branch Office

The CS 1000E system supports the Branch Office feature, which provides central administration of Media Gateway 1000Bs (MG 1000B) at remote sites. Figure 23 shows a CS 1000E system with an MG 1000B installed at a remote branch office.

Figure 23
Branch Office configuration



In this configuration, the MG 1000B is survivable. This ensures that telephone service remains available if the main office fails. For more information, refer to *Branch Office: Installation and Configuration* (553-3001-214).

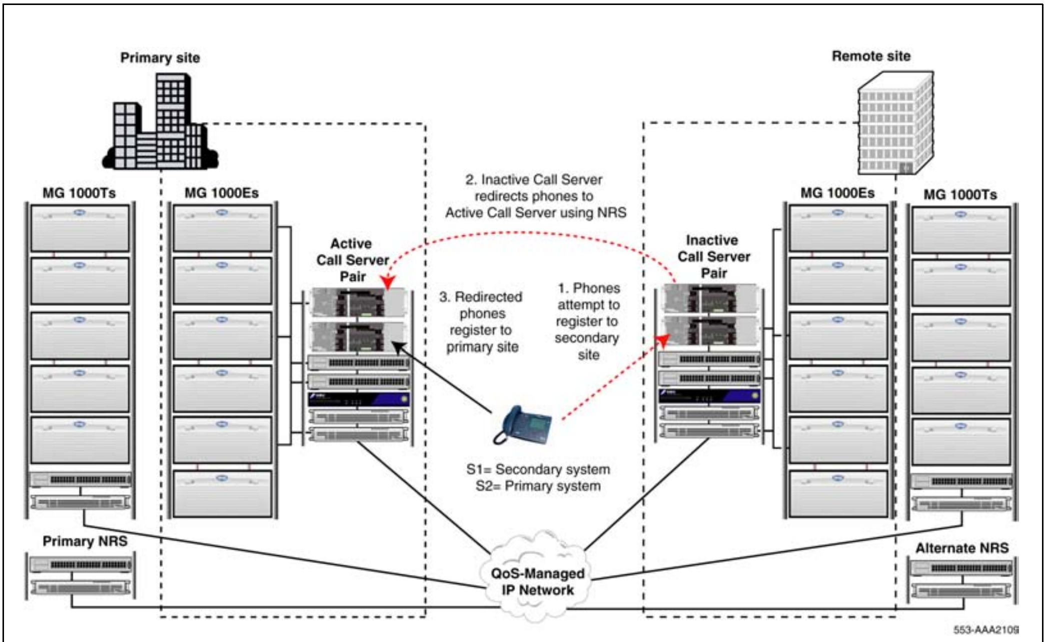
Option 4: Geographic Redundancy

Geographic Redundancy provides an additional layer of system redundancy. It allows a customer to locate a secondary backup system at a distance from a primary system. This ensures redundancy in the event of catastrophic failure of the primary site. With Geographic Redundancy, the configuration and user database of the primary system can be replicated across the WAN.

Figure 23 shows an inactive CS 1000E system backing up an active system using Geographic Redundancy.

> ***Note:*** Geographic Redundancy provides redundancy for IP Phones only.

Figure 24
Geographic Redundancy



For more information on Geographic Redundancy, see *Communication Server 1000: System Redundancy* (553-3001-307).

Preparing a system installation plan

Contents

This section contains information on the following topics:

Introduction

> **WARNING**
>
> Before a CS 1000E system can be installed, a network assessment **must** be performed and the network must be VoIP-ready.
>
> If the minimum VoIP network requirements are not met, the system will not operate properly.
>
> For information on the minimum VoIP network requirements and converging a data network with VoIP, refer to *Converging the Data Network with VoIP* (553-3001-160).

Planning for system installation affects the installation cost, as well as operation and maintenance, and can have an overall effect on system performance. Consider the following requirements (in addition to local and national building and electrical codes) when you plan a system installation.

Select and evaluate sites according to the requirements in this document and the following criteria:

- Space:
  - The site must provide adequate space for unpacking, installation, operation, potential expansion, service, and storage. The site must provide space for sufficient cooling. You may need additional space for a maintenance and technician area.
- Location:
  - The location should be convenient for equipment delivery and close to related work areas. Consider the location of related equipment, such as the distribution frame and batteries for Uninterruptible Power Supply (UPS) units. Also consider cable limitations.
- Grounding and power:
  - Proper grounding and sufficient power facilities must be available.

- Structural integrity:
  — The floor must be strong enough to support anticipated loads and, if applicable, the ceiling must be able to support overhead cable racks.

Creating an installation plan

To assist with the development of the installation plan, create an Installation Outline and a Milestone Chart.

Installation outline

Use Table 2 on page 84 as a guide for preparing a detailed installation plan.

Table 2
Installation plan outline

Procedure	Requirements
Researching site requirements	— Determine fire, security, and safety requirements — Determine equipment room requirements — Determine grounding and power requirements — Determine cable requirements
Planning the site	— Prepare a floor plan — Estimate floor loading — Prepare the building cabling plan
Preparing for delivery and installation	— Prepare for delivery — Prepare for installation

Milestone chart

Planning and monitoring site preparation activities is easier when you use a milestone chart. A milestone chart is a general site planning schedule showing the sequence of activities necessary to complete a job.

Table 3 on page 85 lists typical activities included in a milestone chart. For a complex site, you must create a more detailed chart.

Table 3
Milestone chart

Task	Action
1	Select the site.
2	Plan fire prevention and safety features.
3	Plan the equipment room layout.
4	Plan grounding and power.
5	Plan cable routes and terminations.
6	Plan and start any renovations to the equipment room.
7	Continue site construction and renovation tasks.
8	Install grounding, power, air conditioning, and heating.
9	Install special rigging, such as overhead cable racks and distribution frame equipment, as required.
10	Test site wiring to ensure that minimum requirements are met.
11	Complete construction and ensure that grounding and power are in place.
12	Test air conditioning and heating systems.
13	Make equipment delivery arrangements.
14	Complete equipment room inspection, identifying and resolving any delivery constraints.

When you prepare a milestone chart, consider not only individual operations, but the overall installation schedule. The milestone chart should show the necessary operations in order and may assign a start and end date for each activity.

Fire, security, and safety requirements

Building, fire, and safety codes establish the degree of protection required for an installation. Additional information is available from the National Fire Protection Association (NFPA) in “Standard for the Protection of Electronic Computer/Data Processing Equipment” (NFPA 75) and “National Electrical Code (NEC)” (NFPA 70).

Fire protection and prevention

Expertise is required to properly locate and install:

1. Sprinkler heads
2. Fire and smoke sensing devices
3. Other fire extinguishing equipment

During the planning stage, consult local codes, experts, insurance underwriters, and local building authorities.

You can implement some fire precautions when an equipment area is constructed. For example, extend walls from floor to ceiling, and construct walls, floor, and dropped ceiling of noncombustible material.

If the structural floor is made from combustible materials, cover it with a noncombustible covering and remove all debris between the raised and permanent floors before the system is installed. If there are power connections beneath a raised floor, use waterproof electrical receptacles and connectors.

You can install shatterproof windows and sprinklers outside and above the windows to keep fire from spreading from an adjacent room or building. The roof or floor above the equipment area must be watertight. Design ducts and plumbing for air-conditioning systems to keep fire, heat, and smoke from spreading from one part of a building to another. Install smoke detectors in all appropriate places.

Regularly check services such as steam, water, and power, and inspect pipes for excess condensation, leaks, or corrosion.

Fire extinguishing systems

In most cases, carbon dioxide or water sprinkler systems are the recommended fire extinguishing systems.

Dry-pipe water sprinklers are strongly recommended. This type of system interrupts power to the room and opens a master valve that fills the overhead sprinklers.

Carbon dioxide systems are also effective in containing a fire, but they quickly exhaust the oxygen supply. If you use a carbon dioxide system, you must install an alarm to warn site personnel when carbon dioxide is released. For health and safety reasons, employees must be evacuated within 30 seconds of the release.

DANGER

Nortel does not recommend using Halon or any other fire extinguishing system that is not described above.

Security precautions

You may need to extend and improve existing building security to provide adequate protection for the equipment. For example, you can install safeguards such as tamper proof keylock door controls and electrically taped glass doors and windows that can tie into an alarm system. You can also install a monitoring unit using closed-circuit television.

> ***Note:*** Electric locks, such as push button access code or card reader locks, are not recommended unless you provide a battery backup or a key override.

Protect critical data, such as business records, by storing backups well away from the equipment room. A regular updating program is highly recommended.

Safety procedures and training

Company personnel should be taught how to respond to emergencies; some companies designate trained individuals as security members. Training can include when and how to evacuate personnel and records, notify the fire department, shut off all electrical power, and handle fire extinguishers properly.

In addition, install temperature and humidity monitoring devices (both visual and audible alarm signals) in equipment and storage rooms so people can respond quickly to an emergency.

Occupational noise exposure

If employees are subjected to noise levels exceeding local standards, or the levels listed in 1910.5 of the Occupational Safety and Health Administration (OSHA) Standards, initiate administrative and engineering controls. If these controls do not reduce sound levels effectively, provide protective equipment.

> ***Note:*** The acoustic noise generated by a system ranges from 45 dBA to 60 dBA (decibels "A"-weighted).

Equipment room requirements

The environment for the system (and for storing spare parts) can influence system performance and reliability. Temperature, humidity, and other environmental factors, such as static electricity, must be controlled to meet system operating requirements.

Space requirements

Space and equipment layout requirements differ with each installation. When you plan the site, consider the following requirements:

- Primary storage
- Secondary storage
- Maintenance and technician space

Primary storage

The floor area required for a system depends on the number of racks, the length-to-width ratio of the area, and the location of walls, partitions, windows, and doors. To determine the exact layout required, prepare a detailed floor plan after regarding all of the requirements in this chapter.

Although operating needs determine the general location of terminal devices, these devices must not be located beyond the maximum distances defined by the Terminal Server. Wall jacks and outlets must be provided for all devices located in the equipment room.

Secondary storage

Provide space in the equipment area for storing disks, printer paper, printouts, and daily reports. A secure storage room for spare parts is recommended.

Whenever possible, maintain the same environmental conditions in the equipment room and storage areas. If it is not possible to maintain the environment of the storage area exactly the same as the environment of the operating equipment, give stored materials time to adjust to the equipment room environment before using them.

Maintenance and technician space

You can use the maintenance and technician area as an online work center and a place to store tools, test equipment, system documents, and spare parts. The area should have good lighting and convenient access to the system.

Typical items in a maintenance and technician area include:

- Shelves for instruction books
- Spare parts storage room
- Paper storage area
- Locking cabinet or storage area for backup disks
- Table or desk
- Terminal, printer, or equivalent device

During regular system operation, a terminal, or a modem, or both must be connected permanently to the system to provide a constant I/O interface. You can use more than one terminal or modem. Plan for surface apace, power outlets, and the availability of the terminals/modems before installation.

Temperature and humidity control

Frequent and extended system operation above recommended temperature limits can degrade system reliability. Low humidity can increase static electricity build-up, while high humidity can affect the performance of disks and printers.

Take temperature readings 76 cm (30 in.) from the front of the system. Table 4 shows system operating requirements.

DANGER

Damage to Equipment

Do not expose equipment to absolute temperature limits for more than 72 hours. Do not place heat sources (such as floor heaters) near the equipment.

Table 4
Operating environment

Equipment	Temperature and humidity considerations
CS 1000E	Recommended: — 15° to 30°C (59° to 86°F) — RH 20% to 55%, non-condensing Absolute: — 10° to 45°C (50° to 113°F) — RH 20% to 80%, non-condensing — temperature change less than 10°C (18°F) per hour
Telephones	Absolute: — 0° to 50°C (32° to 122°F) — RH 20% to 80%, non-condensing
Other terminal devices (such as personal computers, data sets, and printers)	Refer to the specific documentation or manufacturer's guidelines

If you operate the system within recommended temperature limits, there are no thermal restrictions on any equipment.

Follow the specifications listed in Table 5 to store or transport equipment.

Table 5
Storage environment

Equipment	Temperature/humidity considerations
CS 1000E Call Server	— –50° to 70°C (–58° to 158°F) — RH 5% to 95%, non-condensing
Telephones	— –50° to 70°C (–58° to 158°F) — RH 5% to 95%, non-condensing
RMD (Compact Flash)	— -25° to -70°C (-13° to -94 °F) — RH 8% to 95%, non-condensing
Media Gateways	— –50° to 70°C (–58° to 158°F) — RH 5% to 95%, non-condensing
Other terminal devices	Refer to the specific Nortel publication or the manufacturer's guidelines
Note: Temperature changes must be less than 30° C (54° F) per hour for storage and during transportation.	

Air conditioning guidelines

Use the following guidelines to estimate air conditioning requirements. Exact requirements must be determined by a qualified air conditioning engineer.

1 The air conditioning system in equipment areas must handle:

- **a** the heat produced by the equipment, room personnel, and lighting; and,
- **b** the heat that comes through walls, windows, floors, and ceilings.

2 A stable ambient operating temperature of approximately 22 degrees C (72 degrees F) is recommended. The temperature differential in the equipment room must not exceed ±3.0 degrees C (±5 degrees F).

Note: For systems with reserve power equipment, consult the manufacturer's specifications for recommended operating temperatures.

3 Heat dissipation from a system is estimated in Btu per hour (Btu/hr). You can estimate the amount of air conditioning required at a rate of one ton of refrigeration for every 12 000 Btu/hr of heat generated in the equipment area plus one ton for each 500 sq ft of floor space.

Note: Each person in the equipment room generates 600 Btu/hr.

CAUTION

Damage to Equipment

Because digital systems require constant power (even if the system is idle), they generate heat continuously. Air conditioning requirements must be met at all times.

4 Table 8 on page 124 and Table 9 on page 125 show the thermal dissipation for system components.

Other environmental factors

In addition to temperature and humidity, many environmental factors must be controlled in equipment areas. The environmental factors that must be controlled include:

- Static electricity
- Vibration
- Electromagnetic and radio frequency interference (EMI/RFI)
- Dust
- Lighting
- Earthquake bracing
- Structural features

Static electricity

Electronic circuits are extremely sensitive to static discharge. Static discharge can damage circuitry permanently, interrupt system operation, and cause lost data.

Static electricity can be caused by physical vibration, friction, and the separation of materials. Other common causes of static electricity build-up are low humidity, certain types of carpeting, the wax on equipment room floors, and plastic-soled shoes. The human body is the most common collector of static electricity. A combination of plastic-soled shoes, certain flooring materials, and low humidity can cause body charges in excess of 15 kV.

> ***Note:*** IEEE Standard 142-1982 recommends that flooring resistance be more than 25 000 ohms and less than 1 million megohms, measured by two electrodes 0.91 m (3 ft) apart on the floor. Each electrode must weigh 2.2 kg (5 lb) and have a dry flat contact area of 6.35 cm (2.5 in.) in diameter.

Antistatic wrist straps, sprays, and mats are available. Nortel recommends at least using an antistatic wrist strap whenever you work on equipment.

Vibration

Vibration can cause the slow deterioration of mechanical parts and, if severe, can cause serious disk errors. Avoid structure-borne vibration and consequent noise transferred to the equipment room. Raised floors must have extra support jacks at strategic places to prevent the transmission of vibration.

Limit vibration in an office environment to a frequency range of 0.5–200 Hz and a G-force magnitude of 0.1 G (in accordance with the Bellcore “Network Equipment Building Systems Generic Equipment Requirements” specification TR-EOP-000063).

Electromagnetic and radio frequency interference

Sources of electromagnetic and EMI/RFI located close to equipment can cause problems with system operation. Common EMI/RFI sources known to disturb system operation include:

- Thunderstorms, static electricity, and high-voltage power lines

- Radar, broadcast stations, and mobile communications
- Power tools, appliances (such as vacuum cleaners), and office business machines (such as copiers)
- Industrial machines and ultrasonic cleaners
- Vehicle ignition, arc welders, and dielectric heaters
- Dimmer switches

Dust

Accumulated dust and dirt can degrade system reliability and performance. Dust and dirt can:

- Scratch the contacts on circuit cards causing intermittent failures
- Have conductive contents that increase static electricity in the environment
- Cause components to operate at higher temperatures

Average dust density for an office environment must be 0.00014 g/m3 or better. False ceilings and tiled floors help maintain dust density requirements.

Lighting

Lighting illumination of 50 to 75 footcandles measured 76 cm (30 in.) above the equipment room floor is recommended. Avoid direct sunlight in the equipment room to prevent malfunctions by devices with light sensors (such as disk units).

Lighting must not be powered from the equipment room service panel. For large system installations, consider provisions for emergency lighting in the equipment room.

Earthquake bracing

Earthquake (seismic) bracing is required or should be considered in some locations.

Structural features

Use sealed concrete, vinyl, or mastic tile for flooring and ensure that it meets the floor loading requirements described later in this document. Avoid using sprayed ceilings or walls.

Grounding and power requirements

Refer to "Power and grounding" on page 109 for detailed information.

Reserve power equipment room

If the reserve power equipment is located in a separate room then that room must meet the following conditions.

1. Well-ventilated and operating at optimum temperature; specific gravity readings are based on 25 degrees C (77 degrees F)
2. Located within the recommended proximity to the system
3. Equipped with protective equipment (such as goggles, face shields, acid-resistant gloves, protective aprons, water for rinsing eyes/skin, and bicarbonate of soda)
4. Well-secured
5. Accessible (the doorway must not be blocked)
6. Meet all floor loading requirements and the noise levels required by OSHA standards 1910.5 (or local standards)

Note: For detailed instructions on battery usage, see ANSI/IEEE Standard 450-1987: "Maintenance, Testing and Replacement of Large Storage Batteries."

Cable requirements

This section describes the types of cable used in the system. It also provides some cabling guidelines.

Cable types

The system uses the following major types of wiring:

- 25-pair main distribution frame (MDF) cables:
  These cables carry voice and data information between gateways and the distribution frame. One end of the cable must be equipped with a 25-pair female connector that terminates on the module input/output (I/O) panel. The other end of the cable terminates on the MDF block.
- Interface cables:
  Interface, or I/O, cables are typically 25-conductor interfaced through RS-232-C connectors. These cables are used to connect data units to printers, host computers, and modems.
- Three Port cables:
  This cable is used to interface between terminal equipment and the terminal port on the Media Gateway. This is a permanent cable on the MG1000T Core, but on the MG1000E it is required only for initial configuration of IP addresses.
- Cat 5 cables:
  These are standard cables used to connect LAN equipment and are terminated with RJ45 connectors. These are specified as either being standard or straight through or as cross over. Not recommended for speeds greater than 100 Mbps.
- Cat 5E (Cat 5 Enhanced) cables:
  The Cat 5E are the same as Cat 5 cables, but made to more stringent requirements. They are also designed for speeds up to 1 Gbps.
- Cat 6 cables:
  The same as Cat 5E, but made to more stringent standards. Designed for speeds up to 1 Gbps.

- Terminal server cables:
  This is a proprietary cable that can be used to interface between the MRV Terminal Server and various system components in order to allow terminal access.
- Twisted-pair telephone cables:
  These cables carry analog voice and digitized voice and data information between distribution frames and terminal devices throughout the building. They connect to 8-pin modular jacks located within 2.4 m (8 ft) of each device.

  Note: Consider cable length requirements and limitations for both initial installation and later growth when you plan a system.

Cable access

The customer is responsible for supplying all access for station, feeder, and riser cabling. This includes (where necessary):

- Conduit
- Floor boring
- Wall boring
- Access into hung ceilings

LAN design

For information on the requirements for creating a robust, redundant network, refer to *Converging the Data Network with VoIP* (553-3001-160).

Keep a record of the IP addresses assigned to system components. See Figure 25 on page 98 for a sample.

Figure 25
Sample IP address record sheet

xx.xx.xxx.128/25				
xx.xx.xxx.129	Gateway			
255.255.255.128	Subnet Mask	TLAN Subnet Mask	255.255.252.0	
xx.xx.xxx.128 – xx.xx.xxx.159	Logical blocks of 32 addresses (first four addresses in each block reserved for Layer 2 and Layer 3 equipment)	Node IP Address	xxx.xx.x.252	
xx.xx.xxx.160 – xx.xx.xxx.191		TLAN Gateway	xxx.xx.x.1	
xx.xx.xxx.192 – xx.xx.xxx.223				
xx.xx.xxx.224 – xx.xx.xxx.255				

ELAN Subnet Number	MAC address (by byte/octet)						Equipment Description	Serial Number	Comment	TLAN Subnet Address	Location	
	B1	B2	B3	B4	B5	B6					Rack	L/S/C
xx.xx.xxx.130	00	0C	F8	xx	xx	xx	Baystack 460	SDNIHR1xxx	ELAN_3		R2	
xx.xx.xxx.133	00	00	75	xx	xx	xx	SSC-0	NNTMG19XKVxx	MGT 01-0		R1	
xx.xx.xxx.134	00	20	D8	xx	xx	xx	Media Card-0	NNTMEJ02Bxxx	MGT 01-0	xxx.xx.x.30	R1	
xx.xx.xxx.135	00	00	75	xx	xx	xx	SSC-1	NNTMG19XKVxx	MGT 01-1		R1	
xx.xx.xxx.136	00	20	D8	xx	xx	xx	Media Card-1	NNTMEJ02Bxxx	MGT 01-1	xxx.xx.x.34	R1	
137-159												
xx.xx.xxx.165	00	00	75	xx	xx	xx	SSC-0	NNTMG19XKVxx	MGT 02-0		R4	
xx.xx.xxx.166	00	20	D8	xx	xx	xx	Media Card	NNTMEJ02Bxxx	MGT 02-0	xxx.xx.x.84	R4	
xx.xx.xxx.167	00	02	B3	xx	xx	xx	Sig Server	NNTM74XC0xxx	Branch Off	xxx.xx.x.75	R3	
xx.xx.xxx.168	00	02	B3	xx	xx	xx	Sig Server	NNTM74XC0xxx	H323_2	xxx.xx.x.70	R4	
xx.xx.xxx.169	00	00	75	xx	xx	xx	SSC	NNTMG19XKVxx	Branch Off		R3	
xx.xx.xxx.170	00	20	D8	xx	xx	xx	Media Card	NNTMEJ02Bxxx	Branch Off	xxx.xx.x.	R3	
xx.xx.xxx.171	00	02	B3	xx	xx	xx	Sig Server	NNTM74XC0xxx	SIP_2	xxx.xx.x.37	R2	
xx.xx.xxx.172	00	00	75	xx	xx	xx	SSC-5	NNTMG19XKVxx	MGE 5		R2	8/0
xx.xx.xxx.173	00	00	75	xx	xx	xx	SSC-6	NNTMG19XKVxx	MGE 6		R2	8/1
174-191												
xx.xx.xxx.196	00	02	B3	xx	xx	xx	Sig Server	NNTM74XC0xxx	SIP/H323_1	xxx.xx.x.	R1	
xx.xx.xxx.197	00	0C	F8	xx	xx	xx	Baystack 460	SDNIHR1xxx	ELAN_1		R2	
xx.xx.xxx.198	00	0C	F8	xx	xx	xx	Baystack 460	SDNIHR1xxx	ELAN_2		R2	
xx.xx.xxx.199	00	01	AF	xx	xx	xx	CPP-2 Core 0	NNTMxxxxxxxx	Core 0			
xx.xx.xxx.200	00	01	AF	xx	xx	xx	CPP-2 Core 1	NNTMxxxxxxxx	Core 1			
xx.xx.xxx.201	00	02	B3	xx	xx	xx	Sig Server	NNTM74XC0xxx	Sig Server 01	xxx.xx.x.18	R2	
xx.xx.xxx.202	00	02	B3	xx	xx	xx	Sig Server	NNTM74XC0xxx	NRS	xxx.xx.x.35	R2	
xx.xx.xxx.203	00	02	B3	xx	xx	xx	Sig Server	NNTM74XC0xxx	Gatekeeper	xxx.xx.x.119	R3	
xx.xx.xxx.204	00	20	D8	xx	xx	xx	Media Card	NNTMEJ02Bxxx	MGE 5	xxx.xx.x.136	R2	8/0/1
xx.xx.xxx.205	00	20	D8	xx	xx	xx	Media Card	NNTMEJ02Bxxx	MGE 6	xxx.xx.x.137	R2	8/1/1
206-223												
xx.xx.xxx.224	08	00	87	xx	xx	xx	Terminal Server	(same as MAC)	TS1	xx.xx.xxx.xx	R2	
xx.xx.xxx.225	08	00	87	xx	xx	xx	Terminal Server	(same as MAC)	TS2	none	R2	
xx.xx.xxx.226	00	0E	C0	xx	xx	xx	CallPilot	AC0xxxxx		xxx.xx.x.30		
xx.xx.xxx.227	00	0E	C0	xx	xx	xx	Symposium	ACxxxxxx	MGate: MGE x	xxx.xx.x.31		
Legend: L/S/C = Loop, Shelf, Card; SSC = Small System Controller; Sig Server = Signaling Server												

ELAN Subnet Number	MAC address (by byte/octet)						Equipment Description	Serial Number	Comment	TLAN Subnet Address	Location	
	B1	B2	B3	B4	B5	B6					Rack	L/S/C
xx.xx.xxx.228	00	0E	C0	xx	xx	xx	Baystack 470	SACC110xxx				
xx.xx.xxx.229	00	01	AF	xx	xx	xx	CPP-2 Core 0	NNTMxxxxxxxx	Geo-Red			
xx.xx.xxx.230	00	01	AF	xx	xx	xx	CPP-2 Core 1	NNTMxxxxxxxx	Geo-Red			
xx.xx.xxx.231	00	02	B3	xx	xx	xx	Sig Server	NNTM74XC0xxx	Geo-Red	xxx.xx.x.130		
							SS Node IP		Geo-Red	xxx.xx.x.129		
							IP Phone		Geo-Red	xxx.xx.x.131		
							IP Phone		Geo-Red	xxx.xx.x.132		
232-255												
Legend: L/S/C = Loop, Shelf, Card; SSC = Small System Controller; Sig Server = Signaling Server												

Preparing a floor plan

Prepare a detailed floor plan for each site. The floor plan must indicate the size and location of:

- the racks, including planned expansion areas
- the service panel
- system terminal, printer, or other terminal devices (such as modems)
- PTFUs (if equipped)
- space for additional equipment, such as reserve power equipment or auxiliary processors

IMPORTANT!

According to the National Fire Code, equipment must be at least 30.5 cm (12 in.) from a sprinkler head.

Ensure that the site configuration meets all requirements of the third-party suppliers of the 19-inch racks.

Creating a building cable plan

To create a building cable plan, complete the following tasks.

1 Show the routing of all wiring, the location and wiring requirements of each terminal device connected to the system, and any other relevant information about the device.

2 Show the location of distribution frames, conduits and access points, and power outlets.

3 Identify the ownership of existing building wire if it is to be used.

4 Perform a random sampling of in-place wiring to ensure that it meets specifications for high-speed lines. All wiring carrying high-speed data must pass a verification test as part of the installation procedures.

5 Identify the location of conduits and floor ducts. If telephone cable is run in conduit then that conduit cannot be used for any other wiring.

6 Provide three pairs of telephone wire from a distribution frame to a nearby telephone jack for each terminal device. Modular jacks must be within 2.0 m (8 ft) of the device.

7 Provide Power over LAN cables to all desktops.

8 Divide the building cable plan into zones. Zones are typically the termination point of conduits throughout the office. Identify each zone on the building cable plan with a letter or number, and assign a block of numbers to each zone. Figure 26 on page 103 illustrates zoning.

Note: Be sure to leave room for expansion.

Wire routing

Refer to the appropriate electrical code for your region for standards you are required to meet. For the US, refer to the National Electrical Code (NEC).

To plan wire routing, establish the start and end point of each cable relative to the location of the terminal devices in the building, then examine the construction of the office to determine the best wiring routes. Consider the following guidelines when performing this task.

- Floors:
  - In the open, wires can run along baseboard, ceiling moldings, or door and window casings. For the safety of employees, never run wire across the top of the floor.
  - When concealed, wires can run inside floor conduits that travel between distribution frames and jacks. (Under-carpet cable is not recommended.)
- Ceilings:

  National and local building codes specify the types of telephone wire that you can run in each type of ceiling. Local building codes take precedence.
- Walls:

  Cables that run vertically should, when possible, run inside a wall, pole, or similar facility for vertical wire drops. Cables that run horizontally cannot be blind-fed through walls.
- Between floors:

  Locate distribution frames as closely to one another as possible. Local coding laws specify whether or not a licensed contractor is required if conduit is installed.
- EMI:

  Data degradation may occur if wires travel near strong EMI sources. See “Electromagnetic and radio frequency interference” on page 93 for a description of common interference sources.

Termination points

Once you have determined the wire routing, establish termination points. Cables can terminate at:

1. the MDF (typically in the equipment room)
2. intermediate distribution frames, typically on each floor in telephone utility closets
3. wall jacks to terminal boxes, typically located near the terminal device

At the distribution frame (also called the cross-connect terminal), house cables terminate on the vertical side of the two-sided frame and cross connect to equipment that is typically located on the horizontal. If you use a color field scheme, house cables typically terminate in the blue field and the equipment terminates on the purple (US) or white (Canada) field.

In all cases, clearly designate the block where the cables terminate with the cable location information and the cable pair assignments. Keep a log book (cable record) of termination information. See Figure 27 on page 104 for an example.

Figure 26
Building cable zones

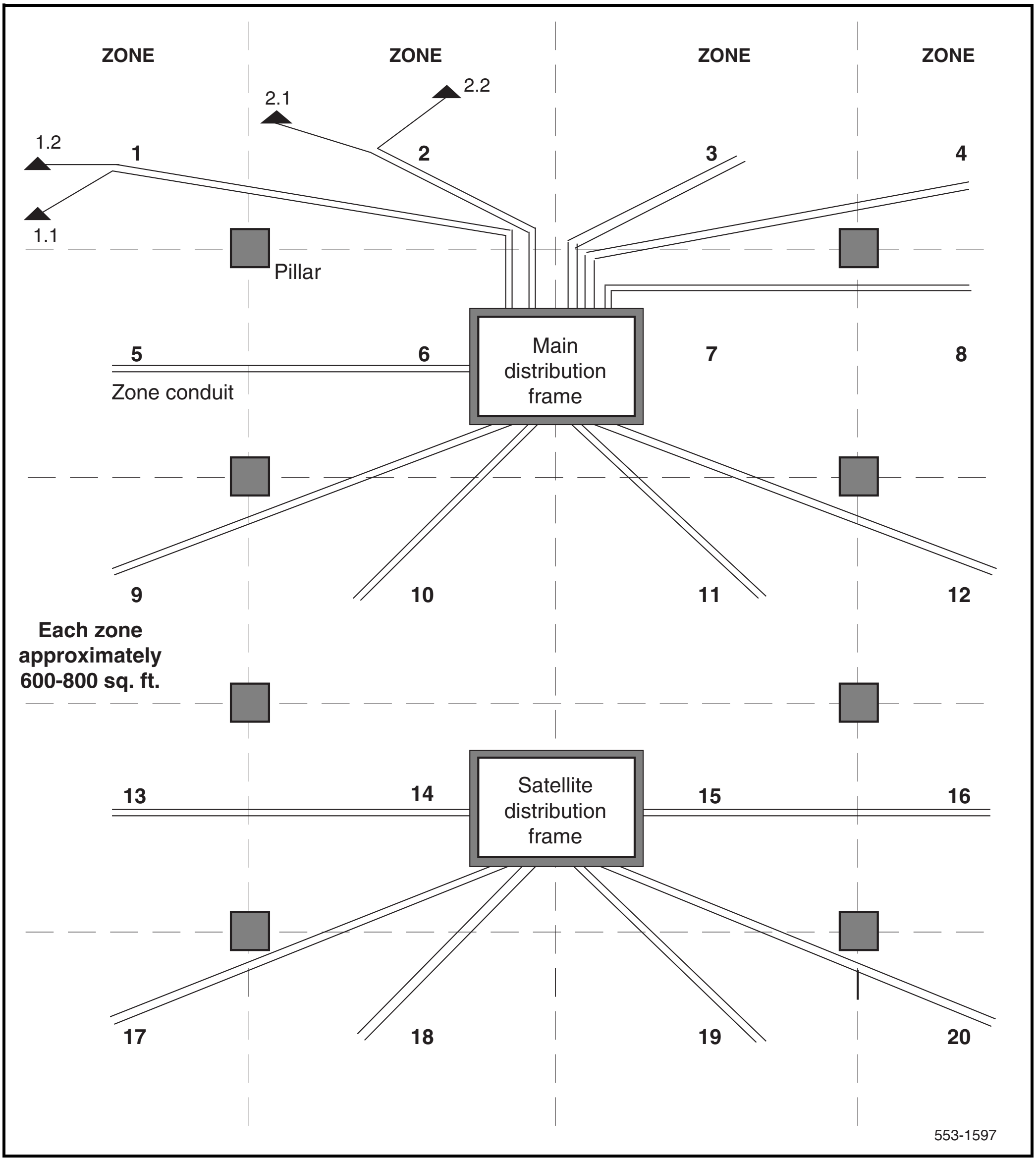


Figure 27
Sample cable record

CABLE RECORD

Customer ______________________________________

Location ____

Cable ______________________ Binder ____________ Page ____ of ____

DN	TN				NAME	FEATURES / REMARKS	TERMINAL DEVICE	BLOCKS	COLOR
	M	S	C	U				DF / HOUSE	
									W BL
									W OR
									W GR
									W BR
									W SL
									R BL
									R OR
									R GR
									R BR
									R SL
									BK BL
									BK OR
									BK GR
									BK BR
									BK SL
									Y BL
									Y OR
									Y GR
									Y BR
									Y SL
									V BL
									V OR
									V GR
									V BR
									V SL

553-1595

Preparing for delivery

When preparing for equipment delivery, answer the following questions:

1. Has a request been made for equipment delivery?
2. Are transportation arrangements to the premises completed?
3. Is a list of all ordered equipment available on site?
4. Is help needed and available for preparing the equipment room?
5. Are unloading and unpacking facilities and tools available?
6. Is help needed and available for delivery?

   Note: Plan to unload equipment as close to the final installation area as possible for an easier, and perhaps safer, installation.

Conducting pre-installation inspections

Obtain any appropriate sign-offs before the site is ready for equipment delivery and installation. Sign-offs can include regulatory items such as electrical inspections, air conditioning inspections, and cable plan approval. In addition, an overall equipment room inspection and a building cable inspection should be performed before installation.

Inspect the equipment room to verify that all physical and environmental requirements are met, system grounding and power equipment is installed and tested, and the equipment layout is marked on the floor.

Inspect the building cable to verify that sufficient distribution frames are provided, conduits or floor ducts to terminal locations are installed, terminal jacks are installed, and sufficient wiring is on hand.

Preparing for installation

The installation plan, work orders, and appropriate documentation should be on hand at the time of installation.

Reviewing the installation plan

The installation plan can consist of the equipment room floor plan, the building cable plan, and an installation and test sequence chart.

The equipment room floor plan should show:

- Racks, including planned expansion areas
- Main distribution frame
- Service panel
- System terminal, printer, or other terminal devices
- External power equipment (such as UPS)
- Cable racks
- PFTUs (if equipped)

The building cable plan should show:

- Cable routing and designation information
- Location of each terminal device
- Type of cable or wiring required for each terminal device
- Location of all distribution frames and system and terminal cross-connect assignments
- Location of conduits and floor ducts, including access points
- Location of power outlets for terminal devices

An installation and test sequence (ITS) chart shows typical installation tasks, the sequence of the tasks, and task start and duration information.

Reviewing the work orders

The work order can include:

- Detailed listing of the equipment ordered
- Terminal Number (TN) assignments
- Directory Number (DN) assignments for each terminal device

- IP assignments for all equipment
- Office Data Administration System (ODAS) designators for each terminal device (if the software package is equipped)
- Features available to each telephone and data telephone
- Administration database entries for telephone and data telephone features

Reviewing the documentation

Instructions for unloading and unpacking system equipment, as well as a full set of standard Nortel technical publications (NTPs), are delivered with each system.

Power and grounding

Contents

This section contains information on the following topics:

Introduction

CS 1000E system components are AC-powered. This section outlines the system's grounding and electrical requirements.

Grounding requirements

For system grounding in new installations, Nortel recommends following ANSI/TIA/EIA-607 (Commercial Building and Bonding Requirements for Telecommunications Equipment).

In building installations where the ANSI/TIA/EIA-607 method is not used, connect the equipment ground to the AC ground at the respective service panel.

If you are having difficulty interpreting the grounding methods in this document, Nortel recommends obtaining the services of a certified power contractor or auditor prior to system installation or cutover

WARNING

Failure to follow grounding recommendations can result in a system installation that is:

- unsafe for personnel handling or using the equipment
- not properly protected from lightning or power transients
- subject to service interruptions

Before installing the equipment and applying AC power, measure the impedance of the building ground reference. An ECOS 1023 POW-R-MATE or similar meter is acceptable for this purpose. Ensure that the ground path connected to the system has an impedance of 4 ohms or less. Make any improvements to the grounding system before attempting installation.

DANGER OF ELECTRIC SHOCK

Never connect the single point ground conductor from the system to structural steel members or electrical conduit. Never tie this conductor to a ground source or grounded electrode that is not hard-wired to the building reference conductor.

System grounding must adhere to the following requirements:

- The ground path must have an impedance of 4 ohms or less.

- Ground conductors must be at least #6 AWG (16 mm^2) at any point (see Table 6 on page 111 for a list of grounding wire requirements specific to some areas).
- Ground conductors must not carry current under normal operating conditions.
- Spliced conductors must not be used. Continuous conductors have lower impedance and are more reliable.
- All conductors must terminate in a permanent way. Make sure all terminations are easily visible and available for maintenance purposes.
- Tag ground connections with a clear message such as “CRITICAL CONNECTION: DO NOT REMOVE OR DISCONNECT.”

Table 6
Area-specific ground wire requirements

Area	Ground wire requirements
Germany	#8 AWG (10 mm^2) green/yellow wire
Other areas in Europe	Not smaller than #6 AWG (16 mm^2) at any point
UK	Two green/yellow wires no thinner than 10 mm^2

For more information about standards and guidelines for grounding telecommunications equipment, refer to ANSI/TIA/EIA-607 (Commercial Building and Bonding Requirements for Telecommunications Equipment).

DANGER OF ELECTRIC SHOCK

For an installed Media Gateway or Media Gateway Expander, link impedance between the ground post of any equipment and the single point ground to which it connects must be less than 0.25 ohms.

> **CAUTION — Damage to Equipment**
>
> Transients in supply conductors and ground systems can damage integrated circuits. This damage can result in unreliable system operation. Damage caused by transients is not always immediately apparent. Degradation can occur over a period of time.

Single Point Ground

Correct grounding of communications systems is necessary to protect equipment from the hazards of surge and noise interference. The Single Point Ground (SPG) method of protecting communications equipment is the Nortel standard. Table 7 describes grounding design considerations.

Table 7
Grounding design considerations (Part 1 of 2)

Safety	• Dissipate unwanted surge energies such as lightning striking on the outside plant • Fuses or breakers open to disrupt the excessive current flow caused by a power fault
Equipment protection	• Grounding for outside plant cable shields and protectors • Grounds for framework and logic references
Electromagnetic compatibility (EMC)	• Conform with electromagnetic compatibility (EMC) grounding requirements
Installation and maintenance	• Cost-effective to install and maintain when part of the initial electrical installation • Correcting violations of national codes after the initial installation is difficult and costly

Table 7
Grounding design considerations (Part 2 of 2)

Powering	• If the equipment is backed up with an Uninterruptible Power Supply (UPS), consider the grounding of all equipment that is part of the telecommunications system as a single system
Advances in technology	• Provides important protection to ensure the effective operation of circuit cards and avoid costly downtime and replacement

DANGER OF ELECTRIC SHOCK

Do not perform work inside electrical panels unless you are a qualified electrician. Do not try to remove bonding conductors without approval from qualified personnel.

In an ANSI/TIA/EIA-607 installation, the Telecommunications Main Grounding Busbar (TMGB)/Telecommunications Grounding Busbar (TGB) links the telecommunications equipment to the ground. Other grounding terminology is:

- building principal ground, normally in a building with one floor
- floor ground bar, normally in buildings with more than one floor

Configure telecommunications subsystems, such as groups of frames or equipment, as separate single-point ground entities connected to the equipment's dedicated service panel via a single-point ground bar. The service panel ground connects to the building principal ground via the main service panel or, in an ANSI/TIA/EIA-607 installation, via the TGB. Refer to Figure 29 on page 115.

Figure 28
ANSI/TIA/EIA-607 grounding schematic

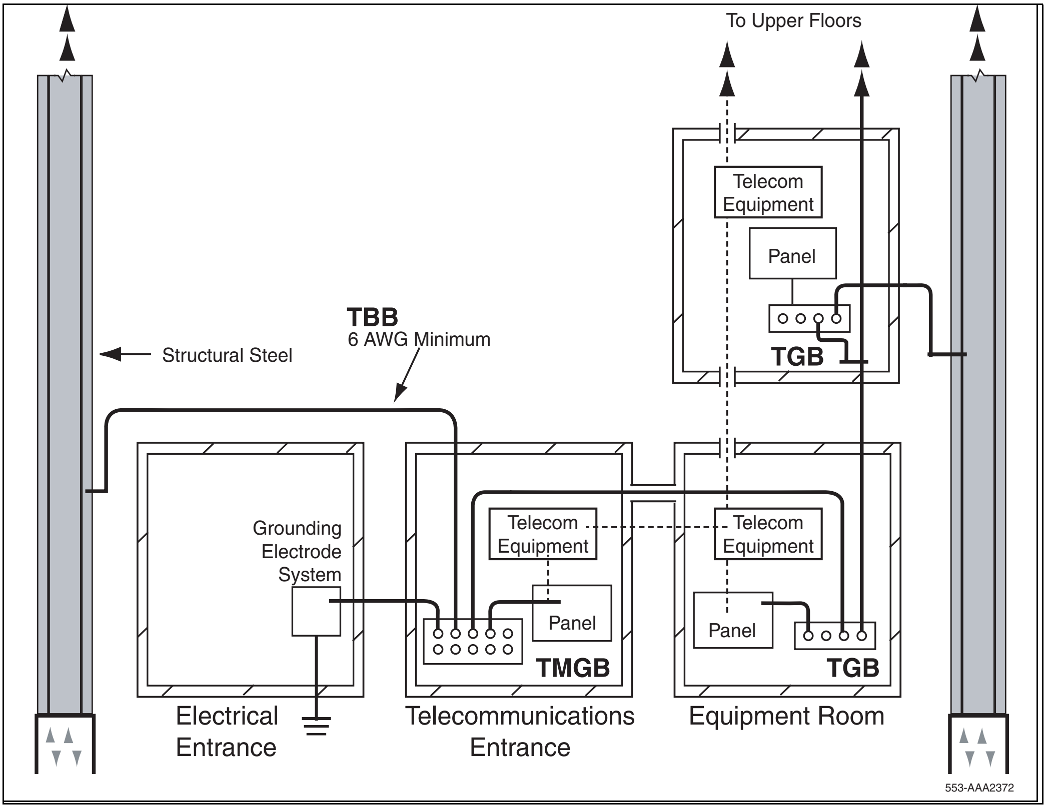
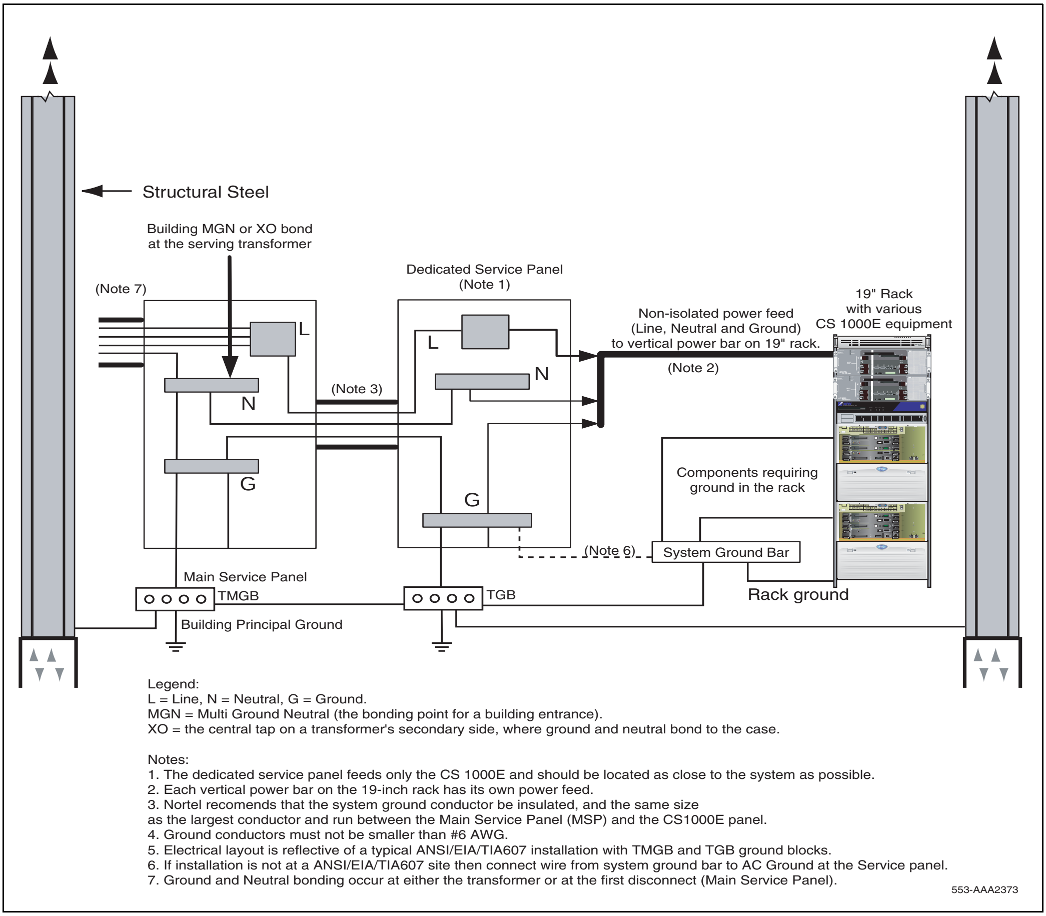


Figure 29
Typical wiring plan



Grounding methods

This section describes the grounding methods for:

- Ground bar (NTBK80) (p. 116)
- Ground bar (NTDU6201) (p. 116)
- CS 1000E (p. 117)

- Signaling Server (p. 117)
- Media Gateway (p. 117)
- Media Gateway Expander (p. 118)
- Multiple components in a rack (p. 118)

> **DANGER OF ELECTRIC SHOCK**
>
> To prevent ground loops, power all CS 1000E system equipment from the same dedicated power panel.

Ground bar (NTBK80)

The NTBK80 ground bar is capable of grounding up to six Media Gateways (either with or without companion Media Gateway Expanders) back to the SPG. See Table 6 on page 111 for area-specific ground wire requirements.

Ground bar (NTDU6201)

If there are more than six Media Gateways (either with or without companion Media Gateway Expanders), use the NTDU6201 ground bar. The NTDU6201 can be adjusted for various mounting configurations. It accepts 35 #6 AWG (16 mm^2) wire connections. The ground bar must terminate at the service panel ground. See Figure 29 on page 115.

CS 1000E

The CS 1000E does not connect to a ground bar. It is properly grounded when:

- The CS 1000E power cord is plugged into the rack's AC outlet. The rack's AC outlet must be grounded to its dedicated electrical panel. This is the preferred method.
- The CS 1000E power cord is plugged into a wall AC outlet. The CS 1000E is grounded outside of the rack via the safety grounding conductor in the power cord. This method only ensures proper grounding of the CS 1000E itself. It does not provide grounding protection for other rack-mounted pieces of equipment. Therefore, ensure that other devices in the rack are properly grounded as required.

Signaling Server

The Signaling Server does not connect to a ground bar. It is properly grounded when:

- The Signaling Server power cord is plugged into the rack's AC outlet. The rack's AC outlet must be grounded to its dedicated electrical panel. This is the preferred method.
- The Signaling Server power cord is plugged into a wall AC outlet. The Signaling Server is grounded outside of the rack via the safety grounding conductor in the power cord. This method only ensures proper grounding of the Signaling Server itself. It does not provide grounding protection for other rack-mounted pieces of equipment. Therefore, ensure that other devices in the rack are properly grounded as required.

Media Gateway

The grounding method used for the Media Gateway depends on the number of units used and whether the units are powered by the same service panel.

All equipment located in a series of equipment racks that are physically bonded together must be grounded to and powered by the same service panel. If additional service panels are required, collocate them beside the original service panel.

If racks are not bonded together, then the equipment located in the racks can be grounded and powered by separate service panels.

Connect a #6 AWG (16 mm^2) ground wire from the rear panel grounding lug of each Media Gateway to the ground bar. See Table 6 on page 111 for area-specific ground wire requirements. Connect the ground bar to a ground source in the dedicated service panel.

> ***Note:*** In the UK, connect the ground wire from the equipment to a ground bar or through a Krone Test Jack Frame.

Media Gateway Expander

The Media Gateway and Media Gateway Expander are considered as the same ground. To ground the Media Gateway Expander, jumper the ground wire from it to the grounded Media Gateway.

IMPORTANT!

Power each Media Gateway and Media Gateway Expander pair from the same service panel.

Multiple components in a rack

To ground multiple pieces of equipment installed in a rack, run a separate connection from the grounding lug on each piece of equipment to the ground bar.

If a piece of equipment in a rack does not have a grounding lug, ground the rack to the ground bar. Grounding the rack in this manner grounds the equipment by the SPG method.

Conduit requirements

Conductive conduit linking panels and equipment is legal for use as a grounding network in most countries. For all CS 1000E system ground paths, route the correct size of insulated copper conductors inside conduit. A ground link that depends on a conduit can defeat the improvements achieved with the installation of dedicated electrical panels and transformers. A grounding failure can result from the following:

- Personnel who service different equipment can separate conduit links. If such a separation occurs between the system and the building ground reference, the conduit cannot provide a ground path. This situation is hazardous.
- Corrosion of metal conduits increases resistance. Threaded connections are prone to corrosion. This problem becomes worse when there are multiple links. Applying paint over the conduit increases the corrosion process.
- Conduit may not be fastened to secure surfaces. Often, the conduit bolts on to structural steel members, which can function as ground conductors to noisy equipment (for example, compressors and motors). Adding noisy equipment into the grounding system can damage the system's performance. The resulting intermittent malfunctions can be difficult to trace.

Commercial power requirements

The CS 1000E system is AC-powered. Optimally, a dedicated electrical panel that is connected to the facility's electrical system powers the system. The dedicated electrical panel provides power only to the CS 1000E system components and its related telecommunications hardware such as TTYs and printers. There is no expectation that system components that are located off-site will be powered by this dedicated electrical panel.

Media Gateway and Expander

Each Media Gateway-Expander pair must share the same electrical breaker and outlet. Refer to "AC input requirements" on page 123 for more information.

> ***Note:*** If the system is equipped with CallPilot, the CallPilot server must connect to the same dedicated service panel that feeds the MG 1000E in which the MGate card resides.

Rack power bars

Power each power bar or rack-mounted power rail on a separate circuit fed from the service panel.

The rating for power bars must be 120 or 240 V, 15 or 20 A, 50-60 Hz, grounded. Power bars are non-isolated ground type.

Powering redundant equipment

Provide power to redundant equipment from dedicated power bars fed from their own dedicated circuits.

Powering auxiliary equipment

Terminals, printers, modems, and other data units used with the CS 1000E or MG 1000T have special wiring requirements. All equipment must be:

- powered from the same electrical panel or transformer as the system
- grounded to the same electrical panel or transformer as the system
- labeled at the electrical panel to prevent a non-authorized power interruption

Alternative AC-powered installation

Use an approved isolation transformer when the power to all system components at a location cannot be supplied by a dedicated electrical panel or the dedicated electrical panel cannot provide optimal conditions. Refer to Table 8 on page 124 and Table 9 on page 125 to determine the system power consumption.

The isolation transformer must have the following characteristics:

- 120/240 V AC input, over-current protected at primary.
- 120/240 V AC available at secondary outputs, each protected by circuit breaker.
- Primary and secondary windings completely isolated from one another.

- Approved for use locally as a stand-alone user product (CSA, UL, or other locally recognized clear markings).
- Capable of providing power to all components operating at the same time at full load.
- Equipment unrelated to the system must not be powered from a transformer that provides service to the system.

Installing an isolation transformer ground

The transformer ground must have separate grounds for primary and secondary windings rather than a common ground. Ground conductors inside the transformer must be correctly sized.

DANGER OF ELECTRIC SHOCK

Nortel does not recommend connecting any CS 1000E system telecommunications ground bus to untested horizontal structural steel or water pipes, or other unreliable ground paths. Use a ground point known to be "clean" and permanent. Place a "DO NOT DISCONNECT" tag on it.

Procedure 1 describes the method to install an isolation transformer without pluggable power cords.

Procedure 1
Installing an isolation transformer without pluggable power cords

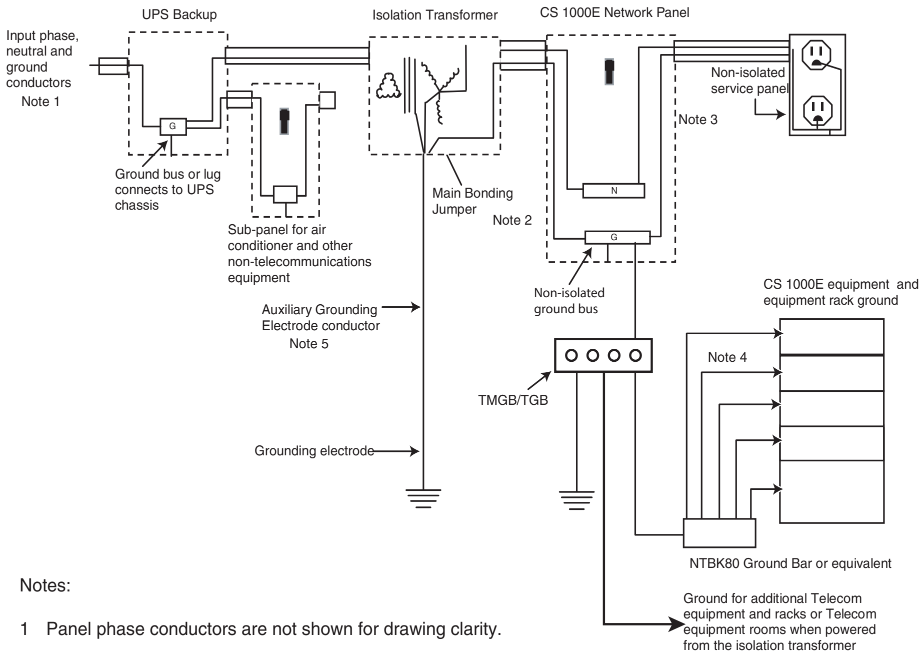
1 If the transformer does not have a pluggable cord, hardwire the transformer to an electrical panel. Route all wires (including grounds) through a single conduit.

Note: Some electrical codes permit the use of conduit as the only ground conductor between pieces of equipment.

2 Run a separate insulated ground conductor through the conduit to hold unit grounds together. Such a conductor maintains the safety ground connection in the event that the conduit becomes corroded or disconnected.

3 Run all ground lines through the same conduit as the phase conductors that serve the equipment. Figure 30 on page 122 shows the isolation transformer connections.

Figure 30
Typical hardwired isolation transformer wiring plan



Notes:

1 Panel phase conductors are not shown for drawing clarity.

2 Nortel recommends that the system ground conductor be insulated and the same size as the largest conductor run between the power source and CS 1000E Panel.

3 Dedicated a/c service panel must be located in the equipment room as close to the CS 1000E system as practically possible.

4 Conductor must not be smaller than #6 AWG.

5 Auxiliary grounding conductor should be short as possible and must be connected to a recognized building ground. (That is, floor ground bar, vertical ground riser, or building principal ground.)

553-AAA3052

End of Procedure

AC input requirements

Refer to Table 8 on page 124 for the AC input requirements of CS 1000E components.

If other data communications equipment is in the same rack as the CS 1000E system, power each piece of equipment from the same electrical panel. Install additional outlets, if necessary.

Because local power specifications vary, consult a qualified local electrician when planning power requirements.

Power consumption

System power consumption depends on the number of components installed.

Table 8 on page 124 summarizes the current, power, and cooling requirements for CS 1000E components. Table 8 shows absolute maximum ratings as well as typical ratings for configured systems. The typical values are provided as a guide to avoid over-engineering, particularly for Uninterruptible Power Supply (UPS) requirements.

Table 8
Current, power, and cooling requirements for CS 1000E components

Component	Current @ 120/240 V AC (A)		Required UPS power (W)		Thermal dissipation (Btu)	
	Maximum	Typical	Maximum	Typical	Maximum	Typical
NTDU62 Core Call Server	2.50/1.25	1.00/0.50	300.00	120.00	1023.90	409.56
NTDU27 Signaling Server	2.00/0.90	0.50/0.25	200.00	60.00	682.60	204.78
NTDU14 Media Gateway (see Note 1)	1.40/0.70	1.17/0.58	300.00	190.00	1023.60	648.30
NTDU15 Media Gateway Expander (see Note 1)	1.15/0.58	1.17/0.58	300.00	145.00	1023.60	494.70
MRV Terminal Server	1.60/0.80	0.40/0.20	192.00	48.00	655.30	163.83
BayStack 470	1.50/0.75	0.60/0.30	90.00	72.00	324.00	245.74
BayStack 460 (Power over LAN not used)	4.70/2.40	0.60/0.30	295.00	72.00	335.00	245.74
BayStack 460 (Power over LAN for 24 IP Phones) (see Note 2)	4.70/2.40	1.20/0.60	364.12	141.12	335.00	245.74

Note 1: Maximum values for the Media Gateway and Expander assume worst case conditions. It is difficult to specify a typical configuration. The typical values in the table are intended as a rough guide for quick estimations. Nortel recommends that qualified personnel take current measurements for a more accurate assessment of UPS and thermal requirements.

Note 2: The maximum AC input for the BayStack 460 includes maximum power of the Power over LAN. The typical rating has been adjusted to reflect configuring for IP Phones (60 mA at 48 V DC).

Note 3: Maximum voltage limits: North America – 90 and 132 V, single phase. Europe and UK – 180 and 250 V, single phase. Frequency: North America – 60 Hz. Europe and UK – 50 Hz. Fuse: Germany – 16 A.

Table 9 provides the power consumption, UPS power requirements, and thermal dissipation of Media Gateway packs (circuit cards and daughterboards) commonly installed in CS 1000E and MG 1000T Media Gateways and Expanders.

Electrical load for analog line cards varies with traffic load. The figures in Table 9 assume that 50% of analog lines are active. TheUPS power wattage figures also take into account the average efficiency of the Media Gateway power supplies.

Table 9
Power and cooling requirements for Media Gateway packs (Part 1 of 2)

Media Gateway pack	Active off-hook (%)	Power consumption (W)	UPS power (W)	Thermal dissipation	
				W	Btu
NTDK20 Small System Controller card	N/A	16	24.0	24.0	81.9
NTDK83 100BaseT daughterboard (dual-port)	N/A	6	9.0	9.0	30.7
NTDK99 100BaseT daughterboard (single-port)	N/A	4	6.0	6.0	20.5
NT5K02 Flexible Analog Line card	50	26	39.0	6.6	22.5
NT8D02 Digital Line card	100	26	39.0	13.0	44.4
NT8D03 Analog Line card	50	26	39.0	6.6	22.5
NT8D09 Analog Message Waiting Line card	50	26	39.0	6.6	22.5
NT8D14 Universal Trunk card*	DID-enabled	28	42.0	42.0	143.3
NT8D15 E&M Trunk card*	N/A	29	43.5	43.5	148.4
NTAK09 1.5MByte DTI/PRI card*	N/A	10	15.0	15.0	51.2
NTAK10 2.0 MByte DTI card*	N/A	12	18.0	18.0	61.4

*In MG 1000T only.

Table 9
Power and cooling requirements for Media Gateway packs (Part 2 of 2)

Media Gateway pack	Active off-hook (%)	Power consumption (W)	UPS power (W)	Thermal dissipation	
				W	Btu
NTAK79 2.0 MByte PRI card*	N/A	12	18.0	18.0	61.4
NTBK50 2.0 MByte PRI card*	N/A	12	18.0	18.0	61.4
NTRB21 TMDI (1.5 Mbyte DTI/ PRI) card*	N/A	12	18.0	18.0	61.4
NTVQ01 Media Card (32-port)	N/A	18	27.0	27.0	92.1
*In MG 1000T only.					

Note 1: The UPS power requirement is the card's power consumption divided by the efficiency factor for the Media Gateway power supply plus peak inrush. For Media Gateways use 1.5 times the wattage to give the UPS wattage, or volt-amps (VA).

Note 2: For digital and analog (500/2500-type) telephones, most thermal dissipation will be external to the switch room. In Table 9, thermal dissipation values for these cards have been adjusted accordingly.

Power consumption worksheets

Table 10 on page 127 and Table 11 on page 128 provide worksheets to determine power consumption for the CS 1000E system.

Prepare one worksheet for the system as a whole (Table 10).

Table 10
CS 1000E system power consumption worksheet

Component		Required UPS power		Thermal dissipation	
	Number of comp. (1)	**Per comp. (W) (2)**	**Total (W) (1) x (2)**	**Per comp. (Btu) (3)**	**Total (Btu) (1) x (3)**
NTDU62 Core Call Server					
NTDU27 Signaling Server					
MRV Terminal Server					
BayStack 470					
BayStack 460 (Power over LAN not used)					
BayStack 460 (Power over LAN for 24 IP Phones)					
NTDU14 Media Gateways*					
NTDU15 Media Gateway Expanders*					
TOTAL					
*Enter the sum of the totals for individual Media Gateways and Expanders (Table 11 on page 128).					

Prepare one worksheet for each Media Gateway and Media Gateway Expander, if equipped (Table 11). Refer to Table 9 on page 125 for the power and thermal dissipation requirements for the individual components.

Table 11
Media Gateway power consumption worksheet

Media Gateway number ________________				
Slot	**Media Gateway Pack**	**Required UPS power (W)**	**Thermal dissipation**	
			(W)	**(Btu)**
0	NTDK20 Small System Controller card	24.0	24.0	81.9
0	NTDK99 100BaseT daughterboard (single port)			
0	NTDK83 100BaseT daughterboard (dual-port)			
1				
2				
3				
4				
Media Gateway Expander				
7				
8				
9				
10				
TOTAL				
Note: Each MG 1000E must have at least one Media Card.				

Heat dissipation

The CS 1000E is equipped with a cooling system and does not have heat dissipation problems under normal applications. Mounting in the rack is not restricted.

See Tables 8 and 9 for the thermal load generated by system components and Media Gateway packs.

For air conditioning purposes, 1 ton = 12 000 Btu.

Uninterruptible Power Supply

An Uninterruptible Power Supply (UPS) generally consists of a combination battery charger (AC/DC converter) and inverter (DC/AC converter), along with associated batteries. The batteries may be internal or external to the UPS. A UPS is not a standby power source, but an online unit with no output interruption when the AC power is interrupted.

There are a number of UPS vendors and systems available. Factors to consider when choosing a UPS include:

- input voltage and frequency range
- output voltage and current capacity
- number and type of output receptacles
- regulatory and safety agency approvals
- efficiency and performance considerations
- alarm and status indications
- battery recharge time
- the maximum time backup power is required
- existing batteries or other power equipment available at the site
- future system growth

UPS sizing

To determine UPS sizing, sum the values given in Table 8 on page 124 and Table 9 on page 125 for UPS requirements for the applicable components and Media Gateway packs. The value in watts (W) is equivalent to a volt-ampere (VA) rating. Size the UPS in terms of its rating in VA (or kVA). For AC-powered systems, NNEC calculates the system power consumption in both watts and volt-amperes.

To determine the sizing and provisioning of UPS batteries, follow the instructions provided by the UPS manufacturer. A general approach is to take the total system power in watts, divide by the UPS inverter efficiency, and convert to battery current drain by dividing by the nominal discharge voltage of the battery string. Then determine the battery requirements in ampere-hours (A-hrs) by multiplying the battery current drain by the required reserve power operating time.

$$Ahr = \left(\frac{W_{total}}{V_{dischg}}\right)T_{reserve}$$

UPS installation

When installing a UPS, follow the vendor's instructions carefully.

Nortel recommends installing a bypass switch during the initial UPS wiring (if the switch function is not inherently a part of the UPS itself). The UPS bypass switch allows the system to run directly from the commercial power source while the UPS is taken off-line during installation, service, or battery maintenance.

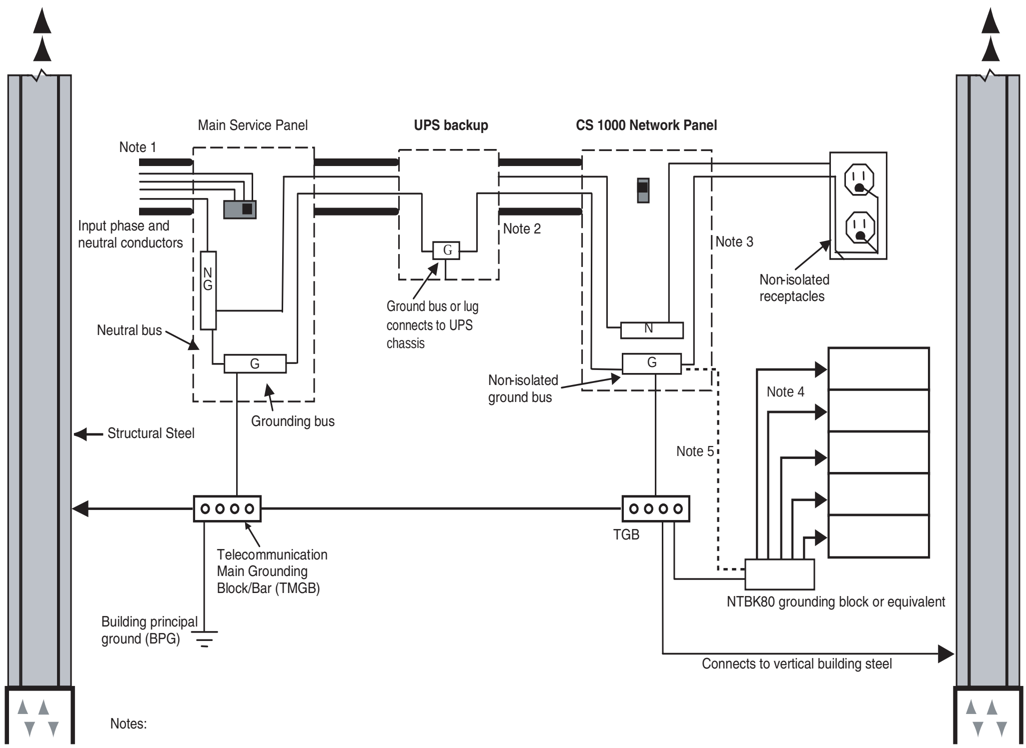
CAUTION

Damage to Equipment

Take care when connecting battery cables to the UPS. Connecting battery cables backward can result in severe damage to the UPS.

Figure 31 on page 131 shows a typical UPS wiring plan.

Figure 31
Typical UPS wiring plan



Notes:

1. Panel phase conductors are not shown for drawing clarity.
2. Nortel Networks recommends that the system ground conductor be insulated and the same size as the largest conductor run between the power supply source and Communication Server 1000 Equipment Panel.
3. Dedicated AC service panel must be located in the equipment room as close to the CS 1000 system as practically possible.
4. Conductor must not be smaller than #6 AWG.
5. Make this alternate connection to the system ground block where installations do not have ANSI/TIA/EIA-607 grounding architecture.

553-AAA2391

Power requirements for IP Phones

The IP Phones and IP Softphone require 16 V AC, 500 mA that is supplied by a local transformer. The appropriate transformer depends on the line voltage, which is different for each country.

IP Phones also accommodate 48 V DC power. IP Phones can be powered over the LAN by a Layer 2 switch such as a BayStack 460 (see “Layer 2 switch" on page 71). For more information about Power over LAN, refer to *Converging the Data Network with VoIP* (553-3001-160).

Design parameters

Contents

This section contains information on the following topics:

Introduction

This section describes design parameters that set an upper boundary on certain system capacities. Changes to these parameters generally require a revision to the software and are constrained by other basic capacities such as memory and traffic or system load. The design parameters are set to provide the best possible balance between limits.

Note on terminology

Each Media Gateway in the CS 1000E or MG 1000T can be connected to an optional Media Gateway Expander in order to increase the number of card slots available. In this chapter, all references to Media Gateways (MG 1000E, MG 1000T, or MG 1000T Expansion) include the optional Media Gateway Expander, if equipped.

System parameters

Table 12 on page 134 lists system parameters and provides their maximum values.

Table 12
System parameters

System parameters	Maximum value	Comments
Customers	100	
Display messages for background terminal	255	
Input/output ports (for example, TTYs and printers)	16	Two physical (Com 1 and Com 2) and fourteen PTYs to Terminal Server (history file counts as one device)
AML/CSL links	16	IP links
TNs – CS 1000E – MG 1000T	 65 536 1744	Software design limit. Actual number of TNs will be constrained by physical capacity, real time, memory, and License limits.

Customer parameters

Table 13 lists customer parameters and their maximum values.

Table 13
Customer parameters

Customer parameters	Maximum value	Comments
Tenants	512	
Dial Intercom Groups	2046	
Members per Dial Intercom Group	100	
Ringing Number Pickup groups	4095	Call Pickup Group 0 = no pickup group
Listed Directory Numbers (direct inward dialing only)	6	
DISA DNs	240	

Console and telephone parameters

Table 14 lists console and telephone-related parameters and their maximum values.

Table 14
Console and telephone related parameters (Part 1 of 2)

Console/telephone parameters	Maximum value	Comments
Consoles per customer	63	
Lamp field arrays per customer	1	May be repeated once on another console.
Lamps per array (all numbers must be consecutive)	150	
Feature keys per attendant console: – M2250	20	

Table 14
Console and telephone related parameters (Part 2 of 2)

Console/telephone parameters	Maximum value	Comments
Incoming call indicators per console	20	
Trunk group busy indicators per console: – M2250	 20	
Additional key/lamp strips: – console – telephones	 2 6	
Add on modules: – M3904 Key Expansion Module (KEM) – IP Phone 2002 KEM – IP Phone 2004 KEM	 2 1 one-page KEM 2 one-page KEM or 1 two-page KEM	
Protect bcs block length	512	

Trunk and route parameters

Table 15 lists trunk and network-related parameters and their maximum values.

Table 15
Trunk and network-related parameters (Part 1 of 2)

Trunk/network parameters	Maximum value	Comments
Trunk routes per customer	512	
Members per trunk route	510	
RAN trunks per RAN route	10	
Trunk access restriction groups	32	

Table 15
Trunk and network-related parameters (Part 2 of 2)

Trunk/network parameters	Maximum value	Comments
Locations in an ESN network	1000 or 16 000	1000 without ESN Location Code Expansion (LOCX) package 400; 16 000 with the LOCX package 400
Basic authorization codes	4096	
Length of basic authcode	14 digits	
Network authorization codes	20 000	ESN networks
Length of network authcode	7 digits	Fixed length defined per customer
NCOS: – CDP – BARS/NFCR – NARS/NSIG/AUTOVON	 3 7 15	
Route lists: – CDP – BARS – NARS	 32 128 256	
Route list entries	64	
NFCR trees	255	New Flexible Code Restriction
IDC trees	255	Incoming DID Digit Conversion
Virtual Trunk D-channels	64	

ACD feature parameters

Table 16 lists ACD feature parameters and their maximum values.

Table 16
ACD feature parameters

ACD parameters	Maximum value	Comments
ACD DNs and CDNs per customer	- 1000 (CP PII, CP PIV) - 240 (CP3, CP4, SSC)	The ACD-E package required, otherwise the limit is 240.
Agent positions per DN	- 1200 (Large systems) - 120 (Small systems - SSC)	Real-time and physical capacity constraints can limit this further.
Agent priorities	48	
Agent IDs per customer	9999	
Agents logged in at one time per system	9999	Real-time constraints may limit this further.
AST DNs per telephone	2	
Number of ACD-ADS customers	5	
Links per VASID	1	

Special feature parameters

Table 17 lists non-ACD feature parameters and their maximum values.

Table 17
Non-ACD feature parameters (Part 1 of 2)

Feature parameters	Maximum value	Comments
Speed call lists per system	8191	The number of speed call lists and the number of DNs per speed call list can be limited by the amount of available memory on the system (protected and unprotected data store).
Number of DNs in speed call list	1000	
Multiple appearances of the same directory number (MADN)	30*	Limited by watchdog timer. *See Steps in a hunting group.
Steps in a hunting group	30*	Marketing objective, limited by watchdog timer. *In combination with MADN, each hunt step with more than 16 appearances is counted as two, so the maximum combination of MADN and hunt steps is 30 MADN and 15 hunt steps.
Number of Call Party Name Display names defined	Variable	Limited by the number of DNs defined and available space in the protected data store.
CPND length: – SL-1 protocol – ISDN protocol	 27 24	 Software design limit. Display IE limitation (DMS switches have a display IE limit of 15).
AWU calls in 5 minutes	500	Marketing objective, constrained by ring generator.

Table 17
Non-ACD feature parameters (Part 2 of 2)

Feature parameters	Maximum value	Comments
Group Call Feature: – Groups per customer – Stations per group	 64 10	
For MG 1000T only: BRI application: – Protocol parameter telephone groups per system – Terminal service profiles (per DSL) DSLs – LTIDs	 16 32 000 640 000	 Software design limit; actual number is constrained by the number of TNs in the system. Each DSL occupies 2 TNs. Software design limit; each DSL can have a maximum of 20 LTIDs. The maximum number of LTIDs is limited by the number of DSLs, by memory, and by real time.

Hardware and capacity parameters

The software design limits are not typically the binding constraints. The number of items of a particular type is usually determined by a combination of loop and slot constraints (if the item requires loops) or by slot constraints alone.

Table 18 lists hardware and capacity parameters and their maximum values.

Table 18
Physical capacity/hardware-related parameters

Physical capacity/hardware parameters	Maximum value (loops)	Comments
VXCT	240	Provide TDS, Conf, and MFS functionality for the cards in that MG 1000E; up to 4 VXCT per MG 1000E; each MG 1000E requires 2 loops.
Total service and terminal loops	256	Each superloop requires 4 loops.

Voice Gateway Media Cards

A Voice Gateway Media Card is any Media Card running the IP Line application.

In the CS 1000E, Voice Gateway Media Cards are used primarily for DSP connections between the TDM devices in an MG 1000E and IP circuits.

Voice Gateway Media Cards can be assigned to any slot other than slot 0. Each MG 1000E must be provisioned with enough Voice Gateway Media Cards to support the TDM devices in that MG 1000E.

Memory-related parameters

Table 19 lists memory-related parameters and their maximum values.

Table 19
Memory-related parameters (Part 1 of 2)

Parameter	Values	
	CS 1000E	**MG 1000T**
Low-priority input buffers — (recommended default)	95 – 5000 (3500)	95 – 1000 (450)
High-priority input buffers — (recommended default)	16 – 5000 (3500)	16 – 1000 (450)
Input buffer size (words)	4	4
500-telephone, trunk and digital telephone output buffer — (recommended default)	16 –2048 (2000)	n/a
Message length (words)	4	4
D-channel input buffer size (bytes)	n/a	261
D-channel output buffer size (bytes)	n/a	266
TTY input buffer size (characters)	512	512
TTY output buffer size (characters)	2048	2048
Number of call registers — (recommended default)	26 – 50 000 (25 000)	26 – 2047 (800)
Call registers assigned to AUX	26–255	26–255
Number of AML msg call registers	25 – the minimum of 25% of total call registers or 255 (default 25)	25 – the minimum of 25% of total call reg-isters or 255 (default 25)

Table 19
Memory-related parameters (Part 2 of 2)

Parameter	Values	
	CS 1000E	**MG 1000T**
Call registers for CSL input queues (CSQI)	255 – the minimum of 25% of total call registers or 4095 (default 255)	255 – the minimum of 25% of total call registers or 4095 (default 255)
Call registers for CSL/AML output queues (CSQO)	255 – the minimum of 25% of total call registers or 4095 (default 255)	255 – the minimum of 25% of total call registers or 4095 (default 255)
Auxiliary input queue	20 – the minimum of 25% of total call registers or 255 (default 20)	20 – the minimum of 25% of total call reg- isters or 255 (default 20)
Auxiliary output queue	20 – the minimum of 25% of total call registers or 255 (default 20)	20 – the minimum of 25% of total call reg- isters or 255 (default 20)
History file buffer length (characters)	0 – 65 535	0 – 65 535

Note 1: In a system with CallPilot, AML, and Symposium, add the number of CSQI and CSQO to the Call Register (CR) requirement obtained from feature impact calculations.

Note 2: The buffer estimates were based on relatively conservative scenarios, which should cover most practical applications in the field. However, most models deal with “average traffic”. When traffic spikes occur, buffers can overflow. In these cases, raise the buffer size, depending on the availability of CRs. The maximum number of buffers allowed for CSQI and CSQO is 25% of NCR or 4095, whichever is less.

Buffer limits

The buffer limit is the maximum number of Call Registers (CR) that can be used for that particular function out of the total CR pool. If the designated limit is larger than needed and there are still spare CRs, the unused CRs will not be tied up by this specific function. Therefore, there is little penalty for overstating the buffer size limit, as long as the limit is within the number of CRs available to the system.

The values provided in Table 19 on page 142 indicate the relative requirements for various buffers. They are the minimum buffer size needed to cover most applications under the constraint of tight memory availability. When increasing buffer sizes, make the increases proportional to the values in Table 19. This guideline applies in all cases except CSQI/CSQO, which is relatively independent of other buffers and can be increased without affecting others.

For example, with a CS 1000E Call Center (maximum 25 000 CRs) using many applications (such as CallPilot), it would be advisable to set the CSQI/ CSQO to a high value (even up to the limit of 4095).

System capacities

Contents

This section contains information on the following topics:

Introduction

This chapter describes the system's primary capacity categories. For each category, this chapter:

- identifies the units in which the capacity is measured
- details the primary physical and functional elements affecting the capacity
- describes actions that can be used to engineer the capacity

"Resource calculations" on page 191 provides the algorithms for engineering the system within the capacity limits. In some cases, applications such as Call Center require detailed engineering. These applications are discussed in "Application engineering" on page 275

Memory size

Table 20 shows the minimum amount of memory required for CS 1000 Release 4.5 software.

Table 20
CS 1000 Release 4.5 memory requirements

Processor	Flash memory required	DRAM memory required	Total memory
Core Call Server (CP PII)	N/A	256 MByte	256 MByte
Core Call Server (CP PIV)	N/A	512 MByte	512 MByte
MG 1000E (SSC)	48 MByte	32 MByte	80 MByte
MG 1000T (SSC)	48 MByte	32 MByte	80 MByte

Table 21 gives the maximum call register count recommended for CS 1000 Release 4.5 software, so that the system's memory requirements do not exceed the processor's memory capacity.

Table 21
Recommended maximum call register counts

System	Recommended call register count	Memory required (SL-1 words)	Memory required (MByte)
CS 1000E	25 000	5 675 000	21.648
Note: Call registers are 227 SL-1 words long. One SL-1 word is 4 bytes.			

Memory engineering

The data store consists of both protected and unprotected database information. Tables 22 on page 148 and 24 on page 156 describe the information stored in each area.

The calculations described in Tables 22 and 24 include references to memory store per item. Table 23 on page 153 provides the memory store per item in protected data store. Table 25 on page 161 provides the memory store per item in unprotected data store. These values are also referred to as the PDS factors and UDS factors, respectively.

The PDS and UDS factors in Tables 23 and 25 are based on assumptions about typical configurations, feature usage, and traffic patterns. The assumptions are specified in Tables 22 and 24, as they become relevant. Refer to Appendix A: "Protected memory requirements" on page 357 for detailed calculations in cases where those assumptions may not apply.

Protected data store

Table 22 describes the protected data store (PDS) area.

Table 22
Protected data store (Part 1 of 5)

Item	Calculation*
Telephones: - analog (500/2500-type) - M2006/2008 - 2216/2616 - M2317 - M3900 - ACD - IP Phones 200x - IP Softphones 2050 - Add-on Modules - Templates - Attendants - Consoles **Assumptions** Average number of: • Features defined per analog (500/2500-type) telephone = 8 • analog (500/2500-type) telephones sharing the same template = 10 • Digital telephones sharing the same template = 2 • Non-key features per digital telephone = 4	Number of items × memory store per item
Data Service (DS)/VMS access TNs	Number of data only ports × memory store per DS/VMS access TN
*Refer to Table 23 on page 153 for the memory store per item (PDS factor). **Not applicable for CS 1000E; applies to MG 1000T.	

Table 22
Protected data store (Part 2 of 5)

Item	Calculation*
Office Data Administration (ODAS)	(Number of data ports only + Total number of telephones + Number of analog trunks) × memory store for ODAS
Customers	(Constant term + Number of customers) × memory store per customer
Directory Number (DN) translator **Assumptions** • The two lowest levels in the DN tree have an average rate of 8 digits. • The rest of the DN tree has a structure that provides the lowest possible digit rate for upper levels.	(5.8 × Number of DNs) + 2 × (2 × Number of ACD DNs) + (Number of ACD positions + Number of DISA DNs) + (memory store per console × Number of consoles) + Number of dial intercom groups
Dial Intercom Group (DIG) translator	Maximum number of DIGs + 2 × (number of DIGs + Total number of the telephones within DIGs)
Direct Inward System Access (DISA)	Number of DISA DNs × memory store per DISA DN
Authorization Code **Assumption** • The length of the authorization code is in the range of 4 through 7	(Number of customers × memory store per customer) + (1.47 × Number of authorization codes)
Speed Call	(Maximum number of Speed Call lists + Number of Speed Call lists) × (3 + 0.26 × Average number of entries per list × DN size)

*Refer to Table 23 on page 153 for the memory store per item (PDS factor).

**Not applicable for CS 1000E; applies to MG 1000T.

Table 22
Protected data store (Part 3 of 5)

Item	Calculation*
Analog trunks	Number of analog trunks × memory store per analog trunk
Trunk route	Constant term + (Number of trunk routes × memory store per trunk route)
Network	Protected overhead + (Number of loops × memory store per loop)
MF sender, DTR	(Number of DTRs × memory store per DTR) + (Number of MF senders × memory store per MF sender)
Virtual Trunks	(Number of D-channels × memory store per D-channel) + (Number of Virtual Trunks × memory store per Virtual Trunk)
ISDN PRI/PRI2**	(Number of D-channels × memory store per D-channel) + (Number of PRI trunks + Number of ISL trunks)
DTI/DTI2	(Number of DTI loops × memory store per DTI loop) + (Number of DTI2 loops × memory store per DTI2 loop)
History file	Size for history file buffer
*Refer to Table 23 on page 153 for the memory store per item (PDS factor). **Not applicable for CS 1000E; applies to MG 1000T.	

Table 22
Protected data store (Part 4 of 5)

Item	Calculation*
Basic Alternate Route Selection/Network Alternate Route Selection (BARS/NARS) **Assumptions** • The length of any code = 3 • The typical structure of the tree for every code (in terms of digit rate) is the following: — 10-10-10... for SPN code — 8 -10-10... for NXX/LOC code — 6-2-10-8-10... for NPA code	5684 + (31.21 × number of NPA Codes) + (1.06 × Number of NXX Codes) + (1.06 × (Number of LOC Codes) + (Number of SPN Codes) + (2 × Number of FCAS Tables)
ISDN Basic Rate Interface (BRI)**	(Number of MISP boards × memory store per MISP board) + (Number of DSLs × memory store per DSL) + (Number of TSPs × memory store per TSP) + (Number of BRI DNs × memory store per BRI DN)
Coordinated Dialing Plan (CDP)	Constant term + (3 × Number of steering codes) + (8 × Number of route lists) + (3 × Total number of entries in route lists)
Call Party Name Display (CPND)	Number of trunk routes + Number of consoles + Number of ACD DNs + Number of SL-1 DNs + Number of digital telephone DNs + Number of Names × (5 + Average length of name) + (Number of 1-digit DIG groups × 11) + (Number of 2-digit DIG groups × 101)

*Refer to Table 23 on page 153 for the memory store per item (PDS factor).

**Not applicable for CS 1000E; applies to MG 1000T.

Table 22
Protected data store (Part 5 of 5)

Item	Calculation*
Feature Group D (FGD) Automatic Number Identification (ANI) Database **Assumptions** • All Numbering Plan Area (NPA) codes designated for BARS/NARS are used for ANI also. • One NPA block for every fifty NPA codes. • Five NXX blocks for each NPA block. • Twenty SUB blocks for each NXX block.	(3 × Number of NPA Codes) + (658 × Number of NPA codes)
Automatic Call Distribution (ACD)/Network ACD (NACD)	(Number of ACD DNs × memory store per ACD DN) + (Number of NACD DNs × memory store per NACD DN) + (Number of ACD positions × memory store per ACD position) + (Number of ACD agents) + (11 × Number of customers)
Protected overhead	Memory store for overhead
*Refer to Table 23 on page 153 for the memory store per item (PDS factor). **Not applicable for CS 1000E; applies to MG 1000T.	

Table 23 lists the memory store per item (PDS factor) used in calculating PDS requirements.

Table 23
PDS factors (units in SL-1 words) (Part 1 of 3)

Feature	Units
System overhead	32 768
analog (500/2500-type) telephones*	58
CLASS telephones	58
M2006/2008 telephones*	105
M2216/2616 telephones*	115
M2317 telephones*	131
M3900 telephones	131
ACD telephones	16
IP Phones 200x	115
IP Softphones 2050	115
Add-on modules	32
Templates	16
Consoles	236
DS/VMS Access TNs	14.5
ISDN BRI (for MG 1000T only):	
— MISP cards	542
— DSLs	153
— TSPs	180
— BRI DNs	47
* See “Protected Memory for Phone Sets: Detail” on page 357.	

Table 23
PDS factors (units in SL-1 words) (Part 2 of 3)

Feature	Units
Analog trunks	54
Virtual Trunks	54
Trunk routes:	
— Constant term	1024
— Trunk routes	238
ISDN PRI/PRI2/ISL:	
— D-channels	137
IP D-Channel (DCIP)	137
ISDN DTI/DTI2/JDMI (for MG 1000T only):	
— DTI loops	70
— DTI2 loops	153
DISA DNs	18
Network:	
— Local loops	91
— Remote loops	95
ODAS	3
Customers:	
— Constant term	1000
— Customers	502
* See “Protected Memory for Phone Sets: Detail” on page 357.	

Table 23
PDS factors (units in SL-1 words) (Part 3 of 3)

Feature	Units
Tone and Digit Switch	2
MF Sender	2
Conference card	2
Digitone Receiver	12
Tone Detector	3
DN Translator (Consoles)	125
Author. Code (Custom.)	199
FGD ANI Database:	
— Constant term	43
— NPA Codes	547
CDP (Constant Term)	637
ACD/NACD:	
— ACD DNs	92
— NACD DNs	174 src 115 dest
— ACD Positions	30
* See “Protected Memory for Phone Sets: Detail” on page 357.	

Unprotected data store

Table 24 describes the unprotected data store (UDS) area.

Table 24
Unprotected data store (Part 1 of 5)

Item	Calculation*
Telephones (every type except BRI telephones)	Number of items × memory store per item where: Memory store per item depends on the telephone type. For example: Number of 2500 telephones × memory store per 2500 telephone Number of telephones with display × memory store per display
Attendant consoles	Number of attendant consoles × memory store per attendant console
BRI telephones**	Constant term + (memory store per MISP × Number of MISPs) + (memory store per DSL × Number of DSLs) + (memory store per BRI line card × Number of BRI line cards) where: MISP = Multi-purpose ISDN Signaling Processor DSL = Digital Subscriber Loop

*Refer to Table 25 on page 161 for the memory store per item (UDS factor).

**Not applicable for CS 1000E; applies to MG 1000T.

Table 24
Unprotected data store (Part 2 of 5)

Item	Calculation*
Analog trunks: — Paging trunks, RAN trunks, Add-on Data Module (ADM), RLA trunks, other analog trunks	Number of paging trunks × memory store per paging trunk Number of other analog trunks × memory store per other analog trunk and so on (Number of other analog trunks = Total number of analog trunks – Number of paging trunks – Number of RAN trunks – Number of ADMs – Number of RLAs)
Virtual Trunks	Number of Virtual Trunks × memory store per Virtual Trunk
Trunks (Call Detail Recording [CDR])	Total number of trunks × memory store per trunk
BRI trunks**	Number of BRI trunks × memory store per BRI trunk
Trunk routes	(Number of trunk routes × memory store per trunk route) + (Total number of trunks ÷16) ***Note:*** Round up the division result.
DTI/DTI2	Number of DTI loops × memory store per DTI loop Number of DTI2 loops × memory store per DTI2 loop
*Refer to Table 25 on page 161 for the memory store per item (UDS factor). **Not applicable for CS 1000E; applies to MG 1000T.	

Table 24
Unprotected data store (Part 3 of 5)

Item	Calculation*
ISDN PRI/PRI2/ISL**	
— PRI	(Number of D-channels × memory store per PRI D-channel) + (Number of output request buffers × memory store per output request buffer) + (2 × [Number of PRI trunks + Number of ISL trunks])
— PRI2	(Number of D-channels × memory store per PRI2 D-channel) + (Number of output request buffers × memory store per output request buffer) + (2 × [Number of PRI2 trunks + Number of ISL trunks])
I/O ports	(Number of TTYs × memory store per TTY) + (Number of CDR links × memory store per CDR link) + (Number of HS links × memory store per HS link) + (Number of APL links × memory store per APL link) + (Number of PMS links × memory store per PMS link) + (Number of Other links × memory store per Other link)
Other items (features): — Local loops, remote loops, secondary tapes, customer, Tone and Digit Switch, MF sender, Conference card, Digitone Receiver, Tone Detector, attendant, background terminal	Number of items × memory store per item
DS/VMS access TNs	Memory store per DS/VMS TN × Number of data only ports
*Refer to Table 25 on page 161 for the memory store per item (UDS factor). **Not applicable for CS 1000E; applies to MG 1000T.	

Table 24
Unprotected data store (Part 4 of 5)

Item	Calculation*
Application Module Link (AML)	Constant term + (Number of AMLs × memory store per AML)
Automatic Call Distribution (ACD):	
— Without ACD-C package	(Number of ACD DNs × 298) + (Number of ACD positions × 34)
— With ACD-C package	Additional memory size: (Number of ACD-C routes × 46) + (Number of ACD-C positions × 42) + [(Number of ACD-C DNs + Number of control directory numbers) × 80] + [(Number of ACD-C trunks + Number of ACD-C CRTs) × 30] + (Number of customers with ACD-C package × 240)
NARS/BARS/Coordinated Dialing Plan (CDP) **Assumption:** • If NTRF package is equipped, then Off Hook Queuing (OHQ) is also equipped	(Memory store per customer × Number of customers) + 2 × ([Number of route lists × memory store per route list] + [Number of routes with OHQ × memory store per route] + [Number of NCOS defined × memory store per NCOS])
*Refer to Table 25 on page 161 for the memory store per item (UDS factor). **Not applicable for CS 1000E; applies to MG 1000T.	

Table 24
Unprotected data store (Part 5 of 5)

Item	Calculation*
Call Registers (CR) **Assumptions:** • Call Register Traffic Factor = 1.865 • The formula for calculating the recommended number of call registers depends on traffic load for the system. • 28 CCS per ACD trunk	Call Registers memory size = Recommended number of call registers × memory store per call register Snacd = (Number of calls overflowed to all target ACD DNs × 2.25) – (Number of calls overflowed to local target ACD DNs × 1.8) (= 0 if the system is not a source node) Tnacd = 0.2 × Number of expected calls overflowed from source (= 0 if the system is not a target node) ISDN CCS = PRI CCS + BRI CCS • ISDN penetration factor: p = ISDN CCS ÷ Total Voice Traffic • ISDN factor: $(1 - p)^2 + [4 \times (1 - p)] \times p + (3 \times p^2)$
If Total Voice Traffic > 3000 CCS, then: If Total Voice Traffic ≤3000 CCS, then:	Recommended number of call registers = (0.04 × Total Voice Traffic) + (0.18 × Number of ACD incoming trunks) + [(Snacd + Tnacd) × 0.03 × ISDN factor] Recommended number of call registers = [(Number of system equipped ports – Number of ACD incoming trunks – Number of ACD agent telephones) × 0.94] + {Number of ACD incoming trunks + [(Snacd + Tnacd) × 0.03]} × ISDN factor
System overhead	Memory store for system overhead

*Refer to Table 25 on page 161 for the memory store per item (UDS factor).

**Not applicable for CS 1000E; applies to MG 1000T.

Table 25 lists the memory store per item (UDS factor) used in calculating UDS requirements.

Table 25
UDS factors (units in SL-1 words) (Part 1 of 3)

Feature	Units
System overhead	32 768
analog (500/2500-type) telephones	43.5
M2006/2008 telephones	89
M2216/2616 telephones	120
M2317 telephones	111.25
M3900 telephones	130
IP Phones 200x	120
IP Softphones 2050	96
Consoles	141
Add-on modules	24
Displays	2
DS/VMS access TNs	16.5
ISDN BRI telephones:	
— Constant term	298
— MISP cards	2270
— DSLs	264
— BRI line cards	96

Table 25
UDS factors (units in SL-1 words) (Part 2 of 3)

Feature	Units
Analog trunks:	
— RAN trunks	74
Broadcast RAN trunks	
— RLA Trunks	46
— AUTOVON Trunks	164
— ADM	172
— Other Analog Trunks	161
Virtual Trunks	161
Trunk routes	416
BRI trunks	148
Virtual Trunk D-Channel (DCIP)	850
DTI/DTI2 JDMI:	
— DTI loops	109
— DTI2 loops	97
PRI/PRI2:	
— D-channels (PRI)	836
— D-channels (PRI2)	850

Table 25
UDS factors (units in SL-1 words) (Part 3 of 3)

Feature	Units
I/O ports:	
— I/O ports (total)	2085
— CDR links	128
— HS links	143
— APL links	311
— PMS links	130
— Other links	512
Local loops	69
Customers	243
Tone and Digit Switch	59
MF Sender	59
Conference cards	191
Digitone Receiver	12
Tone Detector	13
Background terminals	96
AML (CSL):	
— Constant term	147
— AML Links	510
Call Registers	227

Mass storage

The system processor program and data are loaded from hard disk and/or floppies.

Software installation

Software, customer databases, and PEPS are delivered to the system using a Compact Flash card (RMD) inserted into the CP PIV pack faceplate. An installation process copies the software to the on-board Compact Flash (FMD). The software subsequently operates on this on-board Compact Flash (FMD).

Database backup

The faceplate Compact Flash (RMD) can also be used for customer database backups.

Physical capacity

A fully expanded CS 1000E system, with 30 MG 1000E each equipped with an MG 1000E Expander, provides 240 card slots (30 × 8) to support TDM devices and their required DSP resources.

A maximum of 256 loops are available to be used for gateway definitions, VXCT definitions (Conference/TDS), and phantom or virtual loops for telephones and trunks. For more information on phantom and virtual loops, refer to the Global Software Licenses chapter in *Features and Services* (553-3001-306).

Refer to “Assigning loops and card slots in the CS 1000E” on page 329 for information about loop and card slot usage and requirements for the Media Gateways in the CS 1000E.

Signaling and data links

The following signaling and data links are discussed in this section:

- “Physical links” on page 165
- “Functional links” on page 165

Physical links

There are three types of physical links to consider:

- Serial Data Interface (SDI) (p. 165)
- SDI through Terminal Server (p. 165)
- Embedded Local Area Network (ELAN) (p. 165)

Serial Data Interface (SDI)

The SDI is an asynchronous port, providing input access to the system from an OA&M terminal and printing out maintenance messages to a TTY. The CP PIV Call Processor card has two ports, COM 1 and COM 2. COM 1 must be used for system installation and upgrades.

SDI through Terminal Server

The SDI through the Terminal Server are asynchronous ports, providing input access to the system from an OA&M terminal and printing out maintenance messages, traffic reports, and Call Detail Recording (CDR) records to a TTY. These asynchronous ports are programmed to connect automatically to PTY ports in the Call Server. For more information, refer to *Communication Server 1000E: Installation and Configuration* (553-3041-210).

Embedded Local Area Network (ELAN)

The system can communicate with a Host by Ethernet connection through a Network Interface Card (NIC). AML messages are embedded in the communication protocols, and they continue to interface with the system through CSQI and CSQO queues.

The data rate at the NIC port auto-negotiates up to 1000 MB full duplex.

Functional links

For each of the following functions, the type of link and resulting capacity are given.

Application Module Link (AML)

AML is an Ethernet signaling link between the system and an Application Module (AM) connected to the ELAN subnet.

OA&M

The system uses a PTY port via a Terminal Server to connect to a terminal/computer (TTY) to receive maintenance commands or to print traffic reports, maintenance messages, or CDR records.

Property Management System Interface (PMSI)

The PMSI allows the system to interface directly to a customer-provided PMS through an SDI port in a Terminal Server. It is primarily used in Hotel/Motel environments to allow updates of the room status database either from the check-in counter or a guest room. The enhanced PMSI allows retransmission of output messages from the system to a PMS. The maximum baud rate for this asynchronous port is 9600.

Table 26 summarizes the above functional links and interfaces and provides information required to calculate the number of I/O cards needed as an input to the card slot calculations.

Table 26
I/O interface for applications

Application	Type of link/ interface	Type of port	Sync or async
Symposium	ELAN	Ethernet	Sync
CallPilot	ELAN	Ethernet	Sync
CDR	RS232 C	PTY	Async
Property Management System Interface (PMSI)	PMSI Link	PTY	Async
TTY (OA&M)	RS232 C	PTY	Async
Note: PTYs are accessed through serial ports on the Terminal Server.			

CS 1000E network traffic

Traffic is a measure of the time a circuit is occupied. On the system, the circuit normally consists of a path from the telephone or trunk to the terminating telephone or trunk.

This section discusses the following traffic considerations:

- "Loops and superloops" on page 168
- "Lines and trunks" on page 169
- "Service loops and circuits" on page 171
- "Voice Gateway Media Cards" on page 174
- "Traffic capacity engineering algorithms" on page 174

Terminology

Basic traffic terms used in this section are:

- ATTEMPT – any effort on the part of a traffic source to seize a circuit/ channel/timeslot
- CALL – any actual engagement or seizure of a circuit or channel by two parties

- CALLING RATE – the number of calls per line per busy hour (Calls/Line)
- BUSY HOUR – the continuous 60-minute period of day having the highest traffic usage, usually beginning on the hour or half-hour
- HOLDING TIME – the length of time during which a call engages a traffic path or channel
- TRAFFIC – the total occupied time of circuits or channels, generally expressed in CCS or Erlangs (CCS = a circuit occupied 100 seconds; Erlang = a circuit occupied one hour)
- BLOCKING – attempts not accepted by the system due to unavailability of the resource
- OFFERED traffic = CARRIED traffic + BLOCKED traffic
- Traffic load in CCS = Number of calls × AHT ÷ 100 (where AHT = average holding time)
- Network CCS = Total CCS handled by the switching network
or
CCS offered to the network by stations, trunks, attendants, Digitone Receivers, conference circuits, and special features

Loops and superloops

No physical hardware is required in order to provide superloops in the CS 1000E and MG 1000T platforms. Superloops exist in programming only.

CS 1000E

A fully expanded CS 1000E system provides a maximum of 256 loops or 64 superloops. Each superloop provides 120 timeslots, which can be shared by two MG 1000Es. Each superloop can support 1024 Virtual Trunks.

MG 1000T

The number of loops needed in the system can be calculated from lines, trunks, and traffic requirements such as average holding time (AHT) and CCS. Each superloop can carry 3500 CCS of combined station, trunk, attendant console, and Digitone traffic during an average busy season busy hour (ABSBH).

Loop capacity is subject to the Grade-of-Service (GoS) described under "Grade-of-Service" on page 175.

Lines and trunks

The relationship between lines and trunks is relevant for calculating loop requirements.

Voice over IP traffic

In the context of Voice over IP (VoIP) application, the lines include IP Phones and the trunks include IP Peer H.323 Virtual Trunks and SIP Virtual Trunks. The ratio of IP calls to the total line calls, and the ratio of H.323 and SIP Virtual Trunks calls to the total trunk calls, are required parameters. The split of TDM traffic to IP/Virtual Trunks (VT) becomes important, since resources such as Digital Signal Processor (DSP) in Media Cards and H.323 or SIP Virtual Trunks are affected by traffic distribution.

Figure 32 on page 170 is a representation of the traffic flow for different types of calls. Each connection is denoted by a line. Lines crossing the DSP line require a DSP port. For example, IP to IP connections in a CS 1000E system require no DSP and neither do IP to VT, but TDM to TDM do require DSP.

Figure 32
CS 1000E system call types

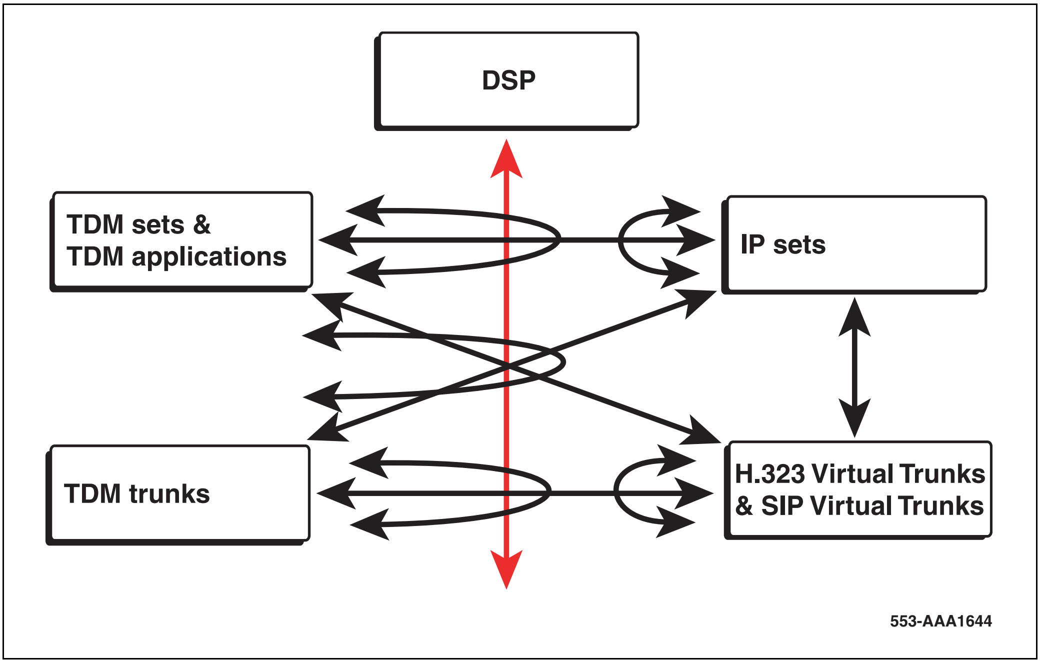


Table 27 lists the resources required for each type of connection.

Table 27
Connection type resources required

Connection Type	Resources
TDM to IP, IP to TDM	DSP
TDM to VT, VT to TDM	DSP and VT
IP to IP	no DSP
IP to VT or VT to IP	VT
TDM to TDM telephone or trunk calls	DSP no VT

Refer to “Resource calculations” on page 191 for the algorithms to calculate the required resources.

Service loops and circuits

Service circuits are required in call processing to provide specific functions to satisfy the requirements of a given application. Service circuits consume system resources, such as physical space, real time, memory, and so on.

In the CS 1000E, Virtual Tone and Conference Circuits (VXCT) must be defined for use by each MG 1000E.

This section describes the traffic characteristics, calculation algorithms, and impact on other system resources of the following types of service circuits:

- TDS (p. 171)
- Conference (p. 171)
- Broadcast circuits (p. 172)
- DTR (p. 173)

TDS

The Tone and Digit Switch (TDS) loop provides dial tone, busy tone, overflow tone, ringing tone, audible ringback tone, DP or dual tone multifrequency (DTMF) outpulsing, and miscellaneous tones. All these tones are provided through the maximum 30 timeslots in the TDS loop.

A minimum of one TDS loop is required in each MG 1000E. The TDS circuits are provided by the MG 1000E’s SSC card. If additional TDS circuits are required in any MG 1000E, a second TDS loop can be configured in it. TDS circuits in an MG 1000E provide tones for TDM telephones or trunks in that MG 1000E only.

Conference

There are 16 conference circuits per conference (CON) loop, for a total of 64 conference circuits per MG 1000E. There are 32 conference circuits (2 loops) on the SSC card and another 32 conference circuits (2 loops) on the dual-port IP daughterboard.

Note: If a single-port IP daughterboard is used, define no more than three conference loops for that MG 1000E. With a single-port daughterboard, there is no way to determine if a fourth conference loop exists, so a fourth conference loop will cause failures for accessing conference circuits.

Conference circuits in the CS 1000E are a system resource

Broadcast circuits

The Nortel Integrated Recorded Announcer (Recorded Announcer) card provides either 8 or 16 ports to support Music, Recorded Announcement (RAN), and Automatic Wake Up. There is a maximum of 60 simultaneous connections to an individual card for broadcast within an MG 1000E. With special provisioning, the limit can be increased to 120 connections (see "Broadcast circuits" on page 335).

IMPORTANT!

Currently, the CS 1000E only supports Recorded Announcement Broadcast and Music Broadcast.

Music

Music Broadcast requires any Music trunk and an external music source or a Recorded Announcer card. The Recorded Announcer has the capability to provide audio input for external music. A CON loop is not required for Music Broadcast.

RAN

RAN trunks are located on eight-port trunk cards on PE shelves just like regular trunk circuits. They provide voice messages to waiting calls. RAN trunks are also needed to provide music to conference loops for music on hold.

Each RAN trunk is connected to one ACD call at a time, for the duration of the RAN message. Different RAN sources require different RAN trunk routes. If the first RAN is different from the second RAN, they need different RAN trunk routes. However, if the same message is to be used, the first RAN and second RAN can use the same route.

Use the following formula to calculate RAN traffic:

$$\text{RAN CCS} = \text{Number of ACD calls using RAN} \times \text{RAN HT} \div 100$$

A RAN message typically runs from 20 seconds to 40 seconds. If the average for a specific application is not known, use a default of 30 seconds. After RAN CCS is obtained, estimate RAN trunk requirements from a Poisson P.01 table or a delay table (such as DTR table) matching the holding time of a RAN message.

DTR

A Digitone Receiver (DTR) serves features involving 2500 telephones or Digitone trunks. In CS 1000E systems, DTRs are not system-wide resources. They support only the telephones and trunks in the MG 1000E in which they reside.

The SSC card provides 16 DTRs, or 8 DTRs and 4 Multifrequency Receivers (MFR). Additional DTRs can be provided by XDTR cards.

There are a number of features that require DTRs. General assumptions for DTR traffic calculations are:

- DTR traffic is inflated by 30% to cover unsuccessful dialing attempts.
- Call holding time used in intraoffice and outgoing call calculations is 135 seconds if actual values are unknown.
- DTR holding times are 6.2 and 14.1 seconds for intraoffice and outgoing calls, respectively.
- The number of incoming calls and outgoing calls are assumed to be equal if actual values are not specified.

The major DTR traffic sources and their calculation procedures are as follows:

1 Calculate intraoffice DTR traffic:

Intraoffice = 100 × DTR station traffic (CCS) ÷ AHT × (R ÷ 2)
(Recall that R is the intraoffice ratio.)

2 Calculate outgoing DTR traffic:

Outgoing = 100 × DTR station traffic (CCS) ÷ AHT × (1 - R ÷ 2)

3 Calculate direct inward dial (DID) DTR traffic:

DID calls = DID DTR trunk traffic (CCS) × 100 ÷ AHT

4 Calculate total DTR traffic:
Total = [(1.3 × 6.2 × intra) + (1.3 × 14.1 × outgoing calls) + (2.5 × DID calls)] ÷ 100

5 See "Digitone receiver load capacity – 6 to 15 second holding time" on page 626 to determine the number of DTRs required. Note that a weighted average for holding times should be used.

Voice Gateway Media Cards

Since the Terminal Proxy Server (TPS) runs on the Signaling Server, Voice Gateway Media Cards do not carry traffic in the CS 1000E. They are used for DSP resources. If TPS is enabled on the cards, they can also assist in downloading firmware to IP Phones during software upgrades.

> ***Note:*** All the Media Cards in a specific MG 1000E must be in the same zone, so that bandwidth management and codec selection can be performed properly.

Traffic capacity engineering algorithms

Traffic capacities of subsystems in the system are estimated based on statistical models that approximate the way a call is handled in that subsystem.

When inputs to the algorithm are lines, trunks, average holding time (AHT), and traffic load (CCS), the algorithms can be used to determine system size.

Alternatively, when the traffic capacity is known for a given configuration, the algorithms can be used to determine the traffic level allowed at the line and trunk level while meeting GoS requirements.

Grade-of-Service

In a broad sense, the Grade-of-Service (GoS) encompasses everything a telephone user perceives as the quality of services rendered. This includes:

- frequency of connection on first attempt
- speed of connection
- accuracy of connection
- average speed of answer by an operator
- quality of transmission

In the context of the system capacity engineering, the primary GoS measures are blocking probability and average delay.

Based on the EIA Subcommittee TR-41.1 Traffic Considerations for PBX Systems, the following GoS requirements must be met:

- Dial tone delay is not greater than 3 seconds for more than 1.5% of call originations.
- The probability of network blocking is 0.01 or less on line-to-line, line-to-trunk, or trunk-to-line connections.
- Blocking for ringing circuits is 0.001 or less.
- Post-dialing delay is less than 1.5 seconds on all calls.

Traffic models

Table 28 summarizes the traffic models that are used in various subsystem engineering procedures.

Table 28
Traffic models

Model	Assumptions	Service criteria	Applicability
Erlang B	Infinite sources (ratio of traffic sources to circuits > 5:1)	Blocked calls cleared (no queueing)	Loop, ringing circuit blocking
Erlang C	Infinite sources	Blocked calls delayed Infinite queue	Dial tone delay, I/O buffers, Digitone, RAN trunks
Poisson	Infinite sources	Blocked calls held for a fixed length	Incoming/outgoing trunks, Digitone, Call Registers, RAN trunks

Typically, the GoS for line-side traffic is based on Erlang B (or Erlang Loss formula) at P.01 GoS. When there is no resource available to process a call entering the system, the call is blocked out of the system. Therefore, the correct model to calculate the call's blocking probability is a "blocked call cleared" model, which is the basis of Erlang B.

When a call is already in the system and seeking a resource (trunk) to go out, the usual model to estimate trunk requirements is based on the Poisson formula. The reasons are:

- The Poisson model is more conservative than Erlang B (in that it projects a higher number of circuits to meet the same GoS). This reflects trunking requirements more accurately, since alternative routing (or routing tables) for outgoing trunk processing tends to increase loading on the trunk group.
- General telephony practice is to provide a better GoS for calls already using system resources (such as tones, digit dialing, and timeslots). Incomplete calls inefficiently waste partial resources. With more trunk circuits equipped, the probability of incomplete calls is lower.

Real-time capacity

Real-time capacity (load) refers to the ability of the Call Server to process instructions resulting from calls in accordance with service criteria.

Existing systems can use methods based on traffic data in order to determine Rated Call Capacity and current utilization levels. Refer to *Traffic Measurement: Formats and Output* (553-3001-450) for a description of the TFS004 call capacity report and for information on interpreting TFS004 output.

If a new switch is being configured, equivalent basic calls must be calculated in order to estimate the processor loading of a proposed configuration.

Equivalent Basic Calls

An Equivalent Basic Call (EBC) is a measure of the real time required to process a basic call. A basic call is defined as a simple, unfeatured call between two IP Phones type 2004. The terminating telephone is allowed to ring three times, then is answered, waits approximately two seconds, and hangs up. The originating telephone then hangs up as well.

When the capacity of a switch is stated in EBC, it is independent of such variables as configuration, feature mix, and usage patterns. It still varies from release to release, and between processors. However, since it is independent of other factors, it is a good way to compare the relative call processing capability of different machines running the same software release.

Table 29 gives the rated capacities of the Call Server processors in systems operating CS 1000 Release 4.5.

Table 29
Real-time capacity (EBC) by system (with CS 1000 Release 4.5 software)

System	Capacity
CS 1000E (CP PII processor)	210 000
CS 1000E (CP PIV processor)	840 000
MG 1000T (SSC)	35 000

Feature impact

Every feature that is applied to a call increases the CP real time consumed by that call. These impacts can be measured and added incrementally to the cost of a basic call to determine the cost of a featured call. This is the basis of the algorithm used by NNEC to determine the rated capacity of a proposed switch configuration.

The incremental impact of a feature, expressed in EBC, is called the real-time factor for that feature. Real-time factors are computed by measuring the incremental real time for the feature in milliseconds, and dividing by the call service time of a basic call.

Each call is modeled as a basic call plus feature increments. For example, an incoming call from a DID trunk terminating on a digital telephone with incoming CDR is modeled as a basic call plus a real-time increment for incoming DID plus an increment for digital telephones plus an increment for incoming CDR.

A second factor is required to determine the overall impact of a feature on a switch. This is the penetration factor. The penetration factor is simply the proportion of calls in the system that invoke the feature.

The real-time impact, in EBC, of a feature on the system is computed as follows:

(Calls) × (penetration factor) × (real-time factor)

The sum of the impacts of all features, plus the number of calls, is the real-time load on the system, in EBC.

For penetration and real-time factors and for the detailed EBC calculations, refer to “System calls” on page 198 and “Real-time calculations” on page 202.

Call Server real-time calculations

The system EBC divided by the processor’s rated capacity (see Table 29 on page 177) yields the fraction for processor utilization. This determines whether the proposed system will handle the load. If the projected real-time load is larger than the system capacity, a processor upgrade is needed.

Traffic peaking of 30% has been incorporated in the derivation of rated capacity. In other words, at 100% rated capacity, the absolute loading of the processor is 70%. Users should not adjust the rated capacity, but the loading percentage can reach 100% and the system will still function well. However, to preserve spare capacity for growth and extra traffic peaking, initial engineering of any site at full 100% loading is not recommended. A more typical initial load is about 85%.

If the configuration is an upgrade to an existing switch, in addition to calculating the new load as described above, users must also factor in CPU utilization data from a current traffic report TFS004. Users apply a formula to convert the existing processor usage to the equivalent loading on the new (and presumably faster) CPU.

Auxiliary processors

Interactions with auxiliary processors also have real-time impacts on the system CP depending on the number and length of messages exchanged. Several applications are described in "Application engineering" on page 275.

Real-time algorithm

As described above, calculating the real-time usage of a configuration requires information on the number of busy hour call attempts and the penetration factors of each feature.

Busy hour calls

If the switch is already running, the number of busy hour calls or call load can be determined from the traffic printout TFS004. The second field of this report (after the header) contains a peg count of CP Attempts. Examine a period of several days (a full week, if possible) to determine the maximum number of CP attempts experienced. This number varies with season, as well. The relevant number is the average of the highest ten values from the busiest four-week period of the year. An estimate is sufficient, based on current observations, if this data is not available.

If the switch is not accessible and call load is not known or estimated from external knowledge, call load can be computed. For this purpose, assumptions about the usage characteristics of telephones and trunks must be made. Refer to Table 34 on page 194 for a description of the parameters that are required and default values, if applicable.

Telephones

As the primary traffic source to the system, telephones have a unique real-time impact on the system. For the major types listed below, the number of telephones of each type must be given, and the CCS and AHT must be estimated. In some cases it may be necessary to separate a single type into low-usage and high-usage categories. For example, a typical office environment with analog (500/2500-type) telephones may have a small call center with agents on analog (500/2500-type) telephones. A typical low-usage default value is 6 CCS. A typical high-usage default value is 28 CCS.

The principal types of telephones include:

- Analog: 500/2500-type, message waiting 500, message waiting 2500, and CLASS telephones
- Digital: M2000 series Meridian Modular Telephone, voice and/or data ports
- Consoles
- IP Phone 2001, IP Phone 2002, IP Phone 2004, IP Phone 2007
- IP Softphone 2050

Trunks

Depending on the type of trunk and application involved, trunks can either be traffic sources, which generate calls to the system, or resources that satisfy traffic demands. Default trunk CCS in an office environment is 26 CCS. Call Center applications may require the default to be as high as 28 to 33 CCS.

Voice

Analog:

- CO
- DID
- WATS

- FX
- CCSA
- TIE E&M
- TIE Loop Start

Digital (for MG 1000T only):

- DTI: number given in terms of links, each of which provides 24 trunks under the North American standard
- PRI: number given in terms of links, each of which provides 23B+D under the North American standard
- European varieties of PRI: VNS, DASS, DPNSS, QSIG, ETSI PRI DID

H.323 Virtual Trunk

An IP Peer H.323 Virtual Trunk identified with a trunk route which is not associated with a physical hardware card.

SIP Virtual Trunk

A Session Initiation Protocol (SIP) Virtual Trunk identified with a trunk route which is not associated with a physical hardware card.

Data

- Sync/Async CP
- Async Modem Pool
- Sync/Async Modem Pool
- Sync/Async Data
- Async Data Lines

RAN

The default value for AHT_{RAN} is 30 seconds.

Music

The default value for AHT_{MUSIC} is 60 seconds.

Signaling Server

The following software components operate on the Signaling Server:

- Terminal Proxy Server (TPS)
- H.323 Gateway (Virtual Trunk)
- SIP Gateway (Virtual Trunk)
- Network Routing Service (NRS)
- H.323 Gatekeeper
- SIP Redirect Server
- Network Connection Service (NCS)
- CS 1000 Element Manager Web Server
- Application Server

All the software elements can coexist on one Signaling Server or reside individually on separate Signaling Servers, depending on traffic and redundancy requirements for each element.

A Signaling Server can also function as an application server for the Personal Directory, Callers List, and Redial List applications and Password administration. See "Application server for Personal Directory, Callers List, and Redial List" on page 188.

Table 30 describes the function and engineering requirements of each element.

Table 30
Elements in Signaling Server (Part 1 of 4)

Element	Function and engineering requirements
Terminal Proxy Server (TPS)	• The TPS handles initial signaling exchanges between an IP Phone and the Signaling Server. • The TPS supports a maximum of 5000 IP Phones on each Signaling Server. • The TPS manages the firmware for the IP Phones that are registered to it. Accordingly, the TPS also manages the updating of the firmware for those IP Phones. • The redundancy of TPS is N+1. Therefore, one extra Signaling Server can be provided to cover TPS functions from N other servers.
H.323 Gateway (Virtual Trunk)	• The IP Peer H.323 Gateway trunk, or H.323 Virtual Trunk, provides the function of a trunk route without a physical presence in the hardware. The H.323 Gateway supports direct, end-to-end voice paths using Virtual Trunks. • The H.323 Signaling software (Virtual Trunk) provides the industry-standard H.323 signaling interface to H.323 Gateways. It supports both en bloc and overlap signaling. This software uses an H.323 Gatekeeper to resolve addressing for systems at different sites. • The H.323 Gateway supports up to 1200 H.323 Virtual Trunks per Signaling Server, assuming a combination of incoming and outgoing H.323 calls (see "Maximum number of SIP and H.323 Virtual Trunks" on page 186). Beyond that, a second Signaling Server is required.

Table 30
Elements in Signaling Server (Part 2 of 4)

Element	Function and engineering requirements
	Note 1: At least 768 MByte of memory is required on the Signaling Server to obtain 1200 H.323 Virtual Trunks. If the Signaling Server has less than 768 MByte of memory, then a maximum of 382 Virtual Trunks can be configured. ***Note 2:*** If H.245 tunneling is not enabled, then a maximum of 900 H.323 Virtual Trunks can be supported on a Signaling Server equipped with at least 768 MByte of memory. • The redundancy mode of the H.323 Gateway is 2 × N. Two H.323 Gateways handling the same route can provide redundancy for each other, but not for other routes.
SIP Gateway (Virtual Trunk)	• The SIP Gateway trunk, or SIP Virtual Trunk, provides a direct media path between users in the CS 1000M domain and users in the SIP domain. • The SIP trunking software functions as: – a SIP User Agent – a signaling gateway for all IP Phones • The SIP Gateway supports a maximum of 1800 SIP Virtual Trunks (see "Maximum number of SIP and H.323 Virtual Trunks" on page 186). • The redundancy mode of the SIP Gateway is 2 × N. Two SIP Gateways handling the same route can provide redundancy for each other, but not for other routes.

Table 30
Elements in Signaling Server (Part 3 of 4)

Element	Function and engineering requirements
Network Routing Service (NRS)	• The NRS has three components: – H.323 Gatekeeper – SIP Redirect Server – Network Connection Service (NCS) • The NRS must reside on the Leader Signaling Server. In a redundant configuration, the NRS is configured as Primary, Alternate, or Failsafe (if required). • The NRS software limit for the combined total number of endpoints and routing entries is 20 000. The limit for the total number of endpoints is 5000 (up to 5000 SIP and up to 2000 H.323 endpoints). • The redundancy of the NRS is in a mode of 2 × N. An alternate NRS can serve only the NRS it is duplicating.
• H.323 Gatekeeper	• All systems in the network register to the H.323 Gatekeeper, which provides telephone number to IP address resolution. • The capacity of the H.323 Gatekeeper is limited by the endpoints it serves and the number of entries at each endpoint. • Potential hardware limits are the Signaling Server processing power and memory limits. • Since the Gatekeeper is a network resource, its capacity is a function of the network configuration and network traffic (IP calls). Some basic network information is required to engineer a Gatekeeper.
• SIP Redirect Server	• The SIP Redirect Server provides telephone number to IP address resolution. It uses a Gateway Location Service to match a fully qualified telephone number with a range of Directory Numbers (DN) and uses a SIP gateway to access that range of DNs.
• Network Connection Service (NCS)	• The NCS provides an interface to the TPS, enabling the TPS to query the NRS using the UNIStim protocol. The NCS is required to support the Media Gateway 1000B, Virtual Office, and Geographic Redundancy features.

Table 30
Elements in Signaling Server (Part 4 of 4)

Element	Function and engineering requirements
CS 1000 Element Manager Web Server	• Has a negligible impact on capacity and can reside with any other element.
Application Server	• The Application Server for the Personal Directory, Callers List, and Redial List feature runs on the Signaling Server. • Only one database can exist in the network, and redundancy is not supported. • The database can co-exist with the other software applications on a Signaling Server. However, if there are more than 1000 users, Nortel recommends that the database be stored on a dedicated Signaling Server, (preferably a Follower). • The Application Server cannot be run on a Signaling Server at a branch office. • For more information on Personal Directory, Callers List, and Redial List, refer to *IP Line: Description, Installation, and Operation* (553-3001-365).
Note: The feasibility of combining the TPS, H.323 Gateway, SIP Gateway, and NRS on a Signaling Server is determined by traffic associated with each element and the required redundancy of each function.	

Maximum number of SIP and H.323 Virtual Trunks

The maximum number of SIP and H.323 channels available on each Signaling Server depends on the number of available File Descriptors (FD) for Virtual Trunks.The maximum number of File Descriptors for Virtual Trunks is 1800.

- Each SIP call uses one FD.
- Each incoming H.323 call uses two FD.
- Each outgoing H.323 call uses one FD.

When no more File Descriptors are available (available FD = 0), new channels added on the Call Server will not be able to register on the Signaling Server.

Each Signaling Server supports up to 1800 Virtual Trunks. The maximum number of SIP and H.323 trunks will depend on traffic patterns, both the split between SIP and H.323 calls and the split between incoming and outgoing H.323 calls. Table 31 gives examples of the maximum number of Virtual Trunks supported for different configurations.

Table 31
Maximum number of Virtual Trunks, per Signaling Server

SIP	H.323*			Total Virtual Trunks
	Incoming	Outgoing	Total H.323	
1800	0	0	0	1800
0	600	600	1200	1200
0	900	0	900	900
600	0	1200	1200	1800
600	300	600	900	1500
*Assumes H.245 tunneling is enabled.				

The formula to calculate the maximum number of Virtual Trunks is:

(Num_of_SIP × 1 FD) + (Num_of_Incoming_H323 × 2 FD) + (Num_of_Outgoing_H323 × 1 FD) <= Max_Num_of_FDs

where Max_Num_of_FDs = 1800

Impact of H.245 tunneling

By default, H.245 tunneling is enabled. Unless there is a specific reason to disable tunneling, such as for maintenance, it should always be enabled. When tunneling is off, the handling capacity of the Signaling Server is reduced to a maximum of 900 H.323 Virtual Trunks.

Application server for Personal Directory, Callers List, and Redial List

The database for the Personal Directory, Callers List, and Redial List features for IP Phones must be located on one Signaling Server. The applications cannot be divided: all users in a system will either have the combined Personal Directory, Callers List, and Redial List features or no feature at all. The Signaling Server can support a database for up to 15 000 users.

- **Personal Directory**: Stores up to 100 entries per user of user names and DNs.
- **Callers List**: Stores up to 100 entries per user of caller ID information and most recent call time.
- **Redial List**: Stores up to 20 entries per user of dialed DNs and received Call Party Name Display with time and date.

The Signaling Server requires a minimum of 512 MByte of memory in order to support the Personal Directory, Callers List, and Redial List applications.

If the system size is relatively small, in terms of number of users as well as calling rates, one Signaling Server can serve both database and normal Signaling Server functions. With the Personal Directory, Callers List, and Redial List database co-resident with other applications (TPS, H.323/SIP Gateways, NRS, Element Manager), a Signaling Server with 512 MByte of memory can serve up to1000 IP users and 382 Virtual Trunks. For larger systems, one additional Signaling Server, on top of the normal requirement for handling signaling traffic, will be required for the Personal Directory, Callers List, and Redial List features.

The amount of memory required to support the Personal Directory, Callers List, and Redial List applications on the Signaling Server depends on the number of IP users and the configuration. Table 32 shows the memory requirements.

Table 32
Signaling Server memory requirements for the Personal Directory, Callers List, and Redial List features

Personal Directory, Callers List, and Redial List configuration	Number of IP users	Number of Virtual Trunks	Required memory
Co-resident with other applications	<= 1000	<= 382	512 MByte
Stand alone	1000 – 8 000	> 382	768 MByte
Stand alone	8 000 – 15 000	> 382	1 Gbyte

There is no redundancy for the Signaling Server dedicated to the Personal Directory, Callers List, and Redial List database. If that Signaling Server fails, the system loses those applications. However, the other Signaling Servers will continue to function normally without the Personal Directory, Callers List, and Redial List features.

Software configuration capacities

The tables in "Design parameters" on page 133 provide maximum configuration capacities for applicable system and feature parameters. A system may not be able to simultaneously accommodate all of the maximum values listed because of system limitations on the real time, memory, or traffic capacity.

IP Telephony node maximums

The maximum number of Voice Gateway Media Cards per node is 30. When more than 30 Voice Gateway Media Cards are needed on a single CS 1000E system, use multiple nodes. The maximum number of Signaling Servers and Voice Gateway Media Cards combined within a node is 35.

CS 1000E capacities

Since IP telephony consumes less processing than TDM, the total number of telephones that a particular platform can support depends on the type of traffic as well as the physical capacity and applications of a specific configuration.

Table 33 on page 190 summarizes the capacities of CS 1000E systems. Values in each cell indicate the total number of telephones that can be supported in a particular configuration. These values are calculated from the point of view of call server processing capacity, not from the point of view of physical card slot capacity.

Note: Values in each cell are exclusive, not additive.

Table 33
CS 1000E traffic capacities summary

Call server	Platform name	Total number of telephones			
		Pure TDM (no trunking)	IP Phones with access to PSTN	Pure IP (no access to PSTN)	Mixed TDM and IP Phones
CP PIV	CS 1000E	3000	N/A	15 000	3000 TDM 10 000 IP

Note 1: Values in each column reflect the total telephones for a configuration. These are absolute limits for pure TDM and pure IP. For mixed TDM and IP, values are for typical configurations. Applications and calling patterns impact call server capacity. NNEC and NTPs are used to calculate practical values preconfiguration. Values beyond these limits must be engineered.

Note 2: Requires using Signaling Servers for TPS.

Note 3: Mixed configuration assumes 8-15% digital trunking to PSTN and no applications.

Zone/IP Telephony Node Engineering

For information on Zone/IP Telephony Node Engineering, refer to *Communication Server 1000M and Meridian 1: Large System Planning and Engineering* (553-3021-120).

Resource calculations

Contents

This section contains information on the following topics:

Introduction

This chapter describes the algorithms implemented by the NNEC tool in order to calculate the resources required by the system.

In many cases, the calculations require user inputs that are the result of pre-engineering performed in accordance with the capacities and guidelines described in “System capacities” on page 145 and “Application engineering” on page 275.

The CS 1000E does not directly support PRI/DTI and BRI trunks and MDECT telephones. These are supported by the MG 1000T (or by other independent switches in the network). The MG 1000T directs calls to the CS 1000E using IP Peer networking. For the CS 1000E, the engineering requirement is the number of Virtual Trunk access ports required to support traffic from the IP Peer gateways of the MG 1000T.

Calculate resource requirements for the MG 1000T separately, as an independent pre-engineering exercise before calculating requirements for the CS 1000E. See "MG 1000T pre-engineering" on page 192 for the guidelines to calculate Digital Signal Processor (DSP), Virtual Trunk, and Signaling Server resource requirements for the MG 1000T.

> ***Note:*** When a proposed new system will be equipped with more ports than the initial configuration will actually use, treat the two sets of input data like two separate configurations. Run each telephone of data through the algorithm and then compare results. For a viable solution, both sets of calculation results must be within the capacities of the proposed system.

MG 1000T pre-engineering

Use the following rules to calculate MG 1000T resource requirements.

DSP ports

The total number of DSP ports required in the MG 1000T is the sum of the following:

1. One DSP port for each PRI or DTI trunk.
2. Two DSP ports for each BRI user.
3. A fixed ratio of DSP ports to MDECT mobile telephones. The recommended ratio for standard Grade-of-Service (GoS) is six MDECT telephones per DSP port. Use a one-to-one ratio for non-blocking access.

   Note: It is not possible to reserve DSP ports for specific service demands. In order not to degrade the non-blocking services provided to TDM trunks in the MG 1000T, do not use a ratio higher than six MDECT telephones per DSP port.

Virtual Trunk access ports

1 The required number of Virtual Trunks is equal to the number of DSP ports calculated for the MG 1000T.

2 Split the Virtual Trunks into Session Initiation Protocol (SIP) and H.323 types.

Note: When engineering the CS 1000E, user input for the number of Virtual Trunks must include the sum of SIP and H.323 Virtual Trunks in all MG 1000T, MG 1000B, and other network IP Peer gateways.

Signaling Servers

The MG 1000T requires one Signaling Server (and one alternate Signaling Server, if desired for redundancy).

- A fully expanded MG 1000T provides 40 card slots.
- Since each PRI trunk must be paired with a DSP port, a maximum of 20 slots can be used for PRI.
- Twenty PRI slots can accommodate up to 600 PRI trunks (for E1; 480 PRI trunks for T1).
- PRI cards, with 30 ports per card, have the highest density of all the cards that can be installed in the MG 1000T and therefore would generate the most traffic.
- One Signaling Server can serve 1200 H.323 Virtual Trunks or 1800 SIP Virtual Trunks. This capacity is much higher than the traffic that can possibly be generated by the physical cards in the MG 1000T.

If the number of ports and Media Cards required in the MG 1000T exceeds the capacity of 40 card slots, another MG 1000T is needed. The second MG 1000T will require its own Signaling Server (and alternate Signaling Server, if desired).

Resource calculation parameters

Table 34 on page 194 describes the major parameters used in the Voice over IP (VoIP) calculations. Some are user input and others are calculated.

Table 34
Major parameters for VoIP resource calculations (Part 1 of 4)

Parameter	Description	Equation	Default value
TDM telephone CCS (L_{TDM})	Sum of all digital and analog telephone and line-side T1/E1 ports, in CCS	(Number of digital telephones + Number of analog telephones + Number of line-side T1/E1 ports) × CCS per telephone	CCS per tele-phone: 5
IP Phone CCS (L_{IP}) (See Note 3 at end of table.)	Sum of all IP and IP ACD agent telephones, in CCS	[(Number of IP Phones – Number of IP ACD agents) × CCS per IP Phone] + (Number of IP agent telephones × CCS per agent)	CCS per tele-phone: 5
MDECT telephone CCS (L_{DECT})	Sum of all MDECT mobile telephones, in CCS	Number of MDECT telephones × CCS per telephone	CCS per tele-phone: 5
Total line CCS (L_{CCS})	Sum of all TDM, IP, and MDECT telephone CCS	TDM telephone CCS (L_{TDM}) + IP telephone CCS (L_{IP}) + MDECT telephone CCS (L_{DECT})	
TDM trunk CCS (T_{TDM})	Sum of all analog and digital trunks, in CCS	(Number of analog trunks + Number of digital trunks) × CCS per trunk	CCS per tele-phone: 26
Converged Desktop ratio (r_{DTP})	Of the total number of telephones, the portion that have the Converged Desktop feature	(Number of telephones with Converged Desktop) ÷ (Total number of telephones)	

Table 34
Major parameters for VoIP resource calculations (Part 2 of 4)

Parameter	Description	Equation	Default value
Converged Desktop CCS (V_{DCCS}) (See Note 2 after the table.)	Converged Desktop CCS calculated as a percentage of total line CCS	Total line CCS (L_{CCS}) × Converged Desktop ratio (r_{DTP})	
SIP CTI TR/87 ratio rMO	Of the total number of sets, the portion that have the SIP CTI/TR87 feature	Number of sets with SIP CTI/TR87 feature ÷ Total number of sets	
H.323 Virtual Trunk CCS (HVT_{CCS})	Sum of all H.323 Virtual Trunks, in CCS	Number of H.323 Virtual Trunks (VT_{323}) × CCS per VT_{323}	
SIP Virtual Trunk CCS (SVT_{CCS})	Sum of all SIP Virtual Trunks, in CCS	Number of SIP Virtual Trunks (VT_{SIP}) × CCS per VT_{SIP}	
H.323 Virtual Trunk ratio (v_H)	Of total Virtual Trunk CCS, the portion that are H.323 Virtual Trunks	H.323 Virtual Trunk CCS (HVT_{CCS}) ÷ [H.323 Virtual Trunk CCS (HVT_{CCS}) + SIP Virtual Trunk CCS (SVT_{CCS})]	
SIP Virtual Trunk ratio (v_S)	Of total Virtual Trunk CCS, the portion that are SIP Virtual Trunks	SIP Virtual Trunk CCS (SVT_{CCS}) ÷ [H.323 Virtual Trunk CCS (HVT_{CCS}) + SIP Virtual Trunk CCS (SVT_{CCS})]	
Virtual Trunk CCS (VT_{CCS})	Sum of H.323 Virtual Trunk CCS and SIP Virtual Trunk CCS	H.323 Virtual Trunk CCS (HVT_{CCS}) + SIP Virtual Trunk CCS (SVT_{CCS})	
Total trunk CCS (T_{TCCS})	Sum of all Virtual Trunk CCS and TDM trunk CCS	Virtual Trunk CCS (VT_{CCS}) + TDM trunk CCS (T_{TDM})	

Table 34
Major parameters for VoIP resource calculations (Part 3 of 4)

Parameter	Description	Equation	Default value
Local CallPilot CCS (CP1) (See Note 4 after the table.)	CallPilot calls within the local node, calculated from number of local CallPilot ports	Local CallPilot ports × CCS per port ($CP1_{CCS}$)	
Network CallPilot CCS (CP2) (See Note 4 after the table.)	Network CallPilot calls to the local node, calculated from number of network CallPilot ports	Network CallPilot ports × CCS per port ($CP2_{CCS}$)	
IP ratio (P) (See Note 3 after the table.)	Of total line CCS, the portion that are from IP Phones	IP Phone CCS (L_{IP}) ÷ Total line CCS (L_{CCS})	
Virtual Trunk ratio (V) (See Note 3 after the table.)	Of total trunk CCS, the portion that are from Virtual Trunk access ports	Virtual Trunk CCS (VT_{CCS}) ÷ Total trunk CCS (T_{TCCS})	
Total system CCS (T_{CCS})	Sum of all line and trunk CCS	Total line CCS (L_{CCS}) + Total trunk CCS (T_{TCCS})	
Intraoffice ratio (R_I)	Of the total number of calls, the portion that are telephone-to-telephone calls		0.30
Tandem ratio (R_T) (See Note 5 after the table.)	Of the total number of calls, the portion that are trunk-to-trunk calls		0.05
Incoming ratio (I)	Of the total number of calls, the portion that are trunk-to-telephone calls		0.40

Table 34
Major parameters for VoIP resource calculations (Part 4 of 4)

Parameter	Description	Equation	Default value
Outgoing ratio (O)	Of the total number of calls, the portion that are telephone-to-trunk calls		
Average holding time (AHT_{XX})	Average holding time for different call types: Telephone-to-telephone (AHT_{SS}) Trunk-to-telephone (AHT_{TS}) — also used for ACD agents (AHT_{AGT}) Telephone-to-trunk (AHT_{ST})) Trunk-to-trunk (AHT_{TT})		60 sec 150 sec 150 sec 180 sec
Weighted average holding time (WAHT)		$(R_I \times AHT_{SS}) + (R_T \times AHT_{TT}) + (I \times AHT_{TS}) + (O \times AHT_{ST})$	
Total calls (T_{CALL})	Total system calls per hour	$0.5 \times T_{CCS} \times 100 \div WAHT$	
Intraoffice calls (C_{SS})	Number of telephone-to-telephone calls	$R_I \times T_{CALL}$	
Tandem calls (C_{TT})	Number of trunk-to-trunk calls	$R_T \times T_{CALL}$	
Originating/outgoing calls (C_{ST})	Number of telephone-to-trunk calls	$O \times T_{CALL}$	
Terminating/incoming calls (C_{TS})	Number of trunk-to-telephone calls	$I \times T_{CALL}$	
DSP calls (C_{DSP})	Number of calls involving DSP		
Virtual Trunk calls (C_{VT})	Number of calls involving Virtual Trunks		
Conference loop ratio (r_{Con})	Ratio of conference loops to traffic loops	(Number of conference loops) ÷ (Total number of loops)	0.07

Note 1: In order to use the system traffic equations, all line-side T1/E1 and PRI trunks must be converted to number of ports. To convert T1 to ports: number of cards x 24. To convert E1 to ports: number of cards x 30.

Note 2: Converged Desktop traffic is part of the SIP Virtual Trunk traffic. The parameter value V_{DCCS} must be less than the capacity of the number of SIP ports (VT_{SIP}).

Note 3: A site is considered to be a call center when the proportion of ACD agent telephones exceeds 15% of the total telephones in the system. For call centers, ACD agent calls are included in the calculations for Call Server usage. However, they are initially excluded from the calculations for DSP and Virtual Trunk resources. Once the DSP and Virtual Trunk resources have been calculated for non-ACD (reduced) traffic, the resources required to support the non-blocking ACD application (one DSP port for each ACD agent) are added back in to the results. The result is the total system DSP and Virtual Trunk requirements. The IP ratio (P) is modified for the non-ACD part of the calculation: P' = (L_{IP} without ACD)/(L_{TDM} without ACD + L_{IP} without ACD + L_{DECT}). The Virtual Trunk ratio (V) remains unchanged. The default traffic value for ACD agent telephones (TDM and IP) is 33 CCS per telephone.

Note 4: CallPilot message traffic is embedded in total line traffic. To calculate the real-time impact on the Call Server, CallPilot ports are converted to calls. Only CallPilot ports serving the local node (CP1) and handling network traffic (CP2) have a real-time impact on the Call Server.

Note 5: The tandem ratio should be kept at a relatively small number for a typical enterprise application, except when the switch serves as a tandem node in a network.

System calls

The total number of calls the system must be engineered to handle is given by:

Total calls (T_{CALL}) = $0.5 \times T_{CCS} \times 100 \div \text{WAHT}$

where weighted average holding time (WAHT) is given by:

$$\text{WAHT} = (R_I \times \text{AHT}_{SS}) + (R_T \times \text{AHT}_{TT}) + (I \times \text{AHT}_{TS}) + (O \times \text{AHT}_{ST})$$

and where AHT is the average holding time of a call in seconds.

The subscript indicates where the call initiated from and terminates on, with S = telephone and T = trunk. For example, AHT_{ST} denotes that the call initiated from a telephone and terminated on a trunk.

Traffic equations and penetration factors for CS 1000E

Total system calls comprise four different types of traffic:

1. Intraoffice calls (C_{SS}) = Total calls (T_{CALL}) × Intraoffice ratio (R_I) (telephone-to-telephone) (page 199)
2. Tandem calls (C_{TT}) = Total calls × Tandem ratio = $T_{CALL} \times R_T$ (trunk-to-trunk) (page 200)
3. Originating/outgoing calls (C_{ST}) = Total calls × Outgoing ratio = $T_{CALL} \times O$ (telephone-to-trunk) (page 200)
4. Terminating/incoming calls (C_{TS}) = Total calls × Incoming ratio = $T_{CALL} \times I$ (trunk-to-telephone) (page 201)

Intraoffice calls (telephone-to-telephone)

Intraoffice calls (C_{SS}) = Total calls (T_{CALL}) × Intraoffice ratio (R_I)

This parcel can be further broken down to three types:

1. Intraoffice IP to IP calls (C_{2IP})
   $= C_{SS} \times P^2$ (require no DSP, no VT)

   $pf1 = C_{SS} \times P^2 \div T_{CALL} = R_I \times P^2$
   pf1 is the penetration factor for the intraoffice IP to IP calls
2. Intraoffice IP to TDM telephone calls (C_{1IP})
   $= C_{SS} \times 2 \times P \times (1 - P)$ (require DSP)

   $pf2 = C_{SS} \times 2 \times P \times (1 - P) \div T_{CALL} = 2 \times R_I \times P \times (1 - P)$
   pf2 is the penetration factor for the intraoffice IP to TDM telephone calls

3 Intraoffice TDM telephone to TDM telephone calls (C_{NoIP})
$= C_{SS} \times (1 - P)^2$ (require two DSP, no VT)

$pf3 = C_{SS} \times (1 - P)^2 \div T_{CALL} = R_I \times (1 - P)^2$
pf3 is the penetration factor for the intraoffice TDM to TDM calls

Tandem calls (trunk-to-trunk)

Tandem calls (C_{TT}) = Total calls × Tandem ratio = $T_{CALL} \times R_T$

The tandem calls can be further broken down into:

1 Tandem VT to TDM trunk calls (C_{T1VT})
= 2 × Tandem VT calls × (1 – V)
$= 2 \times C_{TT} \times V \times (1 - V)$ (require DSP and VT)

$pf4 = 2 \times C_{TT} \times V \times (1 - V) \div T_{CALL} = 2 \times R_T \times V \times (1 - V)$

2 Tandem TDM trunk to TDM trunk calls (C_{T2NoVT})
$= C_{TT} \times (1 - V)^2$ (require two DSP, no VT)

$pf5 = C_{TT} \times (1 - V)^2 \div T_{CALL} = R_T \times (1 - V)^2$

3 Tandem VT (H.323) to VT (SIP) calls (C_{T2HS})
$= C_{TT} \times V^2 \times v_H \times v_S \times 2 \times 2$ (require VT)

$pf6 = 4 \times C_{TT} \times V^2 \times v_H \times v_S \div T_{CALL} = 4 \times R_T \times V^2 \times v_H \times v_S$

where v_H is the fraction of H.323 trunks to total VTs, and v_S is the fraction of SIP trunks to total VTs.

Note: If there is only one type of VT (either v_H or $v_S = 0$), the connection is handled at the Network Routing Service and no calls are offered to the Call Server. In this case, pf6 = 0.

Originating/outgoing calls (telephone-to-trunk) (page 200)

Originating/outgoing calls (C_{ST}) = Total calls × Outgoing ratio = $T_{CALL} \times O$

Originating/outgoing calls can be further broken down into:

1 IP to VT calls (C_{STIV})
$= C_{ST} \times$ (fraction of IP calls) $\times V$
$= C_{ST} \times P \times V$ (require VT)

$pf7 = C_{ST} \times P \times V \div T_{CALL} = O \times P \times V$

2 IP to TDM trunk calls (C_{STID})
$= C_{ST} \times$ (IP calls) $\times (1 - V)$
$= C_{ST} \times P \times (1 - V)$ (require DSP)

$pf8 = C_{ST} \times P \times (1 - V) \div T_{CALL} = O \times P \times (1 - V)$

3 TDM telephone to VT calls (C_{STDV})
$= C_{ST} \times$ (1 – fraction of IP calls) $\times V$
$= C_{ST} \times (1 - P) \times V$ (require DSP, VT)

$pf9 = C_{ST} \times (1 - P) \times V \div T_{CALL} = O \times (1 - P) \times V$

4 TDM telephone to TDM trunk calls (C_{STDD})
$= C_{ST} \times$ (1 – fraction of IP calls) $\times (1 - V)$
$= C_{ST} \times (1 - P) \times (1 - V)$ (require two DSP, no VT)

$pf10 = C_{ST} \times (1 - P) \times (1 - V) \div T_{CALL} = O \times (1 - P) \times (1 - V)$

Terminating/incoming calls (trunk-to-telephone)

Terminating/incoming calls (C_{TS}) = Total calls × Incoming ratio = $T_{CALL} \times I$

Terminating/incoming calls can be further broken down into:

1 VT to TDM telephone calls (C_{TSVD})
$= C_{TS} \times V \times$ (1 – fraction of IP calls)
$= C_{TS} \times V \times (1 - P)$ (require DSP, VT)

$pf11 = C_{TS} \times V \times (1 - P) \div T_{CALL} = I \times V \times (1 - P)$

2 VT to IP Phone calls (C_{TSVI})
$= C_{TS} \times V \times$ (fraction of IP calls)
$= C_{TS} \times V \times P$ (require VT)

$pf12 = C_{TS} \times V \times P \div T_{CALL} = I \times V \times P$

3 TDM trunk to IP Phone calls (C_{TSDI})
$= C_{TS} \times (1 - V) \times$ (fraction of IP calls)
$= C_{TS} \times (1 - V) \times P$ (require DSP)

$$pf13 = C_{TS} \times (1 - V) \times P \div T_{CALL} = I \times (1 - V) \times P$$

4 TDM trunk to TDM telephone calls (C_{TSDD})
$= C_{TS} \times (1 - V) \times (1 -$ fraction of IP calls)
$= C_{TS} \times (1 - V) \times (1 - P)$ (require two DSP, no VT)

$$pf14 = C_{TS} \times (1 - V) \times (1 - P) \div T_{CALL} = I \times (1 - V) \times (1 - P)$$

Resource use equations

The following equations, summing different types of traffic, are used to calculate the required TPS, DSP, and Virtual Trunk resources.

- Calls involving at least one IP Phone and therefore using TPS:

  $$C_{IP} = C_{2IP} + C_{1IP} + C_{STIV} + C_{STID} + C_{TSVI} + C_{TSDI}$$

- Calls that require DSP resources:

  (For CS 1000E)
  $$C_{DSP} = C_{1IP} + (2 \times C_{NoIP}) + C_{T1VT} + (2 \times C_{T2NoVT}) + C_{STID} + C_{STDV} + (2 \times C_{STDD}) + C_{TSVD} + C_{TSDI} + (2 \times C_{TSDD})$$

- Calls that require Virtual Trunk resources:

  $$C_{VT} = C_{T1VT} + C_{T2HS} + C_{STIV} + C_{STDV} + C_{TSVD} + C_{TSVI}$$

  — Calls that require H.323 Virtual Trunks:

  $$HC_{VT} = C_{VT} \times v_H$$

  — Calls that require SIP Virtual Trunks

  $$SC_{VT} = C_{VT} \times v_S$$

Real-time calculations

This section describes the following real-time calculations:

- "Call Server utilization" on page 205

- "Application and feature EBCs" on page 205
- "Call Server real time" on page 207
- "CPU real-time conversion for upgrades" on page 207

The real time required to process a basic IP Phone to IP Phone call is an Equivalent Basic Call (EBC), the unit used to measure other, more complicated feature calls. Every feature call can be converted to EBCs by using its real-time factor (RTF).

RTF = (Real time of a feature call in ms ÷ Real time of a basic call) – 1

There are a total of 14 major combinations of telephone and trunk types of calls in the system. The real-time factor of each call type is denoted by f_i (i = 1 to 14). In addition, there are standard real-time factors for applications and features. Table 35 provides the real-time factors.

Table 35
Real-time factors (Part 1 of 3)

Type of call	Real-time factor
Intraoffice calls:	
IP Phone to IP Phone (f_1)	0.00
IP Phone to TDM telephone (f_2)	2.00
TDM telephone to TDM telephone (f_3)	0.45
Tandem calls:	
Virtual Trunk to analog trunk (f_4)	2.09
Analog trunk to analog trunk (f_5)	2.09
H.323 Virtual Trunk to SIP Virtual Trunk (f_6)	1.93
Originating/outgoing calls:	
IP Phone to Virtual Trunk (f_7)	2.27
IP Phone to analog trunk (f_8)	2.42
TDM telephone to Virtual Trunk (f_9)	2.02

Table 35
Real-time factors (Part 2 of 3)

Type of call	Real-time factor
TDM telephone to analog trunk (f_{10})	1.27
Terminating/incoming calls:	
Virtual Trunk to TDM telephone (f_{11})	1.46
Virtual Trunk to IP Phone (f_{12})	1.60
Analog trunk to IP Phone (f_{13})	2.00
Analog trunk to TDM telephone (f_{14})	1.20
Application/feature calls:	
ACD agent without Symposium (f_{ACD})	0.13
Symposium (f_{SYM})	5.70
CallPilot (f_{CP})	1.70
Nortel Integrated Conference Bridge (f_{MICB})	1.59
Nortel Integrated Recorded Announcer (f_{MIRAN})	0.63
Nortel Integrated Call Assistant (f_{MICA})	0.57
Nortel Hospitality Integrated Voice Service (f_{MIVS})	0.57
Nortel Integrated Call Director (f_{MIPCD})	0.63
BRI ports (f_{BRI})	0.12
MDECT telephone (f_{DECT})	4.25
Intraoffice CDR (f_{ICDR})	0.44
Incoming CDR (f_{CCDR})	0.32
Outgoing CDR (f_{OCDR})	0.32
Tandem CDR (f_{TAN})	0.44
CPND factor (f_{CPND})	0.20

Table 35
Real-time factors (Part 3 of 3)

Type of call	Real-time factor
Converged Desktop factor (f_{DTP})	2.33
Microsoft Office factor (fMO)	2.33
Error term – minor feature overhead (f_{OVRH})	0.25

The real-time factor adjusts for the fact that a feature call generally requires more real time to process than a basic call. The impact on the system is a function of the frequency with which the feature call appears during the busy hour. The penetration factor of a feature is the ratio of that type of feature call to the overall system calls. Refer to "Traffic equations and penetration factors for CS 1000E" on page 199 for the equations to calculate penetration factors for the 14 major call types.

The real-time factors and penetration factors are used to generate the real-time multiplier (RTM), which in turn is used to calculate the overall system EBC.

The real-time multiplier is given by:

$$\mathrm{RTM} = 1 + \mathrm{Error\_term} + \sum_{i}(\text{Real-time factor gi} \times \text{Penetration factor pfi})$$

The Error_term accounts for features such as call transfer, three-way conference, call-forward-no-answer, and others that are hard to single out to calculate real-time impact. The Error_term is usually assigned the value 0.25.

Call Server utilization

System real-time EBC = (Total system calls × Real-time multiplier) + Application and feature EBCs
= (T_{CALL} × RTM) + Application and feature EBCs

Application and feature EBCs

Table 36 lists the equations to calculate the EBC impacts of individual applications and features. The total application and feature EBC impact, which is included in the system real-time EBC calculation, is the sum of these application and feature EBCs.

Table 36
Application and feature EBCs (Part 1 of 2)

Type	Calculation
ACD	ACD agents without Symposium + ACD agents with Symposium where ACD agents without Symposium = (1 – % Symposium) × f_{ACD} × (Number of IP ACD agents + number of TDM agents) × CCS per agent × 100 ÷ AHT_{AGT} and ACD agents with Symposium is user input. (If unknown, assume all ACD agent calls are with Symposium.)
Symposium	% Symposium × f_{SYM} × (Number of IP ACD agents + number of TDM agents) × CCS per agent × 100 ÷ AHT_{AGT}
CallPilot	(Number of Local CallPilot ports + number of Network CallPilot ports) × CCS × 100 ÷ AHT_{CP} × f_{CP}
Internal CDR	$C_{SS} \times f_{ICDR}$
Incoming CDR	$C_{TS} \times f_{CCDR}$
Outgoing CDR	$C_{ST} \times f_{OCDR}$
Tandem CDR	$C_{TT} \times f_{TCDR}$
Integrated Conference Bridge	Number of Integrated Conference Bridge ports × CCS × 100 ÷ AHT_{MICB} × f_{MICB}
Integrated Recorded Announcer	Number of Integrated Recorded Announcer ports × CCS × 100 ÷ AHT_{MIRAN} × f_{MIRAN}
Integrated Call Director	Number of Integrated Call Director ports × CCS × 100 ÷ AHT_{MIPCD} × f_{MIPCD}
Integrated Call Announcer	Number of Integrated Call Announcer ports × CCS × 100 ÷ AHT_{MICA} × f_{MICA}

Table 36
Application and feature EBCs (Part 2 of 2)

Type	Calculation
Hospitality Integrated Voice Services	Number of Hospitality Integrated Voice Services ports × CCS × 100 ÷ $AHT_{MIVS} \times f_{MIVS}$
BRI	# BRI ports × CCS × 100 ÷ $AHT_{BRI} \times f_{BRI}$
MDECT	$L_{DECT} \times 100 \div WAHT \times f_{DECT}$
CPND	$(C_{1IP} + C_{NoIP} + C_{TSVD} + C_{TSDD}) \times f_{CPND}$
Converged Desktop (CD)	$(C_{SS} \times 0.1 + C_{TT} + C_{ST} + C_{TS}) \times r_{DTP} \times f_{DTP}$
SIP CTI/TR87 (MO)	$(C_{SS} \times 0.1 + C_{TT} + C_{ST} + C_{TS}) \times r_{MO} \times f_{MO}$

Call Server real time

Compare the system EBC with the system's CPU rated capacity to determine the processor utilization.

CPU utilization = System real-time EBC ÷ Rated capacity of processor (× 100 to get a percentage)

Refer to Table 29 on page 177 for the rated capacities of CS 1000E and MG 1000T processors.

CPU real-time conversion for upgrades

When upgrading an existing switch, CPU engineering must provide a certain level of spare capacity in order to ensure that the upgrade will be able to handle both the existing site and the new additions. Real-time calculations must include the existing load as well as the new load.

The CPU utilization data from a current traffic report TFS004 provides the existing load. The existing load is then converted to the equivalent loading on the new (and presumably faster) CPU. The final loading on the new processor is the sum of the usual real-time calculations for the new load and the converted existing load. It must be less than or equal to 100% of the rated capacity for the new processor.

Use the following formula to convert the existing processor usage to the new processor equivalent:

$$CRTU = (RTU/100) \times [1 + (SWRC \div 100)] \times CPTU$$

where:

CRTU = CPU loading from the existing switch converted to an equivalent load on the new processor, in percent.

RTU = Current CPU usage, in percent (from the TFS004 report of the existing switch).

SWRC = Software release degradation factor, in percent.
Since every new release is enhanced with new features and capabilities, the processing power of the existing CPU is degraded to some extent (typically 10-20%) by the newer release.

CPTU = Capacity ratio of the existing CPU to the new CPU.
The ratio is always less than 1 (unless the same CPU is used, in which case it is equal to 1).

If CRTU > CPTU, telephone CRTU = CPTU.

Since the capacity ratio is the maximum load the old CPU can offer to the new one, the converted CPU load from the existing processor cannot be greater than the capacity ratio.

Table 37 lists the software release degradation factors for supported software upgrades.

Table 37
Software release degradation factors (SWRC) (Part 1 of 2)

From	Degradation factor (%) to CS 1000 Release 4.5
Rls 18	188
Rls 19	174
Rls 20B	125

Table 37
Software release degradation factors (SWRC) (Part 2 of 2)

From	Degradation factor (%) to CS 1000 Release 4.5
Rls 21B	104
Rls 22	75
Rls 23	62
Rls 23C	58
Rls 24B	28
Rls 25B	18
SR2	16
SR3	14
SR4	9

DSP/Media Card calculations

DSP resources are provided by Media Cards. The total DSP/Media Card requirement is the sum of DSP requirements for various functions, which are calculated separately.

- DSP ports for Conference (p. 211)
- DSP ports for general traffic (p. 212)
- DSP ports for major applications (p. 213)
- Special ACD treatment for non-blocking access to DSP ports (p. 213)
- Total DSP requirements (p. 215)
  - — General configuration (ACD agent telephones < 15% of total telephones) (p. 215)
  - — Call center application (ACD agent telephones > 15% of total telephones) (p. 215)

For reasons explained in the “System capacities” chapter (see “Traffic capacity engineering algorithms” on page 174), the Erlang B model is used to calculate DSP port requirements.

For Media Card 32-port cards, the DSP port requirement must be calculated in increments of 32. Table 38 provides Erlang B and Poisson values for P.01 Grade-of-Service (GoS) in 32-port increments. The DSP resource required to handle the offered traffic is the number of ports corresponding to the first Erlang B CCS capacity greater than the calculated traffic value. The Poisson values are used to calculate Virtual Trunk requirements (see “Virtual Trunk calculations” on page 215).

Table 38
Erlang B and Poisson values, in 32-port increments

Erlang B with P.01 GoS		Poisson with P.01 GoS	
Number of DSP ports	CCS	Number of Virtual Trunk access ports	CCS
32	794	32	732
64	1822	64	1687
96	2891	96	2689
128	3982	128	3713
160	5083	160	4754
192	6192	192	5804

Because DSPs cannot be shared between MG 1000Es, the efficiency of the DSP ports on a Media Card is not as high as in a system-wide group. To calculate port and Media Card requirements, use the following (and round up to the next integer if the result is a fraction):

- 794 CCS per Media Card (32 ports)
- 1822 CCS per two Media Cards (64 ports)
- 2891 CCS per three Media Cards (96 ports)

For example, a calculated value of 2000 CCS requires 3 Media Cards to provide a P.01 GoS (2000 ÷ 1822 = 1.1 = 2 Media Cards + 1 Media Card to round up the fraction).

Refer to “Assigning loops and card slots in the CS 1000E” on page 329 for information on allocating Media Cards to MG 1000Es.

DSP ports for Conference

A DSP channel is required for each IP Phone joining a conference call. The more IP Phones in the system, the higher the demand for DSP channels to access the conference feature.

Additional DSP ports are required for TDM telephones in the CS 1000E. When a TDM telephone connects to a conference port on another MG 1000E, it uses one DSP port to reach the other MG 1000E and a second DSP port to connect to the conference port.

Applications are another source of demand for the conference feature. Conference usage for Integrated Conference Bridge is treated separately, as part of the calculations for application ports. For other applications, the default is two conference loops, with a total of 60 channels, per network group. If a particular application requires a different number of conference ports, use the specific number.

The equation to calculate the number of DSP ports the system requires for Conference is:

Equation 1

Number of DSP ports for Conference
$= [(\text{Total number of telephones}) \times r_{Con} \times 0.4]$

where r_{Con} is the ratio of conference loops to traffic loops. The default value of r_{Con} is 0.07 because, for each network group, there are assumed to be 2 conference loops and 28 traffic loops ($r_{Con} = 2 \div 28 = 0.07$). The default value of r_{Con} can be changed if circumstances warrant.

Since ports generally have light traffic while channels have heavy traffic, the factor 0.4 is applied in Equation 1 to take account of the high concentration of telephones to channels and adjust for the ratio of ports to channels.

DSP ports for general traffic

There are three steps to calculate the number of DSP ports required for general traffic:

1 Calculate the number of calls that require DSP resources.

DSP calls (C_{DSP}) = Intraoffice IP-TDM telephone calls (C_{1IP}) + [2 × Intraoffice TDM telephone-TDM telephone calls (C_{NoIP})] + Tandem VT-TDM trunk calls (C_{T1VT}) + [2 × Tandem TDM trunk-TDM trunk calls (C_{T2NoVT})] + IP-TDM trunk calls (C_{STID}) + TDM telephone-VT calls (C_{STDV}) + [2 × TDM telephone-TDM trunk calls (C_{STDD})] VT-TDM telephone calls (C_{TSVD}) + TDM-IP Phone calls (C_{TSDI}) + [2 × TDM trunk-TDM telephone calls (C_{TSDD})]

$= C_{1IP} + (2 \times C_{NoIP}) + C_{T1VT} + (2 \times C_{T2NoVT}) + C_{STID} + C_{STDV} + (2 \times C_{STDD}) + C_{TSVD} + C_{TSDI} + (2 \times C_{TSDD})$

For sites where the proportion of ACD agent telephones is less than 15% of the total telephones in the system, C_{DSP} includes all general traffic seeking DSP service.

Sites where the proportion of ACD agent telephones exceeds 15% of the total telephones in the system are considered to be call centers. For call centers, C_{DSP} is a reduced total that excludes ACD CCS. See “Special ACD treatment for non-blocking access to DSP ports” on page 213 and Note 3 on page 198.

2 Convert DSP calls to CCS.

DSP CCS = $C_{DSP} \times$ WAHT ÷ 100

3 Using the Erlang B table for P.01 GoS (see Table 38 on page 210), find the corresponding number of DSP ports required.

Equation 2

Number of DSP ports for general traffic = Required number of ports for DSP CCS from Erlang B table

DSP ports for major applications

Provide one DSP port for each application port:

- Integrated Recorded Announcer ports
- Integrated Conference Bridge ports
- Integrated Call Director ports
- Integrated Call Assistant ports
- Hospitality Integrated Voice Service ports
- BRI (SILC ports)
- CallPilot ports
- Agent Greeting ports

Equation 3

Number of DSP ports for applications = DSP for Integrated Recorded Announcer + DSP for Integrated Conference Bridge + ... + DSP for Agent Greeting ports

Special ACD treatment for non-blocking access to DSP ports

The following section applies for call centers, which are defined as sites where the number of TDM agent telephones exceeds 15% of the total TDM telephones in the CS 1000E.

Since both Erlang B and Poisson models assume a high ratio of traffic sources to circuits, using the standard estimate of 36 CCS per agent to calculate DSP requirements for a specified GoS tends to result in over-provisioning. For this reason, rather use the fixed rule of one DSP port for each ACD agent telephone requiring a DSP resource, in order to provide non-blocking access between an ACD agent telephone and a DSP. ACD agent telephones require DSP resources only when calls are coming from TDM trunks to IP agent telephones or from Virtual Trunks to TDM agent telephones.

The ACD agent telephones must be located in the same MG 1000E as the Media Cards providing the DSP resources for the telephones.

Assuming that a group of Media Cards can be reserved for the exclusive use of ACD agents, recalculate the number of DSP ports required for general traffic excluding ACD agent CCS, and then add in DSP ports required for the ACD agent telephones. The steps are as follows:

1 Calculate system CCS excluding ACD agents. Since system CCS is two-way traffic, the traffic associated with both incoming and outgoing trunks terminating on ACD agents must be removed:

Reduced system CCS = Total system CCS (T_{CCS}) – [2 × (Number of ACD agent telephones) × CCS/agent]

2 Recalculate the intraoffice ratio (R_I), IP ratio (P), Virtual Trunk ratio (V), and other ratios to reflect the new distribution of call types without ACD traffic. (See Table 34 on page 194 for the equations to calculate the ratios. See also Note 3 on page 198.)

3 Use the reduced system CCS and new ratios to calculate calls requiring DSP and Virtual Trunk resources. (See “Traffic equations and penetration factors for CS 1000E” on page 199 for the detailed calculations for the different call types.)

4 Convert DSP calls to CCS.

DSP CCS = C_{DSP} × WAHT ÷ 100

5 Using the Erlang B table for P.01 GoS (see Table 38 on page 210), find the corresponding number of DSP ports required (for general traffic without ACD agents).

Equation 2a

Number of DSP ports for general traffic = Required number of ports for DSP CCS from Erlang B table

6 Calculate the DSP requirement for ACD agent telephones. A DSP port is needed when calls are coming from TDM trunks (ratio 1 – V) to IP agent telephones or from Virtual Trunks (ratio V) to TDM agent telephones.

Equation 4

Number of DSP ports = (Number of IP ACD agent telephones) × (1 – V) + (Number of TDM ACD agent telephones) × V

7 In the CS 1000E, additional DSP ports are required for calls from analog trunks to TDM ACD agent telephones in another MG 1000E.

Equation 4e

Additional DSP ports = 2 × (Number of TDM ACD agent telephones) × (1 – V)

Total DSP requirements

General configuration (ACD agent telephones < 15% of total telephones)

Total number of DSP ports = Equation 1 (p. 211) + Equation 2 (p. 212) + Equation 3 (p. 213)

Call center application (ACD agent telephones > 15% of total telephones)

Total number of DSP ports = Equation 1 (p. 211) + Equation 2a (p. 214) + Equation 3 (p. 213) + Equation 4 (p. 214) + Equation 4e (p. 215)

Virtual Trunk calculations

For reasons explained in the “System capacities” chapter (see “Traffic capacity engineering algorithms” on page 174), the Poisson model is used to calculate trunk requirements.

Table 38 on page 210 provides Poisson values for P.01 GoS in 32-port increments. The Virtual Trunk resource required to handle the offered traffic is the number of access ports corresponding to the first Poisson CCS capacity greater than the calculated traffic value.

To obtain the exact number of access ports required, use the following formula. Round up to the next integer if the result is a fraction.

Number of access ports = (Calculated CCS) ÷ (CCS from Table 38) × (Number of access ports for table CCS)

Perform the following steps to calculate the number of access ports required:

1 Estimate the Virtual Trunk requirement by adding together all the calls that require the service of access ports.

Virtual Trunk calls (C_{VT}) = Tandem VT-TDM trunk calls (C_{T1VT}) + IP-VT calls (C_{STIV}) + TDM telephone-VT calls (C_{STDV}) + VT-TDM telephone calls (C_{TSVD}) + VT-IP Phone calls (C_{TSVI}) + H.323-SIP VT calls (C_{T2HS})

$= C_{T1VT} + C_{STIV} + C_{STDV} + C_{TSVD} + C_{TSVI} + C_{T2HS}$

For sites where the proportion of ACD agent telephones is less than 15% of the total telephones in the system, C_{VT} includes all general traffic seeking an access port.

Sites where the proportion of ACD agent telephones exceeds 15% of the total telephones in the system are considered to be call centers. For call centers, C_{VT} is a reduced total that excludes ACD CCS. See "Special ACD treatment for non-blocking access to DSP ports" on page 213 and Note 3 on page 198.

2 Convert Virtual Trunk calls to CCS.

Virtual Trunk CCS (VT_{CCS}) = $C_{VT} \times$ WAHT $\div$ 100

3 For call centers, since the calculated Virtual Trunk calls exclude ACD traffic, restore ACD traffic so that the final number of Virtual Trunks will be sufficient to handle both general and ACD traffic.

Final Virtual Trunk CCS = (Calculated VT_{CCS} without ACD) + [(Number of IP ACD agent telephones) + (Number of TDM ACD agent telephones)] $\times$ V $\times$ (CCS per ACD agent) $\div$ (CCS per trunk)
where:
default CCS per ACD agent = 33 CCS
default CCS per trunk = 28 CCS

The expanded Virtual Trunk CCS is inflated by the ratio of 33/28 to reflect the fact that more Virtual Trunks are needed to carry each agent CCS. This is because the traffic levels engineered for ACD agents and Virtual Trunks are different.

4 Use the SIP and H.323 ratios to determine how the Virtual Trunk access ports will be allocated to the two groups.

SIP Virtual Trunk CCS (SVT_{CCS}) = $VT_{CCS} \times v_S$
H.323 Virtual Trunk CCS (HVT_{CCS}) = $VT_{CCS} \times v_H$

5 Using the Poisson table for P.01 GoS (see Table 38 on page 210 or "Trunk traffic – Erlang B with P.01 Grade-of-Service" on page 616), find the corresponding number of SIP and H.323 access ports required.

Note: Although a Virtual Trunk does not need the physical presence of a superloop, it does utilize a logical superloop. A superloop of 128 timeslots can support 1024 Virtual Trunk channels.

Reducing Virtual Trunk imbalances

The final value for calculated Virtual Trunks and its split into SIP and H.323 may be different from initial user input. If the gap between user input and the calculated result is less than 20%, use either number (although the larger number is preferred). If the gap is bigger, the configuration is not balanced. It may be necessary to re-enter input data, including other input parameters, and fine tune the configuration in order to narrow the gap. See "Reducing imbalances (second round of algorithm calculations)" on page 238.

A discrepancy between calculated and input Virtual Trunks is significant because system resources such as DSP ports and Virtual Trunk licenses depend on the accuracy of the traffic split. Imbalanced Virtual Trunk traffic will render the resulting equipment recommendation unreliable.

For example, if the calculated number of Virtual Trunks is 80 but the original input value was 60, and the user decides to use the original input value of 60 to calculate bandwidth and Signaling Server requirements, the resulting system will likely provide service inferior to the normal expected P.01 GoS. On the other hand, if the user input was 80 and the calculated result is 60, it is up to the user to choose which number to use for further calculations for necessary resources, such as the LAN/WAN bandwidth requirement. Unless the configuration is constrained in some way, the larger of the two values (input number or calculated number) is always preferred.

Bandwidth requirement for access ports

The LAN/WAN bandwidth requirement is based directly on traffic. Therefore, it does not depend on the traffic model used nor on the number of Virtual Trunks (either input or calculated) used for other calculations.

Convert Virtual Trunk calls to erlangs:

$$\text{VT erlangs} = \text{VT}_{\text{CCS}} \div 36$$

Look up the VT erlangs number in a bandwidth table to find the corresponding bandwidth required to carry the Virtual Trunk traffic to other H.323 endpoints. Refer to *Converging the Data Network with VoIP* (553-3001-160) for the bandwidth table and for more information about calculating LAN/WAN bandwidth requirements.

Signaling Server algorithm

The Signaling Server algorithm in the NNEC tool determines the number of Signaling Servers required for a given configuration. The algorithm allows a change in constants for Signaling Server platform or Signaling Server application software releases.

The software components that operate on the Signaling Server are the Network Routing Service (NRS), Terminal Proxy Server (TPS), IP Peer Gateways (H.323 and SIP), and Element Manager. Traffic and user requirements determine whether the software components share a Signaling Server or are served by stand-alone Signaling Servers.

For the applications, there are performance factors and software limit factors. The performance factors are determined through capacity analysis. The software limit factors are defined by the application. Element Manager can collocate with any of the other applications with negligible impact.

In order to calculate the number of Signaling Servers required to support a particular configuration, the algorithm first calculates the amount of Signaling Server resources required by each application, taking redundancy requirements into consideration. The calculation for each application is performed separately. Once the individual requirements are determined, the algorithm proceeds to evaluate sharing options. Then the results are summed to determine the total Signaling Server requirement.

In most cases, the individual calculations divide the configuration's requirement for an applicable parameter (endpoint, call, telephone, trunk) into the system limit for that parameter. The particular application's Signaling Server requirement is determined by the parameter with the largest proportional resource requirement, adjusted for redundancy.

Table 39 defines the variables used in the calculations.

Table 39
Signaling Server algorithm constant and variable definitions (Part 1 of 5)

Algorithm term	Description	Value	Notes
NRA	Network Routing Service (NRS) Alternate required	enter (see Note 2)	Yes or No.
NRC	NRS calls per hour	enter (see Note 2)	Two components (one local, one network): $NRC = NRC_0 + NRC_{NET}$
NRC_{HL}	NRS calls per hour	100 000 (see Note 1)	Hardware limit for Signaling Server.
NRD	NRS CDP + UDP entries	enter (see Note 2)	
NRD_1	NRS CDP + UDP entries limit	20 000 (see Note 4)	Software limit.

Note 1: Constant in the formulas.

Note 2: Variable to be entered into the formula.

Note 3: Constant that will update with platform changes.

Note 4: Constant that will update with system software releases.

Note 5: Calculated result.

Table 39
Signaling Server algorithm constant and variable definitions (Part 2 of 5)

Algorithm term	Description	Value	Notes
NRE	NRS endpoints	enter (see Note 2)	(= 0 if NRS, which is a network-wide resource, is not provisioned in this node)
NRE_1	NRS endpoints limit	5000 (see Note 4)	Software limit.
NRP	NRS product of endpoint and CDP/UDP entries	- (see Note 3)	Interim calculation.
NRP_{SL}	NRS product of endpoint and CDP/UDP entries	20 000 (see Note 4)	Software limit.
GSA	SIP Gateway Alternate required	enter (see Note 2)	Yes or No.
GWA	H.323 Gateway Alternate required	enter (see Note 2)	Yes or No.
C_{IP}	IP Phones calls per hour	enter/ derived (see Note 2)	Busy Hour calls from all IP Phones.
IPC_{HL}	IP Phones calls per hour limit	15 000 (see Note 4)	Hardware limit.
IPL	IP Phones	enter (see Note 2)	

Note 1: Constant in the formulas.

Note 2: Variable to be entered into the formula.

Note 3: Constant that will update with platform changes.

Note 4: Constant that will update with system software releases.

Note 5: Calculated result.

Table 39
Signaling Server algorithm constant and variable definitions (Part 3 of 5)

Algorithm term	Description	Value	Notes
IPL_{DB}	IP Phone limit with Personal Directory/ Callers List/Redial List database	1000 (see Note 1)	IP Phone limit per Signaling Server reduced due to Personal Directory/ Callers List/Redial List database.
IPL_{SL}	IP Phones limit	5000 (see Note 4)	Software limit.
NRD_{HL}	NRS product of endpoint and CDP/UDP entries	20 000 (see Note 1)	Hardware limit.
SSNR	NRS Signaling Server calculation	calc (see Note 5)	Real number requirement (e.g., 1.5) (= 0 if NRS is not provisioned in this node)
SSGW	NRS Signaling Server requirements	calc (see Note 5)	Whole number requirement including Alternate.
SSHR	H.323 Gateway Signaling Server calculation	calc (see Note 5)	Real number requirement (e.g.,1.5).
SSHW	H.323 Gateway Signaling Server requirements	calc (see Note 5)	Whole number requirement including Alternate.
SST	Total count of Signaling Servers required	calc (see Note 5)	

Note 1: Constant in the formulas.

Note 2: Variable to be entered into the formula.

Note 3: Constant that will update with platform changes.

Note 4: Constant that will update with system software releases.

Note 5: Calculated result.

Table 39
Signaling Server algorithm constant and variable definitions (Part 4 of 5)

Algorithm term	Description	Value	Notes
SSTR	TPS Signaling Server calculation	calc (see Note 5)	Real number requirement (e.g.,1.5).
SSTW	TPS Signaling Server requirements	calc (see Note 5)	Whole number requirement including Alternate.
TPSA	TPS N+1 redundancy required	enter (see Note 2)	Yes or No.
$HVTC_{HL}$	H.323 Gateway calls per hour limit	18 000 (see Note 4)	Hardware limit. $HVTC_{HL} = v_H \times C_{VT}$
$SVTC_{HL}$	SIP Gateway calls per hour limit	27 000 (see Note 4)	Hardware limit. $SVTC_{HL} = v_S \times C_{VT}$
VT_{SIP}	SIP Gateway access ports per Signaling Server	1800 (see Note 4)	CPU limit.
VT_{323}	H.323 Gateway access ports per Signaling Server	1200 (see Note 4)	CPU limit.
TR87	The aggregate number of SIP CTI TR/87 required based upon the MCS and LCS calculated. Index 28	enter (see Note 2)	

Note 1: Constant in the formulas.

Note 2: Variable to be entered into the formula.

Note 3: Constant that will update with platform changes.

Note 4: Constant that will update with system software releases.

Note 5: Calculated result.

Table 39
Signaling Server algorithm constant and variable definitions (Part 5 of 5)

Algorithm term	Description	Value	Notes
TR87CL	SIP CTI/TR87 clients	5000 (see Note 4)	CPU Limit
TR87A	SIP CTI/TR87 redundancy required	enter (see Note 2)	Yes or No
SSTR87W	SIP CTI/TR87 SS requirements	calc (see Note 5)	Whole number required including Alternate.
SSTR87	SIP CTI/TR87 calculation	calc (see Note 5)	Real number requirement.

Note 1: Constant in the formulas.

Note 2: Variable to be entered into the formula.

Note 3: Constant that will update with platform changes.

Note 4: Constant that will update with system software releases.

Note 5: Calculated result.

Signaling Server calculations

All the Signaling Server software components can function either on shared or on stand-alone Signaling Servers. System traffic and user requirements (for alternate, redundant, or dedicated Signaling Servers) determine how many Signaling Servers will be required. The Signaling Server algorithm takes account of all these requirements by performing the following calculations in sequence:

1 Signaling Server for Personal Directory/Callers List/Redial List database (SSDB) (p. 224)

2 Network Routing Service calculation (SSNR) (p. 224)

3 Terminal Proxy Server calculation (SSTR) (p. 225)

4 H.323 Gateway calculation (SSHR) (p. 226)

5 SIP Gateway calculation (SSSR) (p. 226)

6 Signalling Server Total (SST) requirement summary (p. 227)

1 Signaling Server for Personal Directory/Callers List/Redial List database (SSDB)

Personal Directory/Callers List/Redial List (PD/CL/RL) calculations assume that the database resides either on a stand-alone Signaling Server or on a Signaling Server shared with all the other applications. This assumption simplifies the engineering and provisioning rules.

SSDB = a if no PD/CL/RL feature

= b if yes on feature, and sharing functions on Signaling Server

= c if yes on feature, and a stand-alone database Signaling Server

2 Network Routing Service calculation (SSNR)

SSNR = larger of:

{

a $NRE \div NRE_l$ endpoints (software limit)

b $NRD \div NRD_l$ dial plan entries (software limit)

c $NRC \div NRC_{HL}$ calls per hour (hardware limit)

}

NRC can be a hardware, CPU, or memory limit. It includes local calls (NRC_0) and network Virtual Trunks (VT_{NET}) for this Network Routing Service.
NRC_0 is obtained from the main switch calculation.
$NRC_{NET} = VT_{NET} \times (\text{CCS per VT}) \times 100 \div WAHT \div 2$
$NRC = NRC_0 + NRC_{NET}$

The calculation for NRC_{NET} requires converting both VT_{323} and VT_{SIP} (from user input) to H.323 and SIP calls. The Signaling Server's capacity for handling SIP calls is different from its capacity for H.323 calls.

Therefore, H.323 calls are converted to SIP calls before the load on the Signaling Server is calculated.

Convert H.323 calls to SIP calls by using the ratio of the real-time factors for calls from IP Phones to SIP and H.323 Virtual Trunks:
$f_{H/S}$ = (H.323 call real time) ÷ (SIP call real time)

Equation (c) in the SSNR calculation becomes:

$= [NRC_S + (f_{H/S} \times NRC_H)] \div NRC_{HLS}$
where:
NRC_S = the sum of local and network SIP calls the NRS is handling
NRC_H = the sum of local and network H.323 calls the NRS is handling
NRC_{HLS} = the Signaling Server's capacity for handling SIP calls

Equation (c) represents the loading of the Signaling Server for handling NRS calls. It is compared with equations (a) and (b) in order to determine the highest of all potential usages.

If the user wants the Network Routing Service in a dedicated Signaling Server, round up SSNR before proceeding with further calculations:

SSNW = ROUNDUP(SSNR) × NRA (= 2 if true; else = 1)
where NRA = if Alternate NRS is needed.

3 Terminal Proxy Server calculation (SSTR)

SSTR = larger of:

{

a If SSDB = a or c,no PD/CL/RL or sharing
$IPL \div IPL_{SL}$ IP Phones limit

b If SSDB = b,with PD/CL/RL and sharing

If $IPL <= IPL_{DB}$,
$IPL \div IPL_{DB}$

If $IPL > IPL_{DB}$,database platform limit (1000 for
$1 + [(IPL - IPL_{DB}) \div IPL_{SL}]$the first Signaling Server)

c $IPC \div IPC_{HL}$ calls per hour limit

}

If the user wants Terminal Proxy Server(s) in a dedicated Signaling Server, round up SSTR before proceeding with further calculations:

SSTW = ROUNDUP(SSTR) + TPSA (= 1 if true; else = 0)
where TPSA = if N+1 redundant TPS is needed.

4 H.323 Gateway calculation (SSHR)

SSHR = larger of:

{

a $HVT \div HVT_{SL}$ number of trunks (software limit)

b $C_{VT} \div HVTC_{HL}$ calls per hour (hardware limit)

}

If the user wants H.323 Gateway(s) in a dedicated Signaling Server, round up SSHR before proceeding with further calculations:

SSHW = ROUNDUP(SSHR) × GWA (= 2 if true; else = 1)
where GWA = if Alternate H.323 Gateway is needed.

5 SIP Gateway calculation (SSSR)

SSSR = larger of:

{

a $SVT \div SVT_{SL}$ number of trunks (software limit)

b $C_{VT} \div SVTC_{HL}$ calls per hour (hardware limit)

}

If the user wants SIP Gateway(s) in a dedicated Signaling Server, round up SSSR before proceeding with further calculations:

SSSW = ROUNDUP(SSSR) × GSA (= 2 if true; else = 1)
where GSA = if Alternate SIP Gateway is needed.

6 SIP CTI/TR87 Calculation

If SIP CTI TR87 feature is present:

SSTR87 = TR87 / TR87CL sw limit - number of clients

If the user wants SIP CTI/TR87 in a dedicated signalling server, then round up SSTR87 before proceeding with further calculations.

SSTR87W = ROUNDUP(SSTR87) × TR87A (=2, if true; else =1)
TR87A = If Alternate SIP CTI/TR87 needed.

7 Signalling Server Total (SST) requirement summary

The final calculation of SST will require picking the formula that suits the configuration and input by the user:

SST = evaluate in order,

a If (SSNR + SSTR + SSHR + SSSR87) < 1

SST = ROUNDUP(SSNR + SSTR + SSHR + SSSR87) + (1 if NRA, GWA, GSA, or TPSA true; else 0) + (1 if SSDB = c; else 0)

If SSTR87 > 0 AND (SSNR > 0 OR SSDB = b) then add a dedicated Signaling Server for SIP CT/TR87, for example:

SST = SST + SSTR87W

Note: A dedicated Signaling Server is required for SIP CTI/TR87 if NRS and PD/RL/CL are present.

OR

b If (SSTR + SSHR + SSSR + SSTR87) < 1 and (SSNR + SSTR + SSHR + SSSR) > 1

SST = SSNW + [ROUNDUP (SSTR + SSHR + SSSR + SSTR87) × (2, if GWA, GSA, TPSA, or TR87A true; else 1)] + (1, if SSDB = c OR SSDB = b and SSTR87 > 0; else 0)

Note: A dedicated Signaling Server is required for SIP CTI/TR87 in the event that SSDB=b. A dedicated Signaling Server is required for PD/RL/CL in the event that SSDB=c.

OR

c If (SSNR + SSHR + SSSR) < 1 and (SSNR + SSTR + SSHR + SSSR) > 1

SST = SSTW + [ROUNDUP(SSNR + SSHR + SSSR) × (2, if NRA, GWA, or GSA true; else 1)] + (1, if SSDB = c; else 0)

If (IPL > 1000) OR (SSTR + SSTR87) > 1 then

SST = SST + SSTR87W

If (IPL < = 1000) AND (SSTR + SSTR87) < 1 AND (TPSA is No) AND (TR87A is Yes) then add an Alternate Signaling Server for SIP CTI TR87, for example:

SST = SST +1

Note: A dedicated Signaling Server is required for SIP CTI/TR87 in the event that the number of IP users is greater than 1000, or TPS and SIP CTI/TR87 cannot co-reside.

OR

d If (SSTR + SSNR + SSSR) < 1 and (SSNR + SSTR + SSHR + SSSR) > 1

SST = SSHW + [ROUNDUP(SSTR + SSNR + SSSR) × (2, if NRA, GSA, or TPSA true; else 1)] + (1 if SSDB = c; else 0)

If (SSHR + SSTR87) > 1 then

SST = SST + SSTR87W

Note: A dedicated Signaling Server is required for SIP CTI/TR87 in the event that H.323 GW and SIP CTI/TR87 cannot co-reside.

If (SSHR + SSTR87) < 1 AND GWA = No AND TR87A = Yes then add an Alternate Signaling Server for SIP CTI TR87, for example:

SST = SST +1

Note: H.323 GW and SIP CTI/TR87 can co-reside, but in the event that H.323 GW does not require an alternate Signaling Server, and SIP CTI/TR87 does, then an additional Signaling Server for SIP CTI/TR87 alternate is required.

OR

e If (SSTR + SSNR + SSHR) < 1 and (SSNR + SSTR + SSHR + SSSR) > 1

SST = SSSW + [ROUNDUP(SSTR + SSNR + SSHR) × (2 if NRA, GWA, or TPSA true; else 1)] + (1 if SSDB = c; else 0)

If (SSSR + SSTR87) > 1 then

SST = SST + SSTR87W

Note: A dedicated Signaling Server is required for SIP CTI/TR87 in the event that the SIP Gateway requires a separate Signaling Server for virtual trunks.

If (SSSR + SSTR87) < 1 AND GSA = No AND TR87A = Yes, then add an Alternate Signaling Server for SIP CTI TR87, for example:

SST = SST +1

Note: SIP Gateway and SIP CTI/TR87 can co-reside, but in the event that the SIP Gateway does not require an alternate, and SIP CTI/TR87 does, then an additional Signaling Server for SIP CTI/TR87 alternate is needed.

Note: When the process reaches this step, it means that (SSGR+SSTR+SSHR+ SSSR)>1, and there is no sharing of the three functions on one Signalling Server. The following procedure is designed to round up the two functions on one Signalling Server:

OR

f If (SSNR + SSTR) < 1 and (SSHR + SSSR) < 1 and (SSGR + SSTR + SSHR + SSSR) > 1

SST = [ROUNDUP(SSNR + SSTR) × (2 if NRA or TPSA true; else 1)] + [ROUNDUP(SSHR + SSSR) × (2 if GWA or GSA true; else 1)] + (1 if SSDB = c; else 0)

If (SSHR + SSSR + SSTR87) > 1 then

SST = SST + SSTR87W

Note: A dedicated Signaling Server is required for SIP CTI/TR87 in the event that SIP CTI/TR87 cannot co-reside with the SIP and H.323 Gateways.

If (SSHR + SSSR + SSTR87) < 1 AND GSA = No AND GWA = No AND TR87A = Yes then add an Alternate Signaling Server for SIP CTI TR87, for example:

SST = SST +1

Note: H.323 GW, SIP GW and SIP CTI/TR87 can co-reside, but in the event that the SIP and H.323 Gateways do not require an alternate Signaling Server, and SIP CTI/TR87 does, an additional Signaling Server for SIP CTI/TR87 alternate is required.

OR

g If (SSNR + SSHR) < 1 and (SSTR + SSSR) < 1 and (SSGR + SSTR + SSHR + SSSR) > 1

SST = [ROUNDUP(SSNR + SSHR) × (2 if NRA or GWA true; else 1)] + [ROUNDUP(SSTR + SSSR) × (2 if TPSA or GSA true; else 1)] + (1 if SSDB = c; else 0)

If (SSTR + SSSR + SSTR87) > 1 then

SST = SST + SSTR87W

Note: A dedicated Signaling Server is required for SIP CTI/TR87 in the event that SIP CTI/TR87 cannot co-reside with TPS and SIP Gateways.

If (IPL > 1000) AND If (SSTR + SSSR + SSTR87) < 1

SST = SST +1

If (SSTR + SSSR + SSTR87) < 1 AND GSA = No AND TPSA = No AND TR87A = Yes then add an Alternate Signaling Server for SIP CTI TR87, for example:

SST = SST +1

Note: SIP Gateway, TPS and SIP CTI/TR87 can co-reside, but in the event that SIP Gateway and TPS do not require an alternate Signaling Server, and SIP CTI/TR87 does, then an additional Signaling Server for SIP CTI/TR87 alternate is necessary.

OR

h If (SSNR + SSSR) < 1 and (SSTR + SSHR) < 1 and (SSGR + SSTR + SSHR + SSSR) > 1

SST = [ROUNDUP(SSNR + SSSR) × (2 if NRA or GSA true; else 1)] + [ROUNDUP(SSTR + SSHR) × (2 if TPSA or GWA true; else 1)] + (1 if SSDB = c; else 0)

Note: Another potential combination of loads on the Signaling Server is that only one pair of functions can share a Server, but the remaining functions are too close to full load on a Signaling Server to share.

If (SSTR + SSHR + SSTR87) > 1 then

SST = SST + SSTR87W

Note: A dedicated Signaling Server is required for SIP CTI/TR87 in the event that SIP CTI/TR87 cannot co-reside with TPS and H.323 Gateway.

If (IPL > 1000) AND If (SSTR + SSHR + SSTR87) < 1

SST = SST + 1

If (SSTR + SSHR + SSTR87) < 1 AND GWA = No AND TPSA = No AND TR87A = Yes then add an Alternate Signaling Server for SIP CTI TR87, for example:

SST = SST +1

Note: H.323 Gateway, TPS, and SIP CTI/TR87 can co-reside, but in the event that H.323 Gateway and TPS do not require an alternate Signaling Server, and SIP CTI/TR87 does, then an additional Signaling Server for SIP CTI/TR87 alternate is needed

OR

i If (SSTR + SSHR) < 1 and (SSGR + SSTR + SSHR + SSSR) > 1

SST = [ROUNDUP(SSNR) × (2 if NRA true; else 1)] + [ROUNDUP(SSSR) × (2 if GSA true; else 1)] + [ROUNDUP(SSTR + SSHR) × (2 if TPSA or GWA true; else 1)] + (1 if SSDB = c; else 0)

If (SSTR + SSHR + SSTR87) > 1 then

SST = SST + SSTR87W

Note: A dedicated Signaling Server is required for SIP CTI/TR87 in the event that SIP CTI/TR87 cannot co-reside with TPS and H.323 Gateways.

If (IPL > 1000) AND If (SSTR + SSHR + SSTR87) < 1

SST = SST +1

If (SSTR + SSHR + SSTR87) < 1 AND GWA = No AND TPSA = No AND TR87A = Yes then add an Alternate Signaling Server for SIP CTI TR87, for example:

SST = SST +1

OR

j If (SSNR + SSTR) < 1 and (SSGR + SSTR + SSHR + SSSR) > 1

SST = [ROUNDUP(SSHR) × (2 if GWA true; else 1)] + [ROUNDUP(SSSR) × (2 if GSA true; else 1)] + [ROUNDUP(SSNR + SSTR) × (2 if NRA or TPSA true; else 1)] + (1 if SSDB = c; else 0)

SST = SST + SSTR87W

Note: A dedicated Signaling Server is required for SIP CTI/TR87. SIP CTI/TR87 cannot co-reside with the NRS.

OR

k If (SSNR + SSHR) < 1 and (SSGR + SSTR + SSHR + SSSR) > 1

SST = [ROUNDUP(SSTR) + (1 if TPSA true; else 0)] + [ROUNDUP(SSSR) × (2 if GSA true; else 1)] + [ROUNDUP(SSNR + SSHR) × (2 if NRA or GWA true; else 1)] + (1 if SSDB = c; else 0)

SST = SST + SSTR87W

Note: A dedicated Signaling Server is required for SIP CTI/TR87. SIP CTI/TR87 cannot co-reside with the NRS.

OR

l If (SSNR + SSSR) < 1 and (SSGR + SSTR + SSHR + SSSR) > 1

SST = [ROUNDUP(SSTR) + (1 if TPSA true; else 0)] + [ROUNDUP(SSHR) × (2 if GWA true; else 1)] + [ROUNDUP(SSNR + SSSR) × (2 if NRA or GSA true; else 1)] + (1 if SSDB = c; else 0)

SST = SST + SSTR87W

Note: A dedicated Signaling Server is required for SIP CTI/TR87. SIP CTI/TR87 cannot co-reside with the NRS.

OR

m If (SSTR + SSSR) < 1 and (SSGR + SSTR + SSHR + SSSR) > 1

SST = [ROUNDUP(SSNR) × (2 if NRA true; else 1)] + [ROUNDUP(SSHR) × (2 if GWA true; else 1)] +

[ROUNDUP(SSTR + SSSR) × (2 if TPSA or GSA true; else 1)] + (1 if SSDB = c; else 0)

If (SSTR + SSSR + SSTR87) > 1 then

SST = SST + SSTR87W

Note: A dedicated Signaling Server is required for SIP CTI/TR87 in the event that SIP CTI/TR87 cannot co-reside with TPS and SIP Gateways.

If (IPL > 1000) AND If (SSTR + SSSR + SSTR87) < 1

SST = SST + 1

If (SSTR + SSSR + SSTR87) < 1 AND GSA = No AND TPSA = No AND TR87A = Yes, then add an Alternate Signaling Server for SIP CTI TR87, for example:

SST = SST +1

OR

n If (SSHR + SSSR) < 1 and (SSGR + SSTR + SSHR + SSSR) > 1

SST = [ROUNDUP(SSNR) × (2 if NRA true; else 1] + ROUNDUP(SSTR) + (1 if TPSA true; else 0) + [ROUNDUP(SSHR + SSSR) × (2 if GWA or GSA true; else 1)] + (1 if SSDB = c; else 0)

If (SSHR + SSSR + SSTR87) > 1 then

SST = SST + SSTR87W

Note: A dedicated Signaling Server is required for SIP CTI/TR87 in the event that SIP CTI/TR87 cannot co-reside with H.323 and SIP Gateways.

If (SSHR + SSSR + SSTR87) < 1 AND GSA = No AND GWA = No AND TR87A = Yes then add an Alternate Signaling Server for SIP CTI TR87, i.e.

SST = SST +1

If the scenario has not fallen into any of the above 14 cases, it is not possible to share Signaling Server functions. Use the following equation to calculate the total Signaling Server requirement:

SST = ROUNDUP(SSNW + SSTW + SSHW + SSSW + SSTR87W) + (1 if SSDB = c; else 0)

Note: Add an additional Signaling Server to the result from the above calculations if the PD/CL/RL database is on a stand alone Signaling Server.

where:

SSNW = SSNR(ROUNDUP if dedicated) + [ROUNDUP(SSNR) × (1 if NRA true; else 0)]

SSTW = SSTR(ROUNDUP if dedicated) + (1 if TPSA true; else 0)

SSHW = SSHR(ROUNDUP if dedicated) + [ROUNDUP(SSHR) × (1 if GWA true; else 0)]

SSSW = SSSR(ROUNDUP if dedicated) + [ROUNDUP(SSSR) × (1 if GSA true; else 0)]

Note: SSXR in the above equations is rounded up before SSXW is calculated. Note that the total SST is the sum of SSXW defined above—not those defined under each individual function.

Note: It is possible that the sum of two or three functions will be greater than 1, but their fractional parts may still be able to share a Signaling Server with the last function's fraction. In order to avoid overstating an individual function's needs and over-provisioning the total requirement, round off the Signaling Server requirement to a higher integer only after the fraction portion of all functions has been summed.

Refer to “Signaling Server calculation” on page 250 for a numerical example illustrating the algorithm.

Maximum number of Failsafe Network Routing Services

This algorithm defines the maximum number of Failsafe Network Routing Services (RSF) that can be configured. The maximum RSF is limited by the Primary Network Routing Service (RSP) configuration.

RSF is less than or equal to RSPE
$RSF = (RDE_L \div RSPE) \times [FR - (RFR_S \text{ or } RFR_C)] \times (DDR \div 24) \times (RSP_C)$

Simplified formulas:

RSF = (16 000 ÷ RSPE) for stand-alone Network Routing Service
RSF = (10 000 ÷ RSPE) for collocated Network Routing Service

Table 40 defines the terms used in the calculations.

Table 40
RSF algorithm constant and variable definitions (Part 1 of 2)

Algorithm term	Description	Value	Notes
DDR	Dynamic Data Resynch	24 (see Note 3)	In one day, the minimum number of synchronizations of dynamic data from Active RD to a RSF.
FR	FTP Resource	10 (see Note 4)	Software limit.

Note 1: Constant in the formulas.

Note 2: Variable to be entered into the formula.

Note 3: Constant that will update with platform changes.

Note 4: Constant that will update with system software releases.

Note 5: Calculated result.

Table 40
RSF algorithm constant and variable definitions (Part 2 of 2)

Algorithm term	Description	Value	Notes
RDE_L	NRS endpoints limit	5000 (see Note 4)	Software limit.
RSF	Maximum Failsafe NRS allowed	calc (see Note 5)	
RSP_C	RSP CPU performance	1.0 (see Note 3)	PIII 700 MHz; 512 MByte; 20 GByte
RSPE	RSP endpoints	enter (see Note 2)	
RFR_C	Reserved FTP Resource Collocated	5 (see Note 4)	Software limit. RSP shares Signaling Server with other applications, such as TPS. Reserve 3 for other applications.
RFR_S	Reserved FTP Resource Standalone	2 (see Note 4)	Software limit. RSP is only application on Signaling Server. Reserve 1 for Static updates and 1 spare.

Note 1: Constant in the formulas.

Note 2: Variable to be entered into the formula.

Note 3: Constant that will update with platform changes.

Note 4: Constant that will update with system software releases.

Note 5: Calculated result.

Reducing imbalances (second round of algorithm calculations)

Input data may not be consistent. For example, there may be a high intraoffice ratio in a call center, or few trunks but a high interoffice ratio. In these cases, the resulting calculations in the NNEC tool will generate a warning message indicating traffic imbalance. The user may want to change the input data and rerun the calculation.

There are two types of imbalances that may occur

- Virtual Trunks (p. 238)
- Line and trunk traffic (p. 239)

Virtual Trunks

When the VT number input by the user differs significantly from the calculated VT number (more than 20% difference), the NNEC tool will use the calculated number and rerun the algorithm to obtain a newer VT number. If the resulting VT number is not stable (in other words, after each rerun, a new calculated VT number is obtained), the program will repeat the calculation cycle up to six times. This recalculation looping is built into the NNEC and occurs automatically, with no user action required. At the end of the recalculation cycle, the user has the choice of using the original input VT number or the final calculated VT number in the configuration.

The user inputs about the number of H.323 Virtual Trunks and SIP Virtual Trunks are a function of other parameters in the system. For example, the number of Virtual Trunks required will be affected by the total number of trunks in the system and by intraoffice/incoming ratios: Virtual Trunks and TDM trunks cannot carry a high volume of trunk traffic if the system is characterized as carrying mostly intraoffice calls. If pre-engineering has not provided consistent ratios and CCS, the VT input numbers tend to diverge from the calculated results based on input trunking ratios.

Use the following formula to calculate the VT CCS to compare against user input, in order to determine the size of the deviation. Note that for this consistency check, H.323 VT CCS and SIP VT CCS are separated out from the VT total by using the user input ratio of H.323 to SIP.

$$HVT = C_{VT} \times v_H \times WAHT \div 100$$

$$SVT = C_{VT} \times v_S \times WAHT \div 100$$

The respective difference between HVT and HVT_{CCS}, and between SVT and SVT_{CCS}, is the deviation between input data and calculated value.

After the automatic NNEC recalculations, if the discrepancy between the input VT number and the final calculated number is still significant (more than 20%), follow the recommendations for reducing line and trunk traffic imbalance (see "Line and trunk traffic" on page 239). Adjusting the number of Virtual Trunks and trunk CCS alone, without changing the intraoffice ratio or its derivatives, may never get to a balanced configuration.

Line and trunk traffic

At the end of the algorithm calculation, if the line and trunk CCS are significantly imbalanced (more than 20% difference), the NNEC tool will generate a warning message. The user can choose whether to change input data and rerun the calculation to have a better balanced system. The recalculation loop starts from the point of entering configuration inputs at the GUI.

Use the following formula to obtain the calculated line CCS to compare against user input, in order to determine the size of the deviation.

$$\text{Calculated line CCS } (LC_{CCS}) = (C_{SS} + C_{ST} + C_{TS}) \times WAHT \div 100$$

The difference between L_{CCS} and LC_{CCS} is the imbalanced line CCS.

Similarly, use the following formula to obtain the calculated trunk CCS to compare against user input, in order to determine the size of the deviation.

$$\text{Calculated total trunk CCS } (TC_{CCS}) = (C_{TT} + C_{ST} + C_{TS}) \times WAHT \div 100$$

The difference between T_{TCCS} and TC_{CCS} is the imbalanced trunk CCS.

Because the calculated CCS factor in traffic ratios, line and trunk CCS can be significantly imbalanced if these ratios are inconsistent. For example, if the intraoffice, incoming, and outgoing ratios are based on contradictory assumptions, the calculated line CCS may be much higher than the number of trunks can absorb.

Table 41 provides tips for users to modify input data so as to steer the algorithm in the right direction. The desired configuration for the input data is when the input numbers for Virtual Trunks, line CCS, and trunk CCS are close to their calculated values (less than 20% difference).

Table 41
Tips to reduce traffic imbalances

When this happens...	Try this...
Line traffic too high	• Reduce CCS per telephone or number of telephones. • Increase the intraoffice ratio.
Trunk traffic too high	• Reduce CCS per trunk or number of trunks. • Reduce the intraoffice ratio. • Increase the tandem ratio (if justified; changing the incoming/outgoing ratio will have no impact on line/trunk traffic imbalance).
Need to change input VT number because other input data has changed	• If changing the input VT number is not an option, keep it and change only the number of TDM trunks. • If the input VT number is not a committed value, use the VT number from the previous run. • When input traffic data is changed, expect the resulting VT number to change accordingly. Modify line data or trunk data one at a time to see the trend of convergence. Otherwise, it is hard to know which variable is most responsible for converging to the desired result.

Illustrative engineering example

The following numerical example is for a general business/office model.

Assumptions

The example uses the following values for key parameters.

> ***Note:*** These parameter values are typical for systems in operation, but the values for the ratios are not the defaults.

- Intraoffice ratio (R_I): 0.35

- Tandem ratio (R_T): 0.03
- Incoming ratio (I): 0.40
- Outgoing ratio (O): 0.22

  In fraction of calls, the above ratios add up to 1.
- AHT_{SS} = 60 [average hold time (AHT) for telephone to telephone ($_{SS}$)]
- AHT_{TS} = 150 [AHT for trunk to telephone ($_{TS}$)]
- AHT_{ST} = 150 [AHT for telephone to trunk ($_{ST}$)]
- AHT_{TT} = 180 [AHT for trunk to trunk ($_{TT}$)]

Given configuration

A CS 1000E system with the following configuration data:

- 1200 digital and analog telephones at 5 CCS/telephone
  - including 30 TDM ACD agents at 33 CCS/agent
- 1600 IP Phones at 5 CCS/IP Phone
  - including 60 IP ACD agent telephones at 33 CCS/IP agent telephone
- 410 trunks
  - including 360 Virtual Trunks (240 H.323 and 120 SIP) at 28 CCS/trunk
    (The numbers for H.323 and SIP Virtual Trunks are input from user response to a GUI request in the NNEC.)
- Network Virtual Trunks served by this Gatekeeper: 800
  (This is another input from the user interface.)
- CallPilot ports at 26 CCS/CP port
  - 36 local CallPilot ports
  - 24 network CallPilot ports (input from user interface)
- Other traffic-insensitive, pre-engineered application ports that require DSP channels and generate real-time feature overhead. For non-blocking configuration, each application port requires one DSP port.
  - Agent greeting ports: 4

- Integrated Conference Bridge ports: 16 (HT = 1800)
- Integrated Recorded Announcer ports: 12 (HT = 90)
- Integrated Call Assistant ports: 8 (HT = 180)
- Hospitality Integrated Voice Service ports: 8 (HT = 90)
- Integrated Call Director ports: 12 (HT = 60)

- Features with processing overhead but no hardware ports:
  - CPND percentage: 20% of TDM telephone calls
  - Converged Desktop percentage: 5% of the following calls: (intraoffice calls × 0.1) + incoming calls + outgoing calls + tandem calls
  - Intraoffice CDR: No (could be yes, but not typical)
  - Incoming CDR: Yes
  - Outgoing CDR: Yes
  - Tandem CDR: Yes
  - Symposium-processed ACD calls: 90%
  - ACD calls without Symposium: 10%

Real-time factors are based on Table 35 on page 203.

Calculations

Note: The calculations in this example were performed by spreadsheet. Some rounding off may have occurred.

- The ACD agent to total telephone ratio = (60 + 30) ÷ (1200 + 1600) = 0.032
  This ratio is less than the 15% threshold, so the site is not considered a call center. All ACD traffic will be included in call distribution calculations. Refer to "DSP ports for general traffic" on page 212 for more information.
- TDM telephones CCS = [(1200 – 30) × 5] + (30 × 33) = 6840 CCS
- IP Phones CCS = [(1600 – 60) × 5] + (60 × 33) = 9680 CCS

- Fraction of IP calls (P) = 9680 ÷ (6840 + 9680) = 0.586
- Weighted average holding time (WAHT) = (60 × 0.35) + (150 × 0.40) + (150 × 0.22) + (180 × 0.03) = 119 seconds
- Total line CCS (L_{CCS}) = 6840 + 9680 = 16 520
- 410 trunks at 28 CCS per trunk:

  Fraction of Virtual Trunks (V) = 360 ÷ 410 = 0.878
  Virtual Trunk traffic (VT_{CCS}) = 360 × 28 = 10 080
  TDM trunk CCS (T_{TDM}) = (410 – 360) × 28 = 1400
  v_H = 240 ÷ (120 + 240) = 0.67
  v_S = 120 ÷ (120 + 240) = 0.33

  Total trunk CCS (T_{TCCS}) = 10 080 + 1400 = 11 480

- Total CCS (T_{CCS}) = 11 480 + 16 520 = 28 000
- Total calls (T_{CALL}) = 0.5 × T_{CCS} × 100 ÷ WAHT
  = 0.5 × 28 000 × 100 ÷ 119 = 11 765
- The system calls are comprised of four different types of traffic: Intraoffice calls (telephone-to-telephone) (C_{SS}); Tandem calls (trunk-to-trunk) (C_{TT}); Originating/Outgoing calls (telephone-to-trunk) (C_{ST}); Terminating/Incoming calls (trunk-to-telephone) (C_{TS}).

1 Intraoffice calls (C_{SS}) = T_{CALL} × R_I
= 11 765 × 0.35 = 4118

a Intraoffice IP to IP calls (C_{2IP}) = C_{SS} × P^2
= 4118 × 0.586 × 0.586 = 1414
(require no DSP, no VT)
pf1 = 1414 ÷ 11 765 = 0.12

b Intraoffice IP to TDM calls (C_{1IP}) = C_{SS} × 2 × P × (1 – P)
= 4118 × 2 × 0.586 × (1 – 0.586) = 1998
(require DSP)
pf2 = 1998 ÷ 11 765 = 0.17

c Intraoffice TDM to TDM (C_{NoIP}) = C_{SS} × $(1 – P)^2$
= 4118 × (1 – 0.586) × (1 – 0.586) = 706
(require 2 DSP, no VT)
pf3 = 706 ÷ 11 765 = 0.06

2 Tandem calls (C_{TT}) = $T_{CALL} \times R_T$
= 11 765 × 0.03 = 353 calls

d Tandem VT to TDM calls (C_{T1VT}) = 2 × C_{TT} × V × (1 – V)
= 2 × 353 × 0.878 × (1 – 0.878) = 76
(require DSP and VT)
pf4 = 76 ÷ 11 765 = 0.01

e Tandem TDM to TDM calls (C_{T2NoVT}) = C_{TT} × (1 – V) × (1 – V)
= 353 × (1 – 0.878) × (1 – 0.878) = 5
(require 2 DSP, no VT)
pf5 = 5 ÷ 11 765 = 0

f Tandem VT (H.323) to VT (SIP) calls (C_{T2HS})
= $C_{TT} \times V^2 \times v_H \times v_S \times 2 \times 2$
= 353 × 0.878 × 0.878 × 0.67 × 0.33 × 4 = 242
(require no DSP, VT)
pf6 = 242 ÷ 11 765 = 0.02

3 Originating/outgoing calls (C_{ST}) = T_{CALL} × O
= 11 765 × 0.22 = 2588 calls

a IP to VT calls (C_{STDI}) = C_{ST} × P × V
= 235 × 0.586 × 0.878 = 1332
(require VT)
pf7 = 1332 ÷ 11 765 = 0.11

b IP to TDM calls (C_{STID}) = C_{ST} × P × (1 – V)
= 2588 × 0.586 × (1 – 0.878) = 185
(require DSP)
pf8 = 185 ÷ 11 765 = 0.02

c TDM to VT calls (C_{STDV}) = C_{ST} × (1 – P) × (V)
= 2588 × (1 – 0.586) × 0.878 = 941
(require DSP, VT)
pf9 = 941 ÷ 11 765 = 0.08

d TDM to TDM calls (C_{STDD}) = C_{ST} × (1 – P) × (1 – V)
= 2588 × (1 – 0.586) × (1 – 0.878) = 131
(require 2 DSP, no VT)
pf10 = 131 ÷ 11 765 = 0.01

4 Terminating/incoming calls (C_{TS}) = $T_{CALL} \times I$
= 11 765 × 0.40 = 4706 calls

a VT to TDM calls (C_{TSVD}) = $C_{TS} \times V \times (1 - P)$
= 4706 × 0.878 × (1 – 0.586) = 1711
(require DSP, VT)
pf11 = 1711 ÷ 11 765 = 0.15

b VT to IP calls (C_{TSVI}) = $C_{TS} \times V \times P$
= 4706 × 0.878 × 0.586 = 2421
(require VT)
pf12 = 2421 ÷ 11 765 = 0.21

c TDM to IP calls (C_{TSDI}) = $C_{TS} \times (1 - V) \times P$
= 4706 × (1 – 0.878) × 0.586 = 336
(require DSP)
pf13 = 336 ÷ 11 765 = 0.03

d TDM to TDM calls (C_{TSDD}) = $C_{TS} \times (1 - V) \times (1 - P)$
= 4706 × (1 – 0.878) × (1 – 0.586) = 238
(require 2 DSP, no VT)
pf14 = 238 ÷ 11 765 = 0.02

- From the above data, the real-time multiplier can be obtained:

  Real-time multiplier per call
  = 1 + (f_1 × pf1) + (f_2 × pf2) + (f_3 × pf3) + ... + (f_{14} × pf14) + Error_term
  = 1 + (0 × 0.12) + (2.0 × 0.17) + (0.45 × 0.06) + (2.09 × 0.01) + (2.09 × 0) + (1.93 × 0.02) +(2.27 × 0.11) + (2.42 × 0.02) + (1.93 × 0.08) + (2.27 × 0.01) + (1.46 × 0.15) + (1.6 × 0.21) + (2.00 × 0.03) + (1.2 × 0.02) + 0.25
  = 2.79

- Calls involving at least one IP Phone (will be needed for Gateway calculation):

  $C_{IP} = C_{2IP} + C_{1IP} + C_{STIV} + C_{STID} + C_{TSVI} + C_{TSDI} = 7686$

- Calls that require DSP resources:

  $C_{DSP} = C_{1IP} + C_{T1VT} + C_{STID} + C_{STDV} + C_{TSVD} + C_{TSDI} = 7405$

- Calls that require Virtual Trunk resources:

  $C_{VT} = C_{T1VT} + C_{T2HS} + C_{STIV} + C_{STDV} + C_{TSVD} + C_{TSVI} = 6722$

  H.323 calls = $C_{VT} \times V_H = 6722 \times 0.67 = 4504$

  SIP calls = $C_{VT} \times V_S = 6722 \times 0.33 = 2218$

Real-time calculation with major applications

- ACD agent calls without Symposium = [(Number of ACD agents) × CCS/agent × 100 ÷ AHT_{TS}] × 0.1 × f_{ACD} = 200 × 0.13 = 26
- Symposium calls EBC = [(Number of agents) × CCS/agent × 100 ÷ AHT_{TS}] × 0.9 × fsym = 1994 × 0.9 × 5.7 = 10 229
- Calculate the impact of other major features and applications.

  Application EBC = [(Number of application ports) × CCS per port × 100 ÷ HT] × real-time factor

Table 42 summarizes the EBC calculations. For those applications requiring DSP resources, it also provides the required DSP ports for applications and features, for later use.

Since DSPs are not a system resource in the CS 1000E, each MG 1000E must provide sufficient DSP resources for non-blocking access to the applications. The rule is to provide one DSP port for each application port in the MG 1000E.

Table 42
Application and feature EBCs and DSP requirements

Application/ Feature	Number of ports	EBC*	Required DSP ports**	Comments
Integrated Conference Bridge	16	37	16	
Integrated Recorded Announcer	12	218	12	
Integrated Call Assistant	8	66	8	
Hospitality Integrated Voice Service	8	132	8	
Integrated Call Director	12	328	12	
Agent greeting	4		4	
CDR - incoming		1506		= 4706 × 0.32
CDR - outgoing		828		= 2588× 0.32
CDR - tandem		155		= 353 × 0.44
CPND		930		= (1998 + 706 + 1711 + 238) × 0.20, where terminating telephone is a TDM
Converged Desktop		939		= 0.05 × 2.33 × [(4118 × 0.1) + 353 + 2588 + 4706]
Basic ACD		26		
Symposium		10 229		
CallPilot		6474	60	
Total		21 868	120	

*Application EBC = (Number of application ports × CCS per port × 100 ÷ HT) × real-time factor

**Required DSP = Number of application ports

- Add the feature EBC to the system EBC to obtain an accurate estimate of the total CPU load:

  Total system real-time EBC = (Total system calls × real-time multiplier) + Application EBC
  = (11 765 × 2.79) + 21 868 = 54 692

New system real-time usage

Compare the total system EBC with the CPU rated capacity to determine the processor utilization.

CPU utilization = 54 692 ÷ 210 000 = 26.0%

In this example, CPU utilization, including application and feature impact, is 26.0%. This loading indicates that the CPU can handle this configuration with ease and has plenty of spare capacity.

DSP calculation for Conference ports

The formula to calculate the DSP requirement for conference ports is based on the number of telephones in the system. Like application ports, non-blocking conference ports must be provided.

DSP channels for conference ports = (Number of TDM telephones + Number of IP Phones × 0.028 = 2800 × 0.028 = 79

DSP calculation without applications

DSP calls (C_{DSP}) = $C_{1IP} + C_{T1VT} + C_{STID} + C_{STDV} + C_{TSVD} + C_{TSDI}$ = 7405

DSP CCS = C_{DSP} × WAHT ÷ 100 = 7405 × 119 ÷ 100 = 8813 CCS

Refer to an Erlang B table (with P.01 GoS) to find the corresponding number of ports, or use the following formula:

Number of DSP ports = DSP CCS ÷ 6192 × 192 = 273

DSP and Media Card calculations

Total DSP ports = DSP for calls + Conference + Applications/features = 273 + 79 + 120 = 472

Number of 32-port Media Cards required = 472 ÷ 32 = 15

For an 8-port Media Card, number of Media Cards required = 472 ÷ 8 = 59

> ***Note:*** Nortel recommends rounding up the Media Card calculation to an integer.

The numbers calculated for required DSP ports and Media Cards can be considered as a minimum requirement. When the cards are allocated to the Media Gateways, there are placement rules that will increase the Media Card requirement (see "Assigning loops and card slots in the CS 1000E" on page 329).

Virtual Trunk calculation

VT calls (C_{VT}) = $C_{T1VT} + C_{T2HS} + C_{STIV} + C_{STDV} + C_{TSVD} + C_{TSVI} = 6722$

H.323 VT calls (HC_{VT}) = $C_{VT} \times v_H = 6722 \times 0.67 = 4504$

SIP VT calls (SC_{VT}) = $C_{VT} \times v_S = 6722 \times 0.33 = 2218$

VT CCS = $C_{VT} \times$ WAHT ÷ 100 = 6722 × 119 ÷ 100 = 8000 CCS

Refer to a Poisson table (with P.01 GoS) to find the corresponding number of trunks, or use the following formula:

> Number of Virtual Trunks = VT CCS ÷ 5804 × 192 = 265
>
> Number of H.323 Virtual Trunks = 265 × 0.67 = 178
> Number of SIP Virtual Trunks = 265 × 0.33 = 88

User input for number of Virtual Trunks was 360. Since this is greater than 265, it is the number that should be used for further resource calculation.

Signaling Server calculation

The following information was obtained from previous calculations or input data:

> Number of IP Phones in the system = 1600
> Number of Virtual Trunks = 360 (H.323 = 240; SIP = 120)
> Calls involving at least one IP Phone (C_{IP}) = 7686
> Calls involving Virtual Trunks (C_{VT}) = GKC_0 = 6722

The following is additional user input to the NNEC tool:

Endpoints served by this NRS: 100
NRS entries (CDP + UDP + …): 1000
Virtual Trunks from other endpoints served by this NRS: 800
NRS alternate (NRA): Yes
TPSA (TPS N+1 redundancy required): Yes
H.323 Gateway alternate (GWA): Yes
SIP Gateway alternate (GSA): Yes
PD/CL/RL feature available to IP Phones: Yes
Sharing database with other traffic: Yes

PD/CL/RL database calculation (SSDB)

SSDB = b

The PD/CL/RL feature is available and sharing is allowed.

Network Routing Service calculation

SSNR = larger of:

{

a $NRE \div NRE_l = 100 \div 5000 = 0.02$endpoints

b $NRD \div NRD_l = 1000 \div 20\,000 = 0.05$dial plan entries

c $NRC \div NRC_{HL}$ calls per hour

}

NRC_0 is obtained from the main switch calculation.
$NRC_{NET} = VT_{NET} \times (CCS \text{ per } VT) \times 100 \div WAHT \div 2$

$= 800 \times 28 \times 100 \div 119 \div 2 = 9412$
$NRC = NRC_0 + NRC_{NET}$

$f_{H/S}$ = (H.323 call real time) ÷ (SIP call real time) = 1800 ÷ 1200 = 1.5

SIP calls = $120 \times 28 \times 100 \div 119 = 2824$
H.323 calls = $240 \times 28 \times 100 \div 119 = 5647$

$NRC \div NRC_{HL} = [(5647 \times 1.5) + 2824 + 9412] \div 100\,000 = 0.21$

This represents the loading of the Signaling Server for handling NRS calls. Compared with the results of equations (a) and (b), 0.21 is the highest of all potential usages.

Since the user wants the NRS in a dedicated Signaling Server, round up SSNR before proceeding with further calculations:

SSNW = ROUNDUP(0.21) × 2 = 2

Terminal Proxy Server calculation

SSTR = larger of:

{

b Since SSDB = b,with PD/CL/RL and sharing
and IPL (1600) > IPL_{DB} (1000),
$1 + [(IPL - 1000) \div IPL_{SL}] = 1 + (600 \div 5000) = 1.12$
(The database server can share the TPS function for 1600
IP telephones without the need for an additional Signaling Server.)

c $IPC \div IPC_{HL} = 7686 \div 15\,000 = 0.51$

}

The larger of the two values is 1.12.

Since the user wants the TPS in a dedicated Signaling Server, round up SSTR before proceeding with further calculations:

SSTW = ROUNDUP(1.12) + 1 = 3

H.323 Gateway calculation

SSHR = larger of:

{

a $HVT \div HVT_{SL} = 240 \div 1200 = 0.2$

b $C_{VT} \div HVTC_{HL} = 4504 \div 18\,000 = 0.25$

}

The larger of the two values is 0.25.

Since the user wants the H.323 Gateway in a dedicated Signaling Server, round up SSHR before proceeding with further calculations:

SSHW = ROUNDUP(0.25) × 2 = 2

5 SIP Gateway calculation (SSSR)

SSSR = larger of:

{

a $SVT \div SVT_{SL} = 120 \div 1800 = 0.07$

b $C_{VT} \div SVTC_{HL} = 2218 \div 27\,000 = 0.08$

}

The larger of the two values is 0.08.

Since the user wants the SIP Gateway in a dedicated Signaling Server, round up SSSR before proceeding with further calculations:

SSSW = ROUNDUP(0.08) × 2 = 2

Total Signaling Server requirement (SST)

The final calculation of SST requires picking the formula that suits the particular configuration and user input.

Since:
SSNR + SSHR + SSSR = 0.20 + 0.25 + 0.08 = 0.53 < 1 and
SSNR + SSTR + SSHR + SSSR = 1.65 > 1

SST = SSTW + [ROUNDUP(SSNR + SSHR + SSSR) × 2] + (0, since SSDB = b, not c)
= 3 + [ROUNDUP(0.53) × 2] = 5

The required number of Signaling Servers for this configuration is 5. The server with the database for the PD/CL/RL feature is sharing processing with the TPS function that handles IP Phones.

Manual adjustment of Signaling Server requirements

The above calculations strictly followed the engineering rules. However, with a relatively small system such as the one in the example, practical observation and adjustments can allow the user to reduce the number of Signaling Servers required.

1 Having the Personal Directory, Callers List, and Redial List database share functions on a Signaling Server limited the number of IP Phones on that Signaling Server to 1000. With a total of 1600 IP Phones in the system, another Signaling Server was required to provide TPS functions for the additional 600 telephones. In this case, it would be better to put all the IP Phones on the second server, since sharing did not reduce the number of Signaling Servers required.

2 To reduce complexity, the mathematical model allows sharing between the database server and TPS only. Separating the TPS function from the applications database (see item 1) frees up the database server to share with other functions.

3 With 1600 IP Phones, the load on a Signaling Server is 0.32 (1600 ÷ 5000). In this example, the sum of the other three functions (NRS, H.323 Gateway, and SIP Gateway) is 0.53. Combining these three functions with TPS for 1600 IP Phones yields a loading of 0.85. Since this loading is less than 1, it means all four functions can be combined on one Signaling Server.

4 The Signaling Server requirement for this configuration can be restated as follows

- **a** 1 Signaling Server for the Personal Directory, Callers List, Redial List applications database
- **b** 1 Signaling Server for all other functions (TPS, NRS, H.323/SIP Gateways)
- **c** 1 redundant/alternate Signaling Server to cover all four functions.
- **d** A total of 3 Signaling Servers for this configuration.

LAN/WAN bandwidth calculation algorithm

The calculation for LAN/WAN bandwidth requirement is based on traffic directly. It does not depend on the traffic model used.

VT traffic in erlangs = $[(240 + 120) \times 28] \div 36 = 280$ erlangs

Regulatory information

Contents

This section contains information on the following topics:

System approval

The CS 1000E system has approvals to be sold in many global markets. Regulatory labels on the back of system equipment contain national and international regulatory information.

Note: Some physical components in systems may have been marketed under different names in the past. Previous naming conventions utilizing the terms *Succession 1000* and *CSE 1000* have been harmonized to use the term *Communication Server 1000*. Similarly, previous naming conventions utilizing the terms *Meridian* and *Option* have been harmonized to use the term *Meridian 1 PBX*. Product names based on earlier naming conventions may still appear in some system documentation and on the system regulatory labels. From the point of view of regulatory standards compliance, the physical equipment is unchanged. As such, all the instructions and warnings in the regulatory sections of this document apply to the Communication Server 1000M, Communication Server 1000S, and Communication Server 1000E systems, as well as the Meridian, Succession 1000, and CSE 1000 systems.

Electromagnetic compatibility

The system meets Class A Electromagnetic compatibility (EMC) requirements for all countries.

CAUTION

In a domestic environment, the system can cause radio interference. In this case, the user could be required to take adequate measures.

Table 43 lists the EMC specifications for the system.

Table 43
EMC specifications for Class A devices (Part 1 of 2)

Jurisdiction	Standard	Description
United States	FCC CFR 47 Part 15	FCC Rules for Radio Frequency Devices (see Note 1a)
Canada	ICES-003	Interference-Causing Equipment Standard: Digital Apparatus
Europe	EN 55022/ CISPR 22	Information technology equipment — Radio disturbance characteristics — Limits and methods of measurement (see Note 2)
	EN 55024	Information technology equipment — Immunity characteristics — Limits and methods of measurement
	EN 61000-3-2	Limits for harmonic current emissions (equipment input current <= 16 A per phase)
	EN 61000-3-3	Limitation of voltage fluctuations and flicker in low-voltage supply systems for equipment with rated current <= 16 A
Australia	CISPR 22/ AS/NZS 3548	Limits and methods of measurement of radio disturbance characteristics of information technology equipment (see Note 2)

Table 43
EMC specifications for Class A devices (Part 2 of 2)

Jurisdiction	Standard	Description
Korea	KN22	Information technology equipment — Radio disturbance characteristics — Limits and methods of measurement
	KN24	Information technology equipment — Immunity characteristics — Limits and methods of measurement
Taiwan	CNS 13438	Limits and methods of measurement of radio disturbance characteristics of information technology equipment
Note 1a: FCC CFR 47 Part 15.21 statement: "Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense." ***Note 1b:*** The user should not make changes or modifications not expressly approved by Nortel. Any such changes could void the user's authority to operate the equipment.		
Note 2: EN 55022/CISPR 22 statement: "WARNING This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures."		

Notice for United States installations

The system complies with Part 68 of the United States Federal Communications Commission (FCC) rules. A label containing the FCC registration number and Ringer Equivalence Number (REN) for the equipment is on the back of each Media Gateway and Media Gateway Expander. If requested, you must provide this information to the telephone company.

Regulatory labels include:

- FCC registration: AB6CAN-61117-MF-E
- FCC registration: AB6CAN-61116-PF-E
- FCC registration: AB6CAN-18924-KF-E
- Service code: 9.0F, 6.0P
- Ringer equivalence (REN): 2.7A

The FCC regulation label includes the REN. This number represents the electrical load applied to your telephone line after you plug the system into the wall jack. The telephone line for your premises does not operate correctly if the total ringer load exceeds the capabilities of the telephone company's Central Office (CO) equipment. If too many ringers connect to the line, there may not be enough energy to ring your system. If the ringer load exceeds the system's capabilities, you can have problems dialing telephone numbers.

For more information about the total REN permitted for your telephone line, contact your local telephone company. However, as a guideline, a total REN of five should support normal operation of your equipment.

If your system equipment causes harm to the telephone network, the telephone company can temporarily discontinue your service. The telephone company can ask you to disconnect the equipment from the network until the problem is corrected and you are sure the equipment is working correctly. If possible, the telephone company notifies you before they disconnect the equipment. You are notified of your right to file a complaint with the FCC.

Your telephone company may make changes in its facilities, equipment, operations, or procedures that can affect the correct operation of your equipment. If the telephone company does make changes, they will give you advance notice. With advance notice, it is possible for you to make arrangements to maintain uninterrupted service.

If you experience trouble with your system equipment, contact your authorized distributor or service center.

You cannot use the equipment on public coin service provided by the telephone company. Connection to party line service is subject to state tariffs.

Contact the state public utility commission, public service commission, or corporation commission for information.

The equipment can provide access to interstate providers of operator services through the use of Equal Access codes. Failure to provide Equal Access capabilities is a violation of the Telephone Operator Consumer Services Improvement Act of 1990 and Part 68 of the FCC Rules.

Hearing aid compatibility

All proprietary telephones used with the system meet with the requirements of FCC Part 68 Rule 68.316 for hearing aid compatibility.

FCC compliance: Registered equipment for Direct Inward Dial calls

Equipment registered for Direct Inward Dial (DID) calls must provide proper answer supervision. Failure to meet this requirement is a violation of part 68 of the FCC's rules.

The definition of correct answer supervision is as follows:

- DID equipment returns answer supervision to the Central Office when DID calls are:
    - — answered by the called telephone
    - — answered by the attendant
    - — routed to a recorded announcement that can be administered by the user
    - — routed to a dial prompt
- DID equipment returns answer supervision on all DID calls forwarded to the Central Office. Exceptions are permitted if a call is not answered, a busy tone is received, or a reorder tone is received.

Radio and TV interference

The system complies with Part 15 of the FCC rules in the United States of America. Operation is subject to the following two conditions:

1 The system must not cause harmful interference.

2 The system must accept any interference received, including interference that can cause undesirable operation.

You can determine the presence of interference by placing a telephone call while monitoring. If the system causes interference to radio or television reception, try to correct the interference by moving the receiving TV or radio antenna if this can be done safely. Then move the TV or radio in relation to the telephone equipment.

If necessary, ask a qualified radio or television technician or supplier for additional information. You can refer to the document “How to Identify and Resolve Radio-TV Interference”, prepared by the Federal Communications Commission. This document is available from:

U.S. Government Printing Office
Washington DC 20402

Notice for Canadian installations

Industry Canada uses a label to identify certified equipment. Certification indicates that the equipment meets certain operations, safety, and protection requirements for telecommunications networks. Industry Canada does not guarantee that the equipment will operate to the user’s satisfaction.

The Load Number (LN) assigned to each terminal device is the percentage of the total load that can be connected to a telephone loop using the device. This number prevents overload. The termination on a loop can have any combination of devices, provided that the total of the Load Numbers does not exceed 100. An alphabetical suffix is also defined in the Load Number for the appropriate ringing type (A or B), if necessary. For example, LN = 20 A indicates a Load Number of 20 and an “A” type ringer.

Before you install any equipment, make sure that it can connect to the facilities of the local telecommunications company. Install the equipment using acceptable methods of connection. In some cases, a certified connector assembly (telephone extension cord) can extend the company's inside wiring associated with a single line individual service. Understand that compliance with the above conditions does not always prevent degradation of service.

Repairs to certified equipment must be made by an authorized Canadian maintenance facility designated by the supplier. If you make repairs or modifications to this equipment, or if the equipment malfunctions, the telephone company can ask you to disconnect the equipment.

Make sure that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, connect together. This precaution is for the users' protection, and is very important in rural areas.

DANGER OF ELECTRIC SHOCK

The system frame ground of each unit must be tied to a reliable building ground reference.

DANGER OF ELECTRIC SHOCK

Do not attempt to make electrical ground connections yourself. Contact your local electrical inspection authority or electrician to make electrical ground connections.

Radio and TV interference

The system does not exceed Class A limits for radio noise emissions from digital apparatus, as set out in the radio interference regulations of Industry Canada (ICES-003).

Canadian and US network connections

Table 44 contains information that must be given to the local telephone company when ordering standard network interface jacks for the system.

Table 44 includes columns for system port identification, Facility Interface Code (FIC), Service Order Code (SOC), Uniform Service Order Code (USOC) jack identification, and associated Nortel equipment part numbers.

Table 44
Network connection specifications (Part 1 of 2)

Ports	Facility Interface Code	Service Order Code	REN	Network jacks	Manufacturer network interface port designation
MTS/WATS					
2-Wire, LSA, L-S (2-Wire, Local Switched Access, Loop-Start)	02LS2	9.0F	2.7A	RJ21X CA21X*	NT8D14
2-Wire, LSA, G-S (2-Wire, Local Switched Access, Ground-Start)	02GS2	9.0F	2.7A	RJ21X CA21X*	NT8D14
2-Wire, LSA, R-B (2-Wire, Local Switched Access, Reverse-Battery)	02RV2-T	9.0F	0.0B	RJ21X CA21X*	NT8D14
1.544 Mbps OSI, SF	04DU9-BN	6.0P	N/A	RJ48 CA48*	NTRB21
1.544 Mbps OSI, SF	04DU9-KN	6.0P	N/A	RJ48 CA48*	NTRB21
Analog PL facilities					
8-port OPX line	OL13C	9.0F	N/A	RJ21X	NT1R20
E&M TIE Trunk (TIE line, lossless, 2-wire type 1 E&M)	TL11M	9.0F	N/A	RJ2EX CA2EX*	NT8D15
* RJ with CA for Canada					

Table 44
Network connection specifications (Part 2 of 2)

Ports	Facility Interface Code	Service Order Code	REN	Network jacks	Manufacturer network interface port designation
E&M 4-Wire DRTT (TIE line, lossless, dial repeating, 4-wire type 1 E&M)	TL31M	9.0F	N/A	RJ2GX CA2GX*	NT8D15
E&M 4-Wire DRTT (TIE line, lossless, dial repeating, 4-wire type 2 E&M)	TL32M	9.0F	N/A	RJ2HX CA2HX*	NT8D15
Digital					
1.544 Mbps superframe	04DU9-BN	6.0P	N/A	N/A	NT5D12
1.544 Mbps extended superframe	04DU9-KN	6.0P	N/A	N/A	NT5D12
* RJ with CA for Canada					

Notice for International installations

If there is not enough planning or technical information available for your country of operation, contact your regional distributor or authority.

European compliance information

The system meets the following European technical regulations: CTR 1, CTR 2, CTR 3, CTR 4, CTR 6, CTR 10, CTR 12, CTR 13, CTR 15, CTR 17, CTR 22, CTR 24, and the I-ETS 300 131.

Supported interfaces

Analog interfaces are approved based on national or European specifications. Digital interfaces are approved based on European specifications.

Safety specifications

The system meets the following European safety specifications: EN 60825, EN 60950, and EN 41003.

Notice for Germany

Empfangen und Auspacken des Communication Server 1000E

Dem Gerät sollte eine Teileliste beiliegen, die alle im Lieferumfang des Systems enthaltenen Teile auflistet. Vergleichen Sie diese Teileliste mit den erhaltenen Teilen. Sollte die Teileliste mit den erhaltenen Teilen nicht übereinstimmen, benachrichtigen Sie unverzüglich den Lieferungsagenten und Nortel. Alle mit dem System bestellten Optionen sind werkseitig installiert und nicht separat auf der Teileliste aufgelistet. Bewahren Sie die Versandkartons auf, um sie ggf. wiederverwenden zu können.

> ***Hinweis:*** Falls die Versandkartons bei Empfang beschädigt sind, sollten Sie den Lieferungsagenten bitten, bei dem Auspacken und der Inspektion des Geräts anwesend zu sein.

1 Stellen Sie sicher, daß sich der Verpackungskarton in aufrechter Position befindet.

2 Schneiden Sie das Verpackungsklebeband vorsichtig mit einem Schneidemesser auf, und öffnen Sie dann den Karton.

3 Entfernen Sie die Kartonverpackung, das Schaumstoff-verpackungsmaterial und die schützende Plastikverpackung.

4 Heben Sie das Chassis vorsichtig aus dem Karton, und plazieren Sie es an dem gewünschten Aufstellungsort.

Richtlinien zum Aufstellen des Systems

Bei der Wahl des Systemstandorts empfiehlt es sich, folgende Punkte in Betracht zu ziehen:

1 Stabilität. Stellen Sie das System in einem Bereich auf, der vor übermäßigen Bewegungen und Erschütterungen geschützt ist.

2 Sicherheit. Installieren Sie das System im Hinblick auf Sicherheit. Sorgen Sie dafür, daß Kabel und Drähte den Zugang nicht behindern.

3 Zugang. Stellen Sie das System so auf, daß es problemlos gewartet werden kann. Bei Wartungsarbeiten ist Zugang zur Vorder- und Rückseite des Systems erforderlich.

4 Betriebsumgebung. Stellen Sie das System in einem Bereich auf, an dem es Hitze, Staub, Rauch und elektrostatischer Entladung (ESE) nicht ausgesetzt ist.

5 Kühlung. Lassen Sie Platz für eine ausreichende Luftzirkulation zur Kühlung. Stellen Sie sicher, daß vor und hinter dem System mindestens 10 cm Freiraum gelassen wird. (Zusätzliche Richtlinien zur Kühlung des Gerätes finden Sie im nächsten Abschnitt.)

Kühlen des Gehäuses

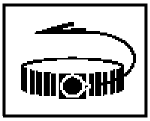
Es ist äußerst wichtig, daß alle Geräte eines Systems sachgemäß gekühlt werden. Die Eingangslufttemperatur der Systemkomponenten muß im allgemeinen unter 50º C (122º F) liegen. Interne, durch Gleichstrom betriebene Ventilatoren kühlen die Laufwerke und Module des Systems ab. Die Übergangsmodule an der Rückseite des Chassis werden durch natürliche Konvektion gekühlt. Um eine ausreichende Kühlung zu gewährleisten, sollten Sie:

- Vor und hinter dem System mindestens 10 cm Freiraum lassen.
- Sicherstellen, daß die Verkleidungen aufgesetzt, alle vorderen und rückwärtigen Schlitze gefüllt und alle Öffnung abgedeckt sind.
- Alle nicht verwendeten Modulschlitze abdecken.

Bei der Installation des Systems in einer bestimmten Betriebsumgebung sollten die technischen Daten zur Betriebsumgebung der

Systemkomponenten beachtet werden. Zum Beispiel: Bei Umgebungstemperaturen über 50º C (122º F) wird der Betrieb von Disketten- und Festplattenlaufwerken nicht mehr zuverlässig. Im Falle eines Gerätes, das in einem Gehäuse installiert ist, sollten Sie beachten, daß die interne Umgebungstemperatur unter Umständen über die maximal mögliche, externe Umgebungstemperatur ansteigen kann.

ESE und Sicherheit



ESE-ANTISTATIKBAND VERWENDEN

Nortel empfiehlt, bei allen Installations- oder Aufrüstarbeiten am System ein Antistatikband und eine ableitende Schaumstoffunterlage zu verwenden. Elektronische Komponenten, wie z.B. Plattenlaufwerke, Platinen und Speichermodule, können gegen ESE äußerst empfindlich sein. Nach dem Entfernen des Bauteils aus dem System oder aus der Schutzhülle wird das Bauteil flach auf eine geerdete und statikfreie Oberfläche gelegt, und im Falle einer Platine mit der Komponentenseite nach oben. Das Bauteil nicht auf der Oberfläche hin und her bewegen.

Ist kein ESE-Arbeitsplatz verfügbar, so können ESE-Gefahren durch das Tragen eines Antistatikbands (in Elektronik- Fachgeschäften erhältlich) vermieden werden. Dabei ist ein Ende des Bandes um das Handgelenk zu legen. Das Erdungsende (normalerweise ein Stück Kupferfolie oder eine Krokodilklemme) an einer elektrischen Masseverbindung anschließen. Hierbei kann es sich um ein Stück Metall handeln, das direkt zur Erde führt (z.B. ein unbeschichtetes Metallrohr) oder ein Metallteil eines geerdeten, elektrischen Gerätes. Ein elektrisches Gerät ist geerdet, wenn es einen dreistiftigen Schukostecker besitzt, der in eine Schuko-Steckdose gesteckt wird. Das System selbst kann nicht als Masseverbindung verwendet werden, weil es bei allen Arbeiten vom Netz getrennt wird.

WARNUNG

Vor dem Ausführen dieser Verfahren ist die Stromzufuhr des Systems auszuschalten und das System vom Stromnetz zu trennen. Wenn der Strom vor dem Öffnen des Systems nicht ausgeschaltet wird, besteht die Gefahr von Körperverletzungen und Beschädigungen des Gerätes. Im Gerät sind gefährliche Spannungen, Strom und Hochenergie vorhanden. An den Anschlußpunkten der Betriebsschalter können gefährliche Spannungen anliegen, auch wenn sich der Schalter in der ausgeschalteten Position befindet. Das System darf nicht bei abgenommener Gehäuseabdeckung betrieben werden. Vor dem Einschalten des Systems ist die Gehäuseabdeckung stets anzubringen.

Sicherheits- und Betriebsnormen

Diese Systeme entsprechen den Sicherheits- und Betriebsnormen, die für einzelne Geräteteile gelten. Es ist jedoch möglich, dieses Produkt mit anderen Einzelteilen zusammen zu verwenden, die ein System ergeben, welches nicht den Systemrichtlinien entspricht. Da Nortel nicht voraussehen kann, welche Geräte mit diesem Gehäuse verwendet werden oder wie dieses Gehäuse verwendet wird, sind der Systemintegrator und der Installateur völlig dafür verantwortlich, daß das gesamte fertiggestellte System den Sicherheitsanforderungen von UL/CSA/VDE sowie den EMI/ HFI-Emissionsgrenzen entspricht.

Vorsichtshinweise zur Lithium-Batterie

Dieses System enthält Lithium-Batterien.

VORSICHT

Bei einem inkorrekten Auswechseln der Lithium-Batterien besteht Explosionsgefahr. Wechseln Sie die Batterien nur mit dem gleichen oder einem gleichwertigen Batterietyp, der von dem Hersteller empfohlen ist, aus. Entsorgen Sie gebrauchte Batterien gemäß den Herstelleranweisungen.

VORSICHT

Bitte nehmen Sie vor Ort keine Wartung bzw. Austausch der Lithium-Batterien selber vor. Um die Batterien sachgemäß warten oder auswechseln zu lassen, setzen Sie sich mit Ihrem Nortel Servicevertreter in Verbindung.

Installation in ein 19-Zoll-Rack

Um das Gerät in ein Rack einzubauen, gehen Sie folgendermaßen vor:

VORSICHT

Befestigen Sie das Chassis nicht oben am Rack. Ein kopflastiges Rack kann Umkippen und Geräte beschädigen sowie Personal verletzen.

Um Verletzungen von Personen oder Beschädigungen der Geräte zu vermeiden sollten folgende Schritte von zwei Personen ausgeführt werden.

1 Schieben Sie das Chassis vorne in das Rack.

2 Befestigen Sie das Chassis mit Schrauben. (Um Genaueres über die hierzu empfohlenen Schraubenarten zu erfahren, wenden Sie sich bitte an den Hersteller des Racks.)

3 Stellen Sie sicher daß der Netzschalter (ON/OFF oder EIN/AUS) am Chassis auf OFF (O) gestellt ist. Ist Ihr System mit einem Spannungswahlschalter versehen, so stellen Sie den Schalter auf die Ihrem Standort gemäße Betriebsspannung.

4 Stecken Sie das Sockelende des Chassisnetzkabels in die Netzsteckbuchse an der Rückseite des Chassis.

5 Installieren Sie alle Kommunikationskabel.

6 Stecken Sie alle Netzkabel in eine geerdete, gegen Spannungsspitzen geschützte Schuko-Steckdose.

7 Um den Netzstrom einzuschalten, stellen Sie den Netzschalter (ON/OFF) an der Rückseite des Chassis auf ON (1). Die normale Startroutine des Systems erfolgt, und das System ist dann einsatzbereit.

WARNUNG

Vor Wartungsarbeiten am Chassis ist das Netzkabel vom Stromnetz zu trennen, um die Gefahr eines elektrischen Schlages oder andere mögliche Gefahren zu reduzieren.

Application engineering

Contents

This section contains information on the following topics:

Introduction

Certain applications have significant capacity impact and require engineering in order to operate properly from a capacity perspective. This section provides suggestions for engineering these applications.

For more information on voice networks, refer to *Converging the Data Network with VoIP* (553-3001-160).

Converged Desktop

The Converged Desktop is a TDM or IP Phone configured to access Multimedia Communication Server (MCS) 5100 multimedia applications through a Session Initiation Protocol (SIP) Virtual Trunk.

Maximum number of Converged Desktop users

In a pure IP system, the CS 1000E can support up to 10 000 Converged Desktop users. However, for a new installation, Nortel recommends configuring no more than 7000 IP users with the Converged Desktop application. This reserves a reasonable amount of real-time capacity for future growth.

SIP access port requirement

Every Converged Desktop call uses a SIP trunk for signaling during the ringing period. In addition, a certain percentage of calls will use the SIP trunk for voice traffic for the entire duration of the call. Therefore, the required number of SIP access ports depends on the number of Converged Desktop users and the percentage of voice calls using SIP trunks for conversation.

Personal Call Assistant requirement

The following types of calls to a Converged Desktop use the Personal Call Assistant (PCA) feature for the duration of ringing time:

- calls originating from an internal phone
- calls originating from any non-SIP trunk
- calls originating from a SIP trunk but not from an MCS 5100

The PCA requirement depends only on the number of Converged Desktop users. It is independent of the percentage of voice calls using SIP trunks for conversation.

Calculating SIP access port and PCA requirements

Table 45 on page 279 shows the required number of SIP access ports and PCAs for different levels of Converged Desktop usage, with P.01 Grade-of-Service (GoS).

The columns under “% voice traffic carried by SIP trunk” indicate the fraction of calls that use a SIP trunk for conversation. A percentage of zero means that the SIP port is used only for signaling during the ringing period and is dropped from the connection once the call is answered.

To use the table, users must know (1) the number of Converged Desktop users and (2) the percentage of Converged Desktop users using SIP trunks to carry voice traffic. The readings below the percentage column are the number of SIP trunks and PCA ports required for a given number of Converged Desktop users.

The number of users shown in Table 45 increments by increasingly large amounts as the number of users increases. If you are calculating requirements for a number of users not shown in the table, use the following formula:

Inputs

- Total Number of Converged Desktop users required (MCS_CD_Users)
- Percentage of calls that will be answered on a soft client configured as a Converged Desktop (P_CD_SIP)
- Total Number of non-Converged desktop users required (MCS_Non_CD_Users)
- Number of Meet-Me Audio Conference ports configured on the MCS (MeetMe_Ports)

Calculations

- Traffic for CD = (MCS_CD_Users) x (CCS per user) x 10%
- Traffic for SIP ports = (MCS_Non_CD_Users) x (CCS per user) + (MCS_CD_Users x P_CD_SIP) x (CCS per user)
- Total SIP Traffic = (Traffic for CD) x (1 - P_CD_SIP) + (Traffic for SIP ports)

- Number of SIP ports = Poisson (Total SIP Traffic) at P.01 + MeetMe_Ports
- Number of MCS PCAs ports = Poisson (Traffic for CD) at P.01
- Number of ACD agents = Number of MCS PCAs ports

If detailed information about the network is not available, use the following formula to estimate the percentage of Converged Desktop users using SIP trunks to carry voice traffic, rounding up the result:

(Number of SIP trunks) ÷ [(Number of SIP trunks) + (Number of H.323 trunks)]

Assumptions

1 The ringing period is 10% of the conversation time. (One ring is a 6-second cycle; the ringing period is usually 2–3 rings; average conversation time is 120–180 seconds.)

2 PCA holding time is equal to the length of the ringing period for each call. This is a conservative assumption, because it implies that every call needs a PCA.

Example

Two hundred Converged Desktop users with 0% SIP trunk conversation require 8 SIP access ports and 8 PCAs. If 20% use SIP for conversation, the requirements are 16 SIP access ports and 8 PCAs.

Table 45
SIP port and PCA requirements for Converged Desktop (with P.01 GoS) (Part 1 of 7)

# CD Users		% voice traffic carried by SIP trunk											
		0	5	10	15	20	25	30	35	40	45	50	100
25	SIP CCS	12.5	18.1	23.8	29.4	35.0	40.6	46.2	51.9	57.5	63.1	68.8	125.0
	SIP port	3	4	4	4	5	5	5	6	6	6	7	9
	PCA	3	3	3	3	3	3	3	3	3	3	3	3
50	SIP CCS	25.0	36.2	47.5	58.8	70.0	81.2	92.5	103.8	115.0	126.2	137.5	250.0
	SIP port	4	5	6	6	7	7	8	8	9	9	10	15
	PCA	4	4	4	4	4	4	4	4	4	4	4	4
75	SIP CCS	37.5	54.4	71.2	88.1	105.0	121.9	138.8	155.6	172.5	189.4	206.2	375.0
	SIP port	5	6	7	8	8	9	10	11	11	12	13	19
	PCA	5	5	5	5	5	5	5	5	5	5	5	5
100	SIP CCS	50.0	72.5	95.0	117.5	140.0	162.5	185.0	207.5	230.0	252.5	275.0	500.0
	SIP port	6	7	8	9	10	11	12	13	14	15	16	24
	PCA	6	6	6	6	6	6	6	6	6	6	6	6

Note: Voice users in CCS = 5 CCS per user. Ratio of ringing time to holding time = 0.1.

Table 45
SIP port and PCA requirements for Converged Desktop (with P.01 GoS) (Part 2 of 7)

# CD Users		% voice traffic carried by SIP trunk											
		0	5	10	15	20	25	30	35	40	45	50	100
125	SIP CCS	62.5	90.6	118.8	146.9	175.0	203.1	231.2	259.4	287.5	315.6	343.8	625.0
	SIP port	6	8	9	10	12	13	14	15	16	17	18	29
	PCA	6	6	6	6	6	6	6	6	6	6	6	6
150	SIP CCS	75.0	108.8	142.5	176.2	210.0	243.8	277.5	311.2	345.0	378.8	412.5	750.0
	SIP port	7	9	10	12	13	14	16	17	18	20	21	33
	PCA	7	7	7	7	7	7	7	7	7	7	7	7
175	SIP CCS	87.5	126.9	166.2	205.6	245.0	284.4	323.8	363.1	402.5	441.9	481.2	875.0
	SIP port	8	9	11	13	14	16	18	19	20	22	23	37
	PCA	8	8	8	8	8	8	8	8	8	8	8	8
200	SIP CCS	100.0	145.0	190.0	235.0	280.0	325.0	370.0	415.0	460.0	505.0	550.0	1000.0
	SIP port	8	10	12	14	16	18	19	21	23	24	26	42
	PCA	8	8	8	8	8	8	8	8	8	8	8	8
225	SIP CCS	112.5	163.1	213.8	264.4	315.0	365.6	416.2	466.9	517.5	568.1	618.8	1125.0
	SIP port	9	11	13	15	17	19	21	23	25	27	28	46
	PCA	9	9	9	9	9	9	9	9	9	9	9	9

Note: Voice users in CCS = 5 CCS per user. Ratio of ringing time to holding time = 0.1.

Table 45
SIP port and PCA requirements for Converged Desktop (with P.01 GoS) (Part 3 of 7)

# CD Users		% voice traffic carried by SIP trunk											
		0	5	10	15	20	25	30	35	40	45	50	100
250	SIP CCS	125.0	181.2	237.5	293.8	350.0	406.2	462.5	518.8	575.0	631.2	687.5	1250.0
	SIP port	9	12	14	16	19	21	23	25	27	29	31	50
	PCA	9	9	9	9	9	9	9	9	9	9	9	9
300	SIP CCS	150.0	217.5	285.0	352.5	420.0	487.5	555.0	622.5	690.0	757.5	825.0	1500.0
	SIP port	10	13	16	19	21	24	26	28	31	33	36	58
	PCA	10	10	10	10	10	10	10	10	10	10	10	10
400	SIP CCS	200.0	290.0	380.0	470.0	560.0	650.0	740.0	830.0	920.0	1010.0	1100.0	2000.0
	SIP port	13	16	20	23	26	29	33	36	39	42	45	74
	PCA	13	13	13	13	13	13	13	13	13	13	13	13
500	SIP CCS	250.0	362.5	475.0	587.5	700.0	812.5	925.0	1037.5	1150.0	1262.5	1375.0	2500.0
	SIP port	15	19	23	27	31	35	39	43	47	50	54	90
	PCA	15	15	15	15	15	15	15	15	15	15	15	15
750	SIP CCS	375.0	543.8	712.5	881.2	1050.0	1218.8	1387.5	1556.2	1725.0	1893.8	2062.5	3750.0
	SIP port	19	26	32	37	43	49	54	60	65	71	76	129
	PCA	19	19	19	19	19	19	19	19	19	19	19	19

Note: Voice users in CCS = 5 CCS per user. Ratio of ringing time to holding time = 0.1.

Table 45
SIP port and PCA requirements for Converged Desktop (with P.01 GoS) (Part 4 of 7)

# CD Users		% voice traffic carried by SIP trunk											
		0	5	10	15	20	25	30	35	40	45	50	100
1000	SIP CCS	500.0	725.0	950.0	1175.0	1400.0	1625.0	1850.0	2075.0	2300.0	2525.0	2750.0	5000.0
	SIP port	24	32	40	47	55	62	69	77	84	91	98	168
	PCA	24	24	24	24	24	24	24	24	24	24	24	24
1250	SIP CCS	625.0	906.2	1187.5	1468.8	1750.0	2031.2	2312.5	2593.8	2875.0	3156.2	3437.5	6250.0
	SIP port	29	38	48	57	66	75	84	93	102	111	120	205
	PCA	29	29	29	29	29	29	29	29	29	29	29	29
1500	SIP CCS	750.0	1087.5	1425.0	1762.5	2100.0	2437.5	2775.0	3112.5	3450.0	3787.5	4125.0	7500.0
	SIP port	33	44	56	67	78	88	99	109	120	130	141	243
	PCA	33	33	33	33	33	33	33	33	33	33	33	33
1750	SIP CCS	875.0	1268.8	1662.5	2056.2	2450.0	2843.8	3237.5	3631.2	4025.0	4418.8	4812.5	8750.0
	SIP port	37	51	63	76	89	101	113	126	138	150	162	280
	PCA	37	37	37	37	37	37	37	37	37	37	37	37
2000	SIP CCS	1000.0	1450.0	1900.0	2350.0	2800.0	3250.0	3700.0	4150.0	4600.0	5050.0	5500.0	10 000.0
	SIP port	42	56	71	85	100	114	128	142	155	169	183	318
	PCA	42	42	42	42	42	42	42	42	42	42	42	42

Note: Voice users in CCS = 5 CCS per user. Ratio of ringing time to holding time = 0.1.

Table 45
SIP port and PCA requirements for Converged Desktop (with P.01 GoS) (Part 5 of 7)

# CD Users		% voice traffic carried by SIP trunk											
		0	5	10	15	20	25	30	35	40	45	50	100
2500	SIP CCS	1250.0	1812.5	2375.0	2937.5	3500.0	4062.5	4625.0	5187.5	5750.0	6312.5	6875.0	12 500.0
	SIP port	50	68	86	104	121	139	156	173	190	207	224	392
	PCA	50	50	50	50	50	50	50	50	50	50	50	50
3000	SIP CCS	1500.0	2175.0	2850.0	3525.0	4200.0	4875.0	5550.0	6225.0	6900.0	7575.0	8250.0	15 000.0
	SIP port	58	80	101	122	143	164	184	205	225	245	266	465
	PCA	58	58	58	58	58	58	58	58	58	58	58	58
3500	SIP CCS	1750.0	2537.5	3325.0	4112.5	4900.0	5687.5	6475.0	7262.5	8050.0	8837.5	9625.0	17 500.0
	SIP port	66	91	116	140	165	188	212	236	260	283	307	538
	PCA	66	66	66	66	66	66	66	66	66	66	66	66
4000	SIP CCS	2000.0	2900.0	3800.0	4700.0	5600.0	6500.0	7400.0	8300.0	9200.0	10 100.0	11 000.0	20 000.0
	SIP port	74	103	131	158	186	213	240	267	294	321	347	611
	PCA	74	74	74	74	74	74	74	74	74	74	74	74
4500	SIP CCS	2250.0	3262.5	4275.0	5287.5	6300.0	7312.5	8325.0	9337.5	10 350	11 362.5	12 375.0	22 500.0
	SIP port	82	114	145	176	207	237	268	298	328	358	388	684
	PCA	82	82	82	82	82	82	82	82	82	82	82	82

Note: Voice users in CCS = 5 CCS per user. Ratio of ringing time to holding time = 0.1.

Table 45
SIP port and PCA requirements for Converged Desktop (with P.01 GoS) (Part 6 of 7)

# CD Users		% voice traffic carried by SIP trunk											
		0	**5**	**10**	**15**	**20**	**25**	**30**	**35**	**40**	**45**	**50**	**100**
5000	SIP CCS	2500	3625	4750	5875	7000	8125	9250	10 375	11 500	12 625	13 750	25 000
	SIP port	90	125	160	194	228	262	295	329	362	395	428	757
	PCA	90	90	90	90	90	90	90	90	90	90	90	90
6000	SIP CCS	3000	4350	5700	7050	8400	9750	11 100	12 450	13 800	15 150	16 500	30 000
	SIP port	106	148	189	230	270	310	350	390	430	470	509	908
	PCA	106	106	106	106	106	106	106	106	106	106	106	106
7000	SIP CCS	3500	5075	6650	8225	9800	11 375	12 950	14 525	16 100	17 675	19 250	35 000
	SIP port	121	170	218	265	312	358	405	451	497	543	589	1057
	PCA	121	121	121	121	121	121	121	121	121	121	121	121
8000	SIP CCS	4000	5800	7600	9400	11 200	13 000	14 800	16 600	18 400	20 200	22 000	40 000
	SIP port	137	192	246	300	353	406	459	512	565	617	669	1205
	PCA	137	137	137	137	137	137	137	137	137	137	137	137
9000	SIP CCS	4500	6525	8550	10 575	12 600	14 625	16 650	18 675	20 700	22 725	24 750	45 000
	SIP port	152	214	274	335	395	454	513	573	632	690	749	1354
	PCA	152	152	152	152	152	152	152	152	152	152	152	152

Note: Voice users in CCS = 5 CCS per user. Ratio of ringing time to holding time = 0.1.

Table 45
SIP port and PCA requirements for Converged Desktop (with P.01 GoS) (Part 7 of 7)

# CD Users		% voice traffic carried by SIP trunk											
		0	5	10	15	20	25	30	35	40	45	50	100
10 000	SIP CCS	5000	7250	9500	11 750	14 000	16 250	18 500	20 750	23 000	25 250	27 500	50 000
	SIP port	168	236	303	369	436	502	568	633	698	767	834	1502
	PCA	168	168	168	168	168	168	168	168	168	168	168	168

Note: Voice users in CCS = 5 CCS per user. Ratio of ringing time to holding time = 0.1.

Microsoft Live Communications Server users

The Nortel Converged Office feature combines the business-grade telephony of the Communication Server 1000 with the real-time multimedia communication and the remote call control provided by Microsoft® Office Live Communications Server 2005 and Microsoft® Office Communicator 2005 products. Nortel Converged Office is defined by the following two components:

- **Remote Call Control with Session Initiation Protocol (SIP) Computer Telephone Integration (CTI) TR/87** provides full Microsoft® Office integration of telephony to control business grade telephony phones from within Microsoft® Office applications, as well as support for a standards-based CTI interface defined by the TR/87 protocol.
- **Telephony Gateway and Services** provides a basic SIP Telephony Gateway for connectivity between Private and Public Telephony networks and Live Communications Server 2005 clients.

Trunking

To handle the traffic between the CS 1000 and the Live Communications Server 2005, you must configure sufficient SIP trunks and Personal Call Assistants (PCAs). The number of additional SIP trunks needed is determined by:

The number of Office Communicator Users using the SIP Gateway feature

multiplied by:

The percentage expected to be on the phone at any given time

For example, 100 Office Communicator SIP Gateway users x 10% on the phone at any given time = 10 additional SIP trunks.

The percentage of users on a phone is decided by standard practice and the environment involved (Call Center, Normal Office, and so on).

PCA trunks are required for each Office Communicator user using the "Twinning" (for SIP Gateway) feature.

Calculating SIP access port and PCA requirements

Table 46 defines the inputs used to calculate SIP access ports and PCA requirements.

Table 46
Inputs

Input	Description
TN_MO_Users	Total Number of Office Communicator users that will be using the SIP Access Ports for voice services
PCA_MO_Users	Number of Office Communicator users that will utilize Personal Call Assistant (PCA). The value entered is in addition to the number you indicate on the Software screen.
P_PCA_SIP	Percentage of PCA calls that will be using the soft client to answer

Calculations:

The following formulas are used to calculate traffic requirements:

Traffic for PCAs = (PCA_MO_Users) x (CCS per user) x (1 - P_PCA_SIP) x 10%

Traffic for SIP ports = (TN_MO_Users - PCA_MO_Users) x (CCS per user) + (PCA_MO_Users x P_PCA_SIP) x (CCS per user)

Total SIP Traffic = (Traffic for PCAs) + (Traffic for SIP ports)

Number of MO SIP ports = Poisson (Total SIP Traffic) at P.01 Grade of Service

* - MO = Microsoft® Office Communicator

Table 47 shows traffic in CCS and number of ports calculated based on Poisson formula at P.01 Grade of Service.

Table 47
Traffic figures (Part 1 of 4)

Traffic (CCS)	Traffic (Erlang)	#Ports
5	0.14	2
10	0.28	3
15	0.42	3
20	0.56	4
25	0.69	4
30	0.83	4
35	0.97	5
40	1.11	5
45	1.25	5
50	1.39	6
55	1.53	6
60	1.67	6

Table 47
Traffic figures (Part 2 of 4)

Traffic (CCS)	Traffic (Erlang)	#Ports
65	1.81	6
70	1.94	7
75	2.08	7
80	2.22	7
85	2.36	7
90	2.5	8
95	2.64	8
100	2.78	8
125	3.47	9
150	4.17	10
175	4.86	12
200	5.56	13
225	6.25	14
250	6.94	15
275	7.64	16
300	8.33	17
325	9.03	18
350	9.72	19
375	10.42	19
400	11.11	20
425	11.81	21
450	12.5	22

Table 47
Traffic figures (Part 3 of 4)

Traffic (CCS)	Traffic (Erlang)	#Ports
475	13.19	23
500	13.89	24
550	15.28	26
600	16.67	28
650	18.06	29
700	19.44	31
750	20.83	33
800	22.22	35
850	23.61	36
900	25	38
950	26.39	40
1000	27.78	42
1500	41.67	58
2000	55.56	74
2500	69.44	90
3000	83.33	106
3500	97.22	121
4000	111.11	137
4500	125	152
5000	138.89	168
6000	166.67	198
7000	194.44	228

Table 47
Traffic figures (Part 4 of 4)

Traffic (CCS)	Traffic (Erlang)	#Ports
8000	222.22	258
9000	250	288
10000	277.78	318
20000	555.56	611
30000	833.33	908
40000	1111.11	1205
50000	1388.89	1502
60000	1666.67	1799
70000	1944.44	2096

SIP CTI/TR87

When planning for capacity with SIP CTI services, there is a fundamental restriction that must be observed:

- For a single call server that supports multiple nodes, each with SIP CTI services enabled, multiple SIP CTI(TR/87) sessions can be established for a given DN through the same node—but not through different nodes.

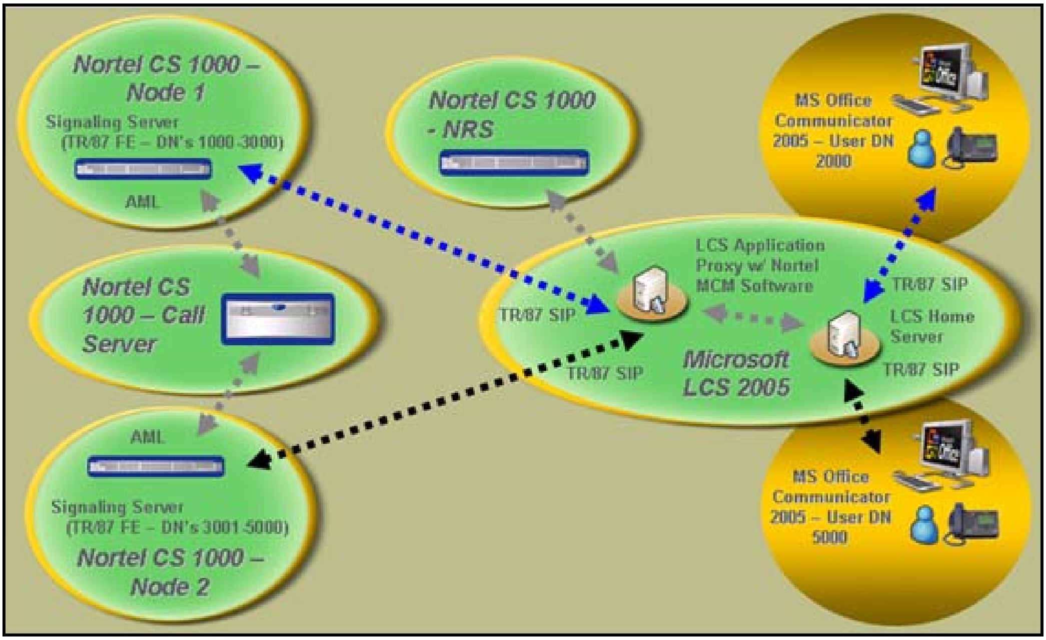
To illustrate this restriction, consider the following high level example:

Client A sends a TR/87 SIP INVITE to Node 1 to monitor DN 1000. The TR/87 association is established. Client B then sends a TR/87 SIP INVITE to Node 1 (the same node) to monitor DN 1000. Both sessions are established successfully. As a result of this sequence, two TR/87 sessions exist for DN 1000 through node 1.

However, if client B attempts to send a TR/87 SIP INVITE to Node 2 (which has an AML link to the same call server as Node 1), the attempt to establish the TR/87 session will fail because the DN is already in use by client A's session through Node 1.

To solve this issue when planning for capacity, SIP routing must ensure that all TR/87 sessions for a given DN always terminate on the same node when there are multiple nodes for a single call server (see Figure 33 on page 291).

Figure 33
Capacity example



This situation may arise in cases where there is an expectation that a single user has multiple clients logged in simultaneously (for example, a client at home, a client in the office, and a mobile client all with TR/87 capability).

Impact on Signaling Server

The maximum number of SIP CTI/TR87 users on a single Signaling Server is 5000. While the Standard Signaling Server memory is 512MB, an upgrade to 1GB is required in the following scenarios:

1. SIP CTI/TR87 is co-resident with PD/RL/CL application
2. SIP CTI/TR87 is co-resident with H.323/SIP GW serving more than 200 ports, or co-resident with Terminal Proxy Server serving more than 1000 IP users.

Impact on Call Server

For different CPUs, the number of supported users is:

- SSC: 750 users
- CP3: 1500 users
- CP4: 2500 users
- CPP PII: 7000 users
- CPP PIV: 15000 users

MCM capacity

The Standard Performance Evaluation Corporation (SPEC) is a non-profit corporation formed to establish, maintain, and endorse a standardized set of relevant benchmarks that can be applied to the newest generation of high-performance computers.

Multimedia Convergence Manager (MCM) is a software component designed specifically for the Nortel Converged Office feature to ensure the proper interoperability between Microsoft® and Nortel systems with respect to protocols, users, and phone numbers managed within the Microsoft® Active Directory®.

MCM capacity numbers depend on the hardware platform this application runs on, and the unit used to identify the platform is SPECint.

A single MCM can support 15000 calls per hour (this is a projected value of 3000 users averaging 5 calls per hour - customers should check this with Windows Performance Monitor), per box, with a SPECint of 13.8.

Since MCM co-resides with Microsoft® Live Communications Server on different platforms, the formula for different hardware platforms is:

Number of calls per hour supported = (15000 x SPECint for a box) / 13.8

The SPECint for each box can be found at www.spec.org.

D-channel

D-channel handling interfaces are based on the Multi-purpose Serial Data Link (MSDL) used in Large Systems.

Parameter values and capacities for the CS 1000E are not yet available. The information in this section is directly applicable to the MG 1000T. It also provides a floor for CS 1000E engineering, since queue sizes and other capacities dependent on the processor will be larger in the CS 1000E.

Engineering considerations

The engineering guidelines assume normal traffic consisting of valid call processing and administrative messages. Engineering rules cannot prevent a piece of equipment on the network from malfunctioning and generating spurious messages, which overload the links. At this point the recovery mechanism becomes essential. The mechanism should be graceful, not requiring manual intervention, and should provide as much diagnostic information as possible, to help isolate the root cause of the problem.

Outgoing messages originate from the system Core Processor (CP), are passed to the D-channel handler, and travel across the appropriate link to the destination. In equilibrium, or over a relatively long period of time (on the order of several minutes), the system cannot generate messages faster than the D-channel handler can process them, than the link can transmit them, or than the destination can process them. Otherwise, messages will build up at the bottleneck and will eventually be lost. The entity with the lowest capacity will be the system bottleneck. For very short periods of time, however, one or more entities may be able to send messages at a higher rate than the system bottleneck, since buffers are available to queue the excess messages. These periods are referred to as bursts. The length of the burst and the size of the burst that can be supported depend on the sizes of the buffers.

Thus, to properly engineer a system, two areas must be considered:

- Equilibrium or steady-state performance, which requires an analysis of the CP processing capacity of the various components of the system, along with link bandwidth. The equilibrium analysis assumes 30% peakedness, which is consistent with models for the system CP.
- Burst performance, which requires an analysis of the buffer utilization of the system.

D-channel handling architecture

The D-channel handler and system exchange messages using an SRAM and interrupt scheme. To prevent any one application from tying up buffer resources, a flow control mechanism is defined at the system and D-channel handling interface level. The flow control mechanism is based on the common window mechanism, in which the number of messages outstanding in the transmit or receive direction per socket, or port, cannot exceed T(K) or R(K), respectively. In the transmit direction, for example, a message is considered outstanding from the time the SL-1 software writes it into the transmit ring until all processing of the message by the D-channel handler is completed. Currently T(K) and R(K) are both set at 30. Each application must queue messages if the flow control threshold is exceeded. Typically, the system task also has a buffer for messages.

An overload control threshold is also implemented in the incoming direction to protect the system Core Processor (CP) from excess messages. If the incoming messages on a single port exceed 200 messages in 2 seconds, the port will be locked out, and a port overload message will be printed. Manual intervention is required to clear the overloaded port. This feature prevents a single port from locking up the whole link.

Several software tasks exist on the D-channel handler. Layer 1 message processing operates at the highest priority. If the link is noisy, Layer 1 processing may starve the Layer 2 and Layer 3 processing tasks, resulting in buffer overflows. If such a problem is suspected, the Protocol Log (PLOG) should be examined. PLOG reporting is requested in LD 96, as described in *Software Input/Output: Administration* (553-3001-311).

D-channel

For interfaces including NI-2, Q-SIG, and Euro-ISDN, Layer 3 processing is also performed on the D-channel handler, thus reducing its capacity. These interfaces are referred to as R20+ interfaces. The steady state message rate allowable for D-channel messages is 29 msg/sec for R20+ interfaces.

The SL-1 software output queue for DCH messages is the Output Buffer (OTBF), which is user configurable for between 1 and 127 buffers in LD 17. This is a single system resource shared by all D-channels.

It is possible to define overload thresholds per D-channel for R20+ interfaces. The ISDN_MCNT (ISDN message count), defined in LD 17, specifies the number of ISDN Layer 3 call control messages allowed per 5-second interval. Overload control thresholds can be set per D-channel, ranging from 60 to 350 messages in a 5-second window, with a default of 300 messages. If the overload control threshold is exceeded, DCH421 is output. When the message rate exceeds the threshold for two consecutive 5-second periods, overload control is invoked and new incoming call requests are rejected by the Layer 3 protocol control in the third 5-second time interval. Layer 3 will resume accepting new calls at the end of the third time interval. This flexibility allows the user to regulate the processing required by a specific R20+ DCH port.

> ***Note:*** The default value implies no overload control, since 300 messages/5 seconds exceeds the rated capacity of 29 messages/second.

Primary Rate Interface network

Equilibrium analysis

A D-channel can be configured to support up to 383 B-channels (or 382 with a backup D-channel) on a T1 or 480 B-channels on an E1. The bandwidth available for messages is 64 kbps. Assumptions for a typical application are: 8 messages/call, 29 bytes/message, including 18 bytes of Layer 3 data and 11 bytes of Layer 2 overhead, 28 hundred call seconds (CCS)/trunk, and 180 second Average Hold Time (AHT)/call. The system capacity is derived from its call-carrying capacity for 100% incoming Primary Rate Interface (PRI) calls.

Under the traffic assumptions described above, the D-channel handler is able to support basic call processing messages for 4 D-channels under normal (steady-state) operation.

Peak analysis

When there is a link restart, STATUS messages are sent to all trunks with established calls. Since the SL-1 software task does not implement flow control on this mechanism, a burst of up to several hundred messages can be sent to the D-channel handler, exceeding flow control thresholds. When this happens, messages back up on the OTBF buffer, possibly resulting in buffer overflow, as indicated by DCH1030 messages. OTBF overflow is also possible after an initialization, since a burst of messages is sent to each D-channel in the system, and the OTBF is a shared system resource.

The system capacity is significantly higher in this scenario than in the steady state one because it is sending out D-channel messages which do not involve call processing. D-channel handling and Link capacities are also higher because, for equilibrium analysis, some capacity is reserved for peaking.

In the worst case scenario for a single D-channel, if the system sends messages at its peak rate, OTBF buffer overflow is possible. Also, once the messages are sent, a burst of responses can be expected in the incoming direction, resulting in additional congestion at the D-channel handler.

This situation also occurs when a backup D-channel becomes active, since STATUS messages are exchanged to resynchronize the link.

To reduce the possibility of this problem occurring, limit the number of B-channels supported by a D-channel, separate D-channels onto several cards so that message bursts are not being sent to ports on the same D-channel handling card after initialization, and increase the size of OTBF to the maximum value of 127.

The Status Enquiry Message Throttle is implemented. This feature applies only to system-to-system interface networks. It allows the user to configure the number of Status Enquiry messages sent within 128 msec on a per-D-channel basis. The SEMT parameter is set in LD 17 with a range between 1 and 5. The default value is 1. Since this feature provides a flow control mechanism for Status Enquiry messages, the likelihood of buffer overload is reduced.

B-channel overload

In an Automatic Call Distribution (ACD) environment in which the number of ACD agents plus the maximum ACD queue length is considerably less than the number of B-channels available for incoming calls, a burst of incoming messages may impact the performance of the D-channel handler as well as the system via the following mechanism: Calls from the CO terminate on a specified ACD queue. When the destination is busy (the destination telephone is busy or the ACD queue has reached its maximum limit of calls), the system immediately releases the call. The CO will immediately present another call to the same destination, which is released immediately by the PBX, and so on.

The B-channel Overload Control feature addresses this problem by delaying the release of an ISDN PRI call by a user-configurable time when the call encounters a busy condition. The delay in releasing the seized B-channel prevents a new call from being presented on the same B-channel, decreasing the incoming call rate. The timer BCOT is set in LD 16 with a range between 0 and 4000 msec.

ISDN Signaling Link network

In an ISDN Signaling Link (ISL) application, a modem is used to transmit ISDN signaling messages. Baud rates are user configurable at the standard RS232/RS422 rates: 300, 1200, 2400, 4800, 9600, and 19 200 bps (see Table 48 on page 298). In this case, the modem baud rate constraint can be the limiting constraint. The messages/second that can be supported by the baud rates are given below, where the values allow for 30% peakedness.

The B-channels that can be supported assume the messaging required for a typical application as described in "Equilibrium analysis" on page 295.

Table 48
ISL link capacities

Modem baud rate	Link capacity (msgs/sec)	B-channels that can be supported
300	1 input 1 output	46
1200	4 input 4 output	180
2400	7 input 7 output	316
4800	15 input 15 output	382(T1)/480(E1)
9600	29 input 29 output	382(T1)/480(E1)
19 200	58 input 58 output	382(T1)/480(E1)

For the baud rates listed in Table 48, the link will be the limiting constraint. The potential peak traffic problems described in "Peak analysis" on page 296 apply here as well, to an even greater extent because of the larger rate mismatch between the system and the system bottleneck. To minimize the risk, set the baud rate as high as possible.

Virtual Network Services network

Concepts applicable to ISL networks also apply to Virtual Network Services (VNS) networks. Up to 4000 VNS DNs (VDN) are supported.

D-channel bit rate

The following guidelines provide the basis for engineering the Network ACD (NACD)/VNS D-channel speed.

The bit rate load on the D-channel equals:

the amount of messages × the octets per message
× the number of messages per second

For example, if Facility Message burst is opened with 25 calls in the queue, then the Call Request queue size is greater than or equal to 25. The outgoing facility call request is 25 messages in one second. The incoming facility call request acknowledges 25 messages in the same second. The outgoing and incoming call requests total 50 messages.

In this example, the bit rate load on the D-channel equals:

50 messages × 70 octets × 8 bits/octet
= 28 800 bits/second

Total bandwidth of a 9600 baud modem is approximately:

9600 baud × 2
= 19 200 bits/second

With a total bandwidth of 19 200 bits/second and a bit rate load of 28 800 bits/second, the D-channel cannot handle the messaging. D-channel messaging will backlog.

If the customer is having problems networking calls during high traffic, then the D-channel may be the cause (especially if the bandwidth is less than 2800 baud). If the D-channel messaging is delayed to the point where VNS call processing gets delayed, the calls will fail to network and many PRI/VNS/DCH messages will be output at both the source and target nodes.

NACD network

A Network ACD (NACD) network is difficult to engineer, since performance depends on specific network configuration details including connectivity, routing tables, the number of nodes, the number of queues at each node, and calling patterns.

Diverting calls in NACD is controlled by Routing Tables with timers. Calls diverted by NACD can be answered by the Source ACD DN or any one of up to 20 Target ACD DNs. Each Target can have an individual timer defined, from 0 to 1800 seconds. By using ISDN D-channel messaging to queue Call

Requests at remote Target ACD DNs, voice calls are not physically diverted until an idle agent is reserved for that call at the remote Target node.

Nortel recommends that the Routing Table be designed so that Call Requests cascade to the network with the timers staggered. The node that is most likely to have available agents should have the smallest timer value. Otherwise Call Requests will flood the network, resulting in inefficient use of network and real-time resources.

An Active Target is available to accept NACD calls, while a Closed Target is closed to incoming calls. When calls in the Call Request queue exceed the Call Request Queue Size (CRQS) threshold, the status changes to Closed. A Status Exchange message is sent from the Target node to the Source ACD DNs indicating the new status. The Target ACD DN remains Closed to further network call requests until the number of calls in the queue is reduced by the Flow Control Threshold (FCTH).

Equilibrium analysis

At the source node, for each call queued to the network but not answered, 4 messages are exchanged. For each call queued to the network and answered, 11 messages are exchanged. Likewise, at the target node, a network call that is queued but not answered requires 4 messages, while a call that is queued and answered requires 11 messages. Messages average 31 bytes.

From a single D-channel perspective, the most difficult network topology is a star network in which each agent node is connected to a tandem node. All messages to the other nodes are sent across the D-channel connected to the tandem node.

As an example, consider a site with 2000 calls arriving locally during the busy hour. The timers in the Routing Table are staggered so that 1000 are answered locally without being queued to the network, 500 are answered locally after being queued to an average of two network target queues, and 500 are answered in the network after being queued to an average of four network target queues. Meanwhile, 200 Logical Call Requests arrive from the network, of which 100 calls are answered.

For this same network, assume now that the timers in the Routing Table are not staggered; instead, Logical Call Requests are broadcast to the 4 target nodes in the network as soon as calls arrive at the local node. Also assume that a total of 4000 calls arrive elsewhere in the network and are queued at local ACD DNs. Even if the calls are answered exactly where they were before, the number of messages exchanged will increase significantly:

- 1500 calls queued on 4 ACD DNs and not answered × 4 msgs/call/DN = 24 000 msgs
- 500 calls answered × 11 msgs/call = 5500 msgs
- 500 calls queued on 3 ACD DNs and not answered × 4 msgs/call/DN = 6000 msgs
- 3900 network calls queued on local DN and not answered × 4 msgs/call = 15 600 msgs
- 100 network calls answered × 11 msgs/call = 1100 msgs
- Total 52 200 msgs/hr
- (52 200 msgs/hr) ÷ (3600 secs/hr) = 14.5 msgs/sec

Peak analysis

When the CRQS threshold is reached, the target queue will broadcast messages to the source ACD DNs informing them that it will no longer accept calls. The size of this outgoing burst of messages depends on the number of source ACD DNs in the network.

Once the FCTH threshold is reached, another Status Exchange message is sent. At that point, Logical Call Request messages are sent by the Source ACD DNs. While the target queue has been closed, many calls may have queued at source ACD DNs, resulting in a burst of Logical Call Request messages once the DN becomes available.

If CRQS values are set high, many messages will be exchanged, with the network emulating a single virtual queue. If the CRQS values are lowered, fewer Call Requests will be sent across the network. However, average source delays may be increased. If FCTH levels are set too low, target nodes can bounce between Active and Closed states, resulting in network congestion and excessive real-time utilization. However, if FCTH levels are set too high, a target node may be inundated with Logical Call Request messages once it becomes available. CRQS is configurable for the range 0 to 255, while FCTH is configurable for the range 10 to 100.

Since the impact of these parameters depends on the configuration, it is not possible to make general recommendations on how to configure them. They should be determined as part of the custom network design process. Contact your local Nortel representative for network engineering services.

Impact of proper engineering of B-channels

In the NACD environment, another problem arises when insufficient B-channels are configured across the network. When an agent becomes available, an Agent Free Notification message is sent to the source node. An ISDN Call Setup message is sent from the source node to the target node. Since no B-channel is available, the agent reservation timer expires, an ISDN Cancellation Message is sent from the target node to the source node, and an ISDN Cancellation Acknowledge message is sent from the source node to the target node. At this point, the agent is still free, so the process repeats until a trunk becomes available or the target closes. This scenario results in a significant amount of message passing.

Trunk requirements under Longest Idle Agent routing

Trunk requirements are usually calculated using the NACD engineering guidelines, whereby call loading for each queue at each site is estimated and used to calculate the required number of trunks between each pair of sites. However, when Longest Idle Agent (LIA) is used as the routing criterion, load estimation becomes difficult. Assuming that any agent can take any call and that agents have equal holding time characteristics, the following procedure provides a method to estimate the number of trunks required between pairs of sites.

Assumptions

1. All agents reside in one common pool and process calls at an equal rate (in other words, they have a common average call service time).
2. An agent having the longest idle time occurs with equal probability among all of the agents during normal operation.
3. Agents appear as one large pool to incoming calls.

With these assumptions, under LIA, calls will be routed proportional to the number of active agents at each site.

Calculation steps

1 Note the number of active agents at each site (n_i) and the total number of active agents over all sites (N).

2 Calculate the proportion of active agents at each site:
$p_i = n_i/N$

3 For each incoming local call arrival stream to site i (A_i, expressed in CPH), calculate the calls routed from site i to site j:
$C_{ij} = A_i \times p_j$

4 Calculate the total calls routed (T, expressed in CPH) between each pair of sites:
$T_{ij} = T_{ji} = C_{ij} + C_{ji}$

5 Apply Erlang B to each T_{ij}, $i < j$, to get the number of required trunks between sites i and j (L_{ij}).

Erlang B requires the following parameters:

a Grade-of-Service (GoS) — probability of a blocked call (in other words, no trunk available) — taken to be 0.01

b Mean Call Service Time (usually in seconds)

c number of calls per hour (CPH)

Refer to "Trunk traffic – Erlang B with P.01 Grade-of-Service" on page 616 for values for Erlang B.

Parameter settings

The following are parameters that can be configured in LD 17 for CS 1000 D-channels. Items are listed with their input ranges, with default values shown in brackets.

1 OTBF 1 - (32) - 127: Size of output buffer for DCH

This parameter configures how many output buffers are allocated for DCH messages outgoing from the system CP to the D-channel handling card. The more that are created, the deeper the buffering. For systems with extensive D-channel messaging, such as call centers using NACD, the parameter should be set at 127. For other systems with moderate levels of D-channel messaging, OTBF should be set at the smaller of the following two quantities: Total B-channels – (30 × MSDL cards with D-channels) or 127.

For example, if a system in a standard office environment is configured with 7 T1 spans, 2 D-channels located on two different NTBK51 daughterboards, and 2 back-up D-channels, the total number of B-channels is (7 × 24) – 4 = 164. OTBF should be configured to be the smaller of 164 – (30 × 2) = 104 and 127 which is 104.

2 T200 2 - (3) - 40: Maximum time for acknowledgment of frame (units of 0.5 secs)

This timer defines how long the D-channel handler's Layer 2 LAPD will wait before it retransmits a frame. It if does not receive an acknowledgment from the far end for a given frame before this timer expires, it will retransmit a frame. Setting this value too low can cause unnecessary retransmissions. The default of 1.5 seconds is long enough for most land connections. Special connections, over radio, for instance, may require higher values.

3 T203 2 - (10) - 40: Link Idle Timer (units of seconds)

This timer defines how long the Layer 2 LAPD will wait without receiving any frames from the far end. If no frames are received for a period of T203 seconds, the Layer 2 will send a frame to the other side to check that the far end is still alive. The expiration of this timer causes the periodic "RR" or Receiver Ready to be sent across an idle link. Setting this value too low causes unnecessary traffic on an idle link. However, setting the value too high will delay the system from detecting that the far end has dropped the link and initiating the recovery process. The value should be higher than T200. It should also be coordinated with the far end so that one end does not use a small value while the other end uses a large value.

4 N200 1 - (3) - 8: Maximum Number of Retransmissions

This value defines how many times the Layer 2 will resend a frame if it does not receive an acknowledgment from the far end. Every time a frame is sent by Layer 2, it expects to receive an acknowledgment. If it does not receive the acknowledgment, it will retransmit the frame N200 times before attempting link recovery action. The default (3) is a standard number of retransmissions and is enough for a good link to accommodate occasional noise on the link. If the link is bad, increasing N200 may keep the D-channel up longer, but in general this is not recommended.

5 N201 4 - (260): Maximum Number of Octets (bytes) in the Information Field

This value defines the maximum I-frame (Info frame) size. There is no reason to reduce the number from the default value unless the system is connected to a system that does not support the 260-byte I-frame.

6 K 1 - (7): Maximum number of outstanding frames

This value defines the window size used by the Layer 2 state machine. The default value of 7 means that the Layer 2 state machine will send up to 7 frames out to the link before it stops and requires an acknowledgment for at least one of the frames. A larger window allows for more efficient transmission. Ideally, the Layer 2 will receive an acknowledgment for a message before reaching the K value so that it can send a constant stream of messages. The disadvantage of a large K value is that more frames must be retransmitted if an acknowledgment is not received. The default value of 7 should be sufficient for all applications. The K value must be the same for both sides of the link.

7 ISDN_MCNT (ISDN Message Count) 60 - (300) - 350: Layer 3 call control messages per 5-second interval

It is possible to define overload thresholds for interfaces on a per-D-channel basis. This flexibility allows the user to regulate the D-channel handler processing required by a specific R20+ DCH port. The default value of 300 messages/5 seconds is equivalent to allowing a single port to utilize the full real-time capacity of the D-channel handler. To limit the real-time utilization of a single R20+ DCH port to $(1 \div n)$ of the real-time capacity of the D-channel handler, for $n > 1$, set ISDN_MCNT to $(300 \div n) \times 1.2$, where the 1.2 factor accounts for the fact that peak periods on different ports are unlikely to occur simultaneously. For example, to limit a single port to one-third of the processing capacity of the D-channel handler, ISDN_MCNT is set to $(300 \div 3) \times 1.2 = 120$.

If the ISDN_MCNT threshold is exceeded for one 5-second period, error message DCH421 is printed. If the threshold is exceeded for two consecutive periods, incoming call requests arriving in the third 5-second interval are rejected by the D-channel handler Layer 3 software. At the end of the third 5-second interval, Layer 3 will resume accepting incoming call requests.

Serial Data Interface (SDI)

The SDI ports on the Small System Controller (SSC) cards in the Media Gateways and on the Terminal Server provide an asynchronous serial data interface to TTYs, printers, modems, and CRTs, High Speed Link (HSL) for ACD, Auxiliary Processor Link (APL) for ACD, ACD-C package displays and reports, and CDR TTYs.

Normally, in the output direction, the SDI Application will pass any character received from the system to the Layer 1 Driver to be sent out over the interface. If XON/XOFF Handling is enabled for printing, the SDI Application will buffer up to 500 characters once an XOFF is received. The system is not aware that an XOFF has been received. After the buffer is full, if further output is received, the oldest data will be discarded. Output resumes when an XON is received or 1 minute has passed since the output was halted by an XOFF. At this point, the contents in the buffer will be emptied first, followed by output from the system. If any data has been discarded, an error message will be sent.

In the input direction, every character received by the Layer 1 Driver will be passed to the SDI Application. The SDI Application will echo any input character unless it is told not to by the system. In Line Editing Mode, the SDI Application will buffer a line of up to 80 characters which can be edited before being sent to the system.

Under certain conditions, control characters can cause messages to bounce between a modem or printer and the system. To avoid these situations, configure modems in dumb mode and disable printer flow control.

The system input buffer is the TTY input buffer, which can store 512 characters. The system output buffer is the TTY output buffer, which can store 2048 characters.

Call Detail Recording records

Call Detail Recording (CDR) records are available in two formats: *FCDR=old* and *FCDR=new*. A typical record for the old format is 100 bytes long while a typical record for the new format is 213 bytes long (see Table 49). Due to the nature of the SDI interface, characters are output one at a time, resulting in 100 messages and 213 messages generated for *FCDR=old* and *FCDR=new*, respectively. Each message requires 10 bits. Based on real-time measurements, the MSDL rated capacity for processing CDR messages is 16 631 messages/second.

Table 49
Link capacities for CDR application (outgoing)

Modem baud rate	Link capacity (msg/sec) (peak)	Calls/Hour for *FCDR=old*	Call/Hour for *FCDR=new*
300	30	831	390
1200	120	3323	1560
2400	240	6646	3120
4800	480	13 292	6241
9600	960	26 585	12 481
19 200	1920	53 169	24 962
38 400	3840	106 338	49 924

Equilibrium analysis

The system capacity for messages per second is conservatively based on the assumption of 100% outgoing calls with *FCDR=new*. Typically, CDR records are not generated for 100% of the calls.

Peak analysis

Since each character is sent as a separate message, every time a CDR record is sent, a traffic peak is generated.

To prevent system buffers from building up, set the baud rate at 38 400. If a lower baud rate is chosen, assume that the CDR application will frequently be in a state of flow control. Note that this is true even if the steady state message rate is low, due to the nature of the SDI interface.

The burst sizes will be even greater if CDR is configured with queue records for incoming ACD calls.

D-channel handler engineering procedure

It is important to engineer the D-channel handler in the context of engineering the entire system. Refer to *Traffic Measurement: Formats and Output* (553-3001-450) for additional information on real-time engineering of the system. In all cases with a user configurable link rate, it is essential that the link be configured so that the rate is high enough to support steady-state requirements and some peakedness. Otherwise, the application messages will occupy system buffers, increasing the chance of buffer overflow.

Table 50 is a high-level worksheet for analysis of D-channel handling capacity. See Table 51 on page 310 through Table 54 on page 313 for the values to use in the worksheet.

Table 50
D-channel handler engineering worksheet

Port	Application	Real Time required	Peak Buffer usage outgoing	Peak Buffer usage incoming
0	______________	_________	_________	_________
1	______________	_________	_________	_________
2	______________	_________	_________	_________
3	______________	_________	_________	_________
Total		_________	_________	_________

Assuming 30% peakedness for the applications, the total real time required should be less than 2 770 000 msec. The projected real-time utilization of the D-channel handler is given by:

Real-time usage = Total Real Time Required ÷ 2 770 000

Nortel recommends that peak buffer usage be less than 60 in each direction. As the peak buffer usage increases over 60, the likelihood of an intermittent buffer-full problem increases.

The following sections provide procedures, including worksheet tables, for calculating the real time required on the D-channel handler for various applications.

In Table 50 on page 308 through Table 54 on page 313, if the calls/hour value is known, insert that value into Column A. Otherwise, follow the guidelines provided. Values in parentheses are default values. For example, the default number of calls/hr/trunk is 15.6. The value in Column E should be inserted in the Real Time Required column of Table 50, and the appropriate Peak Buffer Usage values should be inserted in the corresponding Peak Buffer Usage columns of Table 50.

DCH applications

If several applications share a D-channel, add the final real-time requirements for the applications and then enter the total in the appropriate entry in Table 51.

Table 51
Real-time requirements for D-channel applications

DCH	Calls/hr A	Msgs/call B	Msgs/hr C = A × B	Msec/msg D	Msec E = C × D
ISDN Network	trunks/DCH × calls/hr/trunk (15.6) = ______	8	______	pre-R20: 8.8 R20+: 26.5	______
NACD	NACD agents × calls/hr/agent (18.3) = ______	30	______	pre-R20: 8.8	______
NMS	NMS ports (see note) × calls/hr/port (65) = ______	10	______	pre_R20: 8.8	______
Note: For clarification of the terms "pre-R20" and "R20+," refer to "D-channel" on page 295					

The calculations described for NACD provide a simplified approximation of a "typical" NACD network. If call flows can be predicted or estimated, they can be used to develop a more accurate model using the number of messages. When this is done, the msgs/hr is computed directly, so columns A and B are not used. See "Examples" on page 313 for a detailed example of how this can be done.

If a live system is being modeled, add the "number of all incoming messages received on the D-channel" and the "number of all outgoing messages sent on the D-channel" field from a busy hour TFS009 report to derive the entry for

Column C. See *Traffic Measurement: Formats and Output* (553-3001-450) for details.

Table 52
Peak buffer requirements for D-channel applications

DCH	Outgoing	Incoming
ISDN Network	SEMT (1) × 8	SEMT (1) × 8
NACD	Source ACD DNs + 5 = ____	Network congestion level: • Low: 10 • Medium: 20 • High: 30
NMS	10	10

In the case of an ISL D-channel, ensure that the baud rate of the connection is greater than

(C msgs/hr × 29 bytes/msg × 8 bits/byte) ÷ 3600 sec/hr

where C comes from column C in Table 51 on page 310.

If the baud rate is too low to meet requirements, performance of the entire D-channel handler may be jeopardized, since 30 of the output buffers will be occupied with ISL D-channel messages and the real time spent processing these messages will increase due to additional flow control and queueing logic.

SDI applications

In the HSL analysis, include live agents, automated agents, and CallPilot agents in the agent total. This will compensate for the assumption of simple calls.

Table 53
Real-time requirements for SDI applications

SDI	calls/hr A	msgs/call B	msgs/hr C=A×B	msec/msg D	msec E=C×D
CDR	calls/hr with reports = ______	FCDR = old:100 FCDR = new: 213	______	0.05	______
HSL	agents × calls/agent/hr (18.3) = ______	5	______	8.8	______
TTY	NA	NA	15 000	0.05	______

There are no traffic reports that provide information on the number of SDI messages directly. For CDR records, determine whether CDR is enabled for incoming, outgoing, and/or internal calls. The number of incoming, outgoing, internal, and tandem calls is available from TFC001. Tandem calls are considered both incoming and outgoing. Alternatively, the number of CDR records can be counted directly.

Table 54
Peak buffer requirements for SDI applications

SDI	Outgoing	Incoming	Minimum baud rate
CDR	• 30 if baud rate is less than recommended in Table 49 on page 307	1	(msgs/hr × 10 bits/msg) ÷ (3600 sec/hr) = _____
HSL	• Messages per call — simple: 5 — medium: 10 — complex: 15	1	(msgs/hr × 20 bytes/msg × 9 bits/byte) ÷ (3600 sec/hr) = _____
TTY	10	10	

Examples

NACD network with CDR reports

Consider an NACD network with the topology given in Figure 34 on page 314. The call flow is provided, where arrows indicate where calls enter the network and where they are answered.

Each node has a single ACD DN and calls are queued to the network target DNs as soon as they arrive.

For this network, we wish to determine whether a single D-channel handler on Node B can support DCH1, DCH2, and an SDI port for CDR records on Port 0.

Since we have detailed call flow information, we can develop a messaging model for DCH1 and DCH2 (see Table 55 on page 314).

Figure 34
NACD network

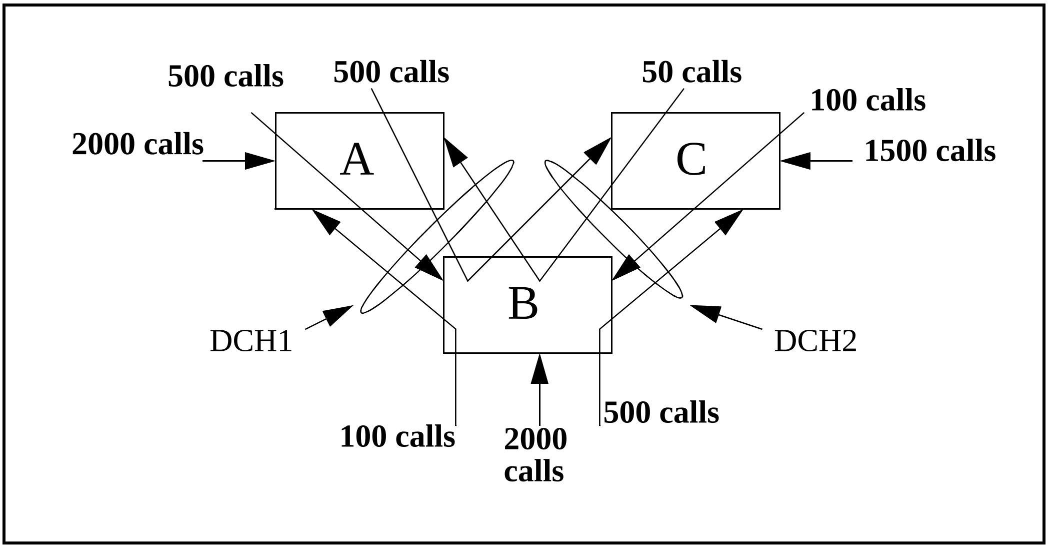


Table 55
NACD Message Model

Originating Node	Total Queued	Queued and answered	Queued but not answered	Total messages	DCH1	DCH2
Node A to Node B	3000	500	2500	15 500	x	x
Node A to Node C	3000	500	2500	15 500	x	x
Node B to Node A	2600	100	2500	11 100	x	
Node B to Node C	2600	500	2100	13 900		x
Node C to Node A	1650	50	1600	6950	x	x
Node C to Node B	1650	100	1550	7300	x	x

The DCH1 and DCH2 columns indicate whether the messages should be included in the DCH1 and DCH2 message count, respectively. For each row, multiply the entry in the "Queued and answered" column by 11 messages and multiply the entry in the "Queued but not answered" column by 4 messages. The sum of these two values is provided in the "Total messages" column. By summing the rows which should be included for DCH1 and DCH2, we derive the total messages for DCH1: 56 350 msg/hr and DCH2: 59 150 msg/hr. Note that these messages do not include the impact of CRQS and FCTH, which are beyond the scope of this analysis (see Table 51 on page 310).

Table 56
Real-time requirements for D-channel applications

DCH	calls/hr A	msgs/call B	msgs/hr C=A×B	msec/msg D	msec E=C×D
NACD DCH1	NA	NA	56 350	pre-R20: 8.8	495 880
NACD DCH2	NA	NA	59 150	pre-R20: 8.8	520 520

Assuming that no non-NACD calls are carried, Node B carries 3750 calls/hour.

Table 57
Real-time requirements for SDI applications

SDI	calls/hr A	msgs/call B	msgs/hr C=A×B	msec/ msg D	msec E=C×D
CDR	calls/hr with reports=3750	FCDR=old: 100 FCDR=new: 213	798 750 (FCDR=new)	0.05	39 938

The total D-channel handler requirements can then be computed:

Table 58
Engineering worksheet

Port	Application	Real Time required	Peak Buffer usage outgoing	Peak Buffer usage incoming
0	CDR	39 938	10	1
1	DCH-NACD	495 880	7	10
2	DCH-NACD	520 520	7	10
3				
Total		1 056 338	24	21

The projected D-channel handler utilization is 1 056 338 ÷ 2 770 000 = 38%. Assuming low network congestion, incoming and outgoing peak buffer usage are below 60, so a single D-channel handler is able to support this configuration. However, due to the potentially high messaging impact of NACD, this should be re-engineered periodically to determine whether the call volumes or call flow patterns have changed.

CallPilot engineering

Refer to *CallPilot Planning and Engineering* (553-7101-101) for engineering details. The abbreviated procedure in this chapter is for system engineering where a rough estimate of CallPilot ports (or channels) is required.

In addition to voice channels, a CallPilot allows fax and speech-recognition media. As a measure of Digital Signal Processing (DSP) power, different media types require different Multimedia Processing Unit (MPU) quantities:

- One voice channel requires one MPU.
- One fax channel requires two MPUs.
- One speech-recognition channel requires four MPUs.

A Multimedia Processing Card (MPC-8) is a credit-card sized PC card that resides in the CallPilot Server. Each MPC-8 has eight MPUs. The maximum number of MPUs in a CallPilot is 96. Any use of non-voice application will reduce the number of channels available for voice traffic.

For an IP source to access CallPilot, the codec must be set for G.711. Since a non-standard proprietary codec is used in CallPilot, a multi-rate transcoding will render the resulting voice samples with very poor quality.

The default holding time for a voice channel user is 40 seconds in the CallPilot port engineering. Another resource to be estimated in CallPilot is storage size. This requires a complicated calculation and will not be covered here. Refer to *CallPilot Planning and Engineering (*553-7101-101) for details.

Once the CCS for each type of media is calculated, sum up the total and refer to capacity tables in the NTP for the MPU requirement based on the offered CCS traffic.

For non-blocking access, provide one DSP port for each CallPilot port equipped.

Call Center

The Call Center is an ACD switch whose calls are mostly incoming, with extensive applications features such as Nortel Hospitality Integrated Voice Services. A port in the Call Center environment, either as an agent telephone or trunk, tends to be more heavily loaded than other types of applications.

System capacity requirements depend on customer application requirements, such as calls processed in a busy hour, and feature suites such as Recorded Announcement (RAN), Music, and Interactive Voice Response (IVR).

ACD

Automatic Call Distribution (ACD) is an optional feature available with the system. It is used by organizations where the calls received are for a service rather than a specific person.

For basic ACD, incoming calls are handled on a first-come, first-served basis and are distributed among the available agents. The agent that has been idle the longest is presented with the first call. This ensures an equitable distribution of incoming calls among agents.

The system is managed or supervised by supervisors who have access to the ACD information through a video display terminal. These supervisors deal with agent-customer transactions and the distribution of incoming calls among agents.

Many sophisticated control mechanisms have been built on the basic ACD features. Various packages of ACD features will have real-time impact on the system CP capacity.

ACD-C1 and C2 packages

ACD Management Reporting provides the ACD customer with timely and accurate statistics relevant to the ACD operation. These statistics form periodic printed reports and ongoing status displays so the customer can monitor changing ACD traffic loads and levels of service and implement corrective action where required.

The ACD-C1 package primarily provides status reporting of the system through a TTY terminal. To control and alter the configuration of the system, the ACD-C2 package is required; it provides the load management commands. The following is a partial list of functions of a supervisor position in the C2 package:

- Assign auto-terminating ACD trunk routes.
- Assign priority status to ACD trunks.
- Reassign ACD agent positions to other ACD DNs.
- set the timers and routes for first and second RAN.
- Define the overflow thresholds.
- Specify a night RAN route.

ACD-D package

The ACD-D system is designed to serve customers whose ACD operation requires sophisticated management reporting and load management capabilities. It has an enhanced management display, as the system is supplemented by an auxiliary data system. The system and the auxiliary processor are connected by data links through SDI ports for communications. Call processing and service management functions are split between the system and the auxiliary processor.

ACD-MAX

ACD-MAX offers a customer managerial control over the ACD operation by providing past performance reporting and current performance displays. It is connected through an SDI port to communicate with the system CP. The ACD-MAX feature makes the necessary calculations of data received from the system to produce ACD report data for current and past performance reports. Every 30 seconds, ACD-MAX takes the last 10 minutes of performance data and uses it to generate statistics for the current performance displays. The accumulated past performance report data is stored on disk every 30 minutes.

ACD-MAX calls impact capacity engineering in the real-time area only.

NACD

The majority of tasks in the engineering of Network ACD (NACD) involve the design of an NACD routing table and the engineering of overflow traffic. The process is too complex to be included here. The engineering procedure in this NTP is for single-node capacity engineering, which accounts for the real-time impact of NACD calls on a switch either as a source node or remote target node. Therefore, the overall design of a network is not in the scope of this document.

RAN and Music

The RAN trunk can be treated just like a normal trunk. The only potential capacity impact is for systems that include RAN trunks in blocking or non-blocking calculations. The calculations determine the total number of loops or card slots required.

Music Broadcast requires any Music trunk and an external music source or a Nortel Integrated Recorded Announcer card. The Integrated Recorded Announcer has the capability to provide audio input for external music. A Conference loop is not required for Music Broadcast.

Refer to "Service loops and circuits" on page 171 for more information.

Symposium Call Center

Symposium is a Host Server that interfaces through an Ethernet to enable the system to provide advanced Call Center features to users. Although Internet Protocol (IP) is used for communications, the underlying message to the system input queue is an Application Module Link (AML) message.

The customer can create simple-to-write scripts in Symposium to control processing of an arriving call that is eventually delivered to an agent queue after following various call processing rules, such as skill set of agent, call priority, and length of waiting time.

The complexity of call handling on the system call processor determines the impact of Symposium Call Center on the system. Depending on the script used, the call processing can include giving RAN, Music, and IVR, all of which require a voice-processing system such as CallPilot.

Symposium Call Center with IP phones and Virtual Trunks

When IP Phones are used as ACD agent telephones, there are certain special engineering rules. The following two additional resources must be engineered:

- Digital Signal Processor (DSP) channels (therefore, Media Cards)
- Virtual Trunks

For non-blocking access, provide one DSP port for each ACD agent configured.

Refer to "Resource calculations" on page 191 for the detailed calculations.

ELAN engineering

The Embedded Local Area Network (ELAN) subnet is designed to handle messaging traffic between the system and its applications, such as Symposium and CallPilot. It is not meant to handle functions of the customer's LAN, which carries customer application traffic.

A 64 kbps link can handle messaging traffic of over 80 000 calls. The ELAN subnet, being an Ethernet with data rate of 10/100/1000MG auto-negotiate, will not be a bottleneck in a Symposium/CallPilot configuration. However, observe the following engineering guidelines to avoid performance problems. For more detailed information, refer to *Converging the Data Network with VoIP* (553-3001-160).

- Ensure that settings on the physical interface of the system to the Ethernet are correct.
- Although no traffic engineering is required on the ELAN subnet, if the loading on the link is extremely high (for example, above 10% on the 10T-10 Mbps), collision on the Ethernet could happen. Use a sniffer to detect any performance problems. Decrease the loading on the link if it is overloaded.
- set a consistent data rate with the application.

Certain remote maintenance applications may utilize the ELAN subnet to access the system from a remote location. Ensure that no other customer LAN traffic is introduced.

HSP LAN Engineering

The High Speed Pipe (HSP) is used to connect two Call Server CPUs in a Campus Redundant environment. The HSP is used to shadow disk and memory information from one CPU to another and to provide heartbeat information (including health information) from one CPU to the other.

Due to the mission critical role that the HSP provides between the active and redundant Call Server, the HSP must be carefully engineered. This section describes the rules governing the engineering of the HSP. For a more detailed description of how the Campus Redundancy feature works, refer to *Communication Server 1000: System Redundancy* (553-3001-307).

The HSP may be connected using a crossover cable directly between the two CPUs, or using networking equipment. When using networking equipment to connect, the HSP ports are assigned unique IP addresses.

The following are recommendations and rules for configuring the HSP network and network interfaces of two Call Server CPUs using network equipment:

- The HSP must be connected through a cross-over cable or by a dedicated VLAN through switches.
- The HSP must be in its own IP subnet. It cannot be combined with the ELAN subnet.
- The minimum throughput of the HSP must be 100 Mbps. Therefore, the HSP port must be 100 Mbps and full duplex. This must be confirmed using the **STAT HSP** command in LD 137 after the equipment is operational. This must also be verified on the network equipment to which the HSP is attached.
- The network switches must be capable of port mapping to 802.1p/Q.
- When running the HSP across network equipment, the HSP must be isolated in its own VLAN. Do not include other traffic in this VLAN. This VLAN must be given higher VLAN priority than any other traffic on the network, except for network control traffic (network control traffic is the traffic necessary to keep the network operational). The VLAN must be 802.1p/Q-capable and must be set to a very high setting so as not to starve the HSP. Nortel strongly recommends 802.1p Level 7 (Network Control and OAM).
- When using third-party vendor network equipment that has not been validated by Nortel, a pre-test of the network must be performed. This test includes mixed traffic going across the networks in different VLANs. The network specifications should meet the round trip delay and packet loss requirements.
- The round trip delay of the HSP VLAN must be less than 30 msec and the packet loss of the HSP VLAN must be below .1 % packet loss.
- The HSP port on the CP PIV is set to auto-negotiate the link speed and duplex. Therefore, the network equipment to which the CP PIV is attached must also use auto-negotiate. Verify that both the CP PIV and the network equipment speed and duplex are a match. The CP PII does not auto-negotiate; instead, it is fixed to 100 Mbps and full-duplex. Verify that both the CP PII and the network equipment speed and duplex are a match.

- Nortel recommends that MLT (Multi Link Trunking) be used across the enterprise IP network for the Campus Redundancy configuration.
- Cabling for the HSP port on the CP PII must be at least Cat 5 cabling. Cabling for the HSP port on the CP PIV must be at least Cat 5e when running the link speed at 1 Gbps.

CAUTION

Duplex mismatches occur in the LAN environment when one side is set to Auto Negotiate and the other is hard configured.

The Auto Negotiate side adapts only to the speed setting of the fixed side. For duplex operations, the Auto Negotiate side sets itself to half-duplex mode. If the forced side is full-duplex, a duplex mismatch occurs.

Switching Equipment

Layer 2 switching equipment

The following equipment supports MLT (Multi Link Trunking), port based VLANs, and 802.1P priority configuration and is recommended for the HSP application.

- 325-24T - Layer 2 VLANs, MLT, 802.3ad
- 325-24G - Layer 2 VLANs, MLT, 802.3ad
- 425-24T - Layer 2 VLANs, MLT, DMLT, 802.3ad
- 425-48T - Layer 2 VLANs, MLT, DMLT, 802.3ad
- 460-24T-PWR - Layer 2 VLANs, MLT, DMLT, , 802.3ad, 802.3af PoE
- 470-24T - Layer 2 VLANs, MLT, DMLT, 802.3ad
- 470-48T - Layer 2 VLANs, MLT, DMLT, 802.3ad
- 5510-24T - Layer 2 VLANs, MLT, DMLT, L3 interVLAN routing
- 5510-48T - Layer 2 VLANs, MLT, DMLT, L3 interVLAN routing

- 5520-24T - Layer 2 VLANs, MLT, DMLT, L3 interVLAN routing, 802.3af PoE
- 5520-48T - Layer 2 VLANs, MLT, DMLT, L3 interVLAN routing, 802.3af PoE
- 8300 - Layer 2 VLANs, MLT, DMLT, L3 interVLAN routing
- 8600 - Layer 2 VLANs, MLT, DMLT, SMLT, 802.3ad, L3 interVLAN routing

Third-party vendor switching equipment

The HSP supports all vendor switching equipment. The following third-party equipment has been tested:

- CISCO WS-3750G 24T-E GE ENH MULTILAYER CAYALYST (Layer 2 VLAN mode)
- 3C17203-3COM US/ 3COM 24-PORT 10/100TX SWITCH W/2
- 3COM 3C17304-US 3COM SS3 SWITCH 4228G 28PORTS EN
- 13240 EXTREME SUMMIT 200-24 SWITCH - 24 PORTS

> ***Note:*** The HSP cannot be routed, and as a result, it cannot be extended through a Layer 3 router unless that device supports a method of providing Layer 2 end-to-end connectivity (Example: Layer 2 tunneling). Therefore, when passing through routing equipment, the HSP must remain in the same subnet from one Call Server to the other (Example: tunneling the HSP over the network).

HSP IP address configuration

The configuration of HSP IP addressing can be performed after the installation process if the default IP addresses are not appropriate for the customer network. Nortel strongly recommends allocation of a network IP address within a customer address space if the network is not dark fiber driven by BayStack470 switches.

CLASS network engineering rules

In a single-group network system, the network internal blocking is determined by the concentration ratio of equipped ports on Intelligent Peripheral Equipment and the number of interfaced loops or superloops. Depending on traffic engineering, a non-blocking network is achievable.

Feature operation

A call originated from Telephone A (or Trunk A) seeks to terminate on a CLASS Telephone B. When Telephone B starts to ring, Telephone A hears ringback. A unit in CLASS Modem (CMOD) is assigned to collect the originator's CND information and waits for the CND delivery interval. After the first ring at Telephone B, a silence period (deliver interval) ensues, and the CMOD unit begins to deliver CND information to the CLASS telephone.

The CND information of a traffic source (Telephone A) is a system information, which is obtained by the system when a call is originated. During the two-second ringing period of the CLASS Telephone B, Telephone A's CND is delivered to CMOD by SSD messages (using signaling channel only). When the CND information is sent from CMOD to CLASS Telephone B, it is delivered through a voice path during the four-second silence cycle of Telephone B. The CMOD unit is held for a duration of six seconds.

The system delivers SSD messages containing CND information to CMOD and then sends it to Telephone B during the delivery interval through a voice path.

Table 59 is the CMOD capacity table. It provides the number of CMOD units required to serve a given number of CLASS telephones with the desired GoS (P.001). The required number of CMOD units should have a capacity range whose upper limit is greater than the number of CLASS telephones equipped in a given configuration.

Table 59
CMOD Unit Capacity (Part 1 of 2)

CMOD Unit	CLASS Telephone	CMOD Unit	CLASS Telephone
1	1-2	33	2339-2436
2	3-7	34	2437-2535
3	8-27	35	2536-2635
4	28-59	36	2637-2735
5	60-100	37	2736-2835
6	101-150	38	2836-2936
7	151-206	39	2937-3037
8	207-267	40	3038-3139
9	268-332	41	3140-3241
10	333-401	42	3242-3344
11	402-473	43	3345-3447
12	474-548	44	3448-3550
13	549-625	45	3551-3653
14	626-704	46	3654-3757
15	705-785	47	3768-3861
16	786-868	48	3862-3966
17	869-953	49	3967-4070
18	954-1039	50	4071-4175
19	1040-1126	51	4176-4281
20	1127-1214	52	4282-4386
21	1215-1298	53	4387-4492

Table 59
CMOD Unit Capacity (Part 2 of 2)

CMOD Unit	CLASS Telephone	CMOD Unit	CLASS Telephone
22	1299-1388	54	4493-4598
23	1389-1480	55	4599-4704
24	1481-1572	56	4705-4811
25	1573-1665	57	4812-4918
26	1666-1759	58	4919-5025
27	1760-1854	59	5026-5132
28	1855-1949	60	5133-5239
29	1950-2046	61	5240-5347
30	2047-2142	62	5348-5455
31	2143-2240	63	5456-5563
32	2241-2338	64	5564-5671

Guidelines for non-Call Center applications

In a non-call center application, there is no significant number of agent telephones. Therefore, no conversion of agent telephones to regular telephones is needed.

Engineering rule (no reconfiguration required)

The following engineering rule should be followed to avoid the need to reconfigure a switch to accommodate the CLASS feature: Provide the number of CMOD units serving all CLASS telephones in the system based on the capacity table (see Table 59).

Guidelines for Call Center applications

Engineering rules (no reconfiguration required)

Follow these engineering rules to avoid the need to reconfigure a switch to accommodate the CLASS feature for a call center environment:

1 Convert agent telephones to regular telephones:

1 agent CLASS telephone = 4 telephones (called equivalent telephones)

2 Sum up the total number of regular CLASS telephones and equivalent CLASS telephones and find the number of CMOD units required based on the capacity table (see Table 59 on page 326).

Configuration parameters

Design parameters are constraints on the system established by design decisions and enforced by software checks. Defaults are provided in the factory-installed database. However, some parameter values must be set manually, through the OA&M interface, to reflect the actual needs of the customer's application.

For guidelines on how to determine appropriate parameter values for call registers, I/O buffers, and so on, see "Design parameters" on page 133 and "Memory engineering" on page 147.

Assigning loops and card slots in the CS 1000E

Contents

This section contains information on the following topics:

Introduction

Calculating the number and assignment of cards and, relatedly, Media Gateways is an iterative procedure, because of specific capacity and usage requirements.

In a CS 1000E system, Digital Signal Processor (DSP), Digitone receiver (DTR), Tone and Digit Switch (TDS), and other services are provided by circuit cards such as Media Cards and the Small System Controller (SSC). These resources are available only to the MG 1000E (with optional Expander) in which the circuit cards reside. Other services, such as Conference, are available as system resources but require MG 1000E-specific DSP resources in order to access them.

"System capacities" on page 145 and "Resource calculations" on page 191 describe the theoretical, traffic-based calculations used by NNEC to estimate the required number of Media Cards and MG 1000Es. This chapter describes the steps to allocate the cards to specific MG 1000Es. The process may result in an increase in the required number of Media Cards and MG 1000Es.

Note on terminology

Each MG 1000E can be connected to an optional MG 1000E Expander in order to increase the number of card slots available. In this chapter, the term *MG 1000E* includes the optional MG 1000E Expander, if equipped.

Loops and superloops

A fully expanded CS 1000E system provides a maximum of 256 loops or 64 superloops. Each superloop must be defined on a loop number that is a multiple of 4.

A superloop can be configured to include two MG 1000Es. In such a case, the first MG 1000E is referred to as shelf 0 and the second as shelf 1.

A maximum of 1024 TNs (= $2 \times 16 \times 32$) from two MG 1000Es can be associated with a superloop. Each superloop provides 120 timeslots.

Virtual superloops

There are no physical timeslots on MG 1000Es. Timeslots are defined within virtual superloops that benefit from the non-blocking timeslot architecture used by IP Phones and Virtual Trunks.

The superloop is layered into 16 banks of virtual superloops interfacing the 16 card slots in the two MG 1000Es. This expands the superloop's 120 timeslots to 1920 timeslots (= 16×120) to service a maximum of 1024 TNs in the address space. MG 1000Es are therefore non-blocking with respect to timeslots.

Internally, a card number separates the banks of software timeslots. Since a superloop is associated with 16 cards, each card is associated with one virtual superloop.

The network-level circuits, such as Conference and Tones, use additional loops outside of this address space. They also use DSPs from within the non-blocking superloops.

VXCT loops

Virtual Tone and Conference Circuits (VXCT) allow tone and conference services to be configured within each MG 1000E. Each VXCT consists of two loops and must start with an even loop number. If there is more than one VXCT defined for a specific MG 1000E, the VXCTs must occupy contiguous double loops. Nortel recommends that VXCT loop numbering start from a number high enough to leave room for all possible MG 1000E superloops. For example, if an MG 1000E has two VXCTs, they can be configured as loops 60 and 62.

Card slot usage and requirements

Table 60 summarizes the physical and logical card slots available in the MG 1000E.

Table 60
Card slots in the MG 1000E (Part 1 of 2)

Slot number		Used for	Comment
Physical	**Logical**		
MG 1000E			
0	0	SSC	Dedicated card slot
1–4	1–4	• Media Cards • Digital line cards • Analog line cards • Analog trunk cards • Application cards	
n/a	5–6	n/a	Not supported

Table 60
Card slots in the MG 1000E (Part 2 of 2)

Slot number		Used for	Comment
Physical	**Logical**		
MG 1000E Expander			
7–10	7–10	• Media Cards • Digital line cards • Analog line cards • Analog trunk cards • Application cards	
Virtual			
n/a	14	DTRs (maximum: 8)	Required if any analog terminals or trunks are equipped in the MG 1000E. (See Note.)
n/a	15	DTRs (maximum: 8)	
n/a	15	MF tone detectors (maximum: 4)	Must be provided on each MG 1000E that requires tone-based signaling.
Note: If DTRs are configured in any other card slot, a receiver hardware pack must be equipped in the slot.			

Assigning loops and cards in the CS 1000E

MG 1000Es are non-blocking with respect to timeslots (see "Virtual superloops" on page 330). Blocking can occur only if an MG 1000E is configured with fewer DSP ports than the line or trunk ports require.

The following rules and guidelines describe methods to balance constraints and usage requirements. Use these guidelines to develop a detailed card slot and loop assignment plan.

Rules and guidelines

1 Place the SSC card in slot 0 of each MG 1000E.

2 There must be at least one Media Card in each MG 1000E.

> **IMPORTANT!**
>
> DSP resources cannot be shared between MG 1000Es. Therefore, each MG 1000E must contain sufficient Media Cards to provide the DSP resources required by the equipment configured in that MG 1000E.

3 There must be at least one TDS loop in each MG 1000E.

4 Allocate the users and Media Cards for dedicated DSPs first, then fill remaining empty slots in MG 1000Es with other IPE cards.

Note: There is no way to reserve DSP resources for dedicated usage (such as Conference). If a system has higher than expected call rates for standard telephones, these standard telephones can effectively hijack DSP resources required for dedicated functions. Therefore, in a system with high call rates for standard telephones, place dedicated and standard resources in different MG 1000Es.

Provision resources in the following order:

a Conference (p. 333)

b TDS (p. 335)

c Broadcast circuits (p. 335)

d Other service circuits (p. 337)

e TDM telephones and TDM agents (p. 338)

f Consoles (p. 338)

g Standard telephones (p. 338)

Conference

Each MG 1000E provides up to 64 conference circuits (ports), which can be used to form conferences of up to 6 parties each. There are 32 conference circuits (2 loops) on the SSC card and another 32 conference circuits (2 loops) on the dual-port IP daughterboard. Users can configure from 0 to 4 conference loops on each MG 1000E, with each loop providing 16 conference circuits.

The conference circuits are available to all MG 1000Es in the system. Calls are assigned to conference circuits on a "round robin" basis. Each conference circuit is accessed through a DSP port in the MG 1000E in which the conference loop is defined. In addition, the device using the service may require another DSP in order to reach the conference port (see "DSP ports for Conference" on page 211).

For non-blocking access, provide an equal number of DSP ports and conference ports. In other words, provide one 32-port Media Card for every pair of defined conference loops.

> ***Note:*** If the SSC card in the MG 1000E is equipped with a single-port IP daughterboard, do not define more than three conference loops for that MG 1000E.

MG 1000E and Media Card calculations for Conference

1 Calculate the number of MG 1000Es required for Conference based on the number of conference circuits needed, in multiples of 60:

Number of MG 1000Es = ROUNDUP(Number of conference circuits ÷ 60)

2 Calculate the number of Media Cards required for Conference based on the number of conference circuits needed, in multiples of 32:

Number of Media Cards = ROUNDUP(Number of conference circuits ÷ 32)

Examples

1 30 conference circuits are needed:

— One MG 1000E has Conference configured. All other MG 1000Es do not have conference circuits provisioned.

— The MG 1000E with Conference requires one Media Card to support the service.

2 33 conference circuits are needed:

- One MG 1000E has Conference configured. All other MG 1000Es do not have conference circuits provisioned.
- The MG 1000E with Conference requires two Media Cards to support the service.

3 100 conference circuits are needed:

- Two MG 1000Es have Conference configured. All other MG 1000Es do not have conference circuits provisioned.
- Each MG 1000E with Conference requires two Media Cards to support the service.

TDS

A minimum of one TDS loop is required in each MG 1000E. The TDS circuits are provided by the MG 1000E's SSC card. If additional TDS circuits are required in any MG 1000E, a second TDS loop can be configured in it.

When a VXCT card is provisioned in order to provide additional conference ports, two additional TDS loops are automatically provisioned as well. However, these two TDS loops are disabled."

Broadcast circuits

Music and Recorded Announcement (RAN) are broadcast circuits. One channel can support many listeners. Each listener needs one DSP port.

In order to maximize the number of simultaneous connections to a Nortel Integrated Recorded Announcer card in one MG 1000E shelf of a superloop, use all the timeslots for the superloop for that card. The software "steals" the timeslots from the other shelf of the superloop, provided the equivalent card slot in the second MG 1000E is not used. Table 61 illustrates the strategy.

Table 61
Example of timeslot sharing in a superloop

MG 1000E 0				MG 1000E 1			
l	**s**	**c**	**Card**	**l**	**s**	**c**	**Card**
0	0	1	Media Card for Conference	0	1	1	[Available for use.]
0	0	2	Media Card for Conference	0	1	2	[Available for use.]
0	0	3	Integrated Recorded Announcer card	0	1	3	[Must be left empty to avoid conflict with Integrated Recorded Announcer card.]
0	0	4	Media Card for RAN/Music	0	1	4	[Available for use.]
0	0	7	Media Card for RAN/Music	0	1	7	[Available for use.]
0	0	8	Media Card for RAN/Music	0	1	8	[Available for use.]
0	0	9	Media Card for RAN/Music	0	1	9	[Available for use.]
0	0	10	[Leave empty — all DSPs in this MG 1000E are allocated to the conference and broadcast circuits, so there is no room for TDM devices.]	0	1	10	[Available for use.]
Legend: l = loop (superloop), s = shelf, c = card							

An alternative strategy is to use just one MG 1000E on a superloop when broadcast circuits are required.

Integrated Recorded Announcer card calculations

Since many listeners can be connected to a single source channel, it is possible that one or two sources on a broadcast source (Recorded Announcer) card could use all of the 120 timeslots available. No other sources could be used on that card.

Two Licenses are relevant for broadcast services:

- RAN CON = the maximum number of simultaneous RAN listeners in a system
- MUS CON = the maximum number of simultaneous music listeners in a system

When (RAN CON + MUS CON) > 120, more than one card is required for the music and RAN source. The following calculation provides the minimum number of cards required:

Number of cards = ROUNDUP[(RAN CON + MUS CON) ÷ 120]

For Recorded Announcer cards, the number of ports being ordered is known. Assuming that port usage and connection load is spread evenly across the Recorded Announcer cards, the calculation can be recast to perform the following check:

If [(RAN CON + MUS CON) ÷ Number of ports] <= 120, then there are sufficient Recorded Announcer cards to support the broadcast functions in the system.

MG 1000E and Media Card calculations for broadcast circuits

Since each Recorded Announcer card can broadcast to up to 120 listeners, each card requires a maximum of four 32-port Media Cards for all music or RAN source channels for that card. Each MG 1000E can support a single fully used music/RAN source card (1 broadcast source card + 4 Media Cards to support it).

- If (RAN CON + MUS CON) <= 32, allocate 1 Media Card and all Recorded Announcer cards to the same MG 1000E.
- If 32 < (RAN CON + MUS CON) <= 120, allocate 4 Media Cards + 1 Recorded Announcer card to the same MG 1000E.

Other service circuits

The list of other service circuits is extensive. It includes, amongst others, cards such as Nortel Integrated applications, CallPilot, and analog trunks.

Provide one DSP port for each channel of the service circuits.

TDM telephones and TDM agents

Provide one DSP port for each TDM telephone or TDM agent. Each XDLC card supports up to 16 TNs. (See also "Non-blocking access for ACD" on page 341.)

Consoles

Each M2250 attendant console and PC Console requires two TNs (originating and terminating) on an XDLC card and one Aux TN (for supervisor function). Nortel also recommends two power TNs per console.

DSPs are used when a call is active on an Attendant loop key. Each side (originating and terminating) requires one DSP, for a total of two DSPs per active/held call on the console.

Queued calls (ICI key indicators) do not consume DSP resources until the Attendant answers the call on a loop key.

DSP calculations

For standard access, provide 4 DSPs per console.

For dedicated DSPs, provide 12 DSPs per console (2×6 loop keys).

Standard telephones

Standard telephones are the average line users configured with a standard configuration.

1 Using a rule of thumb of five telephones per unallocated DSP, distribute line cards to the MG 1000Es with empty slots and unused DSPs.

The rule of thumb is derived as follows:

— A Media Card with 32 DSPs supports 794 CCS. This approximates to 24.8 CCS per DSP ($794 \div 32$).

— The default value for average user traffic is 5 CCS. At 5 CCS per standard user, 24.8 CCS per DSP translates to 5 telephones per DSP.

2 Using a rule of thumb of one Media Card per seven line cards, fill empty MG 1000Es with the remaining line cards and their required Media Cards.

The rule of thumb assumes average traffic of less than 7 CCS per telephone. This is derived as follows:

— There are a total of 8 card slots available in each MG 1000E.

— If 1 card slot is used by a Media Card, a maximum of 7 line cards, or 112 telephones (7 × 16 ports), can be added to the MG 1000E.

— A Media Card with 32 DSPs supports 794 CCS. This is the traffic capacity of this particular MG 1000E.

— A capacity limit of 794 CCS means each telephone must generate less than 7 CCS, on average (794 ÷ 112).

For average traffic of more than 7 CCS per telephone, use Table 62 to determine the number of Media Cards and telephones that can be assigned to an MG 1000E.

Table 62
Maximum number of Media Cards, line cards, and telephones in an MG 1000E

CCS per telephone	Media Cards	Line cards	Telephones*
<= 7.0	1	7	112
<= 8.0	1	6	96
<= 10.0	1	5	80
<= 18.9	2	6	96
<= 22.8	2	5	80
<= 28.5	2	4	64
<= 36.0	3	5	80
*Number of telephones = Number of line cards × 16 ports			

3 Use a similar rule to add trunk cards (XUT) and their required Media Cards. See Table 63.

Table 63
Maximum number of Media Cards, trunk cards, and trunks in an MG 1000E

CCS per telephone	Media Cards	Trunk cards	Trunks*
<= 14.2	1	7	56
<= 36.0	2	6	48
*Number of trunks = Number of trunk cards × 8 ports			

4 To mix line and trunk cards in an MG 1000E, calculate the total CCS for the number of lines and trunks. Then use Table 64 to identify the number of Media Cards required to support that CCS rate.

Table 64
Traffic capacity of Media Cards (Erlang B at P.01)

Total CCS	Number of Media Cards	Number of DSPs
794	1	32
1822	2	64
2891	3	96

CLASS cards

CLASS cards must be placed in the same MG 1000E as the telephones that use the modem ports on the CLASS cards. Therefore, CLASS cards do not consume DSP resources.

The telephones that use the CLASS cards do require DSP resources. The rules for allocating standard telephones apply.

Non-blocking access for ACD

Table 65 describes two alternative recommended configurations to provide non-blocking ACD access to DSP ports. Typically, 33 CCS per agent telephone is engineered. However, in a non-blocking configuration, up to 36 CCS per agent is allowed.

Table 65
Number of Media Cards, line cards, and ACD agents per superloop

Total number of agents*	MG 1000E (shelf 0)			MG 1000E (shelf 1)		
	Media Cards	Line cards	Agents*	Media Cards	Line cards	Agents*
128	2	4	64	2	4	64
160	3	5	80	3	5	80
*Number of agents = Number of digital line cards × 16 ports; CCS per agent: 33–36						

Preparing the final card slot assignment plan

Prepare a final card slot assignment plan as follows:

1 Count the inventory of cards and MG 1000Es developed in accordance with this chapter.

2 Go back to the NNEC theoretical calculations and increment the order requirements to match the modified configuration.

3 Produce the final NNEC configuration report. NNEC output includes the following:

— card locations

— DSP allocations (where Media Card utilization is less than 100%)

— which MG 1000Es must have conference circuits provisioned

— which MG 1000Es must not have conference circuits provisioned

Provisioning

Contents

This section contains information on the following topics:

Introduction

This section provides a high-level overview of the steps required to determine general equipment requirements. Consult your Nortel representative and use a configuration tool, such as NNEC, to fully engineer a system.

IMPORTANT!

The values used in the examples in this chapter are for illustrative purposes only, and should not be interpreted as limits of the system capacity. The values must be adjusted to suit the application of a particular system.

Step 1: Define and forecast growth

Forecast the number of telephones required at two-year and five-year intervals.

The customer determines the number of telephones required when the system is placed in service (cutover). If the customer is unable to provide a two-year and five-year growth forecast, then use an estimate of annual personnel growth in percent to estimate the number of telephones required at the two-year and five-year intervals.

Example

A customer has 500 employees and needs 275 telephones to meet the system cutover. The customer projects an annual increase of 5% of employees based on future business expansion. The employee growth forecast is:

- 500 employees × 0.05 (percent growth) = 25 additional employees at 1 year
- 525 employees × 0.05 = 27 additional employees at 2 years
- 552 employees × 0.05 = 28 additional employees at 3 years
- 580 employees × 0.05 = 29 additional employees at 4 years
- 609 employees × 0.05 = 31 additional employees at 5 years
- 640 employees × 0.05 = 32 additional employees at 6 years

The ratio of telephones to employees is 275 ÷ 500 = 0.55.

To determine the number of telephones required from cutover through a five-year interval, multiply the number of employees required at each of the time periods by the ratio of telephones to employees (0.55).

- 500 employees × 0.55 = 275 telephones required at cutover
- 525 employees × 0.55 = 289 telephones required at 1 year
- 552 employees × 0.55 = 304 telephones required at 2 years
- 580 employees × 0.55 = 319 telephones required at 3 years
- 609 employees × 0.55 = 335 telephones required at 4 years
- 640 employees × 0.55 = 352 telephones required at 5 years

This customer requires 275 telephones at cutover, 304 telephones at two years, and 352 telephones at five years.

Each DN assigned to a telephone requires a TN. Determine the number of TNs required for each customer. Perform this calculation for cutover, two-year, and five-year intervals.

Step 2: Estimate CCS per terminal

Estimate the station and trunk centi-call seconds (CCS) per terminal (CCS/T) using any one of the following methods:

1 Comparative method

2 Manual calculation

3 Default method

Comparative method

Select three existing systems that have an historical record of traffic study data. The criteria for choosing comparative systems are:

1 Similar line size (+25%)

2 Similar business (such as bank, hospital, insurance, manufacturing)

3 Similar locality (urban or rural)

Calculate the average station, trunk, and intra-system CCS/T for the selected systems. Apply these averages to calculate trunk requirements for the system being provisioned.

Manual calculation

Normally, the customer can estimate the number of trunks required at cutover and specify the Grade-of-Service (GoS) to be maintained at two-year and five-year periods (see Table 66 on page 347).

Use an appropriate trunking table (see “Reference tables” on page 615) to obtain estimated trunk group usage for the number of trunks. Divide the number of lines that are accessing the group at cutover into the estimated usage. The result is the CCS/T, which can be used to estimate trunk requirements.

Table 66 provides an example of the manual calculation.

Table 66
Example of manual calculation of CCS/T

Traffic source	Cutover (CCS)		Two years (CCS)		Five years (CCS)	
Line	275 × 6.2 =	1705	304 × 6.2 =	1885	352 × 6.2 =	2183
Trunk	275 × 4.1 =	1128	304 × 4.1 =	1247	352 × 4.1 =	1444
Subtotal		2833		3132		3627
Console		30		30		30
Total system load		2863		3162		3657
Note: Line CCS/T = 6.2; Trunk CCS/T = 4.1; two consoles = 30 CCS.						

Repeat this method for each trunk group in the system, with the exception of small special services trunk groups (such as TIE, WATS, and FX trunks). Normally, customers will tolerate a lesser GoS on these trunk groups.

Default method

Studies conducted estimate that the average line CCS/T is never greater than 5.5 in 90% of all businesses. If attempts to calculate the CCS/T using the comparative method or the manual calculation are not successful, the default of 5.5 line CCS/T can be used.

Determine the network line usage by multiplying the number of lines by 5.5 CCS/T. Then multiply the total by 2 to incorporate the trunk CCS/T. However, this method double-counts the intra-CCS/T, resulting in over-provisioning if the intra-CCS/T is high. Also, this method is not able to forecast individual trunk groups. The trunk and intra-CCS/T are forecast as a group total.

Step 3: Calculate number of trunks required

Once the trunk CCS/T is known and a GoS has been specified by the customer, determine the number of trunks required per trunk group to meet cutover, two-year, and five-year requirements. The following example demonstrates the method.

Example

The customer requires a Poisson 1% blocking GoS (see "Trunk traffic – Poisson 1% blocking" on page 618). The estimated trunk CCS/T is 1.14 for a DID trunk group. Determine the total trunk CCS by multiplying the number of lines by the trunk CCS/T for cutover, two-year, and five-year intervals:

Cutover	275 (lines) × 1.14 (trunk CCS/T) =	313.5 CCS
Two-year	304 (lines) × 1.14 (trunk CCS/T) =	346.56 CCS
Five-year	352 (lines) × 1.14 (trunk CCS/T) =	401.28 CCS

Use "Trunk traffic – Poisson 1% blocking" on page 618 to determine the quantity of trunks required to meet the trunk CCS at cutover, two-year, and five-year intervals. In this case:

- 17 DID trunks are required at cutover
- 18 DID trunks are required in two years
- 21 DID trunk are required in five years

Note: For trunk traffic greater than 4427 CCS, allow 29.5 CCS/T.

Step 4: Calculate line, trunk, and console load

Calculate the loads for the CS 1000E and MG 1000T separately.

CS 1000E

Line load

Calculate line load by multiplying the total number of TNs by the line CCS/T. The number of TNs is determined as follows:

- one TN for every DN assigned to one or more single-line telephones
- one TN for every multi-line telephone without data option
- two TNs for every multi-line telephone with data option

Trunk load

The number of Virtual Trunks to provision is calculated by the ordering and configuration tool as part of the Media Card provisioning calculation. See ”Media Card and Virtual Trunk worksheet” on page 353 for the manual calculation.

Console load

Calculate console load by multiplying the number of consoles by 30 CCS per console.

MG 1000T

Trunk load

Calculate trunk load by multiplying the total number of single- and multi-line TNs that have access to the trunk route by the CCS/T per trunk route.

Step 5: Calculate Digitone receiver requirements

Once station and trunk requirements have been determined for the complete system, calculate the Digitone receiver (DTR) requirements.

See “DTR” on page 173 for information about the DTR resources provided by the NTDK20 Small System Controller (SSC) card and optional, additional XDTR cards.

In the CS 1000E, DTRs are not system-wide resources. They support only the telephones and trunks in the MG 1000E in which they reside. See “DTR” on page 173 for the calculations to determine overall DTR traffic and refer to reference tables “Digitone receiver requirements – Model 1” on page 622 through “Digitone receiver requirements – Model 4” on page 625 to estimate overall system requirements.

The actual provisioning of additional DTR resources will depend on the number of Media Gateways in the system, and the distribution of line and trunk cards within them.

The models in reference tables "Digitone receiver requirements – Model 1" on page 622 through "Digitone receiver requirements – Model 4" on page 625 are based on some common PBX traffic measurements.

Model 1

"Digitone receiver requirements – Model 1" on page 622 is based on the following factors:

- 33% intraoffice calls, 33% incoming calls, and 33% outgoing calls
- 1.5% dial tone delay GoS
- no Digitone DID trunks or incoming Digitone TIE trunks

Model 2

"Digitone receiver requirements – Model 2" on page 623 is based on the following factors:

- the same traffic pattern as Model 1
- Digitone DID trunks or incoming Digitone TIE trunks
- Poisson 0.1% blockage GoS

Model 3

"Digitone receiver requirements – Model 3" on page 624 is based on the following factors:

- 15% intraoffice calls, 28% incoming calls, and 56% outgoing calls
- 1.5% dial tone delay GoS
- no Digitone DID trunks or incoming Digitone TIE trunks

Model 4

"Digitone receiver requirements – Model 4" on page 625 is based on the following factors:

- the same traffic pattern as Model 3
- Digitone DID trunks or incoming Digitone TIE trunks
- Poisson 0.1% blockage GoS

Step 6: Calculate total system load

Total the line, trunk, console, and DTR load for each customer to get the total load figure for cutover, two-year, and five-year intervals.

Perform the calculations separately for the CS 1000E and MG 1000T.

Step 7: Calculate the number of IPE cards required

Using the results of previous calculations for growth forecast and the number of DTRs, calculate the number of IPE cards required. Divide the number of digital telephone TNs, analog (500/2500-type) TNs, and trunk TNs by the number of TN assignments for each card. Round up each calculation to the next integer, then total the number of cards required.

Perform the calculations separately for cutover, two-year, and five-year intervals.

Step 8: Calculate the number of Media Cards required

"Media Card and Virtual Trunk worksheet" on page 353 provides a theoretical, traffic-based calculation for the number of Media Cards required in the system. This is the method followed by the ordering and configuration tool. The results provide a starting point for provisioning. Refer to "Assigning loops and card slots in the CS 1000E" on page 329 for additional rules and tips to distribute the Media Cards amongst the Media Gateways, in order to determine final Media Card requirements.

Step 9: Calculate the number of Signaling Servers required

The ordering and configuration tool calculates the number of Signaling Servers required. Refer to "Signaling Server algorithm" on page 218 for a description of the calculation method. See also "Manual adjustment of Signaling Server requirements" on page 254 for tips on avoiding over-provisioning.

Step 10: Provision conference/TDS loops

The SSC card provides Conference/TDS functions. Refer to “Conference” on page 333 and “TDS” on page 335 for information on provisioning these functions within each MG 1000E.

Step 11: Calculate the number of Media Gateways required

Calculating the required number of Media Gateways is an iterative procedure, because certain resources must be provisioned within each MG 1000E. Refer to “Assigning loops and card slots in the CS 1000E” on page 329.

Step 12: Assign equipment and prepare equipment summary

The ordering and configuration tool produces a summary of the equipment requirements for the complete system at cutover. Assign the equipment. Adjust the equipment summary if necessary as a result of assignment procedures. Use the finalized equipment summary to order the equipment for the system.

> ***Note:*** Another step you may want to consider at this point is system security. For more information, refer to *System Security Management* (553-3001-302).

Media Card and Virtual Trunk worksheet

This worksheet is in two parts:

- Worksheet 1a: Media Card calculation
- Worksheet 1b: Virtual Trunk calculation

Input constants	Input configuration data
R_I – intraoffice calls ratio	Number of analog telephones
R_T – tandem calls ratio	Number of digital telephones
I – incoming calls to total calls ratio	Number of IP Phones
O – outgoing calls to total calls ratio	Number of DECT telephones
P – IP calls to total calls ratio	Number of SIP Virtual Trunks (estimated)
V – Virtual Trunk calls to total trunk calls ratio	Number of H.323 Virtual Trunks (estimated)
v_S – SIP Virtual Trunk calls to total Virtual Trunk calls ratio	
v_H – H.323 Virtual Trunk calls to total Virtual Trunk calls ratio	
r_{CON} – Conference loop to traffic loop ratio (Default = 0.07)	
Hold time in seconds (AHT_{XX})for telephone to telephone, trunk to trunk, telephone to trunk, trunk to telephone	

Worksheet A
Media Card calculation (Part 1 of 2)

Item	Calculation formula
(1) TDM telephone CCS	= (Number of analog telephones + Number of digital telephones + Number of line-side T1/E1 ports) × _____ CCS/telephone
(2) IP Phone CCS	= [(Number of IP Phones – Number of IP ACD agents) × ______ CCS/IP Phone] + (Number of IP agent telephones × ______ CCS/agent)
(3) Total line CCS	= (1) + (2)
(4) TDM trunk CCS	= (Number of TDM trunks) × ____ CCS/trunk
(5) SIP Virtual Trunk CCS	= Number of SIP Virtual Trunks × ____ CCS/trunk
(6) H.323 Virtual Trunk CCS	= Number of H.323 Virtual Trunks × ____ CCS/trunk
(7) Total trunk CCS	= (4) + (5) + (6)
(8) Total system CCS (T_{CCS})	= (3) + (7)
(9) Weighted average holding time (WAHT)	= $(R_I \times AHT_{SS}) + (R_T \times AHT_{TT}) + (I \times AHT_{TS}) + (O \times AHT_{ST})$
(10) Total calls (T_{CALL})	= $0.5 \times T_{CCS} \times 100 \div WAHT$
(11) Calls requiring DSP resources (C_{DSP})	= (a) + [2 × (b)] + (c) + [2 × (d)] + (e) + (f) + [2 × (g)] + (h) + (i) + [2 × (j)]
— (a) Intraoffice IP-TDM telephone calls	= $T_{CALL} \times R_I \times 2 \times P \times (1 - P)$
— (b) Intraoffice TDM-TDM telephone calls	= $T_{CALL} \times R_I \times (1 - P)^2$
— (c) Tandem VT-TDM trunk calls	= $T_{CALL} \times R_T \times 2 \times V \times (1 - V)$
— (d) Tandem TDM-TDM trunk calls	= $T_{CALL} \times R_T \times (1 - V)^2$
— (e) IP Phone-TDM trunk calls	= $T_{CALL} \times O \times P \times (1 - V)$
— (f) TDM telephone-VT calls	= $T_{CALL} \times O \times (1 - P) \times V$

Worksheet A
Media Card calculation (Part 2 of 2)

Item	Calculation formula
— (g) TDM telephone-TDM trunk calls	$= T_{CALL} \times O \times (1 - P) \times (1 - V)$
— (h) VT-TDM telephone calls	$= T_{CALL} \times I \times V \times (1 - P)$
— (i) TDM trunk-IP Phone calls	$= T_{CALL} \times I \times (1 - V) \times P$
— (j) TDM trunk-TDM telephone calls	$= T_{CALL} \times I \times (1 - V) \times (1 - P)$
(12) DSP CCS (CCS_{DSP})	$= C_{DSP} \times WAHT \div 100$
(13) Number of Media Cards required for general traffic	$= CCS_{DSP} \div 794$
(14) DSP channels for Conference	= (Total number of telephones × r_{CON} × 0.4) = (Total number of telephones × 0.028)
(15) DSP channels for applications	= (a) + (b) + (c) + (d) + (e) + (f) + (g)
— (a) CallPilot	= Number of CallPilot ports
— (b) Integrated Recorded Announcer	= Number of Integrated Recorded Announcer ports
— (c) Integrated Conference Bridge	= Number of Integrated Conference Bridge ports
— (d) Integrated Call Director	= Number of Integrated Call Director ports
— (e) Integrated Call Assistant	= Number of Integrated Call Assistant ports
— (f) Hospitality Integrated Voice Service	= Number of Hospitality Integrated Voice Service ports
— (g) Agent Greeting	= Number of Agent Greeting ports
(16) Total DSP channels	= [(13) × 32] + (14) + (15)
(17) Total Media Cards	= Roundup((16) ÷ 32)

Worksheet B
Virtual Trunk calculation

Call type	Calculation formula
(1) Virtual Trunk calls (C_{VT})	= (a) + (b) + (c) + (d) + (e) + (f)
— (a) Tandem VT-TDM trunk calls	$= T_{CALL} \times R_T \times 2 \times V \times (1 - V)$
— (b) IP-VT calls	$= T_{CALL} \times O \times P \times V$
— (c) TDM telephone -VT calls	$= T_{CALL} \times O \times (1 - P) \times V$
— (d) VT-TDM telephone calls	$= T_{CALL} \times I \times V \times (1 - P)$
— (e) VT -IP Phone calls	$= T_{CALL} \times I \times V \times P$
— (f) Tandem VT (H.323) to VT (SIP) calls	$= T_{CALL} \times R_T \times V^2 \times v_H \times v_S \times 2 \times 2$
(2) Virtual Trunk CCS (VT_{CCS})	$= C_{VT} \times WAHT \div 100$
(3) SIP Virtual Trunk calls	$= VT_{CCS} \times v_S$
(4) H.323 Virtual Trunk calls	$= VT_{CCS} \times v_H$
(5) Number of Virtual Trunks	$= \text{Roundup}(VT_{CCS} \div 794 \times 32)$
(6) Virtual Trunk traffic in erlangs	$= \text{Roundup}(VT_{CCS} \div 36)$ use this for LAN/WAN bandwidth calculation

Note: If the calculated number of Virtual Trunks differs significantly from the original estimated number of Virtual Trunks (> 20%), Nortel recommends using the calculated Virtual Trunk number and repeating the calculation procedure to yield a more accurate number for required Media Cards and Virtual Trunks.

Appendix A: Protected memory requirements

Contents

This section contains information on the following topics:

Introduction

Memory calculations are based on assumptions about typical configurations, feature usage, and traffic patterns. This section provides the information required for detailed calculations in cases where those assumptions may not apply.

Protected Memory for Phone Sets: Detail

The protected data blocks for the various telephone types use varying amounts of memory according to what keys/features are configured on the telephone. The tables below can be used to arrive at a precise memory requirement if the details of the feature configurations are known. The maximum size permitted for any telephone's protected data block is 512 words.

PBX telephones

The size of the protected line block for PBX telephones is determined from the following (sizes are in SL-1 words):

Table 67
Size of protected line block for PBX telephones (Units in SL-1 words)

Feature	SL-1 Compool Variable(s)	Units
Basic Line Block	PPBXBLOCK (words 0-24)	25
Template Area	PBX_TEMPL_AREA (words 25-511 of PPBXBLOCK)	0-486
Card Block Component	1/4 PCARDBLOCK (= 10/4)	2.50

The key layout portion of the template requires:

$(4 + nf) \div rs$ words

where “nf” is the number of features defined for the telephone, and “rs” is the number of telephones sharing the same template.

In addition to the basic line block, each feature requires extra data space as shown in Table 68 (sizes are in SL-1 words):

Table 68
Data space requirements for PBX telephone features (units in SL-1 words) (Part 1 of 2)

Feature	SL-1 Compool Variable(s) and/or comment	Units
ACD	P_ACD_KEY_DATA	17
Associate telephone (AST)		3
Authcode	.AUTH_TEMPL_SIZE = .NAUT_MAX(6) * (((.AUTH_LEN_MAX(14) - 1)>>2) + 1)	6-24
Automatic Wakeup	HM_STRUCT	8
Call Forward Number	CFW_STRUC (4-24 digits/4)	1-8
Call Park	CALL_PARK_STRUC	2
Call Party Name Display	PBX_NAME_ENTRY	1
CFCT		2
CFNA/Hunting Number	CFNA_ENTRY	4
Dial Intercom Group	PBX_DIG_STRUC	2
DN	PBX_DN_STRUC	3
EFD DN	EFD_STRUC	4
EHT DN	EHT_STRUC	4
Enhanced Hot Line DN	((Number of digits in DN) ÷ 4) + 1 : 4 – 36 digits	2-10
FAXS	FAXS_BLK	17
FFC SCP PASS	FFC_SCPW_STRUC	2
Hot Line DN	((Number of digits in DN) ÷ 4) + 1 : 4 – 36 digits	2-10
HUNT	HUNT_STRUC	4
Internal Call Forward		19

Table 68
Data space requirements for PBX telephone features (units in SL-1 words) (Part 2 of 2)

Feature	SL-1 Compool Variable(s) and/or comment	Units
Last Number Redial	Number of digits in LNR DN ÷ 4 : (4 – .MAX_LNR_SIZE = 32) ÷ 4	1-8
Manual Line		2
Message Center DN		2
Message Registration	MR_SET_METER	1
Offhook Interdigit Index	OHAS_INDEXES	1
Pretranslation Enhancement	1/2 word (for 255 calling groups)	1/2
SCI/CCOS/RMS		2
Speed Call Controller	SPEED_CALL_STRUC	1
Speed Call User	SPEED_CALL_STRUC	1
Stored Number Redial	# digits in SNR DN / 4 : (4 – .MAX_SNR_DIGITS = 32) ÷ 4	1-8
System Speed Call User	SPEED_CALL_STRUC	1
Tenant Number	TENANT_NUMBER	1

Digital telephones

The size of the protected line block for SL-1 telephones is determined from Table 69.

Table 69
Size of protected line block for Meridian 1 telephones (units in SL-1 words)

Feature	SL-1 Compool Variable(s)	Units
Basic Line Block	PBCSBLOCK (words 0-45)	46
Template Area	BCS_DATA (words 46-511 of PBCSBLOCK)	0–466
Card Block Component	1/4 PCARDBLOCK (9/4)	2.25

The key layout portion of the template for the SL-1 basic telephone requires (4 + the number of key lamp strips × 10) ÷ rs words where rs equals the number of telephones sharing the same template. For digital telephones, the requirement is as follows:

- M2006 = 10 + (number of non-key features) ÷rs
- M2008 = 10 + (number of non-key features) ÷ rs
- M2216 = 20 + 30 × (number of AOM) + (number of non-key features) ÷ rs
- M2616 = 20 + 30 × (number of AOM) + (number of non-key features) ÷ rs
- M2317 = 34 + (number of non-key features) ÷ rs
- M3900 = 34 + (number of non-key features) ÷ rs
- IP Phone 2004 = 20 + (number of non-key features) ÷ rs
- IP Softphone 2050 = 20 + (number of non-key features) ÷ rs

where:

- rs is the number of telephones sharing the same template
- number of AOM equals number of add-on modules

In addition to the basic line block requirement, each feature requires extra data space as shown in Table 70(units are expressed in SL-1 words):

Table 70
Data space requirements for Meridian 1 telephone features (units in SL-1 words) (Part 1 of 6)

Feature	SL-1 Compool Variable(s), service change format, and/or comment	Units
ACD Agent and ID Key	.acd_agent p_acd_key_data KEY xx ACD xxxx(xxx)* yyyy(yyy) *(xxx) - up to 7 digs w/DNXP pkg	17
ACD Display Calls Waiting Key	acd_dwc_ext KEY xx DWC yyyy(yyy)	2
ACD Agent Key (for supervisor)	acd_agt_ext KEY xx AGT yyyy(yyy)	2
ACD Enable Interflow Key	acd_eni_ext KEY xx ENI yyyy(yyy)	2
ACD Night Service DN	acd_nsvc_struc KEY xx NSVC yyyy(yyy)	2
Associate telephone (AST)	bcs_ast_struc AST xx yy	3
Authcode (non-key)	.auth_templ_size (6) * (((.AUTH_LEN_MAX (14) - 1)>>2)+1) AUTH n xxxx	6-24
Autodial Key	(4-32 digits/4) .max_adl_size = 31 KEY xx ADL yy (zzzz)	1-8
Busy/Forward Status Key	bfs_struct KEY xx BFS tn	1
Call Forward Key	cfw_struc : (.cfw_default (4) or (.MAX_CFW_SIZE=31 + 1)digits/4)	1-8
No Hold Conference and Autodial	(same as autodial) KEY xx CA yy zzzz	1-8

Table 70
Data space requirements for Meridian 1 telephone features (units in SL-1 words) (Part 2 of 6)

Feature	SL-1 Compool Variable(s), service change format, and/or comment	Units
No Hold Conference and Direct Hotline	(htl_dn_size + 3 >>2) + wordoffset(bcs_hot_ter_dn) = (3:34)>>2 + 4 = 4-12 KEY xx CH D yy xxxx	4-12
No Hold Conference and Hotline List	wordoffset(bcs_hot_ter_dn) = 4 KEY xx CH L yyyy	4
No Hold Conference and Speed Call	speed_call_struc KEY xx CS yyyy	1
Dial Intercom Group Key	bcs_dig_struc KEY xx DIG xxxx yy R/V	2
DID Route Control	BCS_DRC_STRUC KEY xx DRC yyy	1
Group Call Key	bcs_grcal_entry KEY xx GRC yy	1
Hotline - One Way, Two Way or Intercom	(htl_dn_size + 3 >> 2) + wordoffset(bcs_hot_ter_dn) = 3:34>>2 + 4 = 4-12 KEY xx HOT D dd yyyy(yyy) KEY xx HOT D dd num DN m KEY xx HOT D nn x...x yyyy(yyy) KEY xx HOT I dd num m	4-12
Hotline - One Way or Two Way List	wordoffset(bcs_hot_ter_dn) KEY xx HOT L bbb KEY xx HOT L bbb yyyy(yyy)	4
Internal Call Forward Key	.cfw_default (1) or ((#digs(31) - 1)/4 + 1) : max 8 .max_cfw_size=31 KEY xx ICF 4-(16)-31 xxxx	1-8

Table 70
Data space requirements for Meridian 1 telephone features (units in SL-1 words) (Part 3 of 6)

Feature	SL-1 Compool Variable(s), service change format, and/or comment	Units
Loudspeaker	bcs_dn_struc KEY xx LSPK yyyy	4
Multiple Call Non-ringing DN Key	bcs_dn_entry KEY xx MCN yyyy(yyy)	4
Multiple Call Ringing DN Key	bcs_dn_entry KEY xx MCR yyyy(yyy)	4
Message Registration Key	mr_set_meter KEY xx MRK	1
Message Waiting Key	mwc_entry KEY xx MWK yyyy(yyy)	4
Call Park Key	call_park_struc KEY xx PRK	2
Private Line Non-ringing Key	bcs_dn_entry KEY xx PVN yyyy	4
Private Line Ringing Key	bcs_dn_entry KEY xx PVR yyyy	4
Stored Number Redial Key	.max_rdl_size (31): (1+#saved dn digs(3-31))/4 + 1 KEY xx RDL (yy)	2-8
Ringing Number Pickup Key	bcs_rnpg_entry KEY xx RNP	1
Radio Paging	bcs_dn_entry KEY xx RPAG	4
Speed Call Controller Key	speed_call_struc KEY xx SCC yyyy	1

Table 70
Data space requirements for Meridian 1 telephone features (units in SL-1 words) (Part 4 of 6)

Feature	SL-1 Compool Variable(s), service change format, and/or comment	Units
Single Call Non-ringing DN	bcs_dn_entry KEY xx SCN yyyy	4
Single Call Ringing DN	bcs_dn_entry KEY xx SCR yyyy	4
Speed Call User Key	speed_call_struc KEY xx SCU yyyy	1
Signaling Key	bcs_dn_entry KEY xx SIG yyyy(yyy)	4
System Speed Call Controller Key	speed_call_struc KEY xx SSC yyyy	1
System Speed Call User Key	speed_call_struc KEY xx SSU uu	1
Voice Call Key	bcs_dn_entry KEY xx VCC yyyy	4
Non-key Features		
Data Equipment Mode (flex voice/data tn)	dtm_struc DEM DTE (DCE)	1
Flexible CFNA DN for External Calls	efd_struc EFD xxxx	4
Hunt DN for External Calls	eht_struc EHT xxxx	4
Flexible Call Forward No Answer	afdn_struc FDN xxxx	4
Offhook Alarm Security DN Index for Forced Out of Service	ohas_indexes FSVC (0) - 9	1

Table 70
Data space requirements for Meridian 1 telephone features (units in SL-1 words) (Part 5 of 6)

Feature	SL-1 Compool Variable(s), service change format, and/or comment	Units
Hunt DN (chain) for Internal Calls	hunt_struc HUNT xxxx	4
Alternate Hunt DN (chain) for Internal Calls	ahnt_struc AHNT xxxx	4
Alternate Hunt DN for External Calls	aeht_struc AEHT xxxx	4
Alternate Flexible CFNA DN for External Calls	aefd_struc AEFD xxxx	4
Number of Key Lamp Strips	1 word per KLS in range KLS 1-7	1-7
Last Number Redial Size	.lnr_default(4) or ((xx+1)/4) LNRS xx (4-(16)-32)	1-8
Second DN Sharing Voice Mailbox	bcs_dn_struc SECOND_DN xxxx(xxx)	3
Station Control Password	ffc_scpw_struc SCPW xxxxx	2
Tenant	tenant_number TEN 1-511	1
Template area users for which commands are implicit or entered outside of LD 11		
Ringing Change Key	supp_features	5
Notification Key Lamp	nkl_data	1
Hospitality Data	hsp_set_data	2
Hotel/Motel Info	hm_struct	8
Campon Priorities	povr_struc	1

Table 70
Data space requirements for Meridian 1 telephone features (units in SL-1 words) (Part 6 of 6)

Feature	SL-1 Compool Variable(s), service change format, and/or comment	Units
Sar Group	save_bcs_sgrp	1
Boss-Secretary Filtering - boss	boss_struc	3
Boss-Secretary Filtering - sec'y	sec_struc	1
Call Party Name Display	PBX_NAME_ENTRY	1
FAXS	FAXS_BLK	17
Xdata Unit Downloadable Parameters	xdata_sc_parms	2

Appendix B: Numbering Plan recommendation

Contents

This section contains information on the following topics:

Introduction to the CS 1000E Numbering Plan

Call processing

Using the Gateway Group Prefix (GGP) and call digit type is not mandatory if there is a single CS 1000E associated with a single Network Routing Service (NRS). However, if there are two or more CS 1000E systems, the prefix and call type digit are required.

Standard call processing

Standard call processing encompasses all calls except ESA calls. The connectivity to PSTN or other TDM network is provided by the H.323/SIP gateway (in this document, assumed to be the MG 1000T platform). The Call Server communicates to this gateway via the SIP/H.323 Virtual Trunks. Since there can be multiple gateways, the numbering plan becomes more critical. The numbering plan would aim at minimal configuration on components of CS 1000E to make calls.

This category is divided into two categories: "Outgoing calls – Non-ESA" on page 372 and "Incoming calls – Non-ESA" on page 427. Each category has several scenarios available depending on the call types used. Call Types and related scenarios are listed in Table 71 for outgoing calls, and Table 72 for incoming calls.

Table 71
Outgoing call types

Plan	Call type	Reference
E.164	National	"Outgoing calls – Non-ESA" on page 372
	Local	"Making national calls from CS 1000E" on page 389
	International	"Making international calls from CS 1000E" on page 400
Private	Special	"Making special number calls from CS 1000E" on page 411
	Group Dialing Plans	"Making GDP calls from CS 1000E" on page 417
	Universal Numbering Plan (Coordinated Dialing Plan codes)	"Making UNP with Transferable DNs (TNDN) on CS 1000E — CDP network wide" on page 423

Table 72
Incoming call categories

Plan	Call type	Reference
E.164	Direct Inward Dialing (DID)	"Incoming DID call to CS 1000E" on page 430
Private	Normal	"Normal private network incoming call" on page 427

Note: The sections listed in the tables above provide only concepts and scenarios. Essential provisioning details are provided in "Provisioning procedures" on page 549.

ESA call processing

In general, ESA calls immediately seize a trunk and send the applicable information. Depending on the outgoing trunk medium used, the information may include the emergency services DN, or ESDN; a CAMA trunk typically does not, whereas an ISDN trunk typically does.

For the CS 1000E, the system is more complex. All calls within the CS 1000E are at least Virtual Trunking calls, and are handled as trunk calls. Therefore, the call from the end user at his or her terminal, through the Call Server processing, to the TDM ESA trunk, involves a Virtual Trunk tandem, although it may not use any DSP resources.

The connectivity to PSTN or other TDM network is provided by the H.323/SIP gateway, which may or may not be within an MG 1000E of the Call Server. Nortel recommends that every MG 1000E have at least some form of PSTN access in case of a major emergency, in which all Call Servers are either out-of-service or otherwise unavailable. This improves the overall reliability of the system.

As with other CS 1000 systems, the CS 1000E Call Server communicates to this gateway via the SIP/H.323 Virtual Trunks. Since there can be multiple gateways to which the call should be directed (and are required to ensure that ESA calls get out), the numbering plan becomes more critical. The numbering plan would aim at minimal configuration on components of CS 1000E to make calls.

Let us split the calls into two broad categories:

1 Outgoing calls from the “primary zone”.

2 Outgoing calls from all other zones.

Both of these are discussed in “Making ESA calls from CS 1000E — no local security stations” on page 472. This section discusses the call scenarios involved with CS 1000E. The appendix provides all LD provisioning details; this chapter provides only concepts and scenarios. The essential provisioning details are provided in “Provisioning procedures” on page 549.

Outgoing calls – Non-ESA

The called number as understood by the user is not necessarily the number provisioned. As an example, it is common in North America to provision the system with an SPN “011” to identify a number as an international number. So, the user thinks, “I dial the ESN access code 6, then the international access code 011, then the country code, then...” when in actual fact the Call Server processing based on the SPN provisioning determines the user dialed an SPN 011 (the ESN access code was necessary to identify the number), and all further digits are processed at a device located off the Call Server. All the Call Server knows is, “When the user dials 6 011, send the call to route xyz.” Therefore, the discussion works within the framework that a call dialed by the user translates within the Call Server into a specific number type; this number type is used in all descriptions and scenarios.

Outgoing public network calls from CS 1000E can be broadly categorized into different types of calls that leave the IP domain and travel over TDM resources. Typically, this means a user dialing:

- A Local Number; to the Call Server, this is either a number provisioned as an NXX (in North America) or an SPN
- A National Number; to the Call Server, this is either a number provisioned as an NPA (in North America) or an SPN

- An International Number; to the Call Server, this is provisioned as an SPN
- A Special Number (an SPN other than as listed above; for example, service numbers such as "611" for network service centers or ESA numbers such as 999 for emergency calls)

Private network call types in theory do not leave the network; they terminate on a user within the private network. However, they may go to remote gateways to reach TDM trunking devices. As such, these must also be provisioned. Nortel recommends that the CS 1000E use the Universal Numbering Plan (UNP). The UNP uses ESN CDP codes within its terminals and gateways. The UNP also uses the Group Dialing Plan (GDP), formerly the "UDP" using location codes in TDM ESN, across the network to remote systems. However, outgoing private network dialing can leave the IP domain, and the options include:

- A GDP number; to the Call Server this uses location codes (LOC)
- A UNP number; to the Call Server, this is CDP dialing

Call flow overview

One key concept is the Gateway Group Prefix (GGP). This prefix specifies one ordered list of destination gateways, arranged from lowest to highest cost factor. This concept and term are used frequently in the discussions to follow.

The call flow has four discrete phases, described below.

Call flow phase 1: Digit Analysis

The user dials the desired number. Typically, this means using the ESN access code and number type, followed by the digits to complete the call. (For example, it could be a North American local exchange number – NXX – which has a 7 digit format. Therefore, the user dials the ESN access code – usually 9 – and then the 7 digits.)

The system processes these numbers, and identifies the code and the route list data block index (the RLI) assigned to it. From the RLI, it gets the information about the route selected and the digit manipulation data associated.

Call flow phase 2: Gateway Group Selection

As far as the Call Server is concerned, it knows the route and a digit manipulation data block. The call is leaving over a virtual route, to the Gatekeeper or Redirect Server (collectively, the Network Routing Service, or NRS). However, to select the correct destinations the NRS needs to know the gateway group (or ordered list of gateways, based on costing) required.

The Call Server adds a prefix to the number to allow the NRS to correctly select the gateway group. The CLID is built based on the original dialed number (ignoring the prefix).

Call flow phase 3: Network routing

The NRS provides network routing. This includes least cost routing (possibly with the assistance of the Signaling Server for H.323). The least cost routing has an ordered list of gateway destinations, arranged from lowest to highest cost factor. Note that, although it appears that calls always end up at the lowest cost destination, this is not necessarily the case. If all channels at the lowest cost destination are in use, the NRS attempts the second least expensive choice.

The call terminates at the MG 1000T selected as having the least cost among the gateways currently available.

Call flow phase 4: Call Sent to PSTN (or Private ISDN network)

The call lands on the destination. The Call Server or gateway device removes the GGP and places the call to the PSTN.

Provisioning overview

To carry out the GGP insertion and deletion, the systems involved must be provisioned correctly. For provisioning outgoing calls from CS 1000E, provision the system according to the following steps:

Procedure 2
Provisioning outgoing calls from CS 1000E

1 GGP Planning

CS 1000E is a distributed network switch i.e. the components of the switch are distributed across the QOS-managed IP network. In the network, there could be multiple MG 1000T platforms. So this section of the configuration concentrates on selecting the appropriate gateway for routing the calls over to PSTN.

The gateways are typically identified by using a unique code referred to here as the GGP. This code is a set of digits which must be unique across the whole network within the numbering plan/type of number combination used to provide the GGPs. The GGP is used to steer the calls to the proper gateway for further processing.

This step includes the following sub-steps:

- Destination Analysis

  Before the definition of GGP, the user must decide where the calls are to break out to the PSTN. The user identifies the numbers to terminate at each destination on specific gateways. Note that the same number may have more than one possible destination; for example, two sites in London, England may be usable for calls to a specific PSTN destination there.

  A table, such as the one for storing digit strings in "GGP tables" on page 602, may be useful but is not mandatory.

- Digit String Grouping

  In this part of the provisioning, a unique code GGP is selected. This is "to terminate on a specific PSTN destination", and not "to terminate on a specific gateway". That is, if two sites in London, England can reach a specific London PSTN user, the GGP applies to both.

  The prefix can be designed in any way the system administrator finds useful. However, it is important that planning occur first. A good rule of thumb is to select geographically valid patterns. Select the "larger areas", then smaller subsets, and finally, specific locations within the regions.

  Two examples follow:

  i. GGP equals a continental or sub-continental (country) code within a continent, followed by a location in the continent/ subcontinent, followed by a 2 digit site code. If two digits were

used for the major geographic region, followed by three or four for the minor, followed by two for the site, some potential examples would be:
-01 613 25: continental code 01 — Canada/USA; area code 613, site 25 within the area code.
-44 208 22: continental code 44 — United Kingdom; city code 208 — London, site 22 in London
-17 553 14: continental code 17 — several adjacent countries that do not have a common country code; 553 — a major part of one of those countries, site 14 in that region

ii. GGP equals a specific site number where all sites have a unique index. For example, if there are 217 sites in a network, a three digit code covers them and allows an additional three times as many sites. However, four digits allows much, much more room for expansion.
In the examples, the second approach is used to make the examples as generic as possible; if "4444" is used, it has no special meaning in any market place except if it accidentally matches some entry in a country (or network; "4444" could be the first four digits of location code 444 and number 4xxx). However, this could also be "select the country code 44 for England and site 44 in the country"...
This is also discussed in "GGP tables" on page 602.

- Gateway Group Assembly

  Once the gateway steering code is decided, the gateways need to be grouped together. This grouping of gateways is done on the basis of the cost factor of routing the calls over the QOS-managed IP network.

- Call Type Digit selection

  Depending on the type of numbers dialed, a unique number is assigned to each type of call. This helps in differentiating the type of number the user dialed.

  Depending on location, call type digits can look similar to those listed in Table 73 on page 378.

  This is also covered in the section "GGP tables" on page 602. Worksheet tables for storing call type digits may be useful, but is not mandatory.

2 Numbering plan provisioning on the CS 1000E

This step includes the following sub-steps:

- Digit Manipulation provisioning

  The part involves provisioning digit manipulation tables on the CS 1000E Call Server to outpulse the desired digits, depending on the type of call attempted. It requires having the GGPs and call type digits planned first.

- CLID provisioning

  Since the called party number and call type is different from what is being dialed, the CLID needs to be carefully provisioned on the CS 1000E Call Server so that the called party gets the correct information. The provisioning of this section is same as in a CS 1000M or CS 1000S system. The only difference is the ISPN prompt, which is used extensively to control the CLID being sent out for a call.

- RLI and ESN code provisioning

  This part of the numbering plan provisioning on CS 1000E Call Server is similar to the way it is done on a CS 1000M or CS 1000S system. The user uses the ESN provisioning to define route lists, and then provisions the various digit prefixes, to use the applicable route list indices.

3 NRS provisioning

This step involves configuring numbering plan endpoints on the NRS (gatekeeper or redirect server) for different gateways on the network, depending on the way they are grouped. The GGPs allow the NRS to select the appropriate destination gateways, with the costings as applicable.

4 MG 1000T provisioning on the destination gateway

This is the final step in numbering plan provisioning. This involves provisioning digit manipulation tables on the gateways for proper routing of the calls. The gateways deletes the prefixes and call type digits, changing the call types as per the prefix received.

The following sections contain examples of this method applied to various types of calls.

Table 73
Sample call type digits

	Call type (by location)	
Digit	**North American**	**Outside North America**
1	NXX	local calls using ESN access code 2 and SPNs associated with it, for calls within the local region
2	NPA	long distance calls using ESN access code 1 and SPNs associated with it, for calls within the country and outside the local area
3	International (country code +...)	International (country code +...)
4	CDP	CDP
5	Group Dialing Plan (GDP; used here in lieu of “Universal Dialing Plan” for the location codes, as UDP is an IP protocol, and using UDP for location code calls as well can only create confusion)	Group Dialing Plan

End of Procedure

Call scenario overview

Following the call provisioning details is a series of related call scenarios. Each call scenario contains a scenario description, a table relating the sequence of steps for H.323 and SIP systems, and finally an image outlining the call scenario.

There may be confusion between “busy” and “congested” for readers. The two are similar but not identical. “Busy” means that all physical resources are in use; for example, the TDM timeslots at the destination gateway are all active with calls. “Congestion”, on the other hand, is a short form of “network congestion", and usually indicates that a limited amount of physical resources are available, but some virtual resource is exhausted. (In the CS 1000E, this can be illustrated by using the example of "Virtual Trunks" versus DSP resources. Calls that terminate on an IP device consume virtual resources; ones that terminate on a TDM device use physical resources. It is possible to use up all virtual resources and still have DSP resources idle, so the destination is "congested", not "busy".)

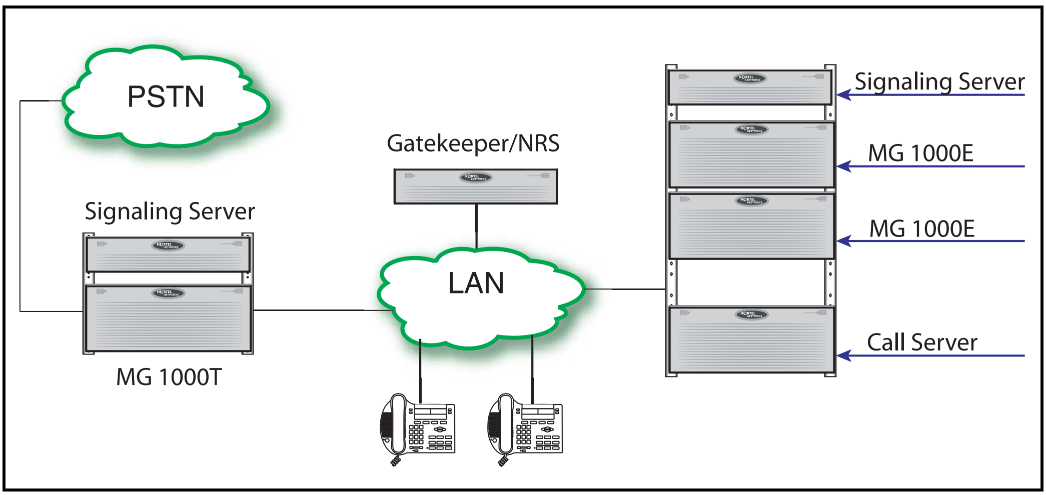
Making local calls from CS 1000E

System diagram

The following figure shows the CS 1000E at lower right, with two MG 1000E systems and a Signaling Server. There are two trunking gateways and Signaling Servers associated with the CS 1000E for these calls, shown on the left. The PSTN is also on the left, with the destination telephone. The LAN — with the gatekeeper and various IP Phones — is in the center.

Assume that the local NXX (North America) or SPN to be provisioned is "968". Assume also that the ESN access code used for local numbers is "9".

Figure 35
Setup for dialing local calls from CS 1000E



System description

In the system shown above, the Call Server is connected to the PSTN by means of two MG 1000T platforms. Procedure 3 describes how to provision the numbering plan on this system for making local calls. For example, a user (with a directory number of 8957) dials 9-968-9108 to reach a local number within the local national code.

Procedure 3
Provisioning local call dialing from CS 1000E

1 GGP Planning

For the network, digit “1” is selected to identify the local numbers.

2 Numbering plan entry on the CS 1000E

Numbering plan entry consists of the following:

- Digit Manipulation provisioning

  After deciding on the number prefixes the user provisions the local node to insert the concatenated group code (4444) and the NXX (North America) or local SPN code (1), as the string “44441”.

  For the listed network, different routes can be handled by having a single RLI having an entry for each route, and DMIs associated with the entry to insert the required digit string 44441, outpulsed prior to the actual digits 968-9108.

- CLID provisioning

  Adding the prefix (and changing the call type to SPN from NXX for North America) requires that the ISPN prompt is turned ON. This is done in the DMI.

- RLI provisioning

  If not done already, provision the RLB that is intended for the use of the local number. Use the DMI defined for this destination.

- ESN Code provisioning

  Configure 968 as an NXX (North America) or local SPN in the Call Server, and associate the respective RLB created. This configuration is same as that of a CS 1000M or CS 1000S system.

3 NRS provisioning

For local calls, the numbering plan entries in the NRS would vary based on the decisions made during planning about the cost factor.

Assume the cost factor is:

- 44441 on Media Gateway 1: cost factor 1
- 44441 on Media Gateway 2: cost factor 2

Then the gatekeeper would be provisioned with this information appropriately.

Create a special DN type entry for DN prefix 44441 on the NRS for Media Gateway 1 with a cost factor of 1, as shown in Figure 36 on page 381.

Create a special DN type routing entry for DN prefix 44441 on Media Gateway 2 with a cost factor of 2, as shown in Figure 37 on page 382.

Figure 36
Adding routing entry on Media Gateway 1

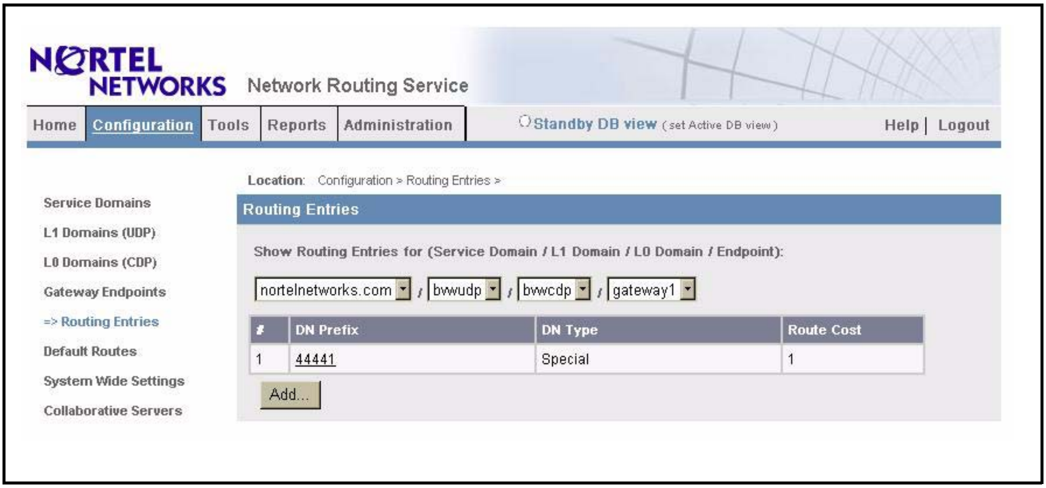


Figure 37
Adding routing entry on Media Gateway 2

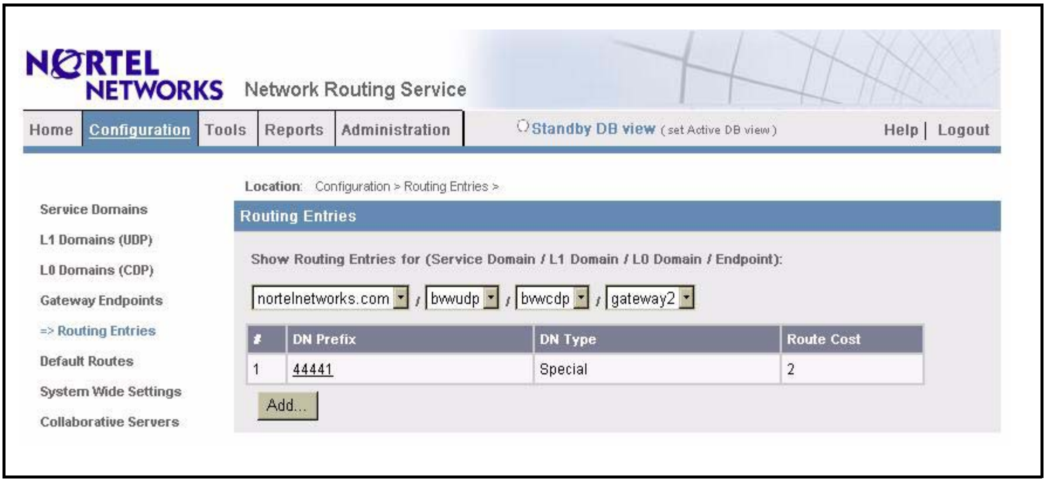
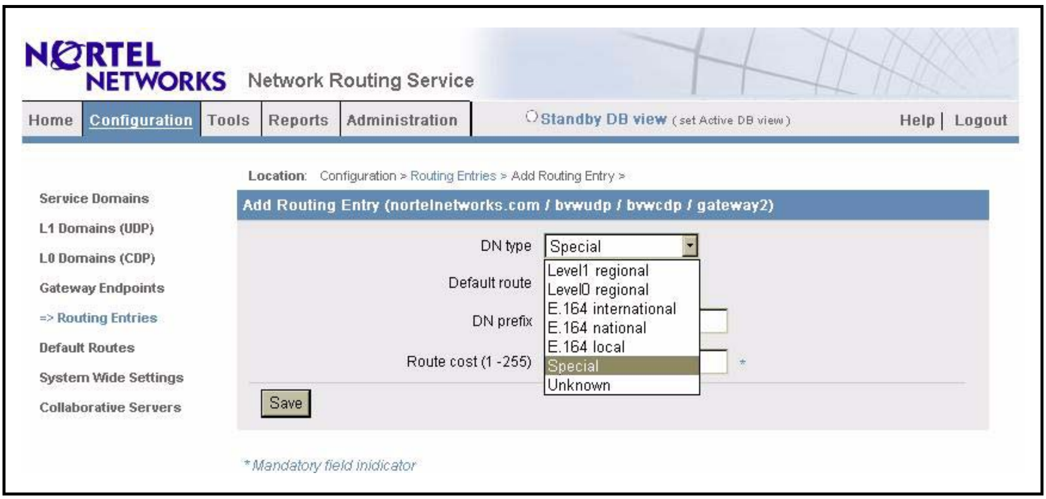


Figure 38
Selecting special DN type while provisioning routing entries



4 MG 1000T provisioning

As was stated earlier, the gateway may or may not be local to the CS 1000E. The provisioning here must occur on the system where the call is actually to leave the IP network. Otherwise, the call fails.

The digits received by the gateway include the prefix 44441. This string needs to be manipulated using digit manipulation tables on the gateway. For the network considered, typical configurations on each of the group gateways would use a DMI that deletes the full string. As an example, for "44441", the DMI entry would look much like the example below, assuming that SPN 44441 used RLI 55, and RLB 55 used DMI 3.

LD 90:

```
SPN 444 41
.....
RLI 55
.....
```

LD 86:

```
RLB
RLI 55
ENTR x
.....
DMI 3
.....

DMI 3
INST
DEL 5
ISPN NO
CTYP <NXX or SPN>
```

End of Procedure

Call scenarios

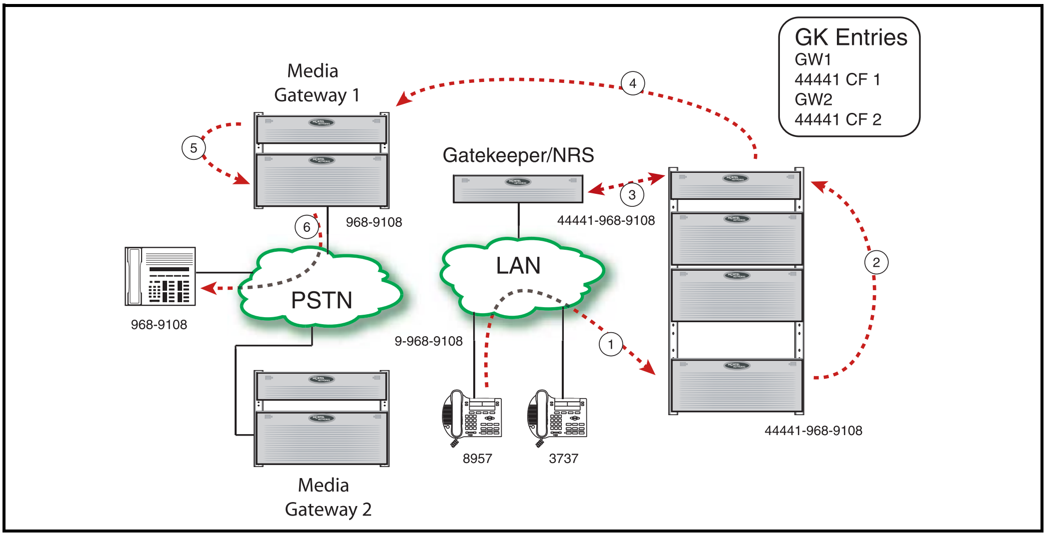
Call scenario 1: CS 1000E user dials a local number (NXX for North America, or SPN) and the first choice gateway is available

In this scenario, the caller (DN 8957) is placing a call at the Call Server, over IP to a gateway to the PSTN, where the call terminates on the desired destination.

Table 74
Call Scenario 1 Sequence

H.323 sequence	SIP sequence
The user dials 9-968-9108. The information is processed by the Call Server.	
After digit manipulation on the Call Server inserts the GGP “4444 1”, the digits outpulsed to the Signaling Server would be 4444 1 968 9108.	
The call is then routed to the Gatekeeper for address resolution. The digit string sent to the GK for address resolution is 44441-968-9108. Since an entry with cost factor “1” is found for 44441, the IP address of the endpoint — Media Gateway 1 — is sent to the requested Signaling Server as the first choice (provided the customer provisioned “least cost routing”, which is outside the scope of this reference). Media Gateway 2 is indicated as an alternate endpoint if least cost routing is available.	The call is then routed to the redirect server for address resolution. The digit string sent for address resolution is 44441-968-9108. Since an entry with cost factor “1” is found for 44441, the IP address of the endpoint — Media Gateway 1 — used to forward the INVITE.
The Signaling Server on the Call Server places the call to the Signaling Server of Media Gateway 1.	The Signaling Server of Media Gateway 1 receives the call.
The digits are now sent to Media Gateway 1 for digit manipulation and routing the call on to PSTN.	
On Media Gateway 1, 44441 is configured as an SPN. The gateway performs the digit manipulation on the digits, and deletes all the digits in the steering code and routes the call on the PSTN.	

Figure 39
Setup explaining Call Scenario 1 for local calls



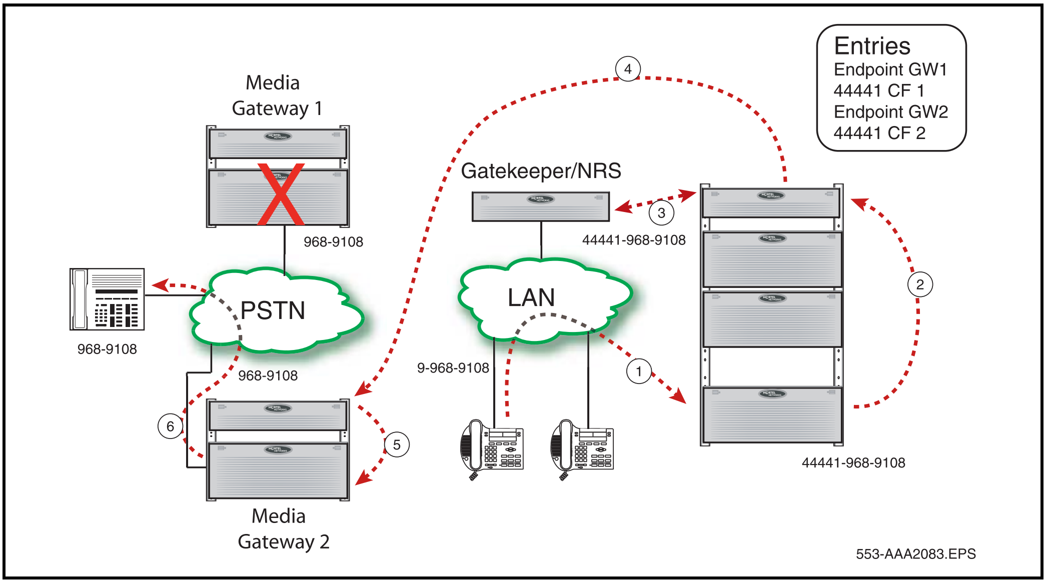
Call scenario 2: CS 1000E user dials a local number (NXX for North America, or SPN) and the first choice gateway in the group is busy or congested

In this scenario, the caller (DN 8957) is placing a call at the Call Server, over IP to a gateway to the PSTN, where the call terminates on the desired destination. However, the “preferred” gateway is not available to process the call, so an alternate handles it.

Table 75
Call Scenario 2 Sequence

H.323 sequence	**SIP sequence**
The user dials 9-968-9108. The information is processed by the Call Server.	
After digit manipulation on the Call Server inserts the GGP “4444 1”, the digits outpulsed to the Signaling Server would be 4444 1 968 9108.	
The call is then routed to the Gatekeeper for address resolution. The digit string sent to the GK for address resolution is 44441-968-9108. Since an entry with cost factor “1” is found for 44441, the IP address of the endpoint — Media Gateway 1 — is sent to the requested Signaling Server as the first choice (provided the customer provisioned “least cost routing”, which is outside the scope of this reference). Media Gateway 2 is indicated as an alternate endpoint if least cost routing is available.	The call is then routed to the redirect server for address resolution. The digit string sent for address resolution is 44441-968-9108. Since an entry with cost factor “1” is found for 44441, the IP address of the endpoint — Media Gateway 1 — used to forward the INVITE. The Signaling Server of Media Gateway 1 receives the call. This gateway is busy or undergoing network congestion. The redirect server re-tries the INVITE to Media Gateway 2.
The call routes to the available gateway. The Signaling Server on the Call Server places the call to the Signaling Server of Media Gateway 1. This gateway is busy or undergoing network congestion. The Signaling Server on the Call Server places the call to the Signaling Server of Media Gateway 2. This gateway accepts the call.	The Signaling Server of Media Gateway 1 receives the call. This gateway accepts the call.
The digits are then sent to Call Server for digit manipulation.	
On Media Gateway 2, 44441 is configured as a SPN. The gateway performs the digit manipulation on the digits, and deletes all the digits in the steering code and routes the call on the PSTN.	

Figure 40
Setup for explaining call scenario 2 for local calls



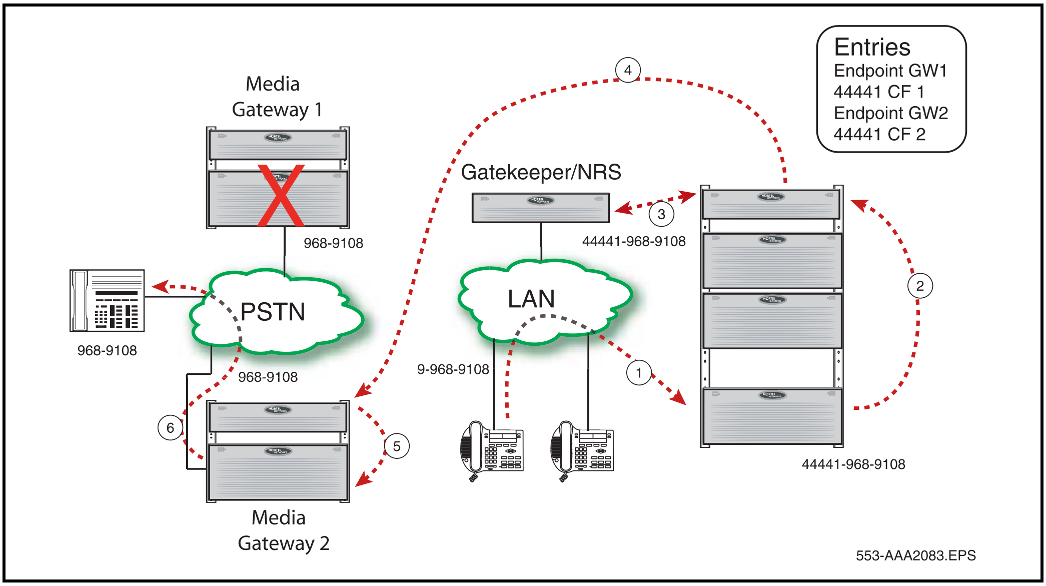
Call scenario 3: CS 1000E user dials a local number (NXX for North America, or SPN) and the first choice gateway in the group is not registered

In this scenario, the caller (DN 8957) is placing a call at the Call Server, over IP to a gateway to the PSTN, where the call terminates on the desired destination. However, the "preferred" gateway is not available to process the call because it is not registered with the gatekeeper/redirect server, so an alternate handles it. (The "X" through the gateway indicates this.)

Table 76
Call Scenario 3 Sequence

<table>
<tr><th>H.323 sequence</th><th>SIP sequence</th></tr>
<tr><td colspan="2">The user dials 9-968-9108. The information is processed by the Call Server.</td></tr>
<tr><td colspan="2">After digit manipulation on the Call Server inserts the GGP “4444 1”, the digits outpulsed to the Signaling Server would be 4444 1 968 9108.</td></tr>
<tr><td>The call is then routed to the Gatekeeper for address resolution. The digit string sent to the GK for address resolution is 44441-968-9108. Since the entry with cost factor “1” is not registered, but an entry of cost factor “2” can be found for 44441, the IP address of the endpoint — Media Gateway 2 — is sent to the requested Signaling Server as the first choice (provided the customer provisioned “least cost routing”, which is outside the scope of this reference). As no other gateways are available, no others are provided in the response.</td><td>The call is then routed to the redirect server for address resolution. The digit string sent for address resolution is 44441-968-9108. Since the entry with cost factor “1” is not registered, but an entry of cost factor “2” can be found for 44441, the IP address of the endpoint — Media Gateway 2 — used to forward the INVITE.</td></tr>
<tr><td>The Signaling Server on the Call Server places the call to the Signaling Server of Media Gateway 2.</td><td>The Signaling Server of Media Gateway 2 receives the call.</td></tr>
<tr><td colspan="2">The digits are then sent to the gateway Call Server for digit manipulation.</td></tr>
<tr><td colspan="2">On Media Gateway 2, 44441 is configured as a SPN. The gateway performs the digit manipulation on the digits, and deletes all the digits in the steering code and routes the call on the PSTN.</td></tr>
</table>

Figure 41
Setup for explaining call scenario 3 for local calls



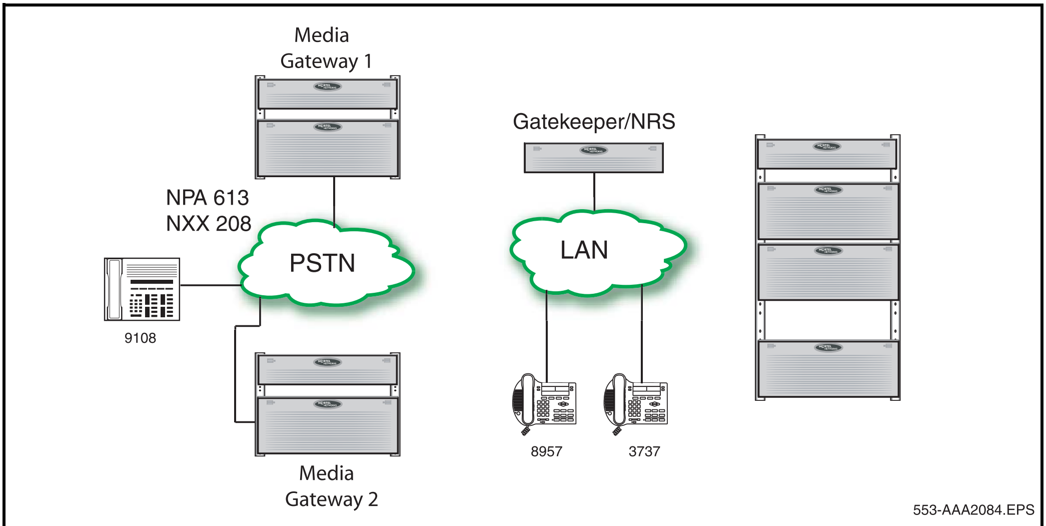
Making national calls from CS 1000E

System diagram

The following figure shows the CS 1000E at the right side, with two MG 1000E systems and a Signaling Server. The PSTN is on the left, with the destination telephone with Media Gateways 1 and 2 connected to it. The LAN — with the gatekeeper and various IP Phones — is in the center.

Assume that the NPA (North America) or national SPN for the geographical region to be provisioned is “1-613”. Assume also that the ESN access code used for national numbers is “6”.

Figure 42
Setup for dialing National numbers from CS 1000E



System description

In the system shown above, the Call Server is connected to the PSTN by means of two MG 1000T platforms, indicated as “Media Gateway 1” and “Media Gateway 2”. Procedure 4 describes how to provision the numbering plan on this system for making national calls. For example, a user (with a directory number 8957) dials 6-1613-208-9108 to reach a national number in Toronto from within the same country.

Procedure 4
Provisioning National number dialing from CS 1000E

1 GGP Planning

GGP planning involves the following procedure:

- Destination Analysis

  It is determined that both Media Gateways 1 and 2 can terminate the call at this destination.

- Digit String Grouping

For the network mentioned above, assume that a unique number set ‘4444’ is selected as a GGP. This code is unique across the whole network specified above. This could be some other code such as a continent/country code such as 95 plus a regional code such as 2274, and a specific site code; for a gateway 17 located in the 613 area code in Canada (assume 01 as the continental code), this would be a reasonable approach, yielding a unique prefix of 0161317.

- Gateway Group Assembly

  The gateways in the network for National calls, can be grouped into Group 1, which includes Media Gateways 1 and 2.

- Call Type Digit selection

  For the network above, digit “2” is selected for national calls.

2 Numbering plan entry on the CS 1000E

Numbering plan entry consists of the following:

- Digit Manipulation provisioning

  After deciding on the number prefixes the user provisions the local node to insert the concatenated group code (4444) and the national number code (2), as the string ‘44442’.

  For the listed network, different routs can be handled by having a single RLI having an entry for each route, and DMIs associated with the entry to insert the required digit string 44442, outpulsed prior to the actual digits 1613-209-9108.

  For more details on DMI provisioning, please refer to the Appendix of the document.

- CLID provisioning

  Adding the prefix (and changing the call type to SPN from NPA for North America) requires that the ISPN prompt is turned ON. This is done in the DMI.

- RLI provisioning

  If not done already, provision the RLB that is intended for the use of the local number. Use the DMI defined for this destination.

- ESN Code provisioning

  Configure 1613 as an NPA (North America) or national SPN in the Call Server and associate the respective RLB created. This configuration is same as that of a CS 1000M or CS 1000S system.

3 NRS provisioning

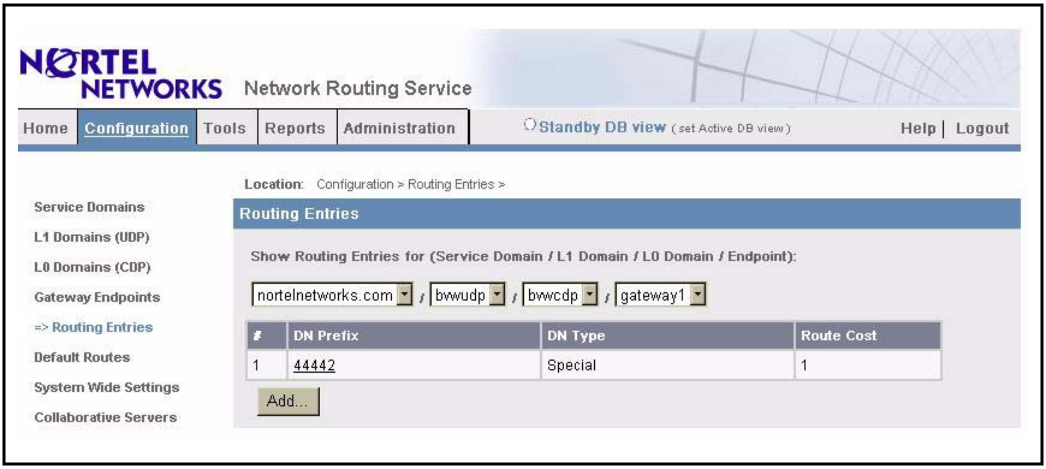
The next step in the configuration is provisioning numbering plan entries in the NRS for each of the gateways. For national calls, the numbering plan entries in the NRS would vary based on the decisions made during the planning about the cost factor. Assume the cost factor is:

- 44442 on Media Gateway 1: cost factor 1
- 44442 on Media Gateway 2: cost factor 2

Then the gatekeeper would be provisioned with this information appropriately.

Create a special DN type routing entry for DN prefix 44442 on the NRS Media Gateway 1 with cost factor 1.

Figure 43
Adding routing entry for Media Gateway 1



Create a special DN type routing entry for DN prefix 44442 on Media Gateway 2 with cost factor 2.

Figure 44
Adding routing entry for Media Gateway 2

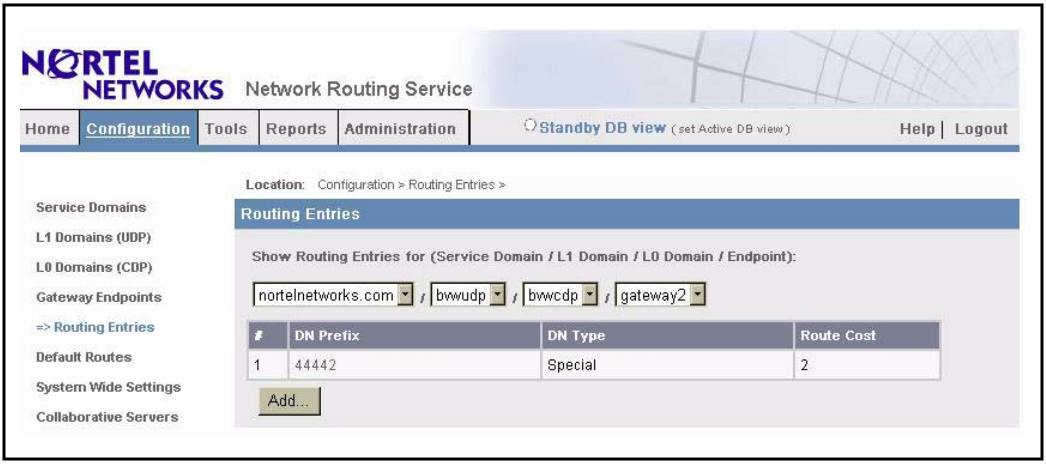
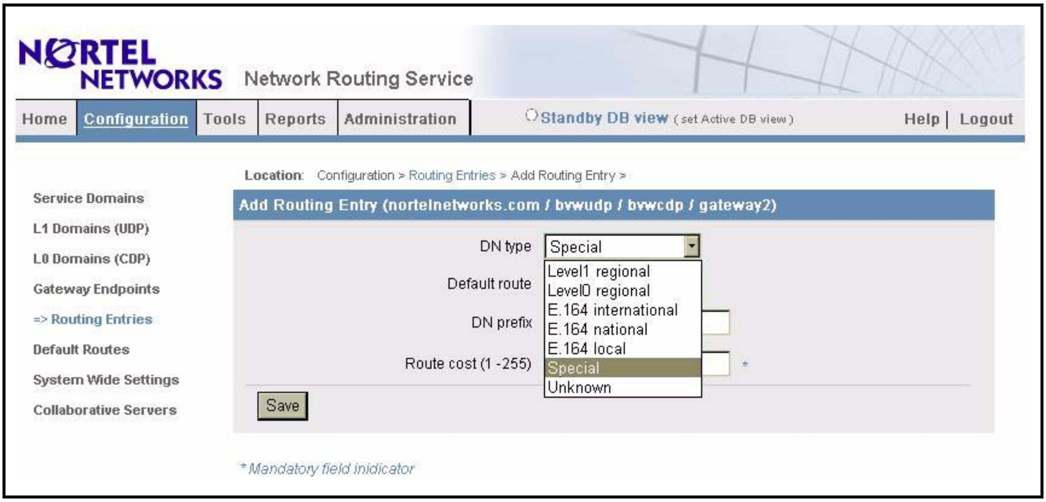


Figure 45
Selecting special DN type



4 Gateway provisioning

As was stated earlier, the gateway may or may not be local to the CS 1000E. The provisioning here must occur on the system where the call is actually to leave the IP network. Otherwise, the call fails.

The digits received by the gateway include the prefix 44442. This string needs to be manipulated using the digit manipulation tables on the gateway. For the network considered, typical configurations on each of the group gateways would use a DMI that deletes the full string. As an example, for “44442”, the DMI entry would look much like the following:, assuming that SPN 44442 used RLI 55, and RLB 55 used DMI 4:

In LD 90:

```
SPN 444 42
.....
RLI 55
.....
```

In LD 86:

```
RLB
RLI 55
ENTR x
.....
DMI 4
.....
```

```
DMI 4
INST
DEL 5
ISPN NO
CTYP <NPA or SPN>
```

End of Procedure

Call scenarios

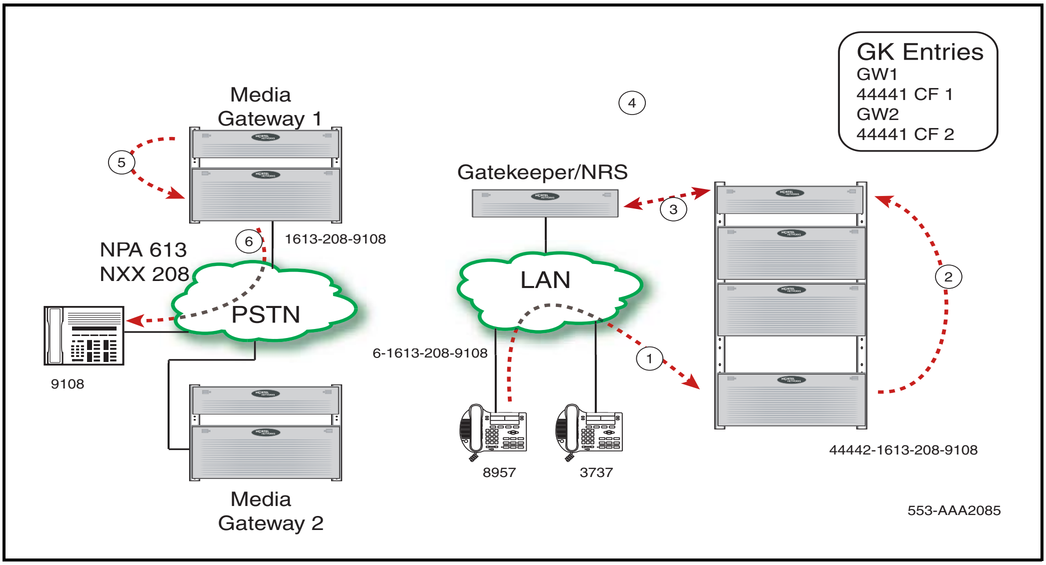
Call scenario 4: CS 1000E user dials a National number (NPA for North America, or SPN) and the first choice gateway is available

In this scenario, the caller (DN 8957) is placing a call at the Call Server, over IP to a gateway to the PSTN, where the call terminates on the desired destination.

Table 77
Call Scenario 4 Sequence

H.323 sequence	SIP sequence
The user dials 6-1613-238-9108. The information is processed by the Call Server.	
After digit manipulation on the Call Server inserts the GGP “4444 2”, the digits outpulsed to the Signaling Server would be 44442 1613 238 9108.	
The call is then routed to the Gatekeeper for address resolution. The digit string sent to the GK for address resolution is 44442-1613-208-9108. Since an entry with cost factor “1” is found for 44442, the IP address of the end point — Media Gateway 1 is sent to the requested Signaling Server as the first choice (provided the customer provisioned “least cost routing”, which is outside the scope of this reference). Media Gateway 2 is indicated as an alternate endpoint if least cost routing is available.	The call is then routed to the redirect server for address resolution. The digit string sent for address resolution is 44442-1613-238-9108. Since an entry with cost factor “1” is found for 44442, the IP address of the endpoint — Media Gateway 1 — used to forward the INVITE.
The Signaling Server on the Call Server places the call to the Signaling Server of Media Gateway 1.	The Signaling Server of Media Gateway 1 receives the call.
The digits are now sent to the gateway Call Server for digit manipulation and routing the call on to PSTN.	
On Media Gateway 1, 44442 is configured as an SPN. The gateway performs the digit manipulation on the digits, and deletes all the digits in the steering code and routes the call on the PSTN.	

Figure 46
Setup for call scenario 4 for dialing a national number



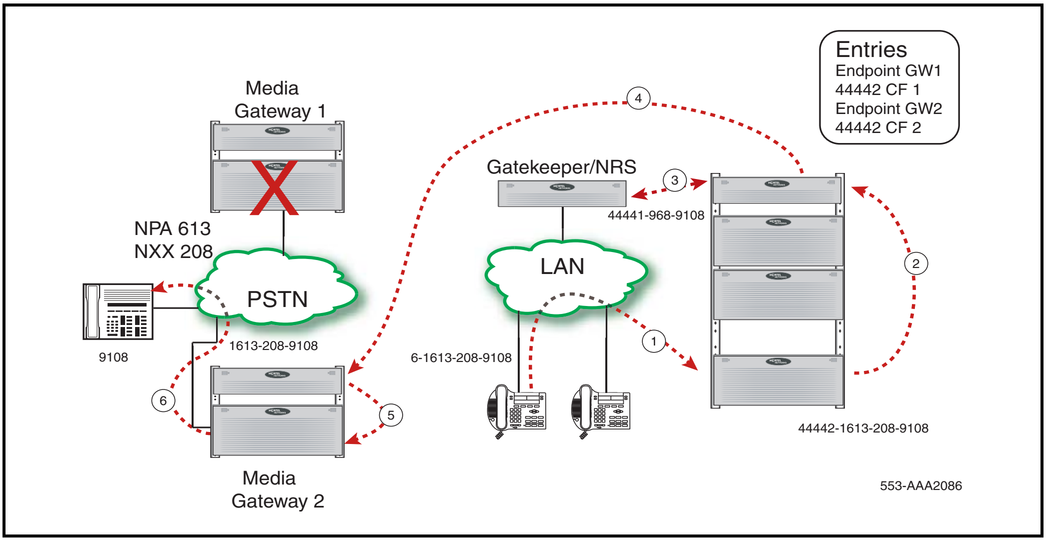
Call scenario 5: CS 1000E user dials a National number (NPA for North America, or SPN) and the first choice gateway in the group is busy or congested

In this scenario, the caller (DN 8957) is placing a call at the Call Server, over IP to a gateway to the PSTN, where the call terminates on the desired destination. However, the "preferred" gateway is not available to process the call, so an alternate handles it.

Table 78
Call Scenario 5 Sequence

<table>
<tr><th>H.323 sequence</th><th>SIP sequence</th></tr>
<tr><td colspan="2">The user dials 9-968-9108. The information is processed by the Call Server.</td></tr>
<tr><td colspan="2">After digit manipulation on the Call Server inserts the GGP “4444 2”, the digits outpulsed to the Signaling Server would be 4444 2 1613 238 9108.</td></tr>
<tr><td>The call is then routed to the Gatekeeper for address resolution. The digit string sent to the GK for address resolution is 44442-1613-208-9108. Since an entry with cost factor “1” is found for 44442, the IP address of the endpoint — Media Gateway 1 — is sent to the requested Signaling Server as the first choice (provided the customer provisioned “least cost routing”, which is outside the scope of this reference).
Media Gateway 2 is indicated as an alternate endpoint if least cost routing is available.</td><td>The call is then routed to the redirect server for address resolution. The digit string sent for address resolution is 44442-1613-238-9108. Since an entry with cost factor “1” is found for 44441, the IP address of the endpoint — Media Gateway 1 — used to forward the INVITE.
1 The Signaling Server of Media Gateway 1 receives the call. This gateway is congested or busy.
2 The redirect server re-tries the INVITE to Media Gateway 2.</td></tr>
<tr><td>The call routes to the available gateway.
1 The Signaling Server on the Call Server places the call to the Signaling Server of Media Gateway 1. This gateway is congested or busy.
2 The Signaling Server on the Call Server places the call to the Signaling Server of Media Gateway 2. This gateway accepts the call.</td><td>The Signaling Server of Media Gateway 2 receives the call. This gateway accepts the call.</td></tr>
<tr><td colspan="2">The digits are then sent to the gateway Call Server for digit manipulation and routing the call over to PSTN.</td></tr>
<tr><td colspan="2">On Media Gateway 2, 44442 is configured as a SPN. The gateway performs the digit manipulation on the digits, and deletes all the digits in the steering code and routes the call on the PSTN.</td></tr>
</table>

Figure 47
Setup for call scenario 5 for dialing national number



Call scenario 6: CS 1000E user dials a National (NPA for North America or SPN) number and the first choice gateway in the group is not registered

In this scenario, the caller (DN 8957) is placing a call at the Call Server, over IP to a gateway to the PSTN, where the call terminates on the desired destination. However, the "preferred" gateway is not available to process the call because it is not registered with the gatekeeper/redirect server, so an alternate handles it. (The "X" through the gateway indicates this.)

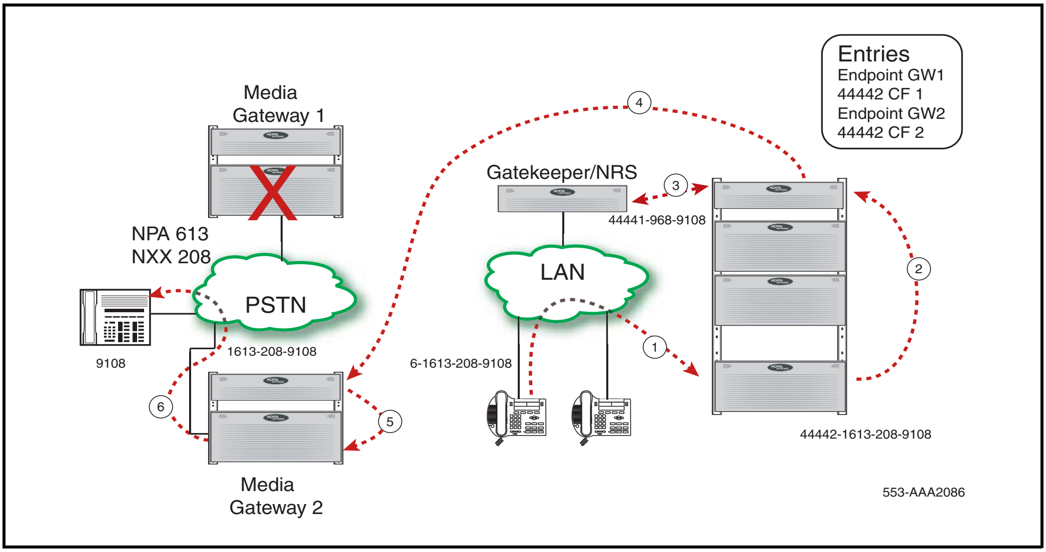
Table 79
Call Scenario 6 Sequence (Part 1 of 2)

H.323 sequence	SIP sequence
The user dials 6-1613-238-9108. The information is processed by the Call Server.	
After digit manipulation on the Call Server inserts the GGP "4444 2", the digits outpulsed to the Signaling Server would be 4444 2 1613 238 9108.	

Table 79
Call Scenario 6 Sequence (Part 2 of 2)

<table>
<tr><th>H.323 sequence</th><th>SIP sequence</th></tr>
<tr><td>The call is then routed to the Gatekeeper for address resolution. The digit string sent to the GK for address resolution is 44442-1613-208-9108. Assuming that the Signaling Server with the cost factor of “1” is not registered to the gatekeeper, it cannot accept traffic. Therefore, an entry with cost factor one is not found for 44442. The GK takes the next end point with cost factor “2” and sends the IP address of this endpoint — Media Gateway 2 is sent to the requested Signaling Server.</td><td>The call is then routed to the redirect server for address resolution. The digit string sent for address resolution is 44442-1613-208-9108. Since the entry with cost factor “1” is not registered, but an entry of cost factor “2” can be found for 44442, the IP address of the endpoint — Media Gateway 2 — used to forward the INVITE.</td></tr>
<tr><td>The Signaling Server on the Call Server places the call to the Signaling Server of Media Gateway 2.</td><td>The Signaling Server of Media Gateway 2 receives the call.</td></tr>
<tr><td colspan="2">The digits are then sent to the gateway Call Server for digit manipulation and routing the call over to PSTN.</td></tr>
<tr><td colspan="2">On Media Gateway 2, 44442 is configured as a SPN. The gateway performs the digit manipulation on the digits, and deletes all the digits in the steering code and routes the call on the PSTN.</td></tr>
</table>

Figure 48
Setup for call scenario 6 for dialing national number



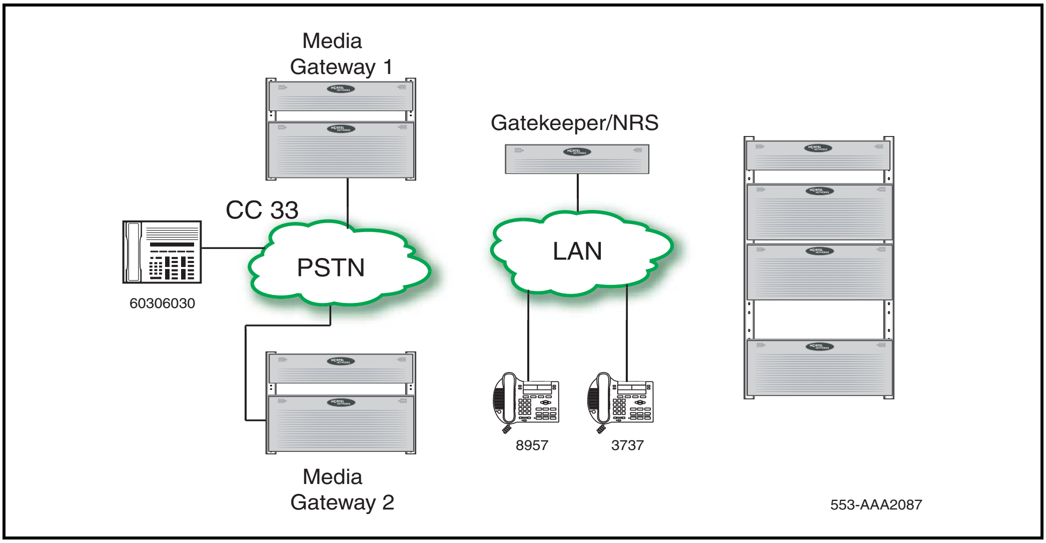
Making international calls from CS 1000E

System diagram

The following figure shows the CS 1000E at right, with two MG 1000E systems and a Signaling Server. The PSTN is on the left, with the destination telephone, and with Media Gateways 1 and 2 connected to it. The LAN — with the gatekeeper and various IP Phones — is in the center.

Assume that the call is to terminate in Paris, France with country code 33. Assume also that the ESN access code used for international numbers is “6”, with the SPN “011” used for international calls.

Figure 49
Basic setup for dialing International Numbers from CS 1000E



System description

In the system shown above, the Call Server is connected to the PSTN by means of two MG 1000T platforms. Procedure 5 describes how to provision the numbering plan on this system for making international calls. For example, a user in North America (with directory number 8957) dials 6-011-33-60306030 to reach an international number in Paris.

Procedure 5
Provisioning International Number dialing from CS 1000E

1 GGP Planning

GGP planning involves the following procedure:

- Destination Analysis

  It is determined that both Media Gateways 1 and 2 can terminate the call at this destination.

- Digit String Grouping

  For the network mentioned above, assume that a unique number set '4444' is selected as a GGP. This code is unique across the whole network specified above. This could be some other code such as a continent/country code such as 95 plus a regional code such as 2274, and a specific site code; for a gateway 17 located in the 613 area code in Canada (assume 01 as the continental code), this would be a reasonable approach, yielding a unique prefix of 0161317.

- Gateway Group Assembly

  The gateways in the network for International calls, can be grouped into Group 1, which includes Media Gateways 1 and 2.

- Call Type Digit selection

  For the network above, digit “3” is selected for international calls.

2 Numbering plan entry on the CS 1000E

Numbering plan entry consists of the following:

- Digit Manipulation provisioning

  Unlike other codes, the international numbers need to delete the “011” prefix. This is an additional requirement for the DMI for international numbers.

  After deciding on the number prefixes the user provisions the local node to insert the concatenated group code (4444) and the INTL code (3), as the string ‘44443’.

  For the listed network, different routs can be handled by having a single RLI having an entry for each route, and DMIs associated with the entry to insert the required digit string 44443, outpulsed prior to the actual digits 33-60306030.

- CLID provisioning

  Changing the call type from SPN to international number requires that the ISPN prompt is turned ON. This is done in the DMI.

  Use CLTP prompt in the SPN block for changing the call type to INTL for CLID purposes.

- RLI provisioning

  If not done already, provision the RLB to use this number. Use the DMI defined for this destination.

- ESN code provisioning

Configure 011 as an SPN in the Call Server and associate the respective RLB created. This configuration is same as that of a CS 1000M or CS 1000S system.

3 NRS provisioning

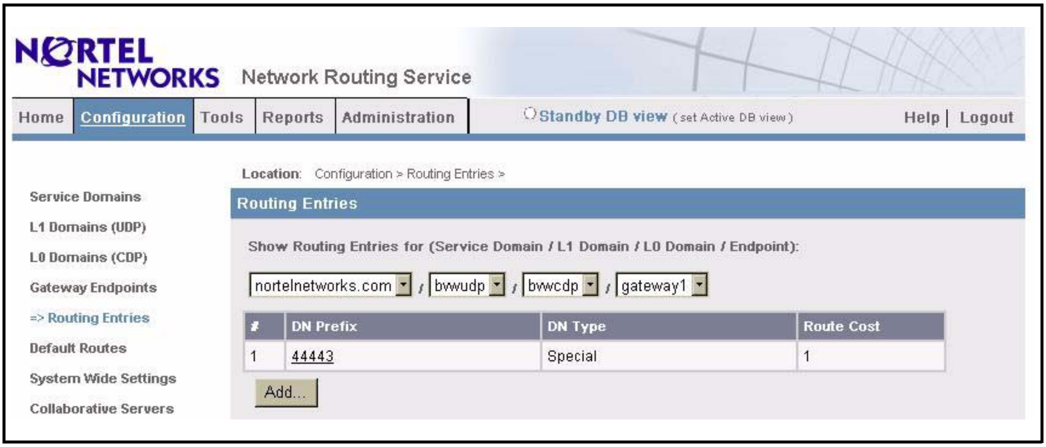
The next step in the configuration is provisioning the numbering plan entries in the NRS for each of the gateways. For local calls, the numbering plan entries in the NRS would vary based on the decisions made during planning about the cost factor. Assume the cost factor is:

- 44443 on Media Gateway 1: cost factor 1
- 44443 on Media Gateway 2: cost factor 2

Then the gatekeeper would be provisioned with this information appropriately.

Create an entry point of special number type with DN prefix of 44443 on Media Gateway 1 with cost factor 1

Figure 50
Adding an entry point on Media Gateway 1



Create a special DN type routing entry point for DN prefix of 44443 on Media Gateway 2 with cost factor 2.

Figure 51
Adding entry point on Media Gateway 2

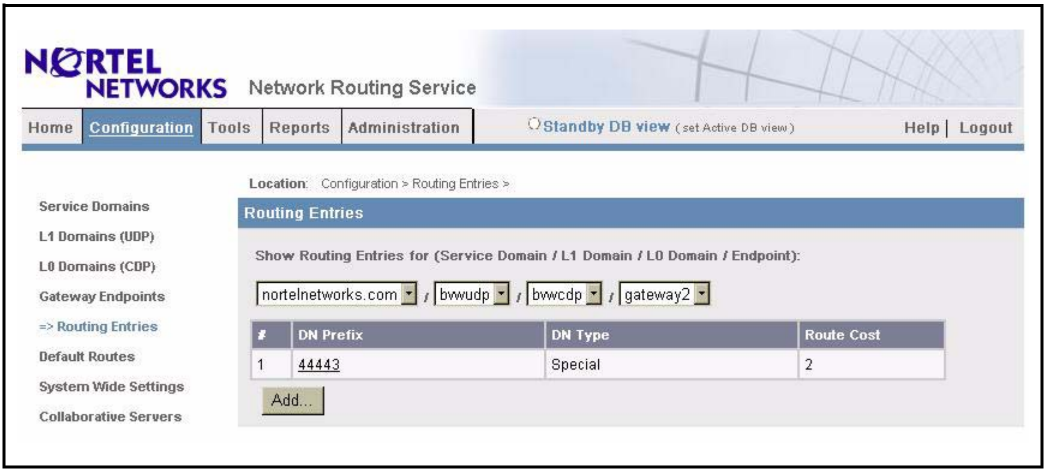
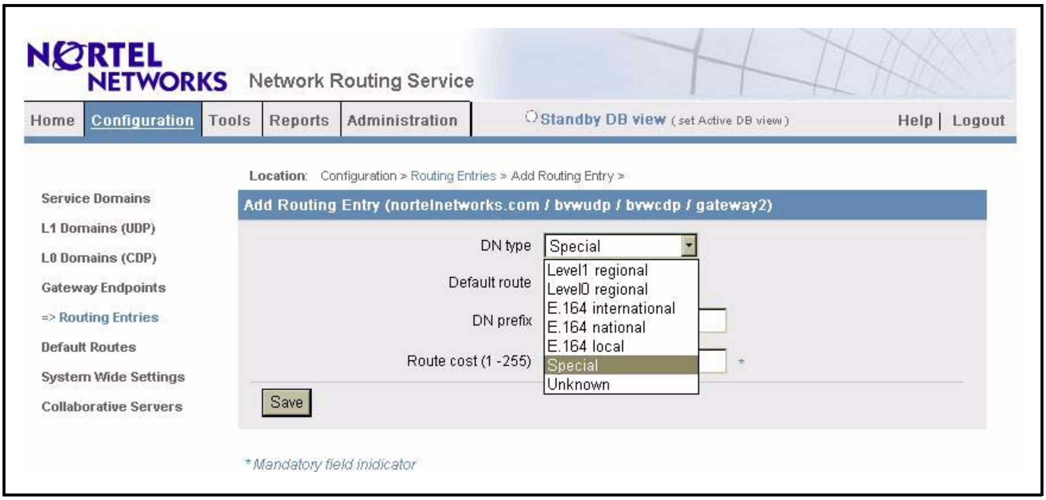


Figure 52
Selecting Special DN type



4 MG 1000T provisioning

As was stated earlier, the gateway may or may not be local to the CS 1000E. The provisioning here must occur on the system where the call is actually to leave the IP network. Otherwise, the call fails.

The digits received by the gateway include the prefix 44443. This string needs to be manipulated using the digit manipulation tables on the gateway. For the network considered, typical configurations on each of the group gateways would use a DMI that deletes the full string. As an example, for “44443”, the DMI entry would look much like the following:, assuming that SPN 44443 used RLI 55, and RLB 55 used DMI 5

In LD 90:

```
SPN 444 43
.....
RLI 55
.....
CLTP INTL
.....
```

In LD 86:

```
RLB
RLI 55
ENTR x
.....
DMI 5
.....
```

```
DMI 5
INST
DEL 5
CTYP INTL
ISPN NO
```

End of Procedure

Call scenarios

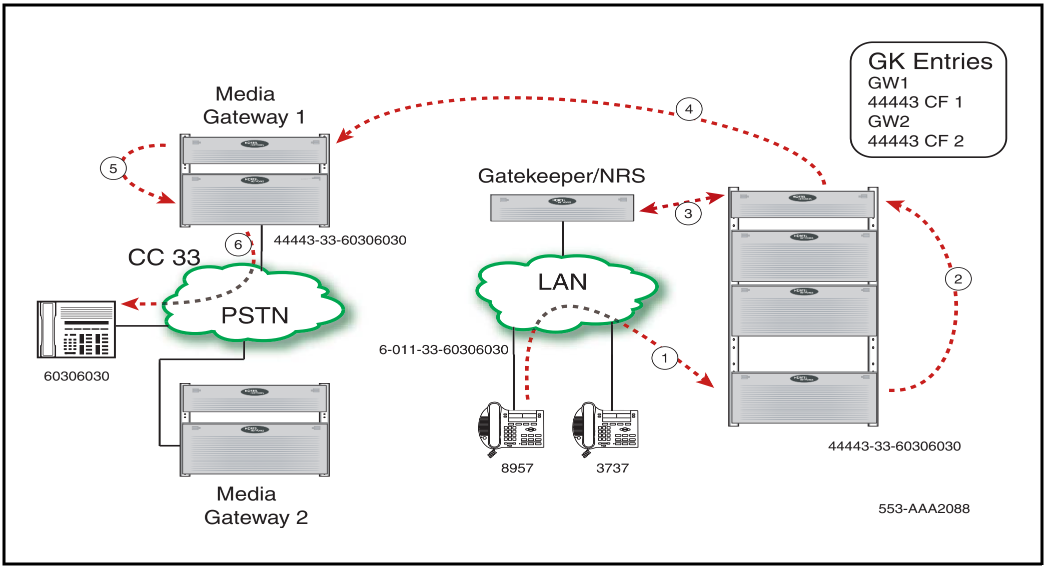
Call scenario 7: CS 1000E user dials an International number and the first choice gateway is available

In this scenario, the caller (DN 8957) is placing a call at the Call Server, over IP to a gateway to the PSTN, where the call terminates on the desired destination.

Table 80
Call Scenario 7 Sequence

H.323 sequence	SIP sequence
The user dials 6-011-33-60306030.	
After digit manipulation on the Call Server deletes the local “international number SPN” (011) and inserts the GGP “4444 3”, the digits outpulsed to the Signaling Server would be 44443-33-60306030.	
The call is then routed to the Gatekeeper for address resolution. The digit string sent to the GK for address resolution is 44443-33-60306030. Since an entry with cost factor One is found for 44443, the IP address of the end point — Media Gateway 1 is sent to the requested Signaling Server as the first choice (provided the customer provisioned “least cost routing”, which is outside the scope of this reference). Media Gateway 2 is indicated as an alternate endpoint if least cost routing is available.	The call is then routed to the Gatekeeper for address resolution. The digit string sent to the GK for address resolution is 44443-33-60306030. Since an entry with cost factor “1” is found for 44443, the IP address of the endpoint — Media Gateway 1 — used to forward the INVITE.
The Signaling Server on the Call Server places the call to the Signaling Server of Media Gateway 1.	The Signaling Server of Media Gateway 1 receives the call.
The digits are now sent to the gateway Call Server for digit manipulation and routing the call on to PSTN.	
On Media Gateway 1, 44443 is configured as an SPN. The gateway performs the digit manipulation on the digits, and deletes all the digits in the steering code and routes the call on the PSTN.	

Figure 53
Setup for call scenario 7 for international dialing from CS 1000E



Call scenario 8: CS 1000E user dials an international number and the first choice gateway in the group is busy or congested

As with **call scenario 2**, there may be confusion between “busy” and “congested” for readers. The two are similar but not identical. “Busy” means that all physical resources are in use; for example, the TDM timeslots at the destination gateway are all active with calls. “Congestion”, on the other hand, is a short form of “network congestion”, and usually indicates that a limited amount of physical resources are available, but some virtual resource is exhausted.

In this scenario, the caller (DN 8957) is placing a call at the Call Server, over IP to a gateway to the PSTN, where the call terminates on the desired destination. However, the "preferred" gateway is not available to process the call, so an alternate handles it.

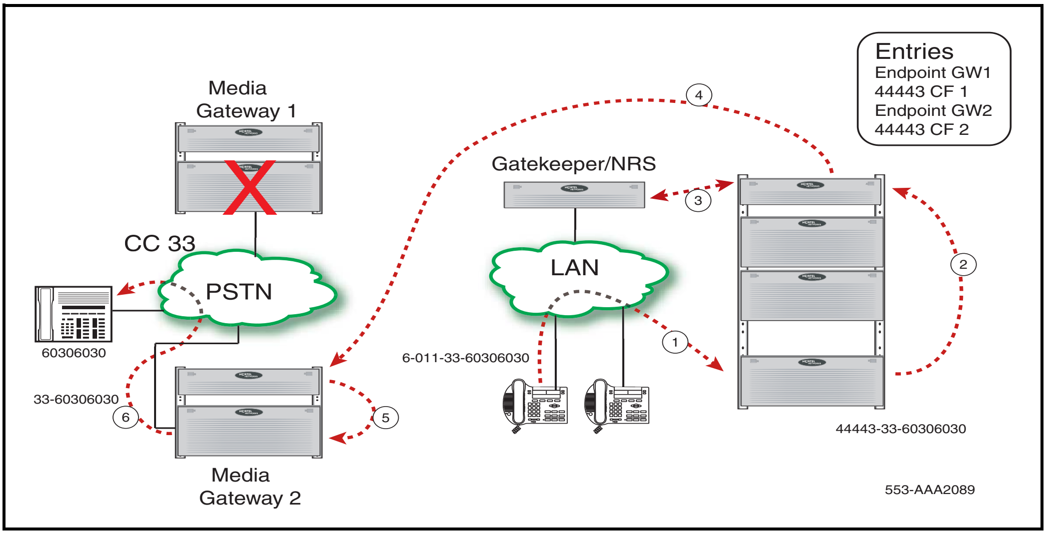
Table 81
Call Scenario 8 Sequence (Part 1 of 2)

<table>
<tr><th>H.323 sequence</th><th>SIP sequence</th></tr>
<tr><td colspan="2">The user dials 6-011-33-60306030.</td></tr>
<tr><td colspan="2">After digit manipulation on the Call Server deletes the local "international number SPN" (011) and inserts the GGP "4444 3", the digits outpulsed to the Signaling Server would be 44443-33-60306030</td></tr>
<tr><td>The call is then routed to the Gatekeeper for address resolution. The digit string sent to the GK for address resolution is 44443-33-60306030. Since an entry with cost factor "1" is found for 44443, the IP address of the endpoint — Media Gateway 1 — is sent to the requested Signaling Server as the first choice (provided the customer provisioned "least cost routing", which is outside the scope of this reference). Media Gateway 2 is indicated as an alternate endpoint if least cost routing is available.</td><td>The call is then routed to the redirect server for address resolution. The digit string sent for address resolution is 44443-33-60306030. Since an entry with cost factor "1" is found for 44443, the IP address of the endpoint — Media Gateway 1 — used to forward the INVITE.
1 The Signaling Server of Media Gateway 1 receives the call. This gateway is congested or busy.
2 The redirect server re-tries the INVITE to Media Gateway 2.</td></tr>
<tr><td>The call routes to the available gateway.
1 The Signaling Server on the Call Server places the call to the Signaling Server of Media Gateway 1. This gateway is congested or busy.
2 The Signaling Server on the Call Server places the call to the Signaling Server of Media Gateway 2. This gateway accepts the call.</td><td>The Signaling Server of Media Gateway 2 receives the call. This gateway accepts the call.</td></tr>
</table>

Table 81
Call Scenario 8 Sequence (Part 2 of 2)

H.323 sequence	SIP sequence
The digits are then sent to the gateway Call Server for digit manipulation and routing the call over to PSTN.	
On Media Gateway 2, 44443 is configured as a SPN. The gateway performs the digit manipulation on the digits, and deletes all the digits in the steering code and routes the call on the PSTN.	

Figure 54
Setup for call scenario 8 for international dialing from CS 1000E



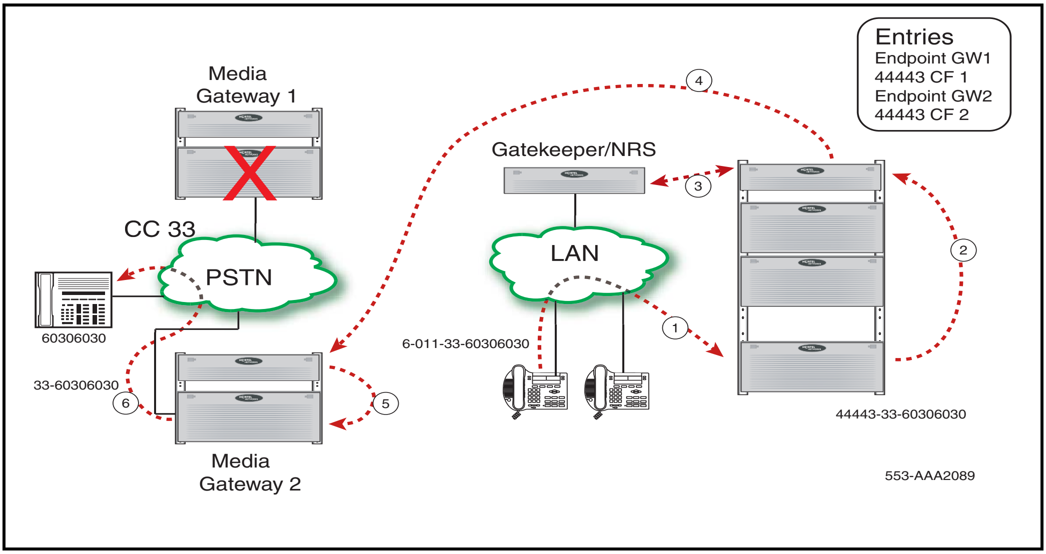
Call scenario 9: CS 1000E user dials an international number and the first choice gateway in the group is not registered

In this scenario, the caller (DN 8957) is placing a call at the Call Server, over IP to a gateway to the PSTN, where the call terminates on the desired destination. However, the "preferred" gateway is not available to process the call because it is not registered with the gatekeeper/redirect server, so an alternate handles it. (The “X” through the gateway indicates this.)

Table 82
Call Scenario 9 Sequence

H.323 sequence	SIP sequence
The user dials 6-011-33-60306030.	The user dials 6-011-33-60306030.
After digit manipulation on the Call Server deletes the local “international number SPN” (011) and inserts the GGP “4444 3”, the digits outpulsed to the Signaling Server would be 44443-33-60306030	After digit manipulation on the Call Server deletes the local “international number SPN” (011) and inserts the GGP “4444 3”, the digits outpulsed to the Signaling Server would be 44443-33-60306030
The call is then routed to the Gatekeeper for address resolution. The digit string sent to the GK for address resolution is 44443-33-60306030. Assuming that the Signaling Server with the cost factor of “1” is not registered to the gatekeeper, it cannot accept traffic. Therefore, an entry with cost factor one is not found for 44443. The GK takes the next end point with cost factor “2” and sends the IP address of this endpoint — Media Gateway 2 is sent to the requested Signaling Server.	The call is then routed to the redirect server for address resolution. The digit string sent for address resolution is 44443-33-60306030. Since the entry with cost factor “1” is not registered, but an entry of cost factor “2” can be found for 44443, the IP address of the endpoint — Media Gateway 2 — used to forward the INVITE.
The digits are then sent to the gateway Call Server for digit manipulation and routing the call over to PSTN.	The Signaling Server of Media Gateway 2 receives the call. This gateway accepts the call.
The Signaling Server on the Call Server places the call to the Signaling Server of Media Gateway 2.	The Signaling Server on the Call Server places the call to the Signaling Server of Media Gateway 2.
On Media Gateway 2, 44443 is configured as a SPN. The gateway performs the digit manipulation on the digits, and deletes all the digits in the steering code and routes the call on the PSTN.	On Media Gateway 2, 44443 is configured as a SPN. The gateway performs the digit manipulation on the digits, and deletes all the digits in the steering code and routes the call on the PSTN.

Figure 55
Setup for call scenario 9 for International dialing from CS 1000E



Making special number calls from CS 1000E

The discussion about SPNs logically should exclude SPNs used for "local" or "national" numbers as these are covered under sections intended specifically for "National" and "Local" numbers. The simplest example of this application is the ability to call "directory assistance" using the North American number 411, which is used as the basis for this discussion. However, other examples exist.

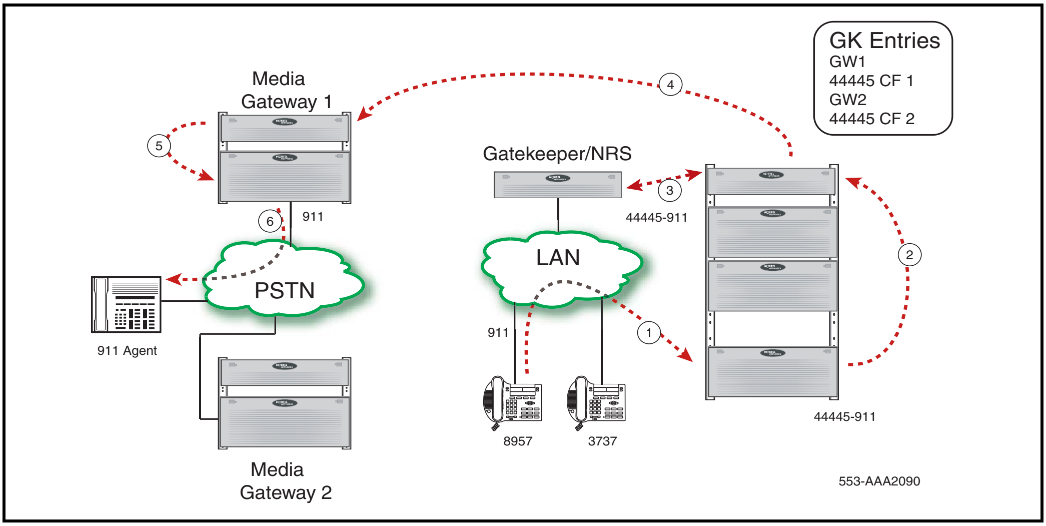
> ***Note:*** Emergency calls such as 911 (North America), 999 (UK), and others should use the ESA feature. For more information about how ESA fits into the CS 1000E dial plan, refer to "ESA calls" on page 434.

System diagram

The following figure shows the CS 1000E at lower right, with two collocated MG 1000E and a Signaling Server. The PSTN is on the left, with the destination telephone with Media Gateways 1 and 2 connected to it. The LAN — with the gatekeeper and various IP Phones — is in the center. Note that one or more of the Media Gateways 1 and 2 may also reside in the same location as the Call Server.

In North America, the local directory assistance number is 411; in other countries the emergency number is some other code. Typically, this uses a specific variant of ESN SPN codes.

Figure 56
Setup for dialing 411 (SPN) number from CS 1000E



System description

In the system shown above, the Call Server is connected to the PSTN by means of two MG 1000T platforms, indicated as "Media Gateway 1" and "Media Gateway 2". Procedure 6 describes how to provision the numbering plan on this system for making directory assistance or other "special number" calls.

In the above network, the PSTN PRI trunks are supported by Media Gateways 1 and 2.

Procedure 6
Provisioning SPN number dialing from CS 1000E

This is identical to the “local” number provisioning for non-North American sites, with the exception that the user may choose to use a separate Call Type Digit. The following provisioning example pre-supposes that the user decides that local (in North America, NXX) calls to regular numbers use “44441” as per the local case example, and calls to services such as directory assistance use a different call type digit.

1 GGP Planning

GGP planning involves the following procedure:

- Destination Analysis

It is determined that both Media Gateways 1 and 2 can terminate the call at this destination.

- Digit String Grouping

For the network mentioned above, assume that a unique number set “4444” is selected as a GGP. This code is unique across the whole network specified above.

This could be some other code such as a continent/country code such as 95 plus a regional code such as 2274, and a specific site code; for a gateway 17 located in the 613 area code in Canada (assume 01 as the continental code), this would be a reasonable approach, yielding a unique prefix of 0161317.

- Gateway Group Assembly

The gateways in the network, for local calls, can be grouped into Group 1, which includes Media Gateways 1 and 2

- Call Type Digit selection

For the network, digit “5” is selected to identify the local SPNs terminating on services and not on user devices.

2 Numbering plan entry on the CS 1000E

Numbering plan entry consists of the following:

- Digit Manipulation provisioning

After deciding on the number prefixes the user provisions the local node to insert the concatenated group code (4444) and the SPN “services” code (5), as the string “44445”.

For the listed network, different routes can be handled by having a single RLI having an entry for each route, and DMIs associated with the entry to insert the required digit string 44445, outpulsed prior to the actual digits such as “411”.

- CLID provisioning

Adding the prefix requires that the ISPN prompt is turned ON. This is done in the DMI.

- RLI provisioning

If not done already, provision the RLB that is intended for the use of the local SPN number. Use the DMI defined for this destination.

- ESN Code provisioning

Configure the number (for example, 411) as a local SPN in the Call Server, and associate the respective RLB created. This configuration is same as that of a CS 1000M or CS 1000S system.

3 NRS provisioning

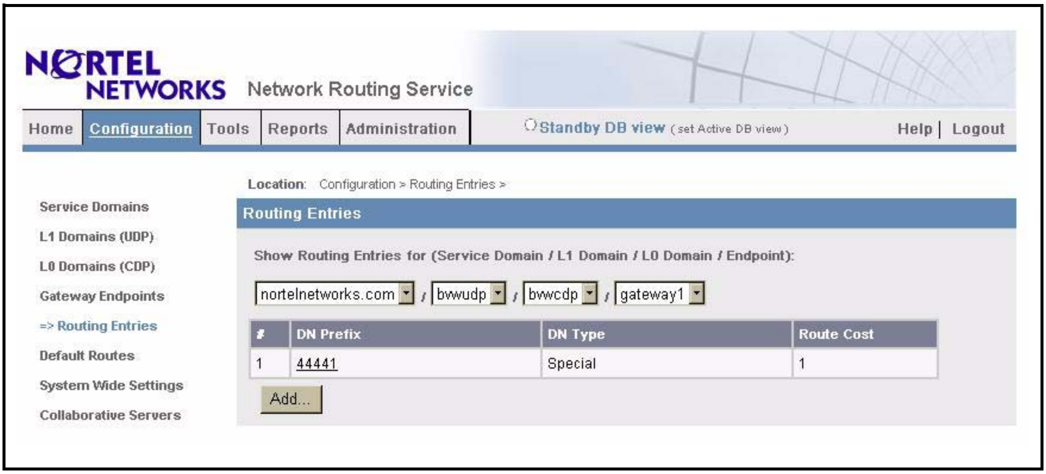
The next step in the configuration is provisioning the numbering plan entries in the NRS for each of the gateways. For local calls, the numbering plan entries in the NRS would vary based on the decisions made during planning about the cost factor. Assume the cost factor is:

- 44445 on Media Gateway 1: cost factor 1
- 44445 on Media Gateway 2: cost factor 2

Then the gatekeeper would be provisioned with this information appropriately.

Create a special DN type entry for DN prefix 44445 on the NRS for Media Gateway 1 with a cost factor of 1.

Figure 57
Adding routing entry on Media Gateway 1



Create a special DN type routing entry for DN prefix 44445 on Media Gateway 2 with a cost factor of 2.

Figure 58
Adding routing entry on Media Gateway 2

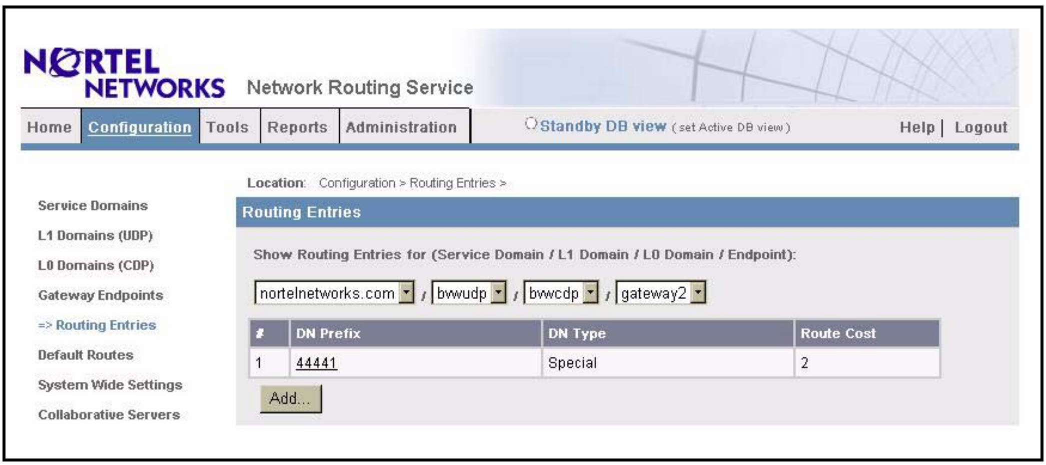
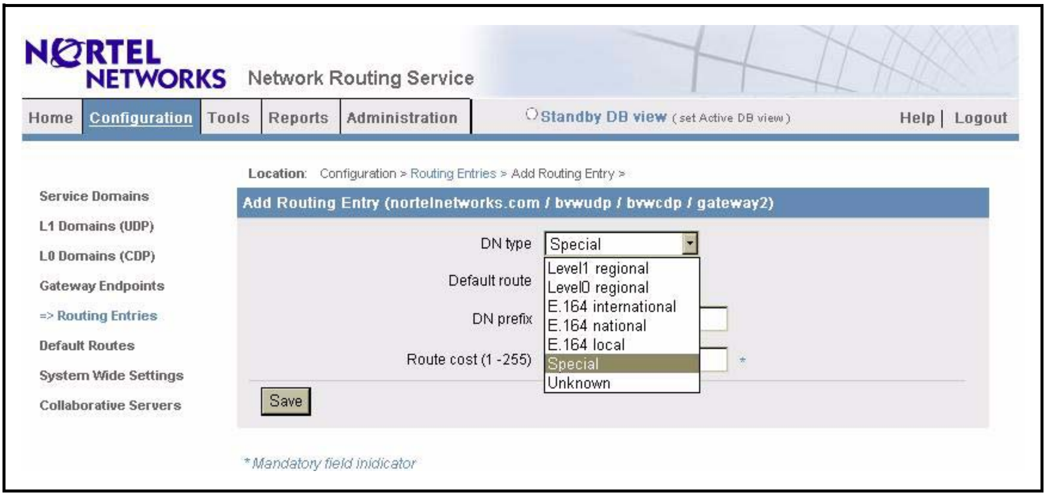


Figure 59
Selecting special DN type while provisioning routing entries



4 MG 1000T provisioning

As was stated earlier, the gateway may or may not be local to the CS 1000E. The provisioning here must occur on the system where the call is actually to leave the IP network. Otherwise, the call fails.

The digits received by the gateway include the prefix 44445. This string needs to be manipulated using digit manipulation tables on the gateway. For the network considered, typical configurations on each of the group gateways would use a DMI that deletes the full string. As an example, for "44445", the DMI entry would look much like the following:, assuming that SPN 44445 used RLI 55, and RLB 55 used DMI 3.

In LD 90:

```
SPN 444 454 11
.....
RLI 55
.....
```

In LD 86:

```
RLB
RLI 55
ENTR x
.....
DMI 3
.....

DMI 3
INST
DEL 5
ISPN NO
CTYP <NXX or SPN>
```

End of Procedure

Making GDP calls from CS 1000E

System diagram

The GDP enables coordinated dialing within a larger network using Location Codes (LOC).

GDP works similar to the location code operation in CS 1000M or CS 1000S systems.

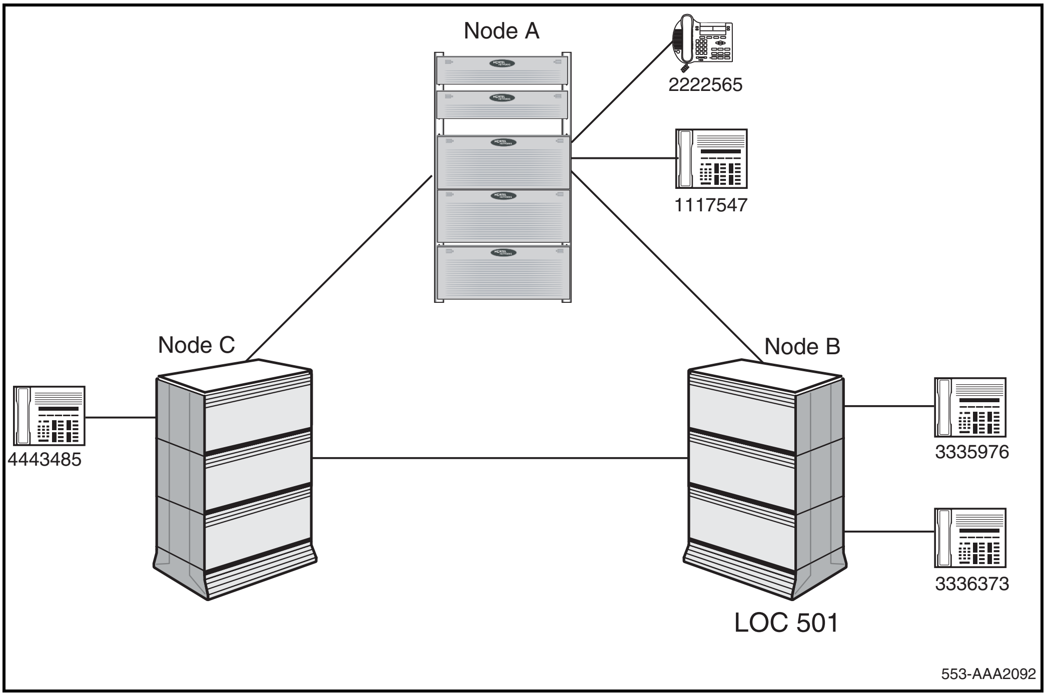
Each group (typically, a CDP zone) has a LOC that has to be dialed from outside the group as a prefix to the group CDP. That is, the goal is to have the LOC and CDP codes working together. In this case, the number dialed to a station can be different when dialed from different locations.

When GDP is used, the maximum number of digits allowed for either LOC+DN, LSC+DN, or DSC+DN cannot exceed 10 digits if the dialing plan is to perform properly.

System description

The following example shows a Home Location code 501 (shown as a LOC, since that is how the other nodes perceive it) for one node (B) only. The other nodes (A and C) may theoretically belong to the same HLOC, but in that case, the local node removes the code and routes via CDP. So, assume that nodes A and C have their own HLOC codes reachable via LOC from the other nodes, but these values are not needed for this discussion; the example revolves around calls from CS 1000E node A to node B. It has definite meaning for the Calling Party Numbers sent to node B, but this discussion is about called number handling.

Figure 60
GDP Setup



In the example shown above, node A has two CDP Local Steering Code (LSC) prefixes — 111 and 222. Node B uses CDP Local Steering Code (LSC) prefix 333 and LOC 501, and node C uses CDP Local Steering Code (LSC) prefix 444. In order to get to station 6373 on node B:

- Using LOC dialing, user 2565 on node A dials 6-501-3336373. (The user could also use UNP and CDP codes to reach node B, but that is outside the scope of this section.)
- Using LOC dialing, user 3485 on node C dials 6-501-3336373. (The user could also use UNP and CDP codes to reach node B, but that is outside the scope of this section.)
- User 5976 on node B dials 6373; this user does not need GDP to reach 6373.

Procedure 7
Provisioning Group Dialing numbers from CS 1000E

Two options exist – use “normal” CS 1000 procedures, or use the GGPs. Using digit manipulation at the originating side causes all connectionless services (such as Network ACD, Network Ring Again, Message Waiting Indication, and others) to fail. So using GGPs – although possible – should be avoided.

As it is anticipated that most users will use the “normal” CS 1000 procedures in order to maintain feature capabilities, they are the only variant discussed.

1 GGP Planning

Not applicable. The LOC applies to a specific node only, so any gateway selection required is done by the remote IP device (Signaling Server).

2 Numbering plan entry on the CS 1000E

Digit manipulation is NOT USED unless as a final alternative the call is to be routed through the PSTN. Likewise, CLID manipulation is NOT USED unless the call routes through the PSTN. In this case, all connectionless features continue to use the first choice entries that do not use a DMI (by definition, if the PSTN is a “final alternative”, all others preceded it).

If not done already, provision the RLB for the use of this number. No special DMI is used; doing so breaks all the connectionless feature capabilities.

Configure 501 as a LOC in the Call Server, and associate the respective RLB created. This configuration is same as that of a CS 1000M or CS 1000S system.

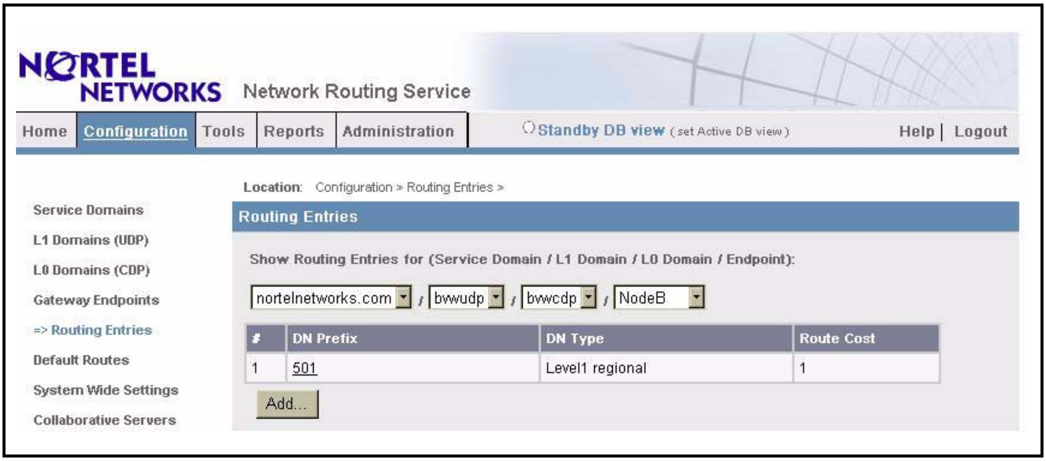
3 NRS provisioning

The next step in the configuration is provisioning the numbering plan entries in the NRS for each of the Nodes. For GDP (LOC) calls, the numbering plan entries in the NRS would vary based on the decisions made during planning.

For the network shown in Figure 60 on page 419, a routing entry 501 of Level 1 is created on Node B Signaling Server for terminating the GDP call on this node.

Create a entry point of Level 1 type on Node B Signaling Server for terminating the call on Node B.

Figure 61
GDP Provisioning in Gatekeeper



If the call is required to overflow to the PSTN because no private network resources are available, the originating Call Server maps the number into a DID capable PSTN number. It is now a local, national, or international number and must be treated as such.

4 Gateway provisioning

Not applicable. The gateway is remote.

Note: The provisioning of the GDP (LOC) is the same as in CS 1000M or CS 1000S systems. The Call Server and gateways of the CS 1000E are on the same CDP domain and can be deployed on a network which has GDP.

End of Procedure

Call scenarios

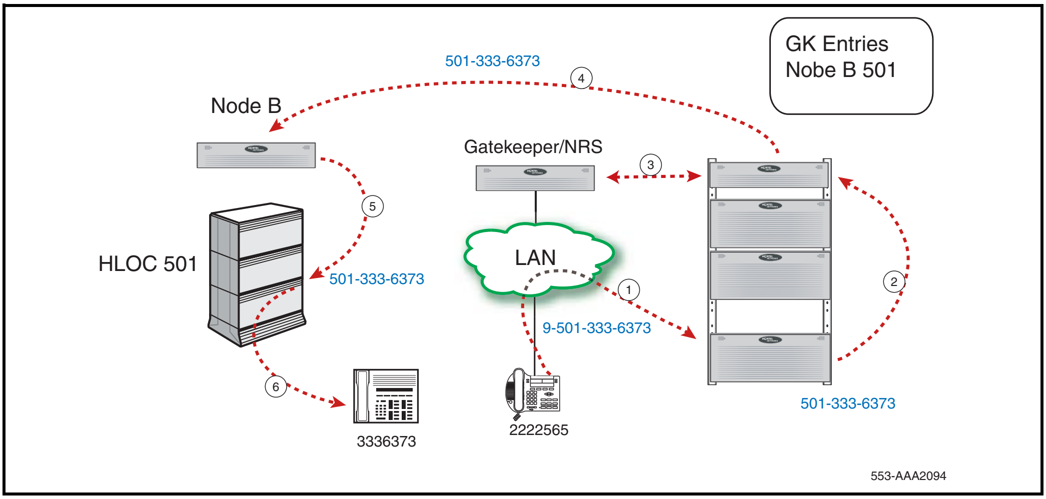
Call scenario 10: CS 1000E user dials a UDP (LOC) number

In this scenario, the caller is placing a call at the Call Server, over IP to Node B site, where the call terminates on the desired destination.

Table 83
Call Scenario 10 sequence

<table>
<tr><th>H.323 sequence</th><th>SIP sequence</th></tr>
<tr><td colspan="2">The user 2565, dials 6-501-3336373.</td></tr>
<tr><td colspan="2">The Call Server detects 501 to be a LOC and routes the call to Signaling Server.</td></tr>
<tr><td>The Signaling Server sends a request to Gatekeeper for address resolution. Assuming that the Signaling Server with the cost factor of “1” registered to the gatekeeper. The IP address of Node B is sent to the requested Signaling Server.</td><td>The call is then routed to the redirect server for address resolution. The digit string sent for address resolution is 501-3336373. Since the entry with cost factor “1” is registered, the IP address of the endpoint — Node B- used to forward the INVITE.</td></tr>
<tr><td>The Signaling Server on the Call Server places the call to the Signaling Server of Node B</td><td>The Signaling Server of Node B receives the call.</td></tr>
<tr><td colspan="2">The call is sent from the Signaling Server to the Call Server on Node B. The Call Server finds that 501 is configured as a HLOC and strips the digits.</td></tr>
<tr><td colspan="2">The call terminates on the telephone.</td></tr>
</table>

Figure 62
Setup explaining call scenario 10 for GDP Call



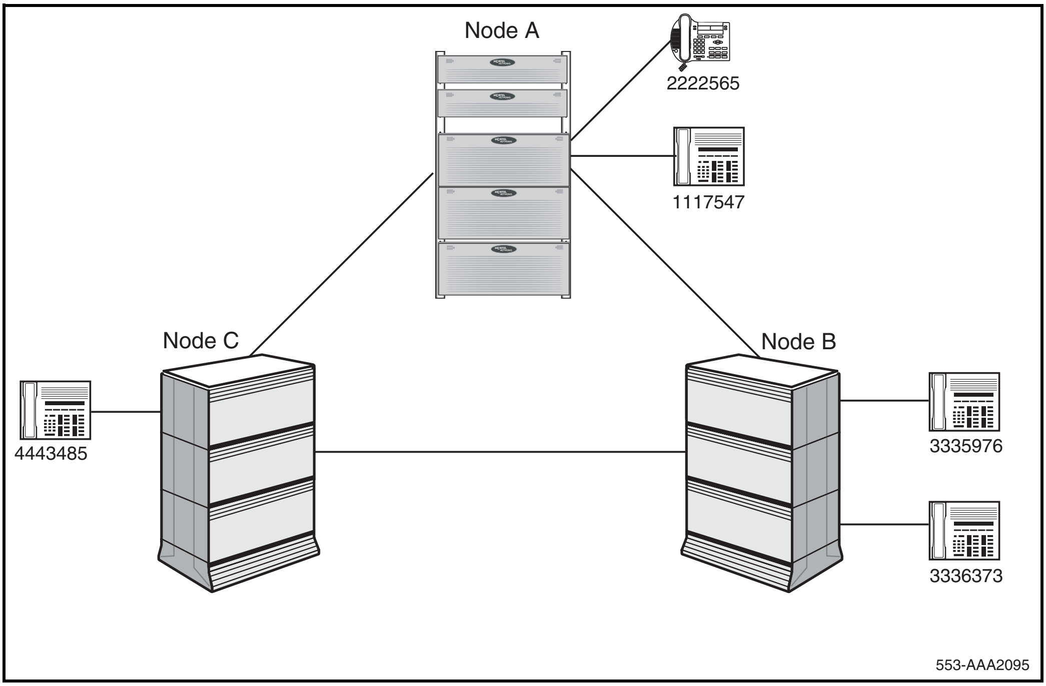
Making UNP with Transferable DNs (TNDN) on CS 1000E — CDP network wide

System diagram

The TNDN provides a facility where in the users moving from one site to another can retain their number.

TNDN using UNP would work the same way as in a CS 1000M or CS 1000S system. Consider the following example to illustrate the TNDN behavior in the network shown in Figure 63 on page 424.

Figure 63
UNP with TNDN

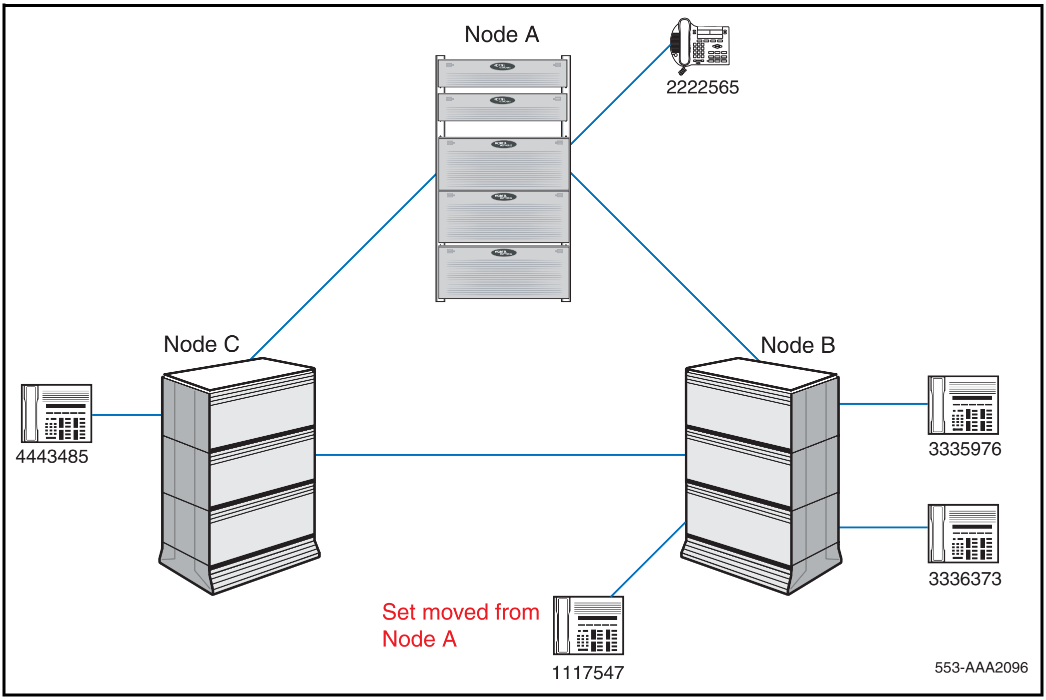


System description

Consider that the network is using a three-digit DSC and LSC. Also note that Node A is CS 1000E node with connectivity to other Nodes over PRI MCDN. In the example shown above, node A has two CDP Local Steering Code (LSC) prefixes — 111 and 222. Node B uses CDP Local Steering Code (LSC) prefix 333, and node C uses CDP Local Steering Code (LSC) prefix 444.

If any user on CS 1000E moves to a different location, the number can be transferred. Consider that the user 1117547 on node A moves to node B as shown in Figure 64 on page 425.

Figure 64
UNP setup after the user has moved to a different location



Procedure 8
Provisioning for UNP dialing on CS 1000E

1 Gateway Selection

Not applicable. The gateway selection is done by the remote IP device (Signaling Server).

2 Numbering plan entry on the CS 1000E

If not already done, associate the route to Signaling Server to the VNR (Vacant number routing).

3 GateKeeper provisioning

The next step in the configuration is provisioning the numbering plan entries in the NRS.

4 Gateway provisioning

Not applicable. The gateway is remote.

Note: The provisioning of UNP for TNDN is same as in CS 1000M or CS 1000S systems.

End of Procedure

Call scenarios

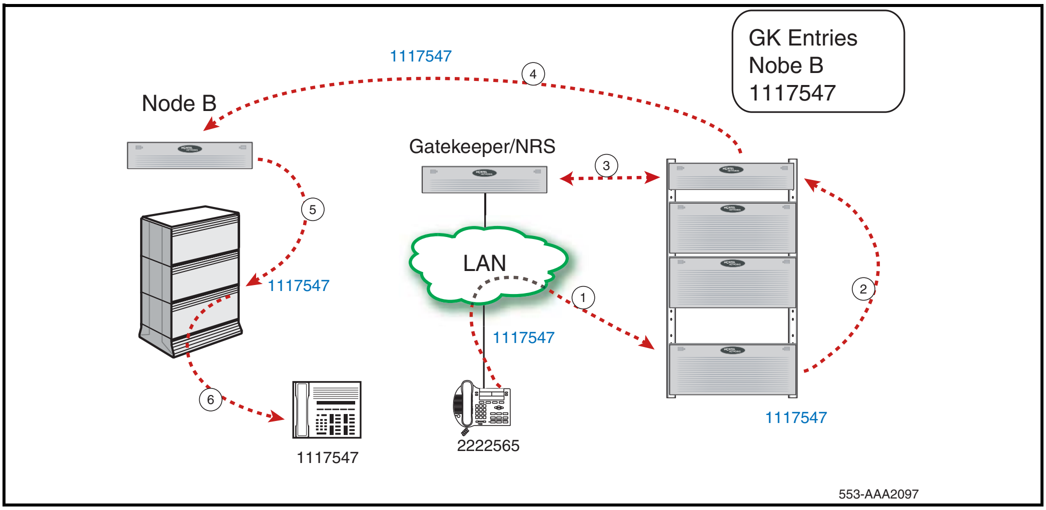
Call scenario 11: Call flow when a telephone moves from CS 1000E

In this scenario, the caller is placing a call at the Call Server, over IP to Node B site, where the call terminates on the desired destination.

Table 84
Call Scenario 11 Sequence

H.323 sequence	SIP sequence
The user 2565, dials 1117567.	
The Call Server detects this as a vacant number and routes the call to Signaling Server over the route configured.	
The Signaling Server sends a request to Gatekeeper for address resolution. Assuming that the Signaling Server with the cost factor of “1” registered to the gatekeeper. The IP address of Node B is sent to the requested Signaling Server.	The call is then routed to the redirect server for address resolution. The digit string sent for address resolution is 1117547. Since the entry with cost factor “1” is registered, the IP address of the endpoint — Node B- used to forward the INVITE.
The Signaling Server on the Call Server places the call to the Signaling Server of Node B	The Signaling Server of Node B receives the call.
The call is sent from the Signaling Server to the Call Server on Node B. The Call Server finds that 1117547 is configured.	
The call terminates on the telephone.	

Figure 65
Setup explaining call scenario 11 for TNDN call



Incoming calls – Non-ESA

Incoming calls to CS 1000E would behave the same way as CS 1000S. The only difference being when the call comes from PSTN to the telephone which is configured on the Call Server.

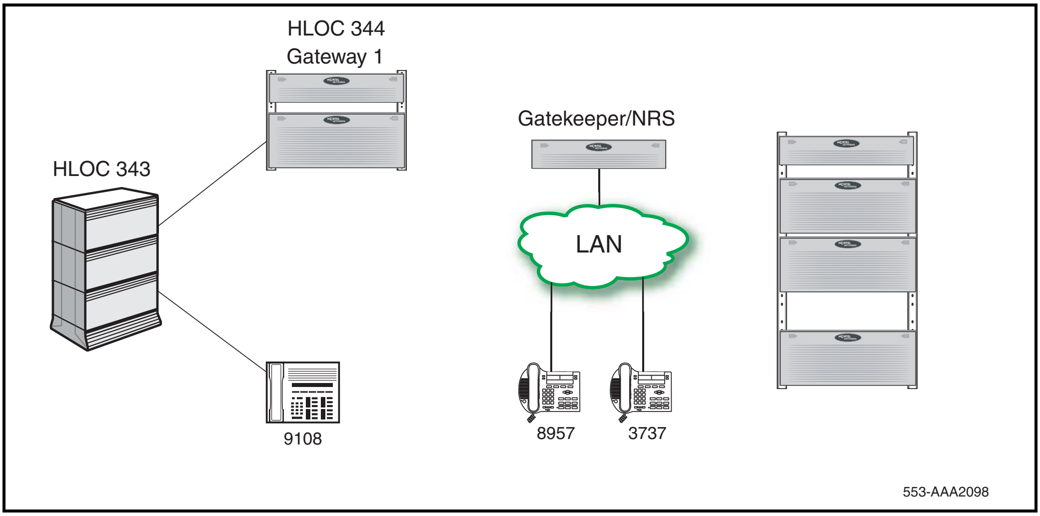
To explain this let us consider the following scenarios

- Incoming UDP (private network) call to CS 1000E
- Incoming DID call (public network) to CS 1000E

Normal private network incoming call

Consider the normal scenario where CS 1000E is setup in a UDP network.The call is made to a telephone which is configured on the Call Server

Figure 66
Setup for incoming call to CS 1000E



System description

A CS 1000E with one (or more) gateway is introduced in a UDP network. The home location code of the various nodes is defined; assume for the discussion that the HLOC of the CS 1000E node is 344 and that of the node where the call is coming in is 343. Consider that the gateway is connected to the UDP network using MCDN.

Procedure 9
Provisioning incoming non-ESA calls

Typically, the gateway where the call entered the network converts it to a UDP location code call.

1 Gateway Selection

Not applicable. The gateway selection is done by the remote IP device (Signaling Server).

2 Numbering plan entry on the CS 1000E

If not done already, provision the RLB for the use of this number. No special DMI is required.

Provision the home location code.

3 NRS provisioning

The next step in the configuration is provisioning the numbering plan entries in the NRS.

4 Gateway provisioning

The Call Server of the gateway connected to the CS 1000E is provisioned to convert the incoming UDP number to a CDP number before routing the call to core call processing on the Call Server. It determines that the received location code is the home location code, and deletes it.

End of Procedure

Call scenarios

Call scenario 12: Incoming UDP call to gateway and the called party is on Call Server

In this scenario, the gateway is connected to another CS 1000E via a PRI trunk and the gateway is in the same CDP domain as Call Server.

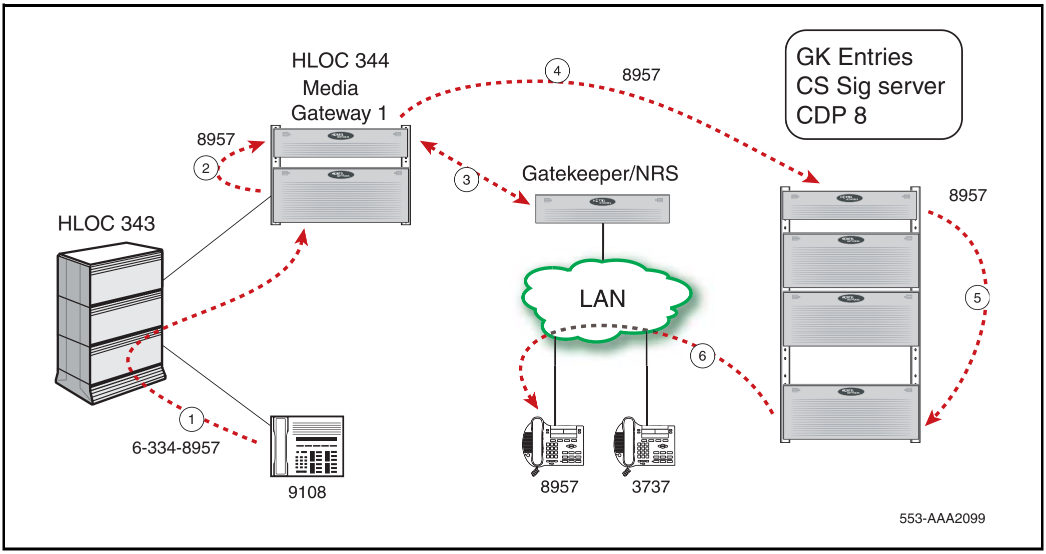
Table 85
Call Scenario 12 Sequence (Part 1 of 2)

H.323 sequence	SIP sequence
The user 9108, dials 6-344-8957. The call is routed by the Node to Media Gateway 1 Call Server.	
The gateway finds 344 as HLOC and strips the code and converts the number to a CDP number and routes the call to the Signaling Server connected.	
The Signaling Server sends a request to the Gatekeeper for address resolution. Assuming that the Signaling Server with the cost factor of “1” registered to the gatekeeper. The IP address of CS 1000E Signaling Server is sent to the requested Signaling Server.	The call is then routed to the redirect server for address resolution. The digit string sent for address resolution is 8957. Since the entry with cost factor “1” is registered, the IP address of the endpoint is used to forward the INVITE.
The Signaling Server then places the call to the Signaling Server of Call Server.	The Signaling Server of the CS 1000E Call Server receives the call.

Table 85
Call Scenario 12 Sequence (Part 2 of 2)

H.323 sequence	SIP sequence
The call is sent from the Signaling Server to the Call Server. The Call Server finds that 8957 is configured.	
The call is terminated on the destination telephone.	

Figure 67
Setup to describe the call scenario 12 for incoming UDP call

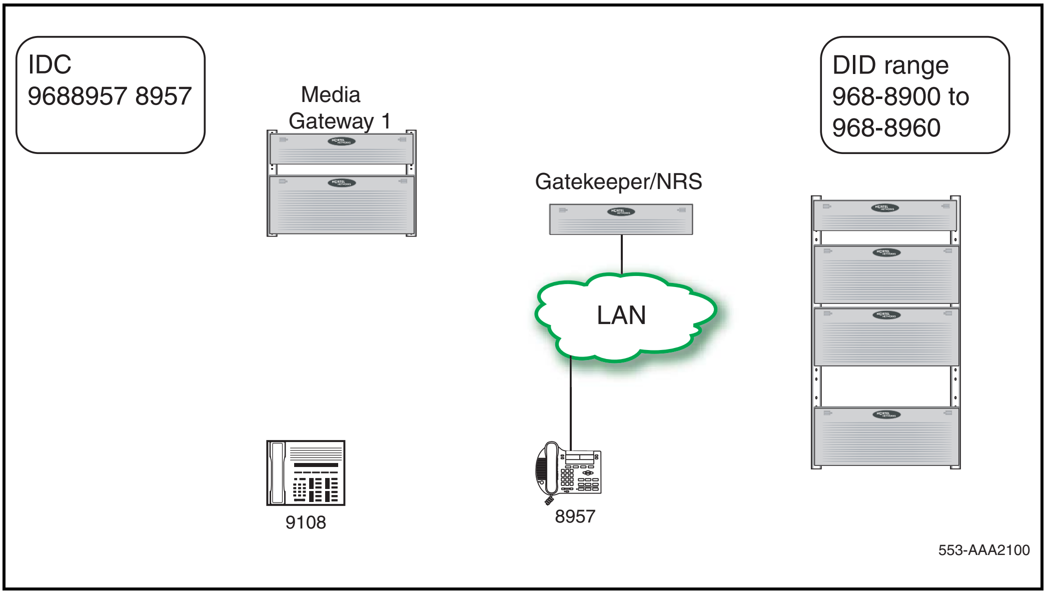


Incoming DID call to CS 1000E

System diagram

Consider the normal scenario where CS 1000E is setup with a PSTN network.The call is made to DID number of a telephone which is configured on the Call Server

Figure 68
Setup for incoming DID call to CS 1000E



System description

CS 1000E with one gateway is connected to a PSTN. The CS 1000E node has a DID range from 968-8900 to 968-8960. Consider that a user on the PSTN makes a call to DID number on CS 1000E.

Procedure 10
Provisioning incoming DID call to CS 1000E

1 Gateway Selection

Not applicable. The gateway selection is done by the remote IP device (Signaling Server).

2 Numbering plan entry on the CS 1000E

If not done already, provision the RLB for the use of this number. No special DMI is required.

3 GateKeeper provisioning

The next step in the configuration is provisioning the numbering plan entries in the NRS.

4 Gateway provisioning

The gateway connected to the CS 1000E is provisioned with an IDC table to convert the incoming DID number to a CDP number before routing the call to the Call Server.

Note that the PRI (or other) gateway relies on the LDN0 at the gateway to determine how many of the trailing digits to translate as the DID number. If the incoming calls are to be treated as 5 digit numbers, the LDN0 must also have 5 digits.

End of Procedure

Call scenarios

Call scenario 13: Incoming DID call to gateway and the called party is on Call Server

In this scenario, the gateway is connected to PSTN and the gateway is in the same CDP domain as Call Server.

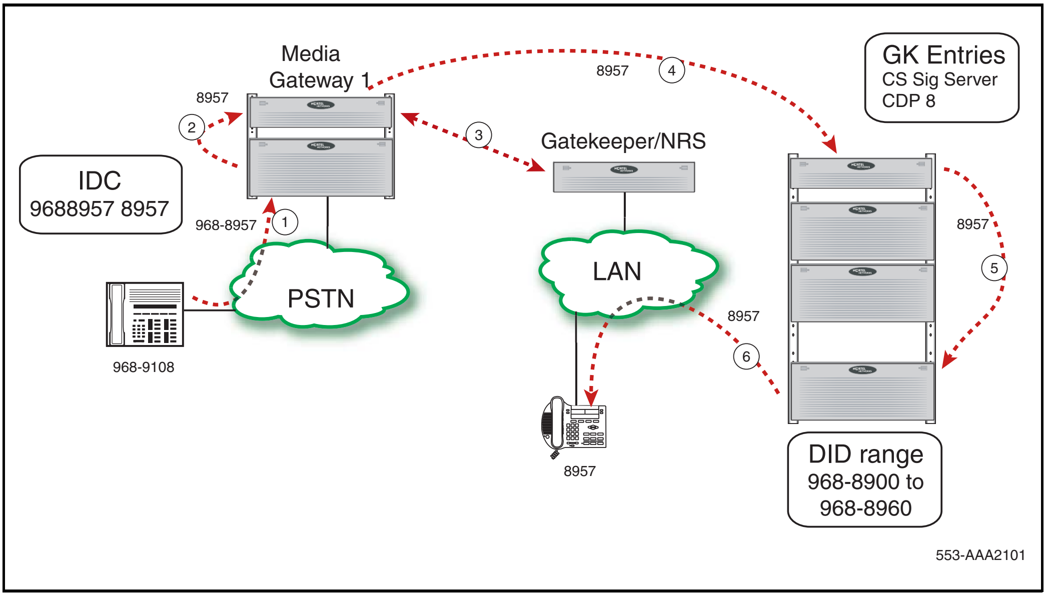
Table 86
Call Scenario 13 Sequence (Part 1 of 2)

H.323 sequence	SIP sequence
The user 968-9108, dials 968-8957.	
The gateway converts the DID number into a CDP number and routes the call to the Signaling Server connected.	
The Signaling Server sends a request to Gatekeeper for address resolution. Assuming that the Signaling Server with the cost factor of “1” registered to the gatekeeper. The IP address of CS 1000E Signaling Server is sent to the requested Signaling Server.	The call is then routed to the redirect server for address resolution. The digit string sent for address resolution is 8957. Since the entry with cost factor “1” is registered, the IP address of the endpoint is used to forward the INVITE.

Table 86
Call Scenario 13 Sequence (Part 2 of 2)

H.323 sequence	SIP sequence
The Signaling Server then places the call to the Signaling Server of Call Server.	The Signaling Server of the CS 1000E Call Server receives the call.
The call is sent from the Signaling Server to the Call Server. The Call Server finds that 8957 is configured.	
The call is terminated on the destination telephone.	

Figure 69
Setup to describe the call scenario 13 for incoming UDP call



ESA calls

Engineering rule list

Engineering rules are discussed in their applicable sections, and summarized in Table 87 for quick reference.

Table 87
Engineering rules list (Part 1 of 2)

#	Rule	Page
1	Trunking gateways must physically connect to the correct E911 area if the call is to reach the correct PSAP.	449
2	Always use "prepend digits" on the Virtual Trunk routes.	449
3	Do not terminate an ESA call from an IP Peer source on a CS 1000E. Terminating on a Trunk Gateway is acceptable.	449
4	For ESA, analog trunks (excluding CAMA) must be either used on the Trunk Gateway, or for calls directly from a security station to the PSAP.	454
5	All MG 1000E systems must be single customer.	460
6	Do not mix types of routes when using STEP routes.	461
7	Provision the ESA parts of the CLID entry block of an incoming analog route to indicate an answering position of some sort on the remote switch.	469
8	An MG 1000E cannot have more than one zone.	469
9	Provide more Virtual Trunks and DSP resources on the Trunk Gateway than the sum total required for all trunks to the PSTN or other networks.	471
10	The number of Virtual Trunks at the security desk on the gateway should be higher than the total of possible outgoing trunks and maximum number of ESA calls being handled by the security desk.	506
11	Avoid using the MG 1000E for a security center. If necessary, it can be done, but it is not recommended.	523
12	If possible, always connect two MG 1000E systems using a CAMA trunk loop-back when placing a security desk on the CS 1000E.	526

Table 87
Engineering rules list (Part 2 of 2)

#	Rule	Page
13	The security desk on the CS 1000E should use local CAMA trunks to the PSTN unless forced to do otherwise.	526
14	If it is on the CS 1000E, the ESA security desk needs a zone exclusively for itself.	535
15	Always omit the ESA locator for the security desk zone.	535
16	The number of Virtual Trunks at the security desk on the MG 1000E should be higher than the total of possible outgoing trunks, maximum number of ESA calls, and average “telephone to trunk calls over Virtual Trunks” count being handled by the security desk.	537

Introduction

In this section, there is frequent reference to “a DID unit”. Readers should refer to “Glossary of terms” on page 610 for definitions of this and other key terms.

> ***Note:*** For ESA calls, the call type is always SPN when using Virtual Trunks. This section is mostly written with details as relating to “North American ESA”. Many of the concepts involved have similar procedures, entities, and so forth in other countries, but the details can diverge wildly. For example, what is a valid ANI length? And what are valid trunks to the PSAP, as CAMA trunks are North American?
> The trunks between a trunking gateway and the public network are market specific. Please refer to the appropriate NTPs to determine the available trunks in a MG 1000T, CS 1000M or CS 1000S for a specific country. The trunks between an MG 1000E and the PSAP are limited to “analog trunks only”, and whenever an ANI is required, the trunks must be CAMA. Typically, without CAMA this means that an ANI is not available, as there is no way to send the ANI. As an example, a basic DID trunk cannot provide a CLID.

For ESA calls from CS 1000E to a trunking gateway, the call type is always SPN when using Virtual Trunks (that is, IP Peer Trunking). The call ceases to be an SPN if it results in a call to the PSTN over ISDN trunks, or for

CAMA trunks it ceases to have a number type and plan when the user places the emergency call.

ESA calls will all leave the private network; the PSAP is within the public network, so this is effectively an axiom here. The “exception” is when the M911 feature is used to provide a local answering position. If the M911 feature is used, the call may return to a private network type of switch such as the CS 1000M or CS 1000S; note, though, that this is a completely independent feature.

An ESA number is typically a “well known digit sequence” consistent throughout a large geographical area. To provide two examples, in the UK the sequence is “999” and in North America it is “911”, but other jurisdictions can and do use other sequences; for that matter, some countries use multiple ESA digit strings. In addition, the number the user dials is not necessarily the number actually sent to the PSAP. Because the ESA feature at the gateway to the PSTN allows digit manipulation to replace the ESA DN or prefix it with directing digits, the called number can end up manipulated.

ESA calls from CS 1000E can be broadly categorized by how those calls are processed by the Call Server before the call leaves the IP domain and travels over TDM resources. The options are:

- A call that is from a DID capable unit residing in the primary zone, which subdivides into:
  - Units that have a fixed location (not capable of being moved without reprovisioning)
  - Mobile units such as soft clients and wireless units, which can move within the zone
- A call that is not from a DID capable unit but still resides in the primary zone, which also subdivides into:
  - Units that have a fixed location (not capable of being moved without reprovisioning)
  - Mobile units such as soft clients and wireless units, which can move within the zone

- A call that is from an analog signaling trunk residing in the primary zone. Typically, this is a trunk used for the remote switch to make emergency calls “when all else fails and no other alternative is available”.
- A call that is from a DID capable unit residing in another zone than the primary zone, which subdivides into:
  - Units that have a fixed location (not capable of being moved without reprovisioning)
  - Mobile units such as soft clients and wireless units, which can move within the zone
- A call that is not from a DID capable unit that does not reside in the primary zone, which also subdivides into:
  - Units that have a fixed location (not capable of being moved without reprovisioning)
  - Mobile units such as soft clients and wireless units, which can move within the zone
- A call that is from an analog signaling trunk that does not reside in the primary zone. Typically, this is a trunk used for the remote switch to make emergency calls “when all else fails and no other alternative is available”.

All ESA calls use a dialable number (the ANI for CAMA; the CLID for ISDN and Virtual Trunks) transmitted to the PSAP, to help to identify the end user placing the call; however, the number and how it is obtained varies based on the service level available. From this perspective, ESA has two main variants.

1 Basic ESA service by the PSTN uses the billing number of a site as the "call-back" number, and to identify the location. For callers on a PBX or Call Server connected to the PSTN, this number — which is provisioned at the PSTN — forces all calls using this trunk to use a common call-back number. For ESA trunks that cannot provide an ANI, this is the only alternative.

2 Enhanced ESA (enhanced 911, or E911) uses a more specific mechanism. The capability was initially specified by the FCC to provide better service to users within a PBX, and may or may not have equivalents in other countries as well. It was designed to accept an identification from the PBX, which must transmit a number — usually called the Automatic Number Identification or ANI — that can be used by the PSAP to isolate the caller's physical location.

All calls handled by a PSAP come from a unit located within the PSAPs "Emergency Services Zone", or ESZ. The PSAPs have access to an Automatic Location Identification database (ALI database) that allows the PSAP operator to determine the caller location or location of the nearest call-back site. The DID capable numbers are usually provisioned in such a way as to allow the PSAP operator to direct the emergency personnel to the correct spot (for example, sending the ambulance staff to a specific pillar number close to the caller).

The norm is to isolate the caller to a specific area, such as the North American target of a 40,000 square foot location, which is approximately one floor on a large office building. This physical area is normally spoken of as the "Emergency Resources Location", or ERL, and should indicate the maximum area in which the caller could be found. Note that the ESZ and ERL has little or nothing to do with the Zone ESA; the ESZ and ERL are PSTN constructs.

This acts as the "maximum area"; however, the location is usually more specific than a "40,000 square foot location". The ANI can serve to locate the caller with a much greater degree of precision. The issue is that the call may be placed through facilities used in common with many other users. In fact, the closest PSAP to the trunk access to the network may be the wrong PSAP for the user.

This brings up a concept — the "tandem emergency network", sometimes called the "public 911 tandem network" or other similar terms. It typically works in parallel with the E911 (Enhanced 911) service, and exists where a number of PSAPs use a common routing service to send the call to the PSAP that really is the closest (or, at least, the closest available).

To avoid confusion talking about "networks", the expression used here is "E911 tandem domain".

An E911 tandem domain may be very large geographically. It is not unrealistic for it to encompass a province, state, or other subsection of a large country, or to enclose a complete country that is small geographically. The only requirements are:

1 All PSAPs within the E911 tandem domain must be reachable from any trunk access within that domain.

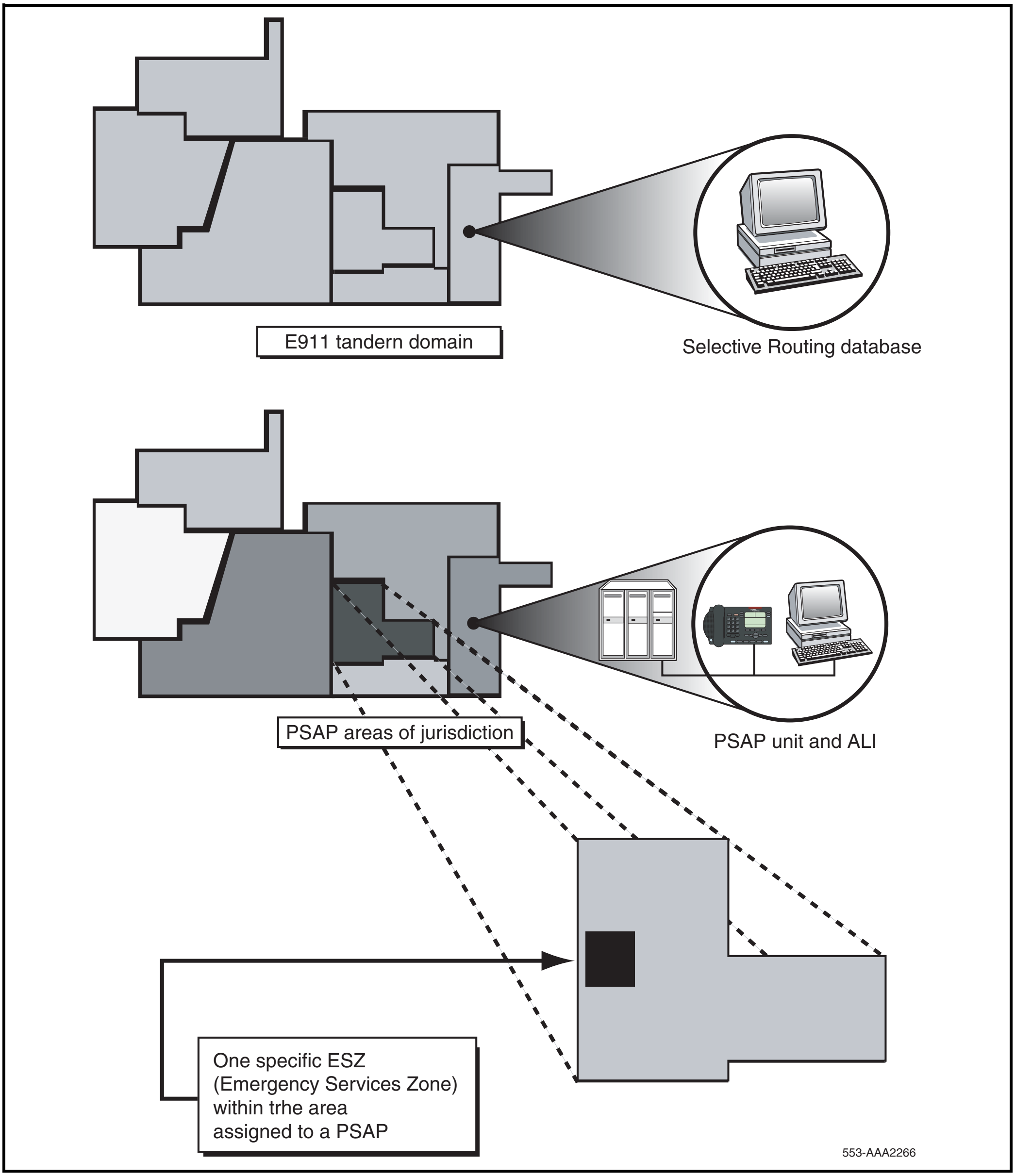
2 The domain must have a "Selective Routing database" to allow calls entering the domain from the private network or PBX to be routed based on the ANI/CLID to the geographically correct PSAP (or closest neighbor, in the event of PSAP congestion or failure). This database may or may not be intertwined with the ALI database; that is a PSTN decision and has no bearing here.

3 Each PSAP has one or more geographical areas (Emergency Resource Locations, or ERLs) within its Emergency Services Zone, that is the specific area in which the PSAP needs to isolate the caller. The ALI must be able to specify the location of the caller.
Note that this ALI may be a fine enough granularity to specify a specific location (such as a 4 person cubical) or coarser grained (for example, a floor).

4 Normally, each PSAP has the capability to transfer the emergency call to another PSAP without loss of information.

Refer to the following figure for more clarification.

Figure 70
E911 tandem domain, PSAP, and ESZ



The theoretical E911 tandem domain at top left in Figure 70 on page 440 is shown with lines within it subdividing it into smaller areas. These represent the boundaries of the 7 internal geographical regions serviced by 7 PSAP centers.

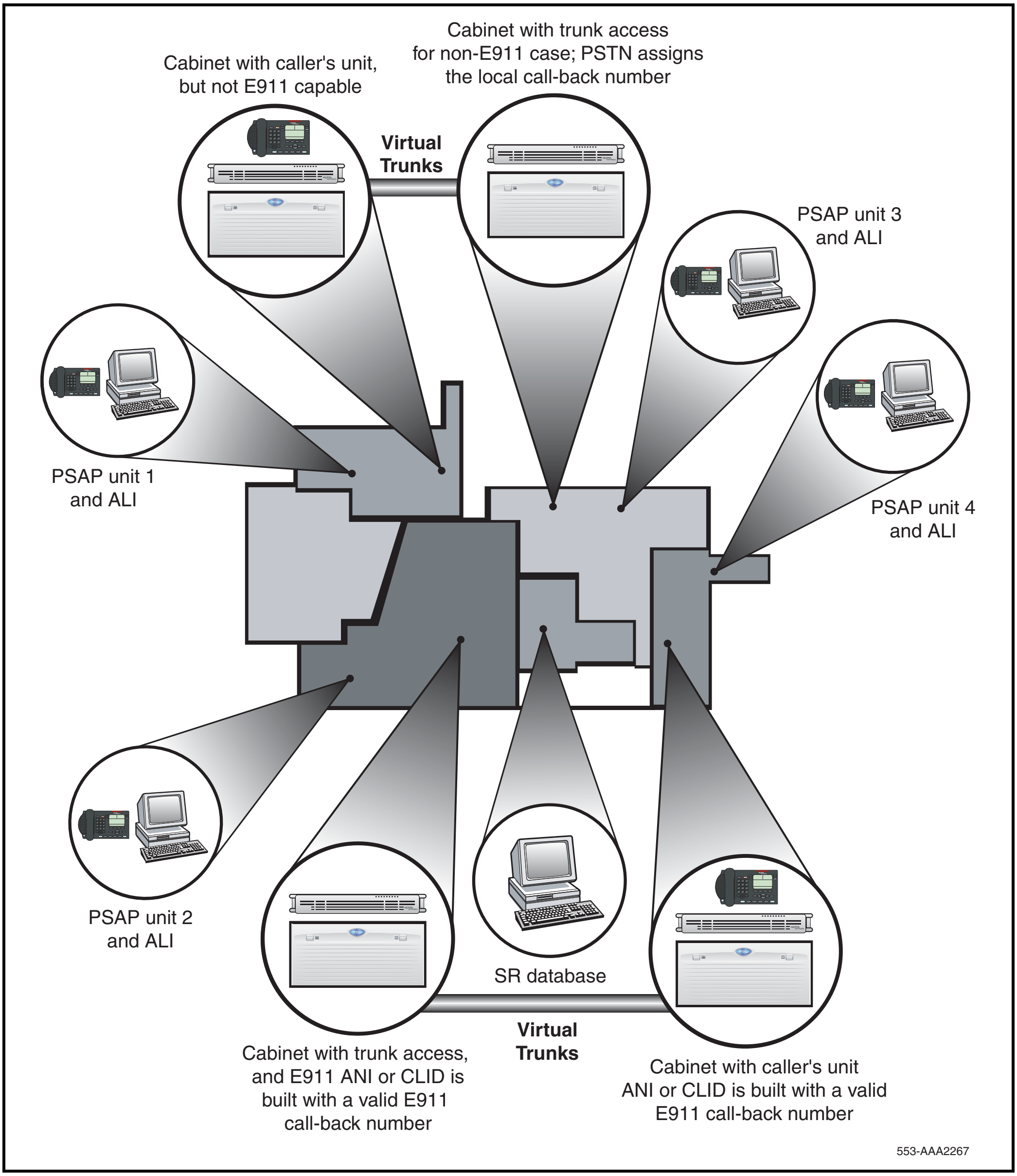
Emergency calls may either use a trunk dedicated for ESA calls between a PBX (or Call Server) and the appropriate PSAP for that switch. In that case, the calls terminate directly on the PSAP without routing. However, the ESA call may also use another trunk type, such as an ISDN trunk. In that case, the message includes the public Emergency Number and the ANI or CLID to allow the call to route successfully. It just needs a mechanism to determine the correct PSAP.

The PSTN provides a procedure to direct the calls correctly. Within the E911 tandem domain is a “Selective Routing” database. Calls to the emergency services are first directed to this device to determine the correct PSAP to handle the call. It takes the ANI (or CLID) and compares it to its list of destinations, identifies the correct PSAP, and forwards the call.

Within a PSAPs area of jurisdiction are usually a relatively large number of users (as opposed to the typical number of users on a PBX). When the Selective Routing database and switch received the call, it routed the call to the PSAP, which presents the call to a PSAP operator and provides additional information from a look-up in the ALI. Note that a caller using enhanced 911 to call the PSAP has the Selective Routing database use the CLID or ANI provided to determine the PSAP. This can identify a user’s location to within as small an area as within several feet of an identification point such as a numbered pillar, or a subsection of a floor. Without E911, the billing number of the trunk is used, so “all callers have the same location”.

In the next figure, two users are in the E911 tandem zone. One has E911; the other does not. In both cases, the users are in a different PSAP area than the trunk to the PSAP (for example, they could be on an expansion cabinet or MG 1000E not collocated with the core Call Server.

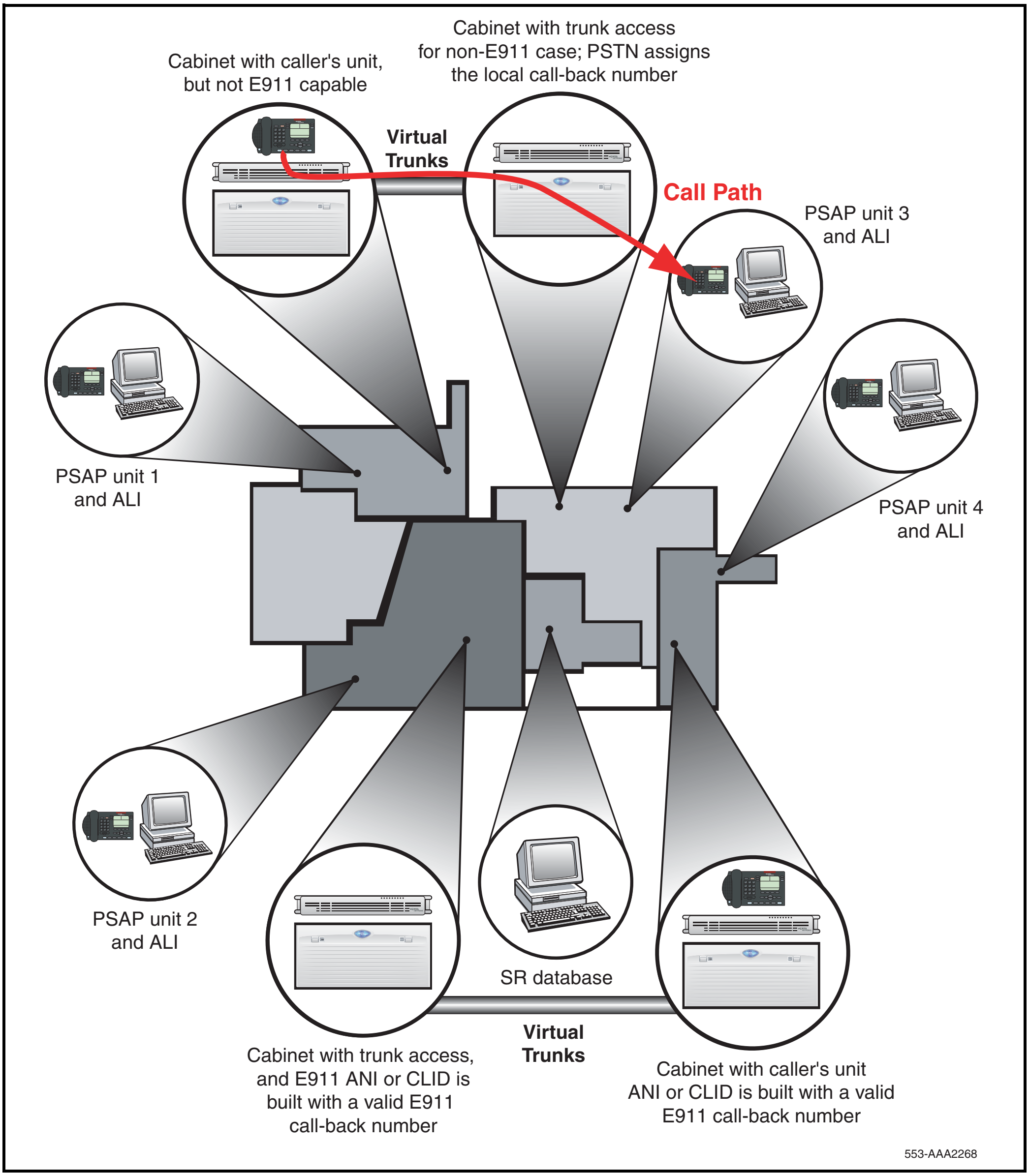
Figure 71
E911 tandem versus basic ESA without E911 — unit locations



In this figure, there are two “customer networks”. One has a switch and a caller located in the geographical area associated with PSAP 1. It connects by IP Virtual Trunks to the cabinet with the trunks to the PSTN, located in the geographical area associated with PSAP 3. The other has the switch and user in PSAP 4, but the trunks in PSAP 2. They share the SR database.

The next figure concentrates on the non-E911 customer. As there is no E911 enabled for this customer, the PSTN assigns the billing number for the customer to all ESA calls, so the call routes to PSAP 3. Unfortunately, the caller is physically an ESZ served by PSAP 1.

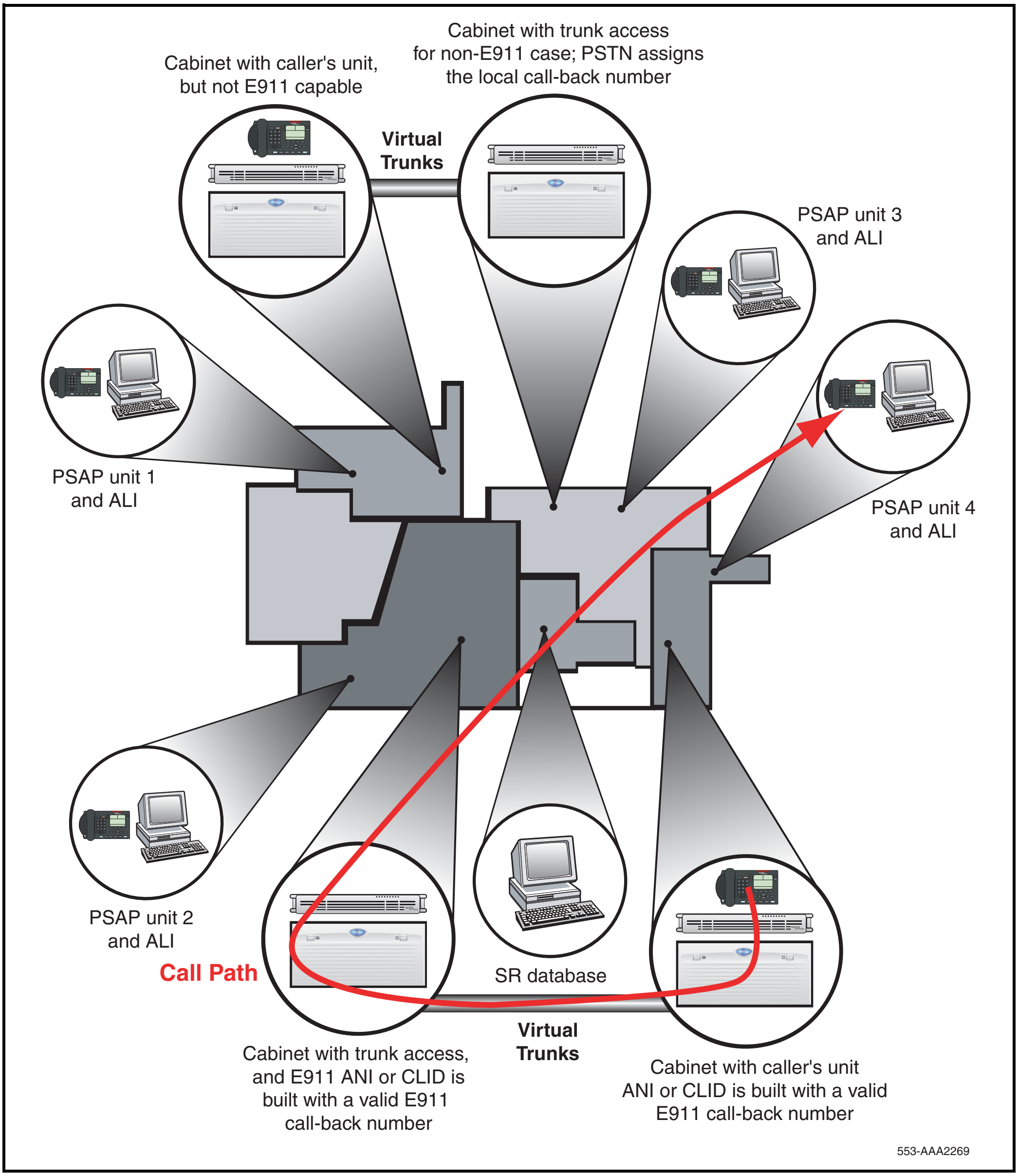
Figure 72
ESA without E911 — call routing



In this figure, because the customer with the user call at top has not subscribed to E911, the PSTN assigned the billing number for the customer to all ESA calls, and so that is used. The call routes to the cabinet/MG 1000E with trunk access, then goes to the PSTN. The PSTN uses the billing number to route to the PSAP 3 (the PSAP of the trunk access device), which is not the one for the user's location. Unfortunately, the caller is physically within an ESZ served by PSAP 1.

Compare this with the E911 handling displayed in Figure 73 below.

Figure 73
ESA with E911 — call routing



The call using E911 also routes the call to the trunk. However, here the E911 is used and a valid ANI (CLID) provided by the originating caller's switch allows the SR database to route the call across several PSAPs to the correct one. Even though the trunk was located in the area served by PSAP 2, the caller — and the CLID/ANI — indicates a user in the area served by PSAP 4, so the correct PSAP is contacted.

The limited area intended for the ANI resolution in the ALI creates problems with IP. A DID capable unit that the Call Server can identify with a specific TN can use the DID number (with any extensions or prefixes required for the specific local authorities). This permits precise locations. A non-DID unit (which includes all analog trunk types except for ones specifically designed to carry a Calling Party Number, such as MFC trunks) has no such number, so it cannot be uniquely identified to the PSAP. At best, it can be isolated to a specific "nearest call-back site". Even more importantly, a mobile unit or one in a zone other than the primary zone cannot even use the DID number:

- The mobile unit could be located at "one of many" locations in the building, so the ability to use the CLID block to build the ANI is possibly a severe error — the DID number may be officially located at one site (for example, on the second floor of tower 1) while the actual user is in another (possibly on the fifth floor of tower 3).
- The unit in the non-primary zone should exit from the same MG 1000E or the nearest MG 1000T. However, if it is IP it is registered to the Call Server but the Call Server has no way to isolate it to a specific physical location — if it "belonged" to the device at the hub of zone "N", it could have been moved to zone "M" and the provisioning would now be out of date. If it is not IP, the unit is on an MG 1000E; it has to use IP signaling in the same manner as the IP unit to complete the call.

Analog trunks also have potential issues associated with them. An analog trunk belonging to a specific route may be assigned a CLID block indirectly, through the route data block. Realistically, this is no more accurate than using the zone locator from the zone ESA (which is discussed in detail later).

The route data block in LD 16 has a "CLEN" prompt, output whenever the ESA package is enabled and the call is not an ISA ISDN route. "CLEN" actually stands for "**CL**ID **EN**try", and should not be confused with the other "CLEN" prompt for the length of the MFC CNI (Calling Number Identification) in India, where it is "**C**NI **LEN**gth". The two prompts occur at radically different locations in the LD prompt sequence; the CLEN for the CLID block is after the "ACOD" (Access Code) prompt; the CLEN for the Indian MFC only is available for an MFC route when INDMF (Indian MFC) is set to YES.

When the TDM route is from a remote switch, it should be point to point. That is, any trunk that belongs to this route must originate on switch A and terminate on switch B. All other provisioning choices are highly discouraged. This does not guarantee that the call is not tandem through the remote switch.

Provided that the user has not intentionally diverged from this provisioning recommendation, a CLID entry block may be defined that provides a reliable ANI for the destination site. If an analog trunk at TN 16 0 2 12 belongs to route 16, and route 16 uses CLID entry block 123, whatever block 123 defines to use for the ANI can be used. In effect, an analog trunk with no CNI capability is the same as any other non-DID fixed location unit, but instead of having the CLID block provisioned against the unit, it is provisioned against the route.

So, this leaves three or four types of CLID entry block:

- Using the DID number as the base for both the ANI and for normal call Calling Party Numbers — used by fixed location DID units only
- Using the DID number as the base for normal call Calling Party Numbers but having a pre-defined site-wide ANI associated with a primary emergency services "callback" answering post — used by mobile DID units
- Using a pilot number (such as an LDN) as the base for normal call Calling Party Numbers but using an ANI for a local emergency services "callback" answering post closer to the end user — used by fixed location non-DID units (and analog trunks)
- Using a pilot number (such as an LDN) as the base for normal call Calling Party Numbers but having a pre-defined site-wide ANI associated with a primary emergency services "callback" answering post — used by mobile non-DID units

If the site has a single emergency services "callback" answering post, the third and fourth CLID entry blocks are identical.

Engineering Rule 1

Trunking gateways must physically connect to the correct E911 area if the call is to reach the correct PSAP.

The trunking gateway must be located in the right E911 tandem domain to get to the correct Selective Routing database, in order to reach the correct PSAP, based on the real location of the MG 1000E or user. To ensure the right PSAP is reached, the ANI or CLID must be built to convey the right information to firstly the SR DB and then to the PSAP, to allow it to make the correct data retrieval from the ALI.

However, it is possible that all “correct” trunking gateways may be in use (for example, a major emergency may have several callers dialing the ESA DN at once). In this case, it may be preferable to at least get “a” PSAP rather than not getting “the right PSAP”. With E911, this may be resolved by the selective routing system to land on the right PSAP.

This is at the discretion of the system administrator.

Engineering Rule 2

Always use “prepend digits” on the Virtual Trunk routes.

“Prepend digits” are the concatenation of the GGP and the digit or digits representing the type of call. If the user does not use prepend digits for the VTRK calls, there can be no more than one PSAP Trunk Gateway list for the entire network. Using “911” as the example, the digits “911” can resolve to only a single least cost routing list of IP addresses in a network. Therefore, all “911” calls try to go to the first entry in the list, attempting the alternate entries if this entry is unavailable, whether it is correct for the caller’s switch or not.

Engineering Rule 3

Do not terminate an ESA call from an IP Peer source on a CS 1000E. Terminating on a Trunk Gateway is acceptable.

Virtual trunk calls do not necessarily use physical resources. If they do not use any DSPs, for example, they are not “anchored” to a specific MG 1000E, and therefore may belong to “an indeterminate one of many zones” locally. Therefore, ZESA really does not apply.

On the other hand, if the call lands on a Trunk Gateway, it uses basic ESA to terminate. As zone ESA is no longer involved, the call succeeds.

Call flow overview

One key concept is the GGP. This prefix is more common in descriptions of the other calls from a CS 1000E, but applies here too. It specifies an ordered list of destination gateways, arranged from lowest to highest cost factor (most preferred to least preferred).

A second major topic is the “primary zone”. For the units served by the Call Server, a bandwidth management zone is associated via provisioning. However, under normal circumstances one MG 1000E is located in the site with the largest number of users. This zone typically also provides service for a number of IP units if the Call Server becomes unavailable, but that is a secondary consideration. As this zone receives “special handling” for all fixed location devices, it needs a convenient handle to discuss it; within this document, this is called the primary zone.

The call flow has four discrete phases, described below.

Call flow phase 1: Digit Analysis on the Call Server

Handling varies based on whether the user is “local” (the normal case, which includes IP Phones registered locally) or remote (using an analog trunk). It has to be one of the two; if using ISDN or other trunks, the call would have been routed over ISDN to the appropriate gateway directly, and the CS 1000E Call Server would not even be aware of the event.

- Local user:

  The user dials the ESA DN. The system identifies the ESA DN, and determines the appropriate zone.

- Remote user dialing into the CS 1000E over an analog trunk:

  Remote analog trunks use the zone assigned to the MG 1000E in which they reside as though it had been assigned as their own zone.

  The user on the remote switch dials the ESA DN. The remote system identifies the ESA DN, determines the correct zone for the trunk if applicable (the remote switch may be a CS 1000E), and attempts to use the (zone) ESA specified trunk route. If it fails to get a trunk, the call steps to an alternate. In this case, the alternate was the analog trunk to the local CS 1000E.

  This should be the only time that a CS 1000E receives a call from another switch for ESA; the call could not go out over the PSTN (or VTRK) remotely, so it stepped to an analog trunk between it and the CS 1000E.

  The outpulsed ESA DN is received by the CS 1000E, and the number analyzed. It is found to be the local ESA DN. The Call Server determines the appropriate zone for the trunk, based on the MG 1000E of the trunk.

Call flow phase 2: Zone processing

The trunk unit has an ESA zone ("Zone ESA data block") assigned, which is the zone assigned to the MG 1000E. For all CS 1000E calls with functioning and reachable Call Servers, the call needs the NRS to route the caller to the correct ESA H.323, or SIP to PSAP Trunk Gateway. Therefore, on the Call Server a ZESA block is used for all calls.

The ZESA data varies based on whether this is the primary zone or any other zone:

- Primary zone (or zones)

  The primary zone is mostly a concept. It is improbable that the system administrator will specifically "name" one or more zone as the primary zone. However, the handling defined for a primary zone is very likely to be provisioned for at least one MG 1000E in the system. This is simple if all MG 1000E systems receiving this treatment belong to the same zone; there truly is only one primary zone in this case, although the zone spans two or more MG 1000E systems. However, this is not necessarily the situation; two separate zones may both need "primary zone" handling.

Assume that a CS 1000E has two or more MG 1000E systems which need to be treated as though they were the primary zone, but belong to separate zones. Any mobile IP units physically located at these devices registered with the Call Server use the site ANI in the CLID entry blocks, so there are no concerns about how to handle these devices. Any other devices on the MG 1000E are either fixed location IP or TDM. If they are fixed location and DID capable, they can use the CLID entry to create a specific ANI for that unit. For all others, the CLID entry block must provide an ANI that can isolate the call to the applicable site. For an analog trunk, this translates as making the CLID entry generate an ANI that resolves to the emergency number on the remote switch and not on the local CS 1000E.

In order to allow using the CLID entry of units in the primary zone to build the ANI, the ZESA block for the primary zone does not have a locator provisioned; this allows the Call Server to identify that the ANI can be built from the ANI provisioning in the CLID entry block. Note that for a fixed location DID unit, the CLID block indicates "DID capable". For a fixed location non-DID block, the CLID entry data must build the ANI of the closest answering point (such as the security desk in the building within a campus). For a mobile unit caller, this is the site ANI. This restriction may be reduced in the future but is the restriction as of CS 1000 Release 4.5.

- Any other zone

  For zones other than the CS 1000E primary zone, the call needs the NRS to route the caller to the correct ESA MG 1000T, but the Call Server cannot distinguish the exact ANI to build. Therefore, as with the primary zone a ZESA block is used. However, in this case the ZESA block must have a Locator provisioned; this allows the Call Server to build the ANI associated with the physical location of the MG 1000E where the unit resides. For a non-primary zone caller, this is the site ANI. This restriction may be reduced in the future but is the restriction as of CS 1000 Release 4.5.

When the ESA handling executes, the On-Site Notification (OSN) record is produced at the applicable TTY or terminal (possibly, in a record file rather than on a traditional terminal). The OSN unit is a unit with the ability to display important information about the ESA call. This usually is located at the security desk or "some other unit where alarm monitoring is located".

There is one OSN telephone per customer, and usually one terminal (TTY) providing OSN records.

Call flow phase 3: Network routing

The ZESA data provides the route number. Note that the route data block has a "STEP" prompt, to indicate an alternate route to use when the indicated route is "all trunks busy". Note that restrictions exist on the type of "step" routes allowed. Refer to"All MG 1000E systems must be single customer." on page 460 and "Do not mix types of routes when using STEP routes." on page 461 and the explanatory text for details.

The ZESA block provides the specific number to transmit as called party number (the SPN GGP and the ESA prefix added to the ESA DN on the IP to TDM trunking gateway). These are mandatory unless the NRS serves only the local CS 1000E. If it serves several, then the ESA DN by itself cannot allow the NRS to select the correct Trunk Gateway list. Therefore, although the prefixes are not really truly mandatory, in a real customer environment the need to differentiate between ESA calls from multiple originators makes them mandatory. The ZESA block also specifies the ESN locator code, used for calls from zones that need a call-back number.

The system seizes resources for the call and transmits the MCDN SETUP to the Signaling Server, which then sends the protocol specific message to the NRS (which may be a gatekeeper, a redirect server, or both). The NRS identifies the destination Media Gateway list, provides the ordered list for "least cost routing" to the Signaling Server, and the call forwards to the destination.

Call flow phase 4: Call Sent to PSTN

The call lands on the destination Trunk Gateway. The Call Server (if the gateway is a MG 1000T, CS 1000M or CS 1000S) or other gateway device invokes local termination, which includes in part removing the GGP. As the number is determined to be the ESA DN on that node, the call routes to the PSTN. However, as this is a trunking gateway, the ANI as received from the originating Call Server in the SIP INVITE or H.323 SETUP is used in the ESA call attempt. An OSN record is generated and possibly the OSN telephone alerted with the applicable display (if NOT on the MG 1000T; there are no “local telephones” there). The PSTN routes the call to the PSAP as determined from the trunk selected and the ANI.

Engineering Rule 4

For ESA, analog trunks (excluding CAMA) must be either used on the Trunk Gateway, or for calls directly from a security station to the PSAP.

Note that a Virtual Trunk can step to or from a CAMA trunk, since the CAMA trunk ignores the dialed digits. CAMA sends the digits specified in the ESA data block provisioned against the DDGT prompt of the ESA data block. It ignores the called digits. Following the DDGT digits, it sends the ANI.

For all other analog trunks, the presence of prepend digits may cause calls to fail. Therefore, other analog trunk types cannot be used when digits must be prepended.

Provisioning overview

To carry out the GGP insertion and deletion, the systems involved must be provisioned correctly. There are two types of trunks that can be used for ESA — local CAMA (or other supported ESA compatible analog) trunks, and trunks on a trunking gateway.

For provisioning ESA calls from CS 1000E to permit use of the trunking gateway, provision the system according to the following steps:

ESA Zones versus Bandwidth Management Zones

With CS 1000 Release 4.5, there is only a single zone associated with a unit — the BWZ (Bandwidth Zone) — and all units have a zone assigned. On the Call Server, each zone has its own ESA parameters provisioned. These parameters allow all IP units or units on the MG 1000E belonging to that zone to use ESA, as they cannot use the Call Server ESA block parameters developed in prior releases; it is not sufficiently flexible to handle multiple zones and to build the prefixes needed for the NRS to correctly route the call.

The Call Server needs to carry out two key functions for every ESA call. Each Call Server has to select the right outgoing trunk to reach the PSTN as close as possible to the right PSAP. The Call Server also needs to be able to identify what information to send to the PSTN as the Calling Party Number or ANI to allow the PSTN to correctly identify the correct PSAP.

The CS 1000E uses the zone ESA parameters to carry out this function for MG 1000E and IP unit users. The routing is based on the destination gateway provisioned for that specific zone. The ANI — which is built either from the ESA zone locator code parameter (if provisioned) or from the CLID entry otherwise — is also built from ESA parameters. However, if the ESA zone locator code is not provisioned, then ***every*** unit in that zone must be able to build a valid ANI to correctly route the caller to the right PSAP.

The telephone is in a zone; however, there is no guarantee that the zone of the IP Phone (which is designed based on the BWZ) matches the ESZ (or, to the Call Server, the “ESA zone” is not necessarily the same as the PSAPs ESZ). The PSAP ESZ may be as small as a single digit number of blocks within a city; the BWZ (and as a result, the ESA zone) may cover a full city. Therefore, the ESA feature has a major interaction with BWZs.

The issue with bandwidth management zones is that they are not necessarily physically collocated. A bandwidth management zone specifies a set of units that must have a common bandwidth handling. However, ESA calls from units should be (and preferably must be) located close enough together to allow emergency services personnel to resolve the location easily.

As an example, a bandwidth management zone on a Call Server may have IP Phones registered from all over a city (for example, New York city has Manhattan, Staten Island, Queens, the Bronx, and so forth). Assuming a WAN with high enough bandwidth it is reasonable that all units are to receive identical bandwidth handling; logically, if the only concern is bandwidth management they should be grouped together. However, each area (such as the Bronx) may have links to a central emergency center located in that region, which redirects the call based on the ANI to the correct Bronx PSAP. Not only should a call to emergency services for a user in the Bronx not be routed to the center (or a PSAP) in Manhattan, but whenever multiple PSAPs exist in a region, the call has to go to the right PSAP.

For a CS 1000 Release 4.5 Call Server with registered units that must be routed to several specific PSAPs, the bandwidth management zone must not exceed the geographical region of the E911 tandem domain in which the PSAP for that zone is found. However, it is understood that under certain circumstances this may not be possible; for example, in a very large office complex the PSTN may allocate two or more PSAPs, but a specific corporate network may have a very small presence in each PSAPs area of coverage. It may be that the corporate network has only one 24 hour staffed emergency callback desk in the complex. In this case, having the callback from the PSAP at least go to someone capable of answering in the right building is an improvement over not being able to get a callback at all.

As a result, Nortel strongly recommends that the bandwidth management zones not exceed the boundaries of the areas served by the PSAP geographically. Having several PSAP centers that could be called from within one BWZ can cause delays in emergency service handling as the calls are transferred between jurisdictions by the emergency services personnel.

Routing ESA calls — implications of “step”

ESA on the CS 1000E requires the system administrator to take a lot of care in provisioning. As an example, in many jurisdictions of the United States and Canada, the emergency number must be “911”. Because ESA handling bypasses all others (effectively preempting all other digit processing treatment), the call processor cannot have a DN that conflicts with these digits. Since “9” is often used for NARS AC2 (the local call Access Code), this is not usually a problem; regular DNs and feature codes cannot collide.

However, even with “9” as ESN access code 2, there needs to be care in provisioning. With “9” as ESN access code 2, the administrator cannot define and use any ESN codes starting with the same digits as the ESA DN. The system may accept them, but as soon as the number matches the ESA DN, ESA is invoked. Using an emergency services number such as “999” as the example, if ESN access code 2 is “9”, the user may be able to provision an access code 2 SPN of 993 and a LOC of 994, but no calls can reach these destinations. As soon as the system detects the “999” at the start, ESA is invoked. See *Emergency Services Access: Description and Administration* (553-3001-313) for details.

The basic ESA feature only provides for a single ESA route per customer on a system. This route may have an alternate accessible via a “hunt list” defined using the STEP prompt in the system provisioning. This may hunt to another, based on restrictions documented in *Emergency Services Access: Description and Administration* (553-3001-313). That is, if the first choice route is “all channels busy”, the STEP prompt indicates a route to try next. If that is also busy, it may also indicate a STEP route.

Note that even though the CS 1000M (or CS 1000S) and CS 1000E allow mixing route types for step routes, in general, the “step” routes on CS 1000E must be of the same type as the main route. If you step from an IP route to a PRI route, the digits inserted for IP are usually invalid on the alternate selection. (As an example, if “44446” is inserted into the IP digit string to allow the NRS to route the call, this confuses a PRI route.)

Therefore, it is a good practice to step from an H.323 route to a SIP route or vice versa, and not to step to any other routes, with the exception of CAMA routes. CAMA routes ignore the dialed digits, transmitting the directing digits (DDGT) as provisioned in the ESA block.

Gateways providing trunk access for ESA should be in the same PSTN Emergency Services Zone (that is, area serviced by a specific PSAP) as the terminals using the gateway, unless the PSTN provides the ability to route the call to a PSAP based on the ANI received. For CS 1000 Release 4.5, that translates as “the same bandwidth management zone”. (In this case, “should be” translates as “must be unless there is an over-riding need not to do so”.)

The calls should leave the network through a trunk at the gateway which is within the same PSTN ESZ. Failure to do so makes it more difficult for the PSAP to identify the correct caller address; however, if no Media Gateways allow trunking to the ESZ in which the terminal is physically installed, “the wrong PSAP is better than no PSAP”. Assuming that the caller can still talk, in the worst case scenario, the answering PSAP may have to transfer the call to the right PSAP, or conference them in.

GGP Planning

Introduction

This is the first step unless the administrator has to execute the provisioning steps used to define ESA data blocks. If the basic requirements are configured already, provisioning starts here.

Although the planning here is identical to "normal SPN" CS 1000E provisioning, providing "terminating side" ESN provisioning on the Call Server for ESA is not normally required. Nortel strongly recommends that the user use "conventional" ESA. None the less, the system administrator may choose to provision ESN alternates using the ESN access codes plus the ESA DN (for example, 6-911 and 9-911) to provide local termination, in case a user panics and enters the ESN access code before entering the ESN DN. In all cases, after local termination results in a normal ESA call, the NRS still looks at the call as an SPN using a GGP, so the planning is still essential.

Details

CS 1000E is a distributed network switch. That is, the components of the switch are distributed across the QOS-managed IP network. In the network, there could be multiple MG 1000T platforms. This section of the configuration concentrates on deciding the appropriate gateway for routing the ESA calls over to PSTN.

The gateways are typically identified by using a unique code referred to here as the GGP, which — together with the called number type indicator — forms the "prepend digits". This code is a set of digits which must be unique across the whole network within the numbering plan/type of number combination used to provide the GGPs. The GGP is used to steer the calls to the proper gateway for further processing.

This step includes the following sub-steps:

- Destination Analysis

  Before the definition of GGP, the user must decide where the ESA calls are to break out to the PSTN. This must be at the trunking gateway that best meets the following selection criteria:

— First choice must always be a gateway in the same physical location as the caller.

— Second choice, used only when the first either does not exist or is unavailable, is the closest trunking gateway to the MG 1000E or the IP unit.

— Third choice (and so forth) are the next closest trunking gateways. It is better to have the call break out to the PSTN within the same city but not at an optimum location than to not get ESA service at all.

- Digit String Grouping

  In this part of the provisioning, a unique code GGP is selected. This is "to terminate on a specific PSTN destination", and not "to terminate on a specific gateway". That is, if two sites in London, England can reach a specific London PSTN user, the GGP applies to both.

  The prefix is built identically to the prefixes for other call types. As with the other examples used (such as for international, national and local calls), the prefix "4444" is assumed in all cases.

- Gateway Group Assembly

  Once the gateway steering code is decided, the gateways need to be grouped together. This grouping of gateways is done on the basis of the cost factor of routing the calls over the QOS-managed IP network. (This planning actually provides the pre-planning for the NRS provisioning. To ESA, the choice is simple: are any trunks free in the route indicated by ESA provisioning?)

- Call Type Digit selection

  To be totally accurate, in theory ESA calls may use a call type digit used for any other calls that delete the correct number of digits and provide local termination. However, this has the potential for misprovisioning, and failure of the ESA feature has too significant an impact to allow administrators the degree of call failure tolerance to take this risk.

  To ensure that the system functions reliably, ESA calls should never share a destination RLI with another call type. Therefore, ESA calls must use a unique call type digit code. This completely separates them from all other call types; the call must terminate locally on the trunking gateway to receive ESA handing there, and must have a completely reliable DMI assigned.

Provisioning the CS 1000E Call Server for basic ESA, and for the primary zone(s)

Prior to any further discussion, there are two rules that are critically important. These are discussed here.

Engineering Rule 5

All MG 1000E systems must be single customer.

An MG 1000E cannot have more than one zone. If a system has two customers they should not share BWZs, because ESA handling on the CS 1000E is currently based on these zones and ESA routing differs based on customer.

Although Enhanced 911 (E911) allows the PSTN to use a database to determine the correct PSAP for a call (based on the ANI), ESA PSAP handling is very volatile without E911. If a call reaches the PSTN for an ESA call without E911, the billing number of that trunk replaces the ANI. Thus, the selected trunk determines what PSAP gets alerted, and not the calling party ANI (and therefore, not the calling party location). Therefore, if ZESA (including Locator codes) is to be used, two customers cannot share one MG 1000E. (Basic ESA using overlay 24 is customer based, so the issue does not arise.)

Also, the ZESA table specifies a route, which is customer specific. From the TN on the MG 1000E, the system determines the customer. From the customer and the ZESA route entry data, the system determines the correct route. However, on a single system, two or mote customers may use the same RDB number (for example, customer 1 and 2 may both have RDB 3). Therefore, since the ZESA data may identify a route that does not exist for all customers, and the ZESA table is zone based, customers must not share zones.

For CS 1000 Release 4.5, the simplest way to ensure the system behaves correctly is to never allow two customers on one MG 1000E, and to never allow two customers in one zone.

Engineering Rule 6

Do not mix types of routes when using STEP routes.

If one route steps to another, they should be of the same type, or one of the two should be a CAMA trunk. A PRI route cannot normally step to an IP Virtual Trunk route and vice versa; the two use different called number type and plan, and — because the PRI trunk does not need to rely on the NRS to select the correct gateway — the actual called numbers are significantly different; there are no “prepend digits” in PRI.

Exception:
A CAMA trunk ignores the called party number provided for the call, using the DDGT as provisioned in the ESA data block in overlay 24. This means that for the “legacy” ESA on a Trunk Gateway the CAMA may step to PRI or — provided the NRS has a list of destinations associated with the ESDN, usable by all callers — VTRK and vice versa, but not both.

It is very highly recommended that routes used for “basic” ESA never step to a VTRK, because the ZESA data is not available to add the prepend digits.

For Zone ESA, the CAMA may step to VTRK or vice versa.

Permitted STEP routes

Refer to the following table for zone ESA handling combinations permitted. The trunks in the "STEP" route type column can be used as alternates to the first mentioned route type.

Table 88
"STEP" usage cases for CS 1000 Release 4.5, primary customer on the system

Original route type	"STEP" route type	Behavior	Comments
Zone ESA handling			
VTRK	CAMA	Call succeeds. Recommended.	CAMA ignores the dialed digits and prepend digits, and inserts the DDGT.
	VTRK	Call succeeds. Recommended.	Both trunks need the prepend; okay.
CAMA[1]	CAMA	Call succeeds. Recommended.	Prepend and/or ESDN are ignored; the DDGT is used instead.
	VTRK[2]	Call succeeds. Conditionally recommended.	CAMA ignores the prepend digits and ESDN digits, and inserts the DDGT. The VTRK uses the prepend and ESDN digits if the call steps to this route.
Basic ESA block handling: Not applicable. The core system cannot use basic ESA to route calls, as that limits the handling to "CAMA only".			
Note 1: CAMA is mandatory for a security desk on the CS 1000E. ***Note 2:*** Not recommended if the security desk application resides on an MG 1000E of the CS 1000E. May be used if the call is to an external PSAP or to a security desk on a Trunk Gateway.			

In the following table, some of the rows are shaded. These are "theoretically possible" in that provisioning the NRS with one least cost routing list of IP destinations for the base ESA DN allows calls to complete. However, they are not recommended, since all calls from anywhere in the network that use this

NRS will use the same least cost routing list, whether it makes sense to do so or not.

Therefore, as long as the user provisions the system with the NRS routing ESA calls to a valid destination telephone where they can exit to “a PSAP”, this can work. It is not recommended, though, since it is highly unlikely that it is the correct PSAP.

Table 89
“STEP” usage cases for CS 1000 Release 4.5, on the Trunk Gateway (Part 1 of 2)

Original route type	“STEP” route type	Behavior	Comments
PRI/BRI	PRI/BRI	Call succeeds. Recommended.	The PRI/BRI can use the ESDN if the call steps to this route.
	CAMA	Call succeeds. Recommended.	CAMA ignores the ESDN digits and inserts the DDGT.
	VTRK[1]	Not recommended, but theoretically usable.	The NRS must be provisioned to send all calls using this ESDN to a single list of Trunk Gateways.
CAMA	PRI/BRI	Call succeeds. Recommended.	CAMA ignores the ESDN digits and inserts the DDGT. The PRI/BRI can use the ESDN if the call steps to this route.
	CAMA	Call succeeds. Recommended.	CAMA ignores the ESDN digits and inserts the DDGT.
	VTRK[1]	Not recommended, but theoretically usable.	The NRS must be provisioned to send all calls using this ESDN to a single list of Trunk Gateways.

Table 89
“STEP” usage cases for CS 1000 Release 4.5, on the Trunk Gateway (Part 2 of 2)

Original route type	“STEP” route type	Behavior	Comments
VTRK[2]	PRI/BRI	Not recommended, but theoretically usable.	The NRS must be provisioned to send all calls using this ESDN to a single list of Trunk Gateways.
	CAMA	Not recommended, but theoretically usable.	The NRS must be provisioned to send all calls using this ESDN to a single list of Trunk Gateways. CAMA ignores the ESDN digits, and inserts the DDGT.
	VTRK	Not recommended, but theoretically usable.	The NRS must be provisioned to send all calls using this ESDN to a single list of Trunk Gateways.
Basic ESA block handling Note that because a call using “normal ESA” sends only the ESA DN unless the provisioning replaces the number with the directing digits, the ESA DN is a single entry in the NRS. The result is that all calls using the NRS routes to the same gateway. Therefore, although feasible, using VTRK without ZESA is not recommended.			
Note 1: If it must be used, use this only at the trunking gateway, when the gateway is a CS 1000M or CS 1000S. ***Note 2:*** This configuration, although possible, is “a bad idea”. It basically decides to not use local trunks, and instead routes to remote trunks. If VTRK was used as the only choice (that is, no local trunks existed), this would make more logical sense, except for the point of having a trunking gateway without trunks.			

The following are “not currently supported”. PRI and BRI do not yet exist on the MG 1000E systems of the CS 1000E.

Table 90
Unsupported "STEP" usage cases on the CS 1000E core system

Original route type	"STEP" route type	Behavior	Comments
VTRK	PRI/BRI[1]	Even if the PRI/BRI existed on the MG 1000E, the call would fail.	VTRK call has prepend digits; these cause the call to fail at the destination side.
PRI/BRI	PRI/BRI	If the CS 1000E supported PRI or BRI on the main system, call would succeed.	No prepend required; do not configure a prepend for this scenario. The system sends the ESDN digits.
	CAMA	If the CS 1000E supported PRI or BRI on the main system, call would succeed.	No prepend required; do not configure a prepend for this scenario. The system sends the ESDN digits. CAMA ignores the ESDN digits and inserts the DDGT.
	VTRK	If the CS 1000E supported PRI or BRI on the main system, and prepend was not needed, the call would succeed. If prepend digits are required by the NRS, call would fail.	VTRK call needs prepend digits; lack of these cause the call to fail at the destination side unless there is one ESA Trunk Gateway for the entire network.
CAMA	PRI/BRI	If the CS 1000E supported PRI or BRI on the main system, call would succeed.	No prepend required; do not configure a prepend for this scenario. CAMA ignores the ESDN digits and inserts the DDGT. The PRI/BRI uses the ESDN if the call steps to this route.
Zone ESA handling Not currently possible using ZESA — theoretical combinations, and the results if they could be used with the current handling.			
Not possible at this time. The PRI/BRI is on a MG 1000T, CS 1000E, CS 1000M or CS 1000S, none of which currently support ZESA for trunks.			

Provisioning

This step includes the following sub-steps:

- ESA provisioning

  The ESA data block must be provisioned. However, this is mostly to allow the user to specify the ESA DN, as the ESA data block is accessed only by users whose units are physically located on the Call Server; for CS 1000E, all TDM and IP units are remote, even if they register directly to the Call Server.

  The ESA data block includes the “ESDN” prompt. This is where the user enters the “911”, “999”, or other applicable emergency number.

  After provisioning the basic ESA, the user provisions zone ESA (ZESA) data for this zone, with the data entered excluding the locator code (see the CLID section). The user also defines the ESA prefix, which in this case is the GGP code and called number type digit. In this way the NRS can route the call to the correct TDM trunking gateway.

  If the country has more than one ESA DN, then one of two options is selected. One option might be that on-site notification is not used and the call bypasses ESA to reach the PSAP.

  Another option might be that all ESDNs are mapped using CDP (Local Steering Codes and DMIs) or other features into a common ESA DN. At this point either a call is placed to a local security desk (which has hot-line keys pre-provisioned to reach all external ESA DNs) or the call routes to “the best generic choice” in the PSTN.

- CLID provisioning

  For the CS 1000E, the ESA data block provisioning is close to superfluous. The system administrator enters the ESDN, and has to enter a route. The administrator also enters the emergency number (up to four digits) to be transmitted on CAMA trunks, but the DFCL is all but irrelevant; the DFCL cannot be used for the zones with the possible exception of the zone selected as the primary zone. Even then, it is only used if some form of error meant no ANI could be built otherwise.

Refer to *Emergency Services Access: Description and Administration* (553-3001-313) for more details about this data block.

For the CS 1000E, the CLID entry blocks are necessary for units in the primary zone. It has no real use for units residing physically in all other zones in so far as ESA is concerned.

Within the CLID entry blocks defined as a part of overlay 15 are several fields related to ESA calls; the others usually apply to non-ESA calls. The ESA fields are:

— ESA_HLCL — "ESA Home Local code" — the E.164 prefix for a DID capable number, or the full E.164 number of the closest emergency callback answering site.

— ESA_INHN — "ESA calls insert Home National prefix" — prepend the local exchange number generated from the ESA_HLCL (and DID DN, if applicable) by the home national code. Note that the home national code (HNTN) is also used for normal call purposes.

— ESA_APDN — "ESA Append DN" — use the DID directory number (DN) as the final digits in the ANI.

Non-ESA fields used from the CLID entry block include:

— HNTN — "Home National prefix" — the city code, area code, or other regional code prefix as defined by the telecommunication authorities.

A brief commentary on "multiple appearance DNs" is required. A single directory number may appear on several units; however, it is only formally associated with the "Multiple Appearance Redirection Prime" unit for ESA purposes. That is, the PSAP associates the DN with a specific location, and if the number appears at several locations the emergency services may be mis-routed. For a multiple appearance DN, only assign the CLID entry that uses this DN as part of the ANI when provisioning the prime (the “MARP”); all others cannot use this.

Instead, for other units provisioned with this DN, either provision the DN to use the “floor” (or other local) call-back number, or provision a different DID DN on the unit as the one with a CLID entry.

For DID capable fixed location units, provision either the DID DN (if it is the prime for that DN) or the closest call-back site (the building security desk, for example) as the ESA HLCL code.

For all mobile units registered with the Call Server as part of the primary zone, the CLID entry block may specify a DID number for normal calls, but the ESA call-back number must be the site callback and not the local callback. The local callback may not even be on the same side of the city as the caller, and at least the main site callback is usually staffed with personnel (and has the On-Site Notification terminal and phone) to allow the staff to assist emergency center personnel in locating the emergency caller.

The user provisioning includes zone ESA (ZESA) data for this zone excluding the locator code. This causes the ESA function to use the CLID block to build the ESA ANI. If the locator code is used, all calls to the PSAP uses a single site call-back number, and none are able to indicate the correct destination to emergency services staff.

A commentary on analog trunk routes also applies. These only provide a calling number if the route is “Feature Group D” or has “IANI” set to YES in the RDB; practically, the administrator and service personnel should assume that no CLID is provided. Therefore, in almost all cases the analog trunk builds an ANI based exclusively on the CLID entry data for the CLID block associated with the route data block. Note that this ANI must point back to the originating PBX or switch and not to the CS 1000E. If the ANI indicates the local CS 1000E but the real caller is several blocks to several kilometers away, the emergency services response time is impaired. Or:

Engineering Rule 7

Provision the ESA parts of the CLID entry block of an incoming analog route to indicate an answering position of some sort on the remote switch.

For example, if the remote switch is a Meridian 1 running X11 release 25.40, it would have a default ANI, used if no ANI could be built otherwise; build this ANI in the CLID entry block for the analog trunk.

Zone based provisioning on the CS 1000E Call Server

Engineering Rule 8

An MG 1000E cannot have more than one zone.

If a system has two customers they should not share BWZs, and ESA PSAP handling is very volatile without E911. The route is also customer specific, although it is conceivable that an administrator could make all ESA routes numbered the same (for example, on all customers on a system, the route 123 may be reserved for ESA routes). Practically, though, that is “not recommended”, as it is very easy to miss one customer.

This step includes the following sub-steps:

- ESA provisioning

  The ESA DN was provisioned for the “primary zone”; no more is needed for the “basic” ESA data provisioning. However, the ESA zone provisioning is needed.

  The user provisioning includes zone ESA (ZESA) data for this zone including the locator code, which is the site call-back number. This causes the ESA function to use the “pre-built” default information to ensure a callback that allows some form of recovery.

- CLID provisioning

  For units in an MG 1000E whose zone is not considered as a primary zone, all calls use the site call-back DN unless all links to the Call Server are lost. In this case, provided one or more reachable MG 1000E has CAMA trunks, the MG 1000E reverts to a “survivability” mode and the MG 1000E can handle limited ESA calls by having the Call Server send the call to that MG 1000E. However, any mobile telephones temporarily located at this MG 1000E that are not “homed” to the zone of this MG 1000E will not have any service.

The user provisioning includes zone ESA (ZESA) data for this zone including the locator code, which is the site call-back number. This causes the ESA function to use the “pre-built” default information to ensure a callback that allows some form of recovery. In this way, the emergency services staff can contact the site primary on-site notification center to get further data.

Provisioning on the MG 1000E

This is only needed if the MG 1000E has “ESA survivability” by being able to place calls to an MG 1000E which has a local ESA usable trunk route (CAMA, for example, but it could be any analog trunk to the PSTN; “any PSAP is better than no PSAP”). Note that an MG 1000E does not provide survivability support if all Call Servers are out of service, but may provide service if the connection between the CS 1000E and the NRS or Trunk Gateways is lost.

This step includes the following sub-steps:

- ESA provisioning

  If an MG 1000E is to be capable of providing ESA trunking services to the local users if the network resources are unavailable, the analog signaling route must be provisioned (CAMA preferred). However, this is only used for the purpose of providing a trunking gateway to TDM emergency services if the network link fails. Effectively, this is a “STEP” from the route specified in the ZESA entry to a CAMA route. For all others, the transmitted number has no meaning.

  Note that an MG 1000E can only provide access for units associated with the same customer on the CS 1000E. If two customers exist, unless there are trunks connecting the two, no ESA access can be provided to a customer unless it has a route defined for ESA use.

  The ESA data block is provisioned as per a stand-alone CS 1000 system. Refer to *Emergency Services Access: Description and Administration* (553-3001-313) for details.

NRS provisioning

This step involves configuring the ESA numbering plan endpoints on the NRS (gatekeeper or redirect server) allowing ESA callers access to the different gateways on the network, depending on the way they are grouped. The GGPs allow the NRS to select the appropriate destination gateways, with the costings as applicable.

Wherever possible, a collocated gateway is used. Failing that, the next closest gateway is used. This continues until all gateways that can realistically be used have been provisioned. ("Realistically", since it is possible to provision a British ESA call to use a TDM trunking gateway in Australia, but it is pointless to do so.)

MG 1000T provisioning on the destination gateway

Engineering Rule 9

Provide more Virtual Trunks and DSP resources on the Trunk Gateway than the sum total required for all trunks to the PSTN or other networks.

If a Trunk Gateway has 100 external trunks (counting "normal" and "reserved for ESA") and no telephones, and only 100 Virtual Trunks terminate here, it is possible that the "normal" PSTN trunks are fully used. If another call comes in for one of these trunks, it uses a Virtual Trunk resource until the call is rejected. That means an ESA call may not be able to place a call to the ESA trunk route.

If the gateway has 120 Virtual Trunks, 90 PRI/BRI and analog trunks to other switches (including the PSTN) and 10 reserved for CAMA (ESA) use, the turn around time to clear a "no resources" call is short enough that the ESA calls can obtain trunks — until all trunks to the PSTN are used.

This is the final step in ESA provisioning. This involves provisioning digit manipulation tables on the gateways for proper routing of the calls. The gateways are provisioned with SPN codes that delete the prefixes and call type digits, and carry out local termination.

> ***Note:*** An MG 1000E can only have analog trunks on it. The only type of analog trunk supporting an ANI and tested (and therefore the only one currently approved) is the CAMA trunk. Others may be used, but the ANI — if any — may not be correct. As an example, a ground start COT would have the site billing number assigned as its “ANI”.

The following sections give examples of the aforementioned method applied to various types of calls.

Making ESA calls from CS 1000E — no local security stations

Refer to *Emergency Services Access: Description and Administration* (553-3001-313) for details.

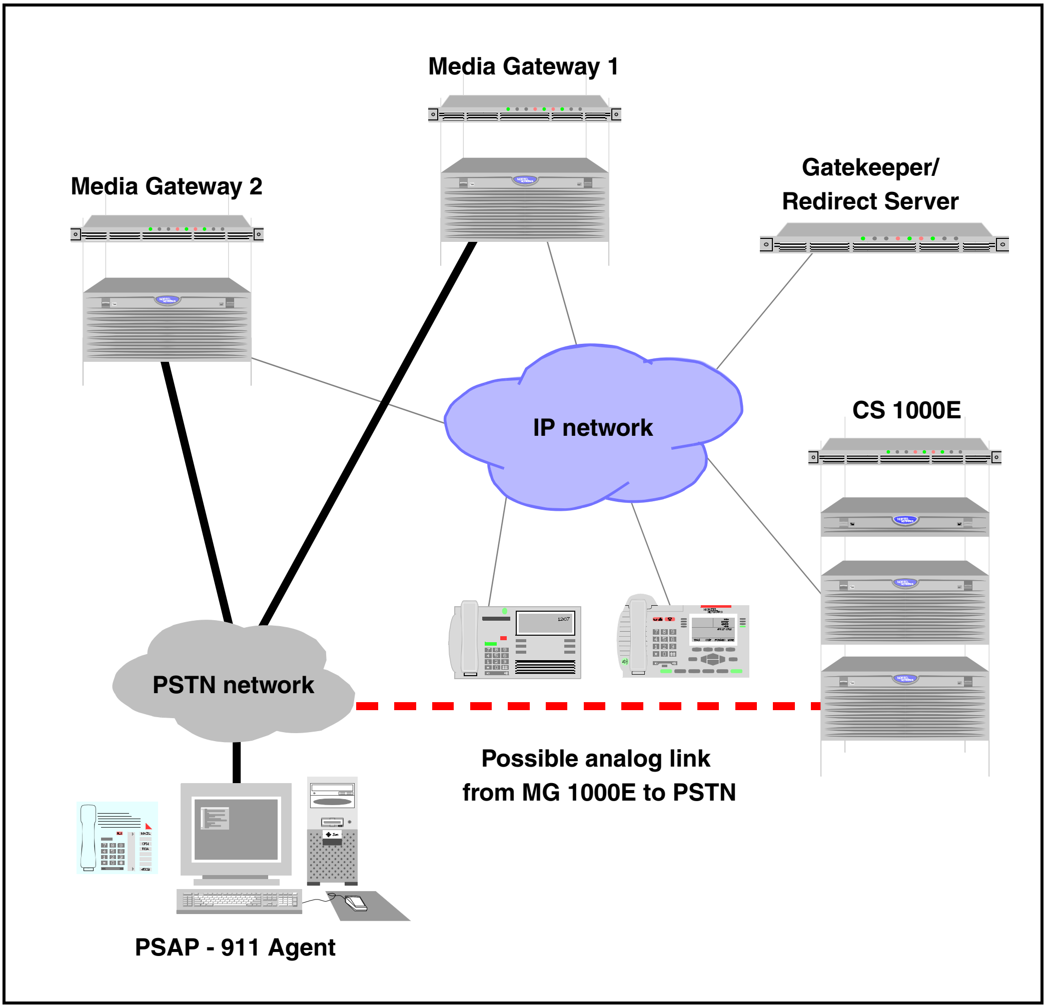
System diagram

The following figure shows the CS 1000E at right, with two collocated MG 1000E systems (which may or may not have H.323 or SIP to TDM trunking gateways) and a Signaling Server. The PSTN is on the left, with the destination PSAP site, and Media Gateway1 and 2 are connected to the PSTN. The LAN — with the NRS and various IP Phones — is in the center. Note that one or more of the Media Gateway1 and 2 may also reside in the same location as the Call Server (as opposed to the MG 1000E). Note also that an analog trunk (such as CAMA) may also connect the CS 1000E with the PSTN for ESA.

In North America, the emergency number is 911; in other countries the emergency number could be 999 or some other code.

As an example let us consider a user in North America dialing an emergency number — 911. Typically, this uses a specific variant of ESN SPN codes.

Figure 74
Setup for dialing ESA 911 (SPN) numbers from CS 1000E



System description

In the system shown above, the Call Server is connected to the PSTN by means of two MG 1000T platforms, indicated as “Media Gateway 1” and “Media Gateway 2”. It may also have a CAMA trunk route (or other analog trunk route) connecting it to the PSTN, for ESA. Procedure 11 describes how to provision the numbering plan on this system for making emergency or other “special number” calls.

The regular form of ESA calls on CAMA and PRI calls are supported by the CS 1000E via the MG 1000T. Since the connectivity between the Call Server and the gateway is via SIP or H.323, a special dialing plan is required to:

- be able to reach the correct gateway in a network, and
- be capable of notifying the correct PSAP.

In the above network, the CAMA trunks and/or the PSTN PRI trunks are supported by Media Gateway1 and 2.

CAMA trunks may also be available on an MG 1000E within the CS 1000E. This may be used as either a first choice or as "step" routes from the Virtual Trunks if all channels are in use. These are accessed using the “STEP” capability of the RDB.

Procedure 11
Provisioning ESA 911 (SPN) numbers from CS 1000E

Emergency numbers have some extra pre-work prior to provisioning the zone information; the applicable steps are:

- Provision the Call Server ESA data
- Provision any MG 1000E systems requiring ESA data

1 Prepare the ESA provisioning on the Call Server

Refer also to “Engineering Rule 6” on page 461.

For the Call Server, the applicable steps are:

- Determine the dialing plan for ESA calls.

  This requires the system administrator to be cautious while provisioning. The ESA DN must not conflict with other dialable DNs. If conflicts exist, they should be cleared first, prior to provisioning ESA.

  Refer to *Emergency Services Access: Description and Administration* (553-3001-313) for more details.

- Configure the Virtual Trunk at Call Server.

Readers can use either the Element Manager or command line interface for this procedure. Refer to *IP Peer Networking: Installation and Configuration* (553-3001-213) for details.

Configure Virtual Trunks on the Call Server using the procedure given in *IP Peer Networking: Installation and Configuration* (553-3001-213).

The Virtual Trunks must be configured and enabled from the Call Server for the emergency calls to originate from the Call Server.

- Configure ESA at the Call Server.

  — Administration for ESA in general

  The administrator configures ESA in overlay 24 on the Call Server. This is the same procedure used on the CS 1000M or CS 1000S. However, as all calls are ZESA routed, much of this provisioning is ignored during call processing.

  — Administration for digital or analog telephones located in an MG 1000E

  This is handled in step 4 on page 477, using the ZESA table provisioned in LD 117.

  — Administration for IP Phones (which are within zones)

  This is handled in step 4 on page 477, using the ZESA table provisioned in LD 117.

2 Prepare the ESA provisioning on the MG 1000E

To supplement ESA provisioning, CAMA trunks in the MG 1000E can be used either as a first choice or as "step" routes from the Virtual Trunks.

Note: If the link between the Call Server and the MG 1000E is lost, no calls can reach the PSAP from this node.

For ESA calls to be routed over CAMA trunks, the applicable steps are:

- Determine the requirements for ESA calls over local CAMA.

  CAMA trunks can be used either as a first choice, or as “step” routes from the Virtual Trunks; however, they use different “called party” digits than the Virtual Trunks. The directing digits ("DDGT") provides the digits sent to the PSTN, in lieu of the dialed ESA DN.

- Configure the hardware appropriately. The calls can only leave the MG 1000E through a trunk located within the MG 1000E; logically, this is also within the same PSTN ESZ.
- Configure the ESA route, with TGAR screening to block non-ESA calls. Provision this as a "step" on the Virtual Trunk RDB.

3 GGP Planning

GGP planning involves the following procedure:

- Destination Analysis

  Determine what gateways can service this call properly, and which is preferred.

  In this example, assume that Media Gateway1 and 2 exist (as well as others, but only 1 and 2 are of interest). It is determined that both Media Gateways 1 and 2 can terminate the call at this destination. However, Media Gateway 1 is on the same floor of the same building as the caller; Media Gateway 2 is across the street. Therefore, 1 is preferred.

- Digit Analysis

  Create the GGP, if not already created. In general, this should be the same one as used for other call types.

- Gateway Group Selection

  "Formally", group the gateways together in the order of preference, and document this for later reference and use.

  The gateways in the network, for special number calls, can be grouped into Group 1, which includes Media Gateways 1 and 2

- Call type Digit Set selection

  Select the identifying digit or digit string.

  For the network example, a digit or digit string such as the digit "6" is selected to identify the ESA and differentiate it from "true special numbers". In this example, a different code than the non-ESA SPN was used. It could be the same, but that makes provisioning more awkward. To the user at the unit, it still looks the same.

4 ESA data entry on the CS 1000E Call Server

To use ESA in IP zones, it is necessary for calls from IP Phones registered at the Call Server or MG 1000E systems to supply a unique identifying prefix to the Gatekeeper when the ESA calls are being routed, so that the Gatekeeper can select a distinct route for each gateway. This prefix is configured with the zone data. This is done using the ZESA table provisioned in overlay 117.

- CLID provisioning

  Either the CLID (from the CLID entry provisioned for the calling number) or the ESA Locator code is used. This depends in part on whether the locator code was provisioned; if it was not, fixed location phones use a CLID based on the CLID entry. If the locator code is defined, all phones (IP and TDM) within the zone use the locator code.

  Make sure that the CLID entry blocks are set up to build the ANI correctly, should the locator code not be used.

- Configure an ESA zone on the Call Server.

  This only applies to IP Line or MG 1000E calls as only telephones using IP to communicate with the Call Server currently belong to zones. It is done in the Call Server via the CLI, using LD 117.

  `CHG ZESA <zone> <ESA Rte #> <AC> <ESA Prefix> <ESA Locator>`

  After setting the values, enable the ESA zone

  `ENL ZBR <Zone>`

  The `CHG ZESA` command defines the ESA parameters for the zone, where:

  — Zone = Zone number for ESA calls

  — ESA Rte # = Virtual Trunk route to gateway. According to ESA requirements this trunk is to be reserved for outgoing calls; that means that the route should not be used for incoming calls. To do this, the route may be provisioned with a TGAR blocking all calls incoming, or for the prompt of "ICOG" (Incoming or Outgoing) it may be defined as an "OGT" (Outgoing Trunk).

  Blocking calls incoming by ICOG or TGAR is highly recommended. Otherwise, there is the risk of not getting resources for ESA calls. The user must ensure that sufficient channels are available to ensure availability.

— AC = Access Code to add to dialed digits.

  If no AC is required, AC0 is to be entered in place of AC1 or AC2. If the access code is required, it must be entered. Note, though, that the call is sent over SIP or H.323 as a call of type SPN, so the receipt of the call at a properly provisioned destination route automatically triggers SPN handling. Note that the destination route at the gateway must have "INAC YES".

  If the destination is not a CS 1000 system, it is probably not INAC capable. Under those circumstances it may be necessary to insert either access code 1 or access code 2. This is the exception rather than the norm, as it implies a non-enterprise Nortel or third-party gateway that is both intelligent enough to handle the "6-44446-911" by deleting all leading digits, but not sufficiently capable to identify an SPN.

  (This allows the remote Call Server to initiate ESN handling of the received number.)

— ESA Prefix = Mandatory digit string added to start of ESDN (ESA DN).

  This provides the "ESN SPN prefix code" for the gatekeeper, allowing it to uniquely identify the correct target gateway. Nortel recommends conforming to the usage practices in place for other calls. That is, if the GGP is "4444" and the type "6" is selected for "SPN to SPN" calls, the user sets the ESA prefix to 44446.

  Note that the user may decide to allow all calls from all CS 1000Es to use a single list. That is, they may decide that they do not care which gateway is used. Although this is highly discouraged, if a user wants to use the ESA DN without prepended digits, the administrator may enter "NONE" to indicate "add no digits".

  Note also that CAMA trunks (including ones on an MG 1000E) ignore the ESA prepend digits prefix.

— ESA Locator = The full Direct Inward Dial telephone number to be sent as the CLID (ISDN) or ANI (CAMA), for use by the PSAP to locate the source of the call.

The ESA locator is considered “optional but highly recommended”. If the locator number is present, all callers belonging to this zone use this locator number. This allows the system to guarantee a return call to the same site. As a consequence, the ESA Locator must be the DN assigned to a DID capable fixed location set physically within the same zone as the ESA caller.

If the Locator code is absent, the system tries to create an equivalent using the CLID and the applicable CLID entry. For most callers this should work, as long as the CLID entries are provisioned correctly. The CLID built using the ESA data within the CLID entry block is used, and the number sent out as the ANI can be used to call back. On the other hand, if that fails, ESA handling uses the Default ESA Calling Number defined for the customer. Reasons for failure include, but are not limited to, an invalid CLID entry index, lack of ESA data in the CLID block making the generated CLID of an invalid format, and the lack of a DN which can build a CLID. Note, though, that the CLID entry can allow the administrator to define a default CLID block building some generic CLID, such as the LDN, the security desk DN, and so forth.

Note: Nortel recommends using the Locator code for all zones except the primary zone (where the largest number of TDM telephones and fixed location IP Phones are located). All other zones use the locator code.

The user may decide to explicitly indicate that no locator code is used. If this is done, the administrator may enter “NONE” to indicate “no locator”. Although not recommended, it is also not forbidden. It is expected that the user will leave the entry blank as an implied “NONE” rather than typing in additional characters. “Blank” equals “none”.

After setting the values, enable the ESA zone

ENL ZBR <Zone>

- ESN provisioning if desired
  - — Digit Manipulation provisioning

    Not required. The ESN access code is automatically deleted by the system.

— RLI provisioning

If the administrator chooses not to provision the ESN data to allow the ESN access code followed by the ESA DN (6-911, etc.), this is not required. If the administrator provisions the ESN access codes plus the ESA DN (6-911 and 9-911), a RLI with local termination is needed, although the access code is automatically deleted; the ESA DN remains. Therefore, no further manipulation is needed.

— SPN provisioning

Nortel recommends in *Emergency Services Access: Description and Administration* (553-3001-313) that the administrator provision the ESDN as an SPN in both the AC1 and AC2 network translation tables. In this way, regardless of which was entered, the ESA call can still complete.

For the ESA SPN, use the RLI provisioned above with local termination.

Once the local termination occurs, the call uses normal ESA handling. Therefore, the call uses the route selected in the overlay 117 zone ESA provisioning, unless required to step to an alternate.

5 ESA data entry for analog trunks on the MG 1000E systems

If the MG 1000E does not have local trunks capable of routing a call to the PSAP, this is not required.

The MG 1000E only processes ESA calls when the link to the NRS is unavailable, or a cataclysmic failure in the wider network makes the trunking gateways unavailable or fully occupied.

The user provisions and defines the local (CAMA) trunks, and defines the route as a step route of the normal Virtual Trunk route.

- ESN provisioning if desired

  — Digit Manipulation provisioning

  Not required. The ESN access code is automatically deleted by the system.

  — RLI provisioning

If the administrator chooses not to provision the ESN data to allow the ESN access code followed by the ESA DN (6-911, etc.), this is not required. If the administrator provisions the ESN access codes plus the ESA DN (6-911 and 9-911), a RLI with local termination is needed, although the access code is automatically deleted; the ESA DN remains. Therefore, no further manipulation is needed.

Once the local termination occurs, the call uses normal ESA handling. Therefore, the call uses the route selected in the LD 117 zone ESA provisioning, unless required to step to an alternate.

— SPN provisioning

Nortel recommends in *Emergency Services Access: Description and Administration* (553-3001-313) that the administrator provision the ESDN as an SPN in both the AC1 and AC2 network translation tables. In this way, regardless of which was entered, the ESA call can still complete.

For the ESA SPN, use the RLI provisioned above with local termination.

6 NRS provisioning

Since based on the network planning defined for this example the digit string outpulsed is 44446911, the end point in the NRS database can be a special number entry for 44446.

This step is the process of provisioning the numbering plan entries in the NRS for each of the gateways. For special number calls (such as ESA), the numbering plan entries in the NRS would vary based on the decisions made during planning about the cost factor. Assume the cost factor is:

- 44446 on Media Gateway 1: cost factor 1
- 44446 on Media Gateway 2: cost factor 2

then the gatekeeper would be provisioned with this information appropriately.

Note: This is when the decisions about the egress gateway are critical. The administrator must try to ensure that the nearest trunk to the PSTN to a caller's terminal is the one selected for the call. Refer to "Destination Analysis" on page 458 for more information.

For configuring this section, Element Manager is required. For more details refer to *IP Peer Networking: Installation and Configuration* (553-3001-213).

7 MG 1000T provisioning

See "Engineering Rule 9" on page 471 for more details.

As was stated earlier, the preferred gateway should be local to the caller's terminal on the CS 1000E. The provisioning here must occur on the system where the call is actually to leave the IP network. Otherwise, the call fails.

Note that the steps closely mirror the steps for normal ESA, when the ESA call is tandem; for comparison, refer to *Emergency Services Access: Description and Administration* (553-3001-313). The major deviation is in the area of the Virtual Trunk provisioning.

- Configure the emergency trunk on the gateway (CAMA or PRI).

Note: It should not be necessary to configure a VTRK as an alternative on the trunking gateway; if all CAMA and PRI trunks are occupied or otherwise unavailable, the call drops back to the originating Signaling Server to try the next alternative, and if all alternatives are unavailable, to the CS 1000E and the "STEP" is invoked there. If the originating CS 1000E Signaling Server cannot reach a gateway to use, the trunking gateway will be unable to reach one either.

- Configure Virtual Trunks

  Before a call can come on the Virtual Trunks, the trunks must be configured.

  Nortel recommends that some channels of the Virtual Trunk be blocked from making calls to the IP domain, to ensure that channels are available for calls from IP to TDM. If a gateway is a MG 1000T without telephones, and there are 10 PSTN trunks or channels reserved for ESA (that is, belonging to a route used only for the ESA data block) and other 200 PSTN and private network trunks, then no more than 210 calls can go from the TDM domain to the IP network. The ESA calls are all "to the PSAP". Therefore, if there are 250 virtual channels, at least 40 can be reserved for calls from the IP network to the TDM network. (In this way, if an ESA call should leave the IP domain on a Virtual Trunk "intended" for all other calls, there will still be a channel for a call to or from the non-ESA trunks.)

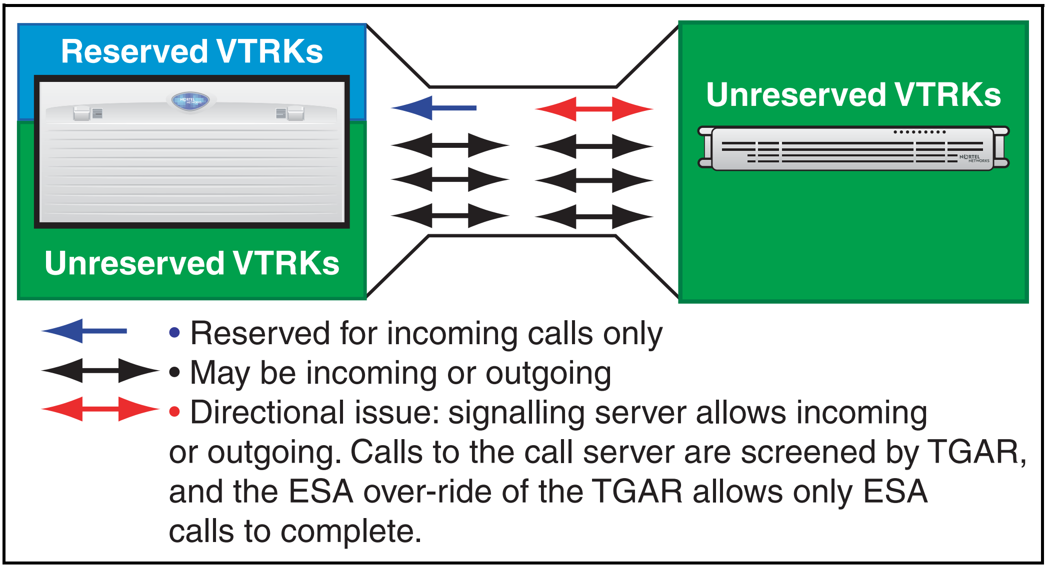
  The simplest way to ensure these channels are reserved for calls to the TDM network is to mark them as incoming on the Trunk Gateway.

This can be achieved by setting the ICOG to ICT. This would ensure that these Virtual Trunk channels are not used for regular calls from this gateway to the IP domain. However, this does not guarantee that "IP to TDM" calls from the Signaling Server to destinations other than ESA is unable to use this block.

At this time, no mechanism exists to ensure that only ESA calls uses certain resources. Therefore, use "Engineering Rule 9" on page 471. This allows the administrator to engineer in the capability.

Figure 75 on page 483 illustrates the issue.

Figure 75
Directional issues for the Signaling Server, re ICT trunks



- Configure ESN at the gateway.

  A Special Number (SPN) is configured on the gateway. This SPN is for the ESA calls from the Call Server. This needs to be provisioned at all gateways where the call could exit the IP domain to be sent to the PSTN over TDM services.

  The SPN must use:

  — A Digit Manipulation Index which deletes all the incoming digits. This may mean either all digits, or all digits except for the ESDN.

In the example, since 44446911 is received, a DMI can be configured to delete the full received digit string including the 911 and insert the local ESDN in its place. This is of great utility when the ESA DN varies between locations. (Alternatively, the ESDN may be left intact. For example, in North America the ESDN is always 911; this could be left and only the 44446 deleted.)

— A RLB which has LTER (Local Termination) turned on, and using the DMI defined as deleting the prefix. This triggers re-processing of the call after the digits are removed, rather than simply tandeming the call.

When an SPN is configured, ESA determines that the call is from a trunk and forwards the correct ANI data as it tandems the call.

- Configure ESA at the gateway.

  This configuration is the same as for the switch providing the outgoing side of a normal, non-IP tandem CAMA/PRI trunk ESA call. That is, if the call was PRI to ESA, provisioning the ESA side follows a specific procedure. That procedure also applies here.

  ESA configuration enables the Virtual Trunk ESA call from Call Server to be tandem over to CAMA or PRI trunk.

  When an ESA call is received, the gateway would recognize the incoming ESN prepend digits and delete all the digits except for the ESDN left for a PRI egress (SPN configuration from Step 3), or all digits (any ESA trunk type) after which it inserts the local ESA DN. Then the call is routed to the local (regular) ESA processing. ESA recognizes the call as an emergency call and routes the call correctly.

ESA overrides all restrictions. So configure trunks with restrictions so that other features cannot use the same trunks. This may not be fully possible, though, if the Signaling Server may be terminating calls “for other routes” on the Call Server. To the Signaling Server, there is only one route. On the other hand, channels can be reserved for calls from the Call Server to the Signaling Server. No other calls may use these Virtual Trunks in this direction.

End of Procedure

Call scenarios

All scenarios assume an ESA DN of 911; it could just as easily be any other ESA DN. Also, assume that the GGP and call type digit is “44445”.

To invoke an ESA call, the user dials the ESA code (911). The local device (in this case, the Call Server) identifies the number as being the ESA code. For CS 1000E, it matches the telephone to the corresponding ESA zone as provisioned, and uses the information in the ESA zone data to manipulate the digit and select the outgoing route.

The NRS server receives the request, and processes the GGP. When it identifies the applicable egress gateways, the call proceeds to the destination gateway.

At the destination gateway, the SPN has the number manipulated by ESN and the altered number receives “local termination”; the number is re-processed. When that happens, the ESA number is identified from the “new” dialed digits, and local ESA handling is used as though the call originated on that gateway.

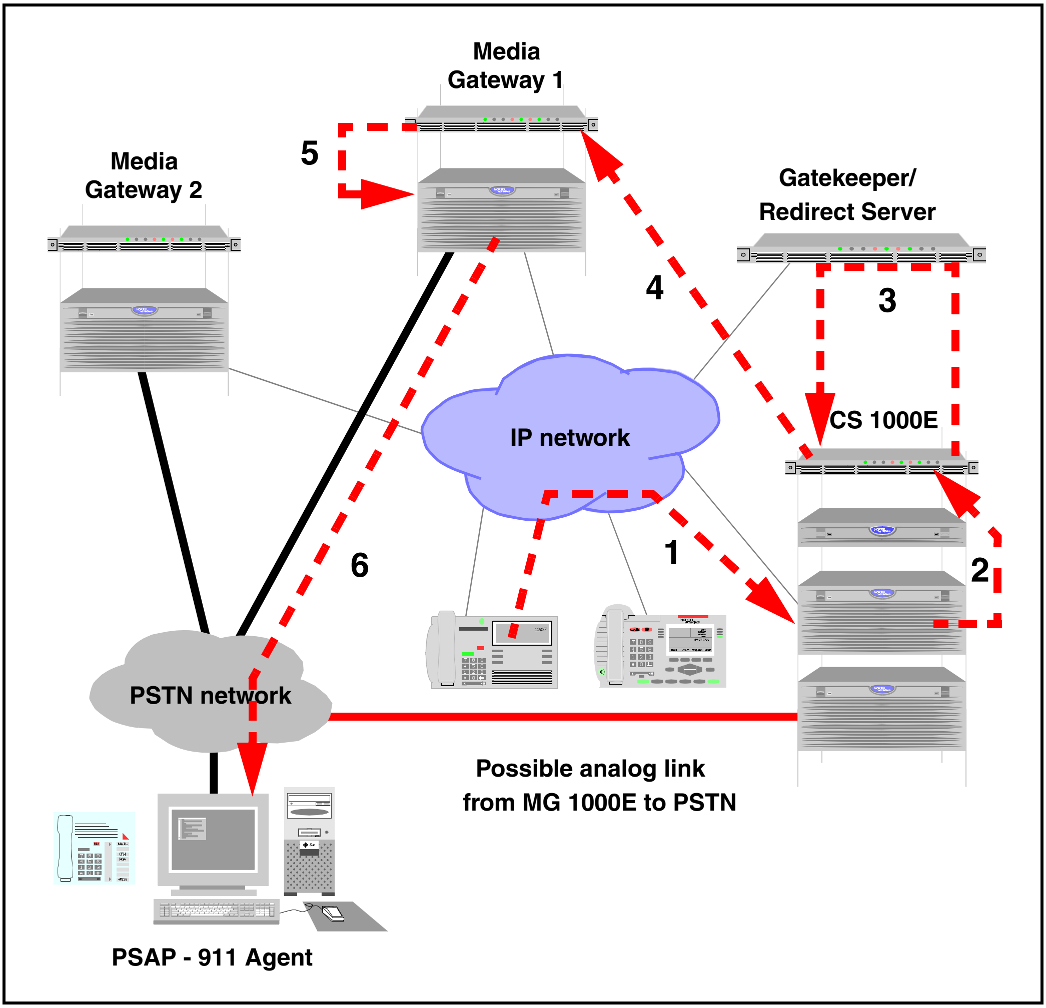
Call scenario 14: User dials 911 and the first gateway is available

In this scenario, the caller (DN 8957) is placing a call at the Call Server, over IP to a gateway to the PSTN, where the call terminates on the desired destination.

Table 91
Call Scenario 14 sequence

<table>
<tr><th>H.323 sequence</th><th>SIP sequence</th></tr>
<tr><td colspan="2">The user 8957, dials 911.</td></tr>
<tr><td colspan="2">The Call Server does digit manipulation in the form of ZESA and prepends 44445 to the called number 911. The outpulsed digit to the Signaling Server is 44445 911. The ANI is built according to the rules pertaining to the zone (locator code present?) and the terminal CLID entry provisioning.</td></tr>
<tr><td>The Signaling Server sends a request to Gatekeeper for address resolution. Since the gatekeeper is able to find an entry for 44445 with a cost factor of 1 on Media Gateway 1, it send the IP address of Media Gateway 1 to the requesting Signaling Server.
Media Gateway 2 is indicated as an alternate endpoint if least cost routing is available.</td><td>The call is then routed to the redirect server for address resolution. The digit string sent for address resolution is 44445-911. Since an entry with cost factor “1” is found for 44445, the IP address of the endpoint —
Media Gateway 1 — used to forward the INVITE.</td></tr>
<tr><td>The Signaling Server then transmits the H.225.0 SETUP to the gateway.</td><td>The Signaling Server of Media Gateway 1 receives and then accepts the call.</td></tr>
<tr><td colspan="2">The call is sent from the Signaling Server to the Call Server on the gateway for routing the call.</td></tr>
<tr><td colspan="2">On Media Gateway 1, since 44445 is configured as a SPN with an RLI associated with it using digit manipulation to delete the steering code and providing local termination, the digit string is stripped and the call is handled as a local ESA call. Normally, this means that the call is routed over the CAMA/PRI trunks to the nearest PSAP.</td></tr>
</table>

Figure 76
Setup for call scenario 14 for making ESA 911 call



Call scenario 15: User Dials 911 and Media Gateway 1 is busy or congested

In this scenario, the caller (DN 8957) places a call at the Call Server, over IP to a gateway to the PSTN, where the call terminates on the desired destination. However, the “preferred” gateway is not available to process the call, so an alternate handles it.

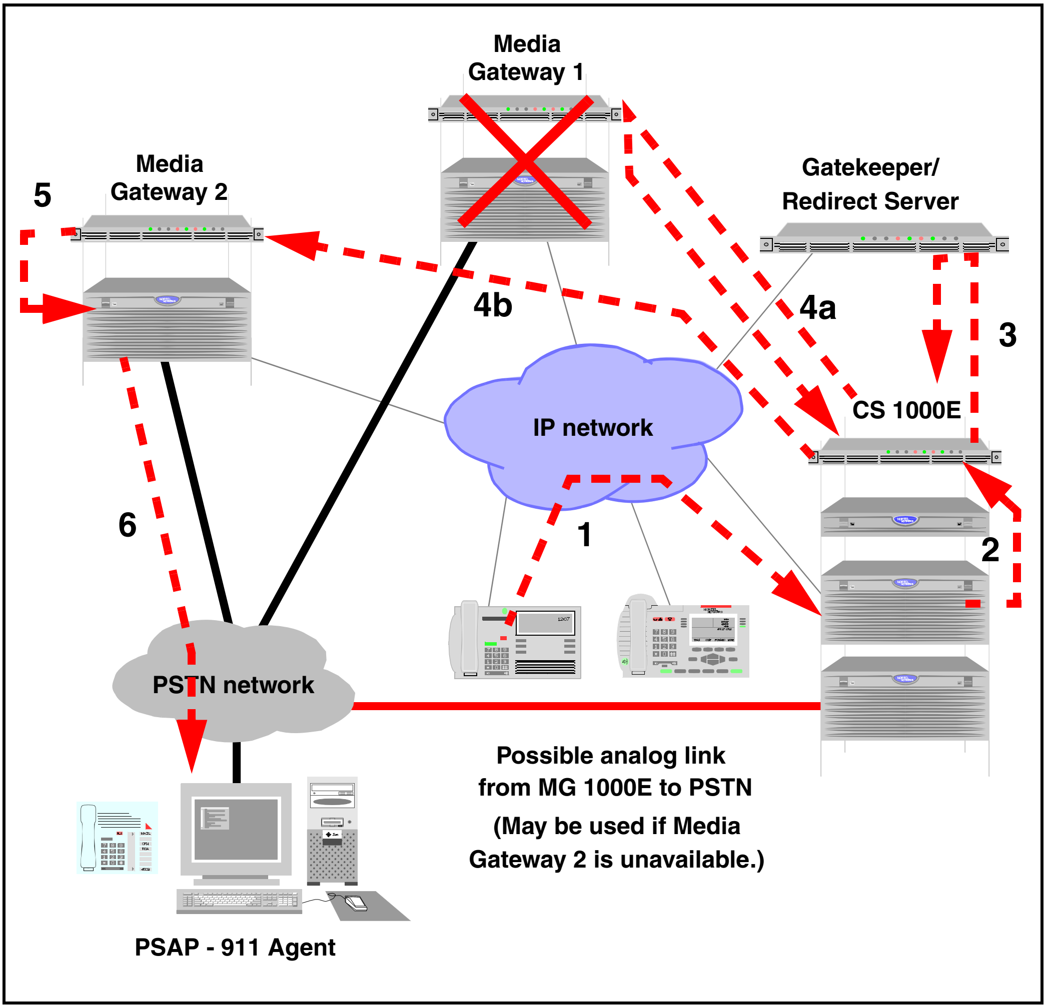
Table 92
Call Scenario 15 Sequence (Part 1 of 2)

H.323 sequence	SIP sequence
The user 8957, dials 911.	
The Call Server does digit manipulation in the form of ZESA and prepends 44445 to the called number 911. So the outpulsed digit to the Signaling Server is 44445 911. The ANI is built according to the rules pertaining to the zone (locator code present?) and the terminal CLID entry provisioning.	
The Signaling Server sends a request to Gatekeeper for address resolution. Since an entry with cost factor “1” is found for 44445, the IP address of the endpoint — Media Gateway 1 — is sent to the requested Signaling Server as the first choice (provided the customer provisioned “least cost routing”, which is outside the scope of this reference). Media Gateway 2 is indicated as an alternate endpoint if least cost routing is available.	The call is then routed to the redirect server for address resolution. The digit string sent for address resolution is 44445-911. Since an entry with cost factor “1” is found for 44445, the IP address of the endpoint — Media Gateway 1 — is used to forward the INVITE. The redirection clearing message is returned to the originator, together with the IP addresses of possible destinations.

Table 92
Call Scenario 15 Sequence (Part 2 of 2)

<table>
<tr><th>H.323 sequence</th><th>SIP sequence</th></tr>
<tr><td>The call routes to the available gateway.
1 The Signaling Server on the Call Server sends the SETUP to the Signaling Server of Media Gateway 1. This gateway is congested or busy, and rejects the call. (The congested/busy status could be on either the IP or the TDM side of the gateway. If no IP resources are left, the call cannot reach the TDM, so the call is rejected. Else, if it reaches the gateway Call Server and no trunks are available, it also rejects the call.)
2 The Signaling Server on the Call Server sends the SETUP to the Signaling Server of Media Gateway 2. This gateway accepts the call.</td><td>The call routes to the available gateway.
1 The Signaling Server on the Call Server sends the INVITE to the Signaling Server of Media Gateway 1. This gateway is congested or busy, and rejects the call. (The congested/busy status could be on either the IP or the TDM side of the gateway. If no IP resources are left, the call cannot reach the TDM, so the call is rejected. Else, if it reaches the gateway Call Server and no trunks are available, it also rejects the call.)
2 The Signaling Server re-tries the INVITE to Media Gateway 2. The Signaling Server of Media Gateway 2 receives the call. This gateway accepts the call.</td></tr>
<tr><td colspan="2">The call is sent from the Signaling Server to the Call Server on the gateway for routing the call.</td></tr>
<tr><td colspan="2">On Media Gateway 2, since 44445 is configured as a SPN with an RLI associated with it using digit manipulation to delete the steering code and providing local termination, the digit string is stripped and the call is handled as a local ESA call. Normally, this means that the call is routed over the CAMA/PRI trunks to the nearest PSAP. Note that “Selective Routing” allows a call to be redirected to the correct PSAP based on the ANI, provided the call arrives at the PSTN at some point within a limited geographical area. If the second choice route is outside the “hub 911” area, then the call will not receive the highest levels of service.</td></tr>
<tr><td colspan="2">Should no Trunk Gateway resources be available, the call clears back to the originating Call Server. If a local STEP route (for example, a CAMA trunk) is provisioned, the system tries to send the call using the STEP route.</td></tr>
</table>

Figure 77
Setup for call scenario 15 for making ESA 911 call from CS 1000E



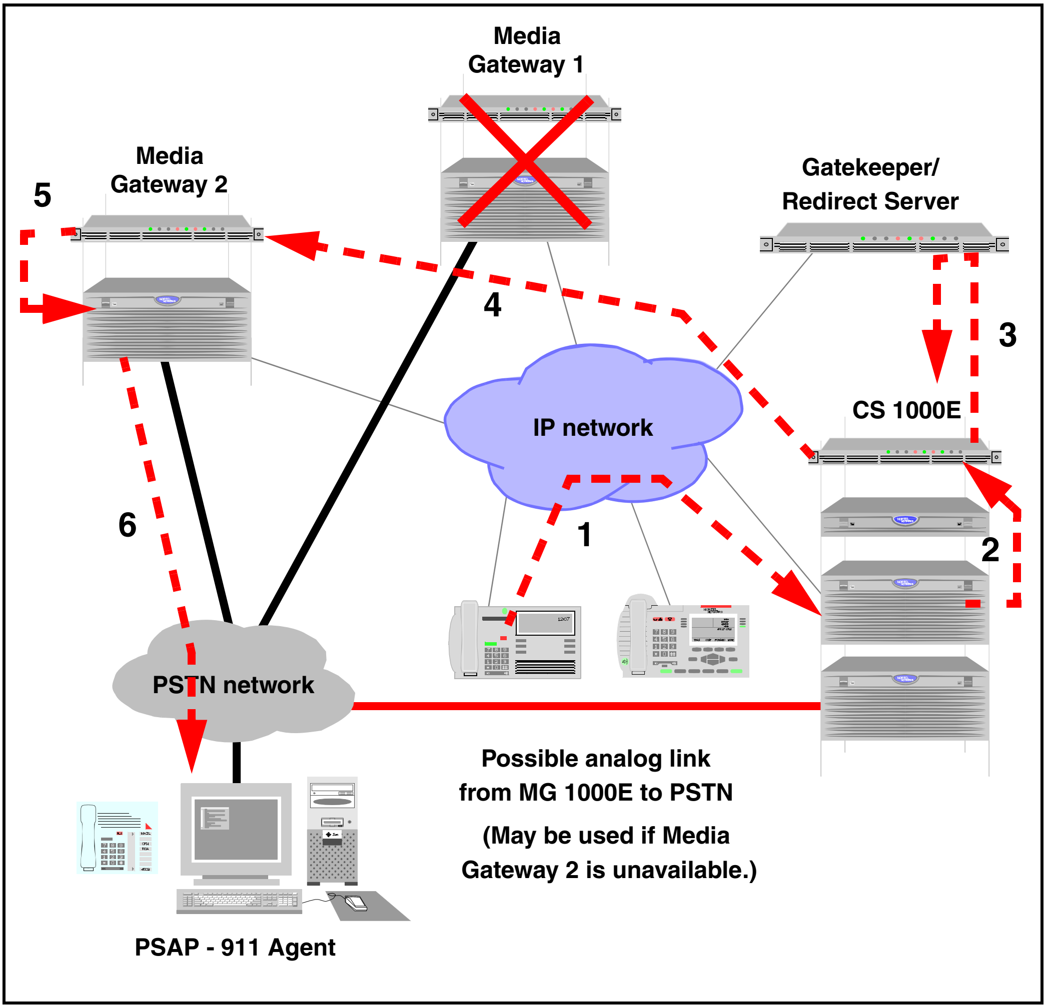
Call scenario 16: User Dials 911 and Media Gateway 1 is not registered

In this scenario, the caller (DN 8957) places a call at the Call Server, over IP to a gateway to the PSTN, where the call terminates on the desired destination. However, the "preferred" gateway is not available to process the call because it is not registered with the gatekeeper/redirect server, so an alternate handles it. (The “X” through the gateway indicates this.)

Table 93
Call Scenario 16 Sequence

H.323 sequence	SIP sequence
The user 8957, dials 911.	
The Call Server does digit manipulation in the form of ZESA and prepends 44445 to the called number 911. The outpulsed digit to the Signaling Server is 44445 911. The ANI is built according to the rules pertaining to the zone (locator code present?) and the terminal CLID entry provisioning.	
The Signaling Server sends a request to Gatekeeper for address resolution. Since the Signaling Server with the cost factor of “1” is not registered to the gatekeeper, it cannot accept traffic. Therefore, an entry with cost factor one is not found for 44445. The GK takes the next end point with cost factor “2” and sends the IP address of this endpoint — Media Gateway 2 is sent to the requested Signaling Server.	The call is then routed to the redirect server for address resolution. The digit string sent for address resolution is 44445-911. Since the entry with cost factor “1” is not registered, but an entry of cost factor “2” can be found for 44445, the IP address of the endpoint — Media Gateway 2 — used to forward the INVITE.
The Signaling Server on the Call Server sends the SETUP to the Signaling Server of Media Gateway 2.	The Signaling Server of Media Gateway 2 receives the call. This gateway accepts the call.
The call is sent from the Signaling Server to the Call Server on the gateway for routing the call.	
On Media Gateway 2, since 44445 is configured as a SPN with an RLI associated with it using digit manipulation to delete the steering code and providing local termination, the digit string is stripped and the call is handled as a local ESA call. Normally, this means that the call is routed over the CAMA/PRI trunks to the nearest PSAP. Note that “Selective Routing” allows a call to be redirected to the correct PSAP based on the ANI, provided the call arrives at the PSTN at some point within a limited geographical area. If the second choice route is outside the “hub 911” area, then the call will not receive the highest levels of service.	
Should no Trunk Gateway resources be available, the call clears back to the originating Call Server. If a local STEP route (for example, a CAMA trunk) is provisioned, the system tries to send the call using the STEP route.	

Figure 78
Setup for call scenario 16 for making ESA 911 call from CS 1000E



Making ESA calls from CS 1000E — with local security stations

In this case, the call routes to a local security desk that deals with the call first, only bringing in the external PSAP if unable to handle the call locally (that is, external resources are needed) or the site is currently unattended.

Refer to *Emergency Services Access: Description and Administration* (553-3001-313) for details. The stand-alone configuration settings specifically discuss security stations.

Using ACD is the preferred method of call handling, as it leaves the ANI unchanged when the call routes to the security desk. It also leaves it available in the event of a night call forward (for example, when the security station is un-staffed due to some emergency requiring all available security personnel, the ANI is still there for the call when it routes to the PSAP).

In the CS 1000E it is not possible to have a MG 1000T Trunk Gateway provide an emergency desk. Instead, a CS 1000M or CS 1000S has to be used for this purpose.

There are two options here. The security station may be:

- on a CS 1000M or CS 1000S acting as a Trunk Gateway, or
- on the CS 1000E.

For several reasons, the system designer and administrator is strongly advised to use the CS 1000M or CS 1000S as a Trunk Gateway to act as the security desk and to not use an MG 1000E on the CS 1000E for this function. Several of the advantages are:

- Better hardware usage and availability
    - — CAMA is not supported in most countries. This means that a CAMA loop-back or outgoing trunk may not be possible on the CS 1000E. Therefore, no supported analog trunk with ANI may be available.

- Using a CS 1000E as the security desk always requires a loop-back or hair pin of some sort. Some of these do not support ANI transmission (CAMA is the only one currently supported that can reside on the CS 1000E). However, if the security desk is the only entity or unit on the CS 1000 Trunk Gateway, then no loop-backs of any sort are needed.
- Using a MG 1000E for the security desk makes one additional customer mandatory (which means that one additional MG 1000E is mandatory). On the CS 1000M or CS 1000S, it may be necessary to add one or two line cards, but typically no shelves are needed.
- If any IP calls are to reach the CS 1000E security desk (first example: two CS 1000E nodes may share a security desk; second example: as a fail-safe in case all the loop-back channels are in use; third example: CAMA trunks not supported in this country), an additional Signaling Server is needed for the MG 1000E housing the security desk. Unless two customers are needed on the trunking gateway, no additional Signaling Servers are required there. However, if the user wants to get absolute separation of ESA calls from all others, the user may use the second Signaling Server with its associated routes anyway. This is optional, not mandatory; it is mandatory for the second customer on the security desk's dedicated MG 1000E.
- Fewer trunk resources required with the CS 1000M or CS 1000S as the security desk system. Less Virtual Trunks tied up by emergency calls, as only a single call to the Trunk Gateway is needed.

• Better configuration

- As long as the security desk is the sole occupant of the trunking gateway (and in principle, the trunking gateway is supposed to be VTRK to TDM trunk only), except at the security desk node this is provisioned exactly as though it was a CS 1000E system without a security desk. Having the security desk on the Trunk Gateway makes it invisible to the rest of the system. On the other hand, provisioning a MG 1000E to provide the security desk is a complex provisioning sequence.

- Putting the security desk on a separate CS 1000M or CS 1000S means that the channels on this node can become “the last local Trunk Gateway” option for calls from this CS 1000E. This makes the availability of channels for ESA (for which this is first choice) more of an “engineering the number of Virtual Trunks” issue rather than using complicated provisioning.
- CAMA loop-backs (required for MG 1000E security desks) require packages not needed otherwise (specifically, to read from a CAMA trunk the M911 package is needed). If the security desk is on the CS 1000M or CS 1000S, there are no loop-backs unless there are two customers on the Trunk Gateway, and then PRI trunks can provide this capability without needing the M911 package.

- Better robustness
  - If the CS 1000M or CS 1000S security desk switch is a casualty of the emergency, it is easy to use least cost routing to go to a secondary channel to the PSAP. It goes immediately if the system is down, as it is the same ESA handling as was used for the “no security desk” case. Or, it goes a short period later triggered by ISDN timers if the Virtual Trunks are still live, but the actual agent center is not answering or not available. By comparison, the MG 1000E as a security station may be able to STEP immediately if the CAMA trunks are down, but if they are not, the call can effectively hang. The signaling over CAMA trunks is more primitive than over the IP network.
  - Multiple security desks may be made available if using CS 1000M or CS 1000S. Two separate CS 1000E systems with a CS 1000M or CS 1000S as a trunking gateway may share security desks as a redundancy measure. If one loses its security desk, the other may be able to provide all services except the on-site notification TTY “on the fly”, by being the first alternate in the least cost routing list.

Security station on the CS 1000M or CS 1000S Trunk Gateway

System diagram

The following figure shows the CS 1000E at lower right, with two collocated MG 1000E systems (which may or may not have collocated H.323 or SIP to TDM trunking gateways) and a Signaling Server. The PSTN is on the left, with the destination PSAP site, and Media Gateway1 and 2 are connected to the PSTN. The LAN — with the NRS and various IP Phones — is in the center. Note that one or more of the Media Gateway1 and 2 may also reside in the same location as the Call Server (as opposed to the MG 1000E). This is expected to be common for a MG 1000T.

A local security desk is located on one of the CS 1000 Trunk Gateways, which must therefore be a CS 1000M or CS 1000S. To guarantee trunk availability for the ESA handling, this is effectively a second customer on that system, with only Virtual Trunks (and therefore its own Signaling Server), links to the PSAP, and the security center equipment.

In North America, the emergency number is 911; in other countries the emergency number could be 999 or some other code.

As an example let us consider a user in North America dialing an emergency number — 911. Typically, this uses a specific variant of ESN SPN codes.

Figure 79
Setup for dialing ESA 911 (SPN) number from CS 1000E

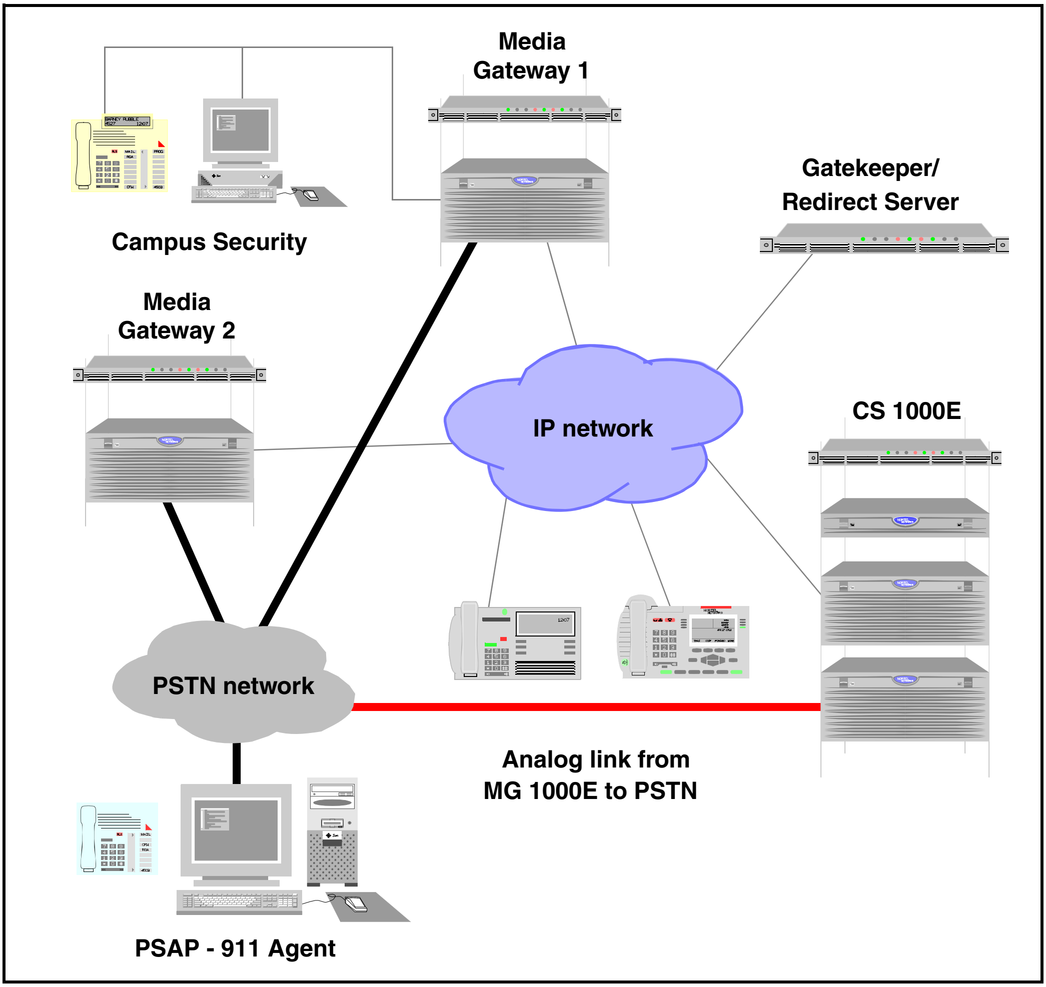
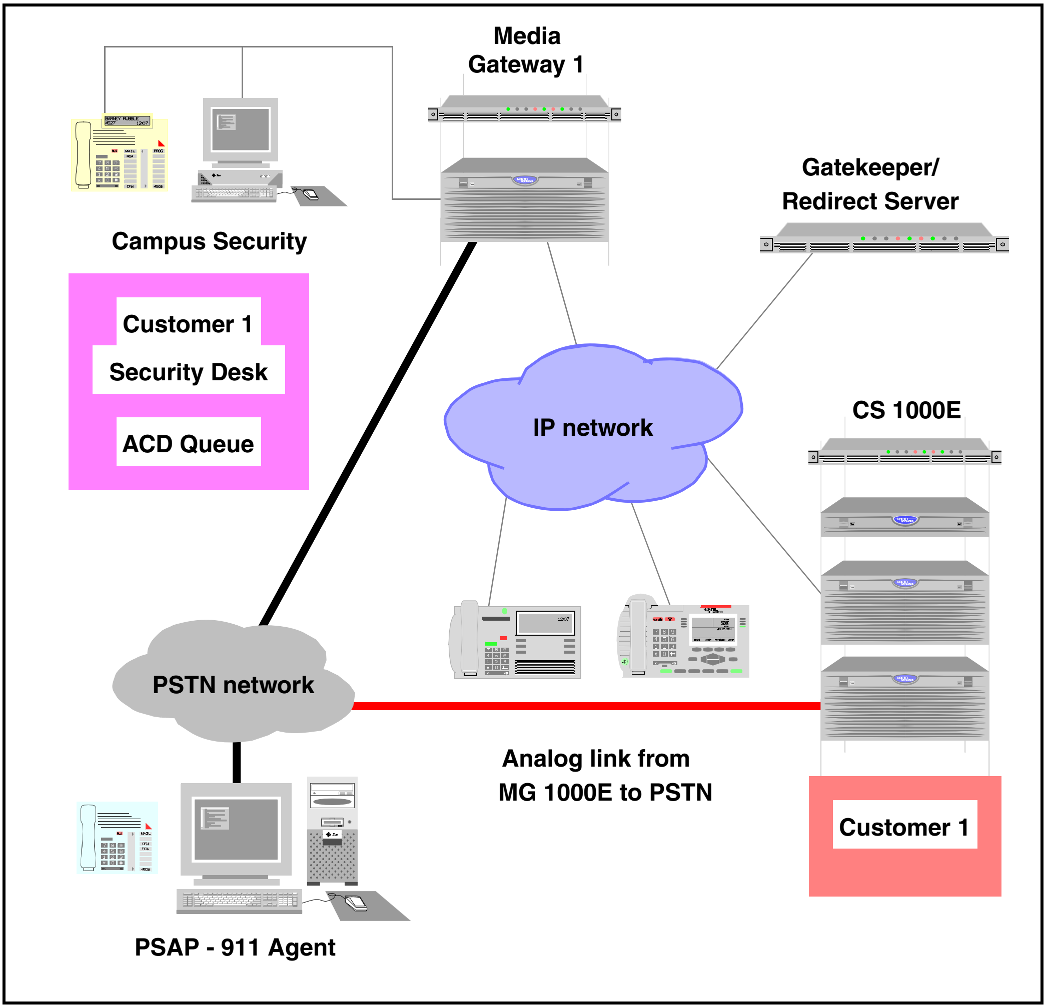


Figure 80
Network elements



System description

In the system shown above, the Call Server is connected to the PSTN by means of two MG 1000T platforms, indicated as “Media Gateway 1” (both Figure 79 and Figure 80) and “Media Gateway 2” (omitted from Figure 80 as it is not used in this scenario). It may also have a CAMA trunk route (or other analog trunk route) connecting it to the PSTN, for ESA. Media Gateway 1 also has the campus security desk. Procedure 12 describes how to provision the numbering plan on this system for making emergency or other "special number" calls.

The regular form of ESA calls on CAMA and PRI calls are supported by the CS 1000E via the MG 1000T. Since the connectivity between the Call Server and the gateway is via SIP or H.323, a special dialing plan is required to:

- be able to reach the correct gateway in a network, and
- be capable of notifying the correct PSAP.

In the above network, the main CAMA trunks and/or the PSTN PRI trunks are supported by Media Gateway1 and 2. However, this is not enough for the "security desk" model; the calls must attempt to terminate first on the Trunk Gateway with the security desk.

This means that whenever the ordered list of the Trunk Gateways is created, the lowest cost gateway must be the gateway with the security desk. Others place second, third, fourth, and so on, as applicable.

CAMA trunks may also be available on an MG 1000E within the CS 1000E. This provides "one last chance" if the link from the CS 1000E to its trunking gateways is completely unavailable or all channels are in use. These are accessed using the "STEP" capability of the RDB.

Procedure 12
Provisioning ESA 911 (SPN) number from CS 1000E

Emergency numbers have some extra pre-work prior to provisioning the zone information; the applicable steps are:

- Create all necessary CDBs — one for the security desk, one for "any other telephones on the system".
- Create the security center customer, including provisioning. This is similar to the stand-alone configuration of a security desk defined in *Emergency Services Access: Description and Administration* (553-3001-313), except that instead of using CAMA or "traditional"

ISDN trunks for incoming emergency calls from the balance of the network, the incoming call uses IP Virtual Trunks.

- Provision the Call Server ESA data for the security desk customer and the main CS 1000E system.

1 Create CDBs on the Trunk Gateway

The security desk needs to be on its own customer. If the security desk is to be able to call the ESA DN, and all other ESA calls route to the security desk, then no other telephones can be on the security desk customer. The ESA cannot route both to the trunks (for the security center, also called the "On Site Answering Position"), and to the security center (for all telephones).

All other telephones — if applicable — are on the non-security desk customer.

Note that whenever the security desk CDB is the only CDB needed for telephones, all of the PSTN trunks may also be here.

2 Define the customer for the security desk

A second Signaling Server on the Trunk Gateway is advantageous to ensure that the security center has non-blocking function, but the system can be engineered to get basically the same effect, by making this gateway the "last choice" for all calls from the IP domain. Only security center originated calls (and emergency calls, both incoming and to the PSTN) should be able to use these routes.

The provisioning steps are:

- Define the CDB, if not already created.
- Define ACD capability for the customer (ACD allows the system to forward the original call information to the PSAP if the call must be rerouted to the external emergency services). Ensure that the system is able to do a night call forward.

  ESA allows two options here. Either the telephones are ACD agents, or the telephones can be night call forwarded (NCFW) to a normal system DN, which appears as a MADN on all telephones used for the security desk. However, if the "normal telephones" are used, the security desk must be manually put into "Call Forward all calls" to the ESA DN whenever it is not staffed, and must also be CFNA to a telephone which is permanently CFW to the ESA DN. For details, refer to *Emergency Services Access: Description and Administration* (553-3001-313).

- Define all user terminals and equipment (ACD auxiliary devices, etc.).
- Define the virtual routes for this customer. Add the Virtual Trunks. Ensure that there are enough to be able to handle any “excess” ESA calls.
- Provision the ESN. Specifically, provision an RLI to perform local termination, deleting all digits and inserting the ACD queue DN used for the security desk. Provision the Network Translations to use this RLI when the GGP and calling number type for ESA calls are detected.
- Make sure that the OSN units are located at the security desk associated with the security center.

3 Prepare the ESA provisioning on the Call Server

For the Call Server, the applicable steps are:

- Determine the dialing plan for ESA calls on the non-security center customer.
- This is the same as provisioning without a security desk.
- Determine the dialing plan for ESA calls on the security center customer.

  In this case, the transmitted number is different than the number for the main customer. This allows the NRS to differentiate between a call to security and a call to the PSAP, and route the call to the security desk.
- Configure the Virtual Trunk at Call Server.

  Readers can use either the Element Manager or command line interface for this procedure. Refer to *IP Peer Networking: Installation and Configuration* (553-3001-213) for details.

  Configure Virtual Trunks on the Call Server using the procedure given in the *IP Peer Networking: Installation and Configuration* (553-3001-213).

  The Virtual Trunks must be configured and enabled from the Call Server for the emergency calls to originate from the Call Server.
- Configure ESA at the Call Server for both customers.

— Administration for ESA in general

The administrator configures ESA in overlay 24 on the Call Server. Use the same procedure on the CS 1000E, the security desk CS 1000, and the trunking MG 1000T, CS 1000M or CS 1000S.

— Administration for digital or analog telephones located in an MG 1000E

Handled in step 4 on page 477, using the ZESA table provisioned in LD 117.

— Administration for IP Phones (which are within zones)

Handled in step 4 on page 477, using the ZESA table provisioned in LD 117.

4 Prepare the ESA provisioning on the MG 1000E

It may be asked why this step is still necessary if the calls are routed to the security desk. However, in the event of an emergency the security desk may be affected and unreachable. This provisioning allows the caller the chance to still get ESA service even if the Trunk Gateway with the security desk or the NRS are affected. Note that a local CAMA trunk is required to carry out this function fully, although any analog trunk that cannot send the ANI could be given basic ESA handling by the PSTN. Therefore, the site billing number is used.

For the MG 1000E to function when contact is lost to the Call Server of the security desk or the NRS server, the applicable steps are:

- Determine the dialing plan for ESA calls.

  The calls can only leave the MG 1000E through a trunk located within the MG 1000E; logically, this is also within the same PSTN ESZ.

  The calls can only leave the MG 1000E through a trunk located within the MG 1000E; logically, this is also within the same PSTN ESZ.

- Configure ESA to terminate calls on trunks at the MG 1000E.

  The directing digits must be defined for the CAMA trunks. The administrator configures these as part of ESA in overlay 24 on the Call Server. This is the same procedure used on the CS 1000M or CS 1000S. The DDGT entry is needed when the call steps to the CAMA trunk.

  The administrator provisions the CAMA trunk as a step route in the VTRK RDB.

5 GGP Planning — from the CS 1000E

This is the first step unless the administrator has to execute the provisioning steps used to define ESA (from step 1, 2, 3, and 4). If the basic requirements are configured already, provisioning starts here.

GGP planning involves the following procedure for the “normal user” customer:

- Destination Analysis

  Determine what gateways can service this call properly, and which is preferred.

  The call is a VTRK call only; it terminates on the security desk, but may “least cost route” to other gateways if unable to terminate on the security desk. In addition, it may STEP to a CAMA trunk if necessary, but this is local.

- Digit Analysis

  Create the GGP, if not already created. In general, this should be the same one as used for other call types.

  For the network mentioned above, assume that a unique number set “4444” is selected as a GGP. This code is unique across the whole network specified above.

- Gateway Group Selection

  “Formally”, group the gateways together in the order of preference, and document this for later reference and use.

  The “gateway group” is the VTRK routes associated with the security desk customer on the Trunk Gateway, with alternate routing to other gateways that can send the call to the PSTN.

- Call type Digit Set selection

  Select the identifying digit or digit string.

  For the network, a digit or digit string (for example, “6”) is selected to identify the ESA and differentiate it from “true special numbers”. In this example, a different code than the non-ESA SPN was used. It could be the same, but that makes provisioning more awkward. To the user it still looks the same.

6 GGP Planning — from the CS 1000 Trunk Gateway

GGP planning is not required for the security desk customer; the security desk is at the Trunk Gateway.

7 ESA data entry on the CS 1000E Call Server

To enable ESA for IP zones, it is necessary for calls from IP Phones registered at the Call Server or MG 1000E systems to supply a unique identifying prefix to the NRS when the ESA calls are being routed, so that the NRS can select a distinct route for each gateway. This prefix is configured with the zone data. This is done using the ZESA table provisioned in overlay 117.

- Configure an ESA zone on the Call Server.

  This only applies to IP Line or MG 1000E calls as only telephones using IP to communicate with the Call Server currently belong to zones. It is done in the Call Server via the CLI, using LD 117.

  CHG ZESA <zone> <ESA Rte #> <AC> <ESA Prefix> <ESA Locator>

  After setting the values, enable the ESA zone

  ENL ZBR <Zone>

- CLID provisioning

  Either the CLID (from the CLID entry provisioned for the calling number) or the ESA Locator code is used. This depends in part on whether the locator code was provisioned; if it was not, fixed location phones use a CLID based on the CLID entry. If the locator code is defined, all phones (IP and TDM) within the zone use the locator code.

8 ESN related data entry on the security desk Call Server

ACD provisioning: as per *Emergency Services Access: Description and Administration* (553-3001-313), if not already done.

ESN provisioning on the security center customer

- Digit Manipulation provisioning

  Define a DMI to delete everything and insert the security center's ACD queue DN.

- RLI provisioning

  Provision an RLI to do local termination using the DMI to replace the called party number with the local security desk DN.

- SPN provisioning

  Define an SPN based on the ESA digits sent on the call from the main customer. For the ESA SPN, use the RLI provisioned above with local termination.

9 ESA data entry for the MG 1000E systems

As per the case where no security desk exists. If the call falls back to the MG 1000E, it is because the security desk is unreachable.

10 NRS provisioning

There is one SPN required — that from the main node. None is required from the security center. The example uses “44446” as the SPN.

Main node:

Since based on the network planning defined for this example the digit string outpulsed is 44446911, the end point in the NRS database can be a special number entry for 44446.

This step is the process of provisioning the numbering plan entries in the NRS for each of the gateways. For special number calls (such as ESA), the numbering plan entries in the NRS would vary based on the decisions made during planning about the cost factor. However, as the security desk is only over IP, only the Signaling Server of the security desk needs to be provisioned. If there are other gateways that can pass this call to the PSAP, they may be provisioned as alternates, but the security desk CS 1000 must be the first choice.

Since based on the network planning defined for this example the digit string outpulsed is 44446911, the end point in the NRS database can be a special number entry for 44446. (This is deleted and replaced with the security desk number when the call is received.)

Security center node:

Since normal ESA is used, zone ESA does not apply; in fact, only the CS 1000E supports zone ESA. Therefore, an SPN to the NRS is not possible.

For configuring this section Element Manager is required. For more details refer to *IP Peer Networking: Installation and Configuration* (553-3001-213).

11 MG 1000T provisioning

Engineering Rule 10

The number of Virtual Trunks at the security desk on the gateway should be higher than the total of possible outgoing trunks and maximum number of ESA calls being handled by the security desk.

The number of extra Virtual Trunks is to be determined by analysis of expected traffic. If all of the non-ESA routes were in use, and more calls came in to use these routes, the blocked calls would temporarily seize Virtual Trunk resources. Therefore, unless extra trunks exist on the IP side of the gateway, calls that could succeed (TDM trunks are available) will fail (no Virtual Trunks available).

See also “Engineering Rule 9” on page 471 for more details.

The preferred gateway must be the gateway with the security desk.

Further choices should be the most logical ones geographically and in terms of service availability (for example, if a closer trunk has only basic ESA at the PSAP while a more distant one has Enhanced ESA and is served by the same “Selective Router”, the more distant gateway makes more sense). However, this is standard NRS provisioning, so it is not discussed further here.

The provisioning in this step must occur on the system where the call is actually to leave the IP network. Otherwise, the call fails.

Note that the steps closely mirror the steps for normal ESA, when the ESA call is tandem. The major deviation is in the area of the Virtual Trunk provisioning.

- Configure the emergency trunk on the gateway (CAMA or PRI).
- Configure Virtual Trunks

Before a call can come on the Virtual Trunks, the trunks must be configured.

Note that the route which is associated with this function should have access to only incoming calls. This can be achieved by setting the ICOG to ICT. This would ensure that these Virtual Trunk channels are not used for regular calls from this gateway to the IP domain. However, this does not guarantee that “IP to TDM" calls from the Signaling Server to destinations other than ESA is unable to use this block.

At this time, no mechanism exists to ensure that only ESA calls uses certain resources. Therefore, use *Provide more Virtual Trunks and DSP resources on the Trunk Gateway than the sum total required for all trunks to the PSTN or other networks.* This allows the administrator to engineer in the capability.

- Make sure that the Security Desk provisioning has completed. If a second customer exists on this gateway, then a form of hair-pin is required to allow the second customer to reach the security desk.
  - A valid route type such as a PRI route is provisioned with two cards. These are back to back.
  - Local ESA calls access one card in this back to back hair-pin.
  - Manipulates the digits to make the call re-processable. For example, this could be the number to access the ACD queue on the security desk.
  - For analog trunks, the opposite card uses INST to insert digits to make the call re-processable.
  - For PRI or other ISDN trunks, the opposite card's D channel uses NARS and an RLI/DMI to manipulate digits to make the call re-processable.
- Configure ESN at the both the Security Desk gateway and the other Trunk Gateways.
- Configure ESN at the both the Security Desk gateway and the other Trunk Gateways.

  A Special Number (SPN) is configured on the gateway. This SPN is for the ESA calls from the Call Server.

  The SPN must use:

  - A Digit Manipulation Index which deletes all the incoming digits. For the normal Trunk Gateway this may mean either all digits, or all digits except for the ESDN. In the example, since 44447911 is received, a DMI can be configured to delete the full received digit string including the 911 and insert the local ESDN in its place. This is of great utility when the ESA DN varies between locations. (Alternatively, the ESDN may be left intact. For example, in North America the ESDN is always 911; this could be left and only the 44447 deleted.)
  - A RLB which has LTER (Local Termination) turned on, and using the DMI defined as deleting the prefix. This triggers re-processing of the call after the digits are removed, rather than simply tandeming the call.

    When an SPN is configured, ESA determines that the call is from a trunk and forwards the correct ANI data as it tandems the call.

- Configure ESA at the other Trunk Gateways.

  This configuration is the same as for the switch providing the outgoing side of a normal, non-IP tandem CAMA/PRI trunk ESA call. That is, if the call was PRI to ESA, provisioning the ESA side follows a specific procedure. That procedure also applies here.

  ESA configuration enables the Virtual Trunk ESA call from Call Server to be tandem over to CAMA or PRI trunk.

When an ESA call is received, the gateway would recognize the incoming digits and deletes all the digits except for the ESDN left for a PRI egress (SPN configuration from Step 3), or all digits (any ESA trunk type). Then the call is routed to the local (regular) ESA processing. ESA recognizes the call as an emergency call and routes the call correctly.

ESA overrides all restrictions. So configure trunks with restrictions so that other features cannot use the same trunks. This may not be fully possible, though, if the Signaling Server may be terminating calls "for other routes" on the Call Server. To the Signaling Server, there is only one route. On the other hand, channels can be reserved for calls from the Call Server to the

Signaling Server. No other calls may use these Virtual Trunks in this direction.

End of Procedure

Call scenarios

All scenarios assume an ESA DN of 911; it could just as easily be any other ESA DN. Assume a security desk DN of 2020. Also, assume that the GGP and call type digit is “44446” for ESA calls placed from the rest of the system.

To invoke an ESA call, the user dials the ESA code (911). The local device (in this case, the Call Server) identifies the number as being the ESA code. For CS 1000E, it matches the telephone to the corresponding ESA zone as provisioned, and uses the information in the ESA zone data to manipulate the digit and select the outgoing route.

The NRS server receives the request, and processes the GGP. When it identifies the applicable egress gateways, the call proceeds to the destination gateway.

At the destination gateway, the SPN has the number manipulated by ESN and the altered number receives “local termination”; the number is re-processed. When that happens, the ESA number is identified from the “new” dialed digits, and local ESA handling is used as though the call originated on that gateway.

The user can theoretically have other units on the security desk customer, but this is very highly discouraged. Calls from these units will not reach the security desk, without excessively complex provisioning.

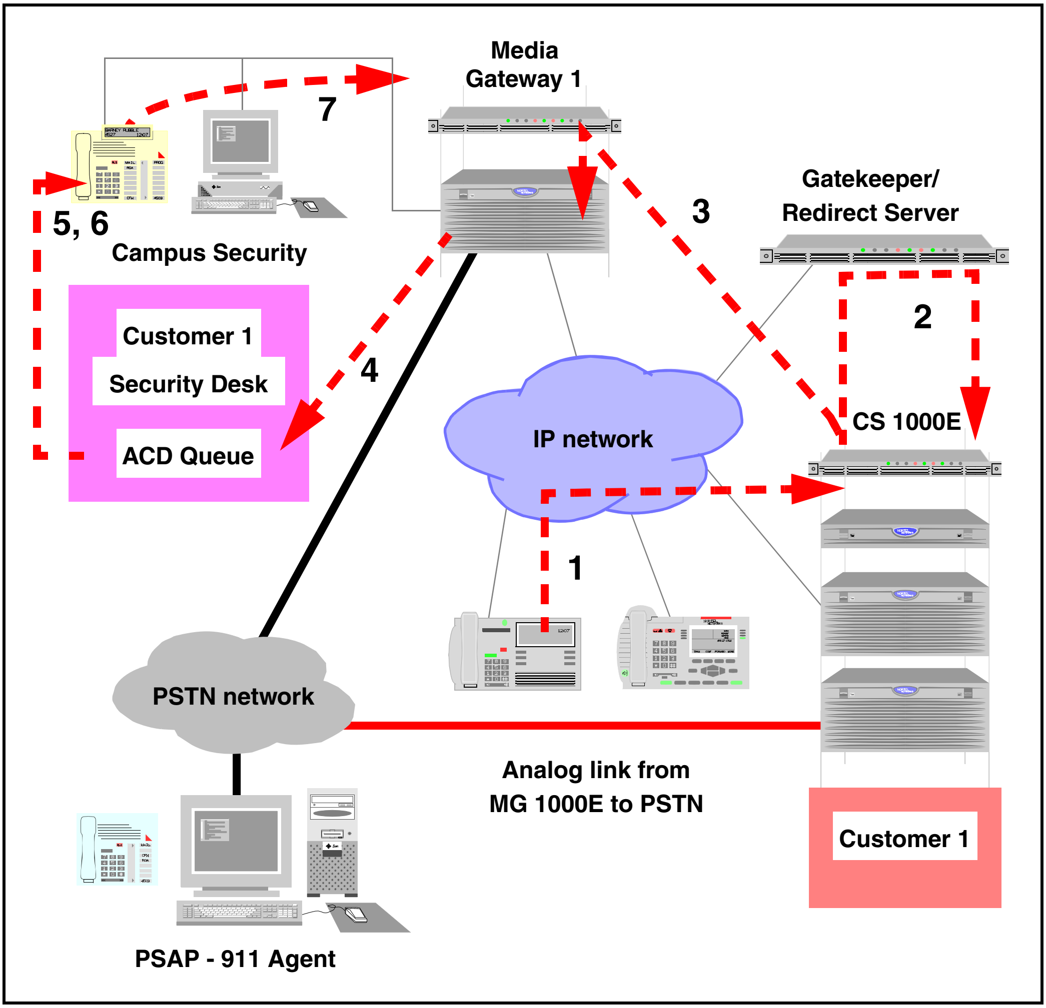
If the security desk customer has only the Security Desk (Campus Security,...) and no other telephones, provisioning is simple. Only calls to and from the Security Desk use trunking resources there; as a consequence, only ESA type calls use either the VTRKs here or the Signaling Server for this customer.

Note that the ACD agents or telephones reached from the ACD night call forward treatment cannot belong to a zone; they are on the gateway.

Note also that the ACD agent or other telephone has a "no-hold conference/ auto-dial" key or some similar function to actually place a call to the external ESA number. This makes "an immediate" call (no digits need to be dialed) and keeps the caller in the call throughout ("no-hold conference"). Because it is a conference, the local security desk operator can provide any essential information to the PSAP, should this be required.

In jurisdictions that require the ESA caller to not be in conference, "auto-hold" and a hotline type of key operation replaces the no-hold conference auto-dial.

Figure 81
Initial call — originated from remote CS 1000E



As is shown above, the call from the user at the CS 1000E customer 1 routes through the IP network to the ACD queue on the Trunk Gateway customer 2. Here, it is sent to an ACD agent or a user terminal.

The call flow for the call placed to the security desk is as follows:

1 A caller on CS 1000E customer 1 dials 911. The ESA call is ZESA routed to the IP domain, using a dial plan entry as per the dial plan recommendations- assume “61327-911”. An OSN record is generated.

2 The gatekeeper or NRS resolves to the IP address of customer 1 security desk Signaling Server.

3 The call terminates at the Call Server for customer 2. Because the number comes in as an SPN “61327-911” and not as the ESA DN of “911”, ESA handling is not invoked. Instead, “normal” NARS handling applies.

4 The SPN resolves to a RLI using local termination. Local termination deletes the called number (“61327-911”) and inserts the ACD DN of the ACD queue used for the security desk (for example, “2020”).

5 ACD terminates the call at an agent or by NCFW to a user terminal (perhaps using a multiple appearance DN). If set up to do so, the ACD auxiliary modules provide extra information about the caller.

6 No OSN record is generated on the security desk customer at this time.

7 Should the answering position operator need to make a call to the external PSAP, he or she presses the “no-hold conference auto-dial” key to make the second call. Details of this are in a following flow. Refer to “Call scenario 20: User dials 911 and the security desk is available” on page 543, and the following cases.

If the security desk call is completed, the call may be as complete as it needs to get. For example, if the call was something a university security force could handle then the call might progress no further. However, if some outside agency was needed — for example, the fire department — then the security desk personnel would invoke ESA.

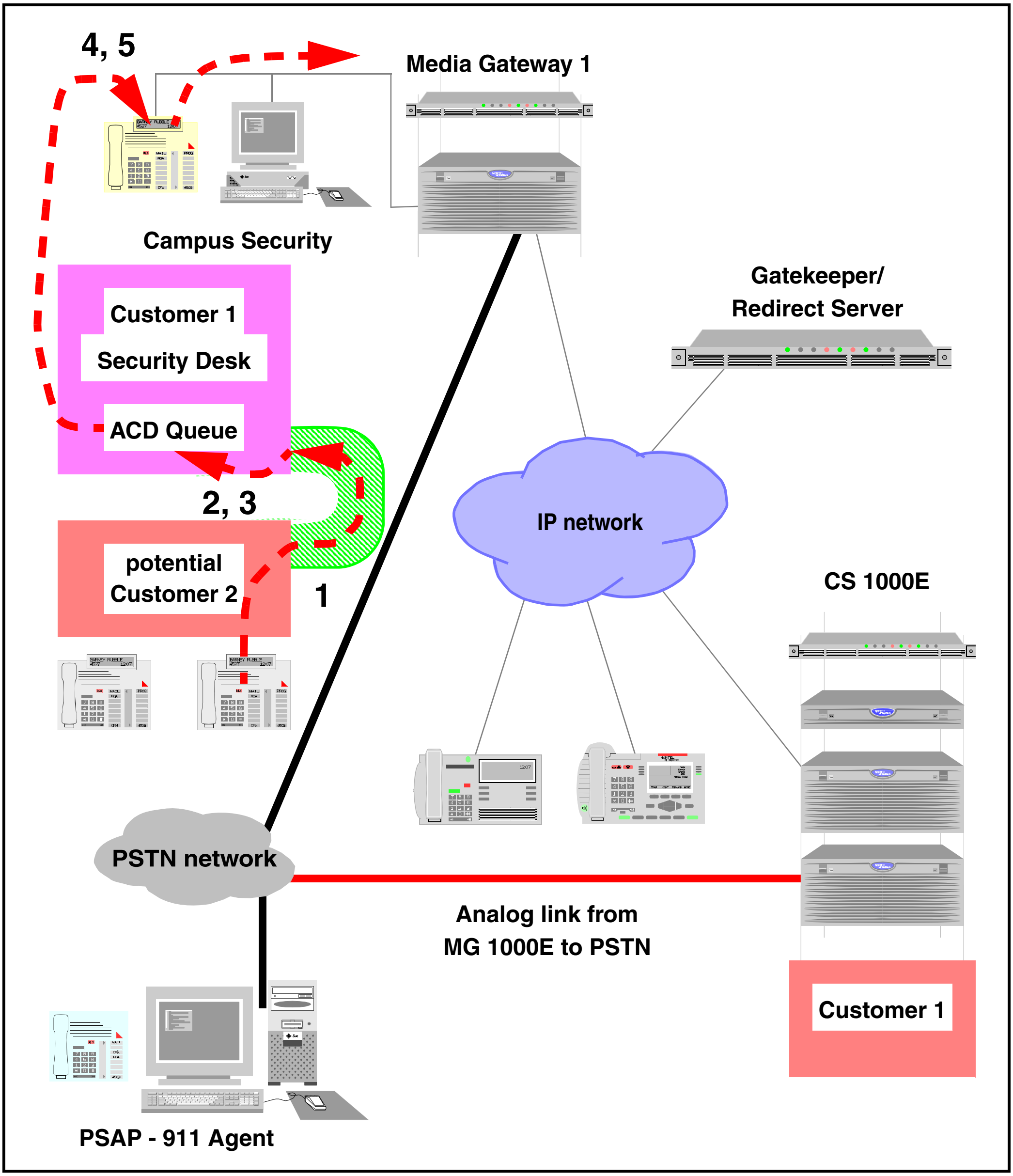
Because the security desk operator uses ESA, the call goes directly out over a trunk within the Trunk Gateway; it cannot traverse IP to use a different Trunk Gateway. It looks like “basic” ESA on another CS 1000 variant. (Because there is no way in ESA to prepend the digits required, the call cannot route over IP. However, because the security desk really wants to use local services, there is no need to use the VTRK.)

The use of ESA in this manner has one slight wrinkle. Local customers on the Trunk Gateway usually use either a PRI loop-back (Figure 82) or Virtual Trunks (Figure 83) to reach the security desk, too. Refer to the following figures and discussion.

Again, it is very strongly recommended that unless there is an over-riding reason to put other telephones at the Trunk Gateway customer with the security desk, no other telephones should exist there.

If there is only the Security Desk (Campus Security,...) on the second customer at the Trunk Gateway, provisioning is simple. Only calls to and from the Security Desk use trunking resources there; as a consequence, only ESA type calls use either the VTRKs here or the Signaling Server for this customer.

Figure 82
Initial call — “local call” from other customer, using PRI loop-back



The following flow applies.

1 The caller on the non-security desk customer dials 911. ESA call is routed to the security desk, over PRI, over a form of hair-pin. Typically, this means that a small number of ISDN trunks are back to back on this customer, and that the incoming call is manipulated into a number that can route to the ACD queue. An OSN record is generated.

2 Call terminates at the Call Server for customer 1, on the Trunk Gateway. LTER maps it into the ACD queue DN.

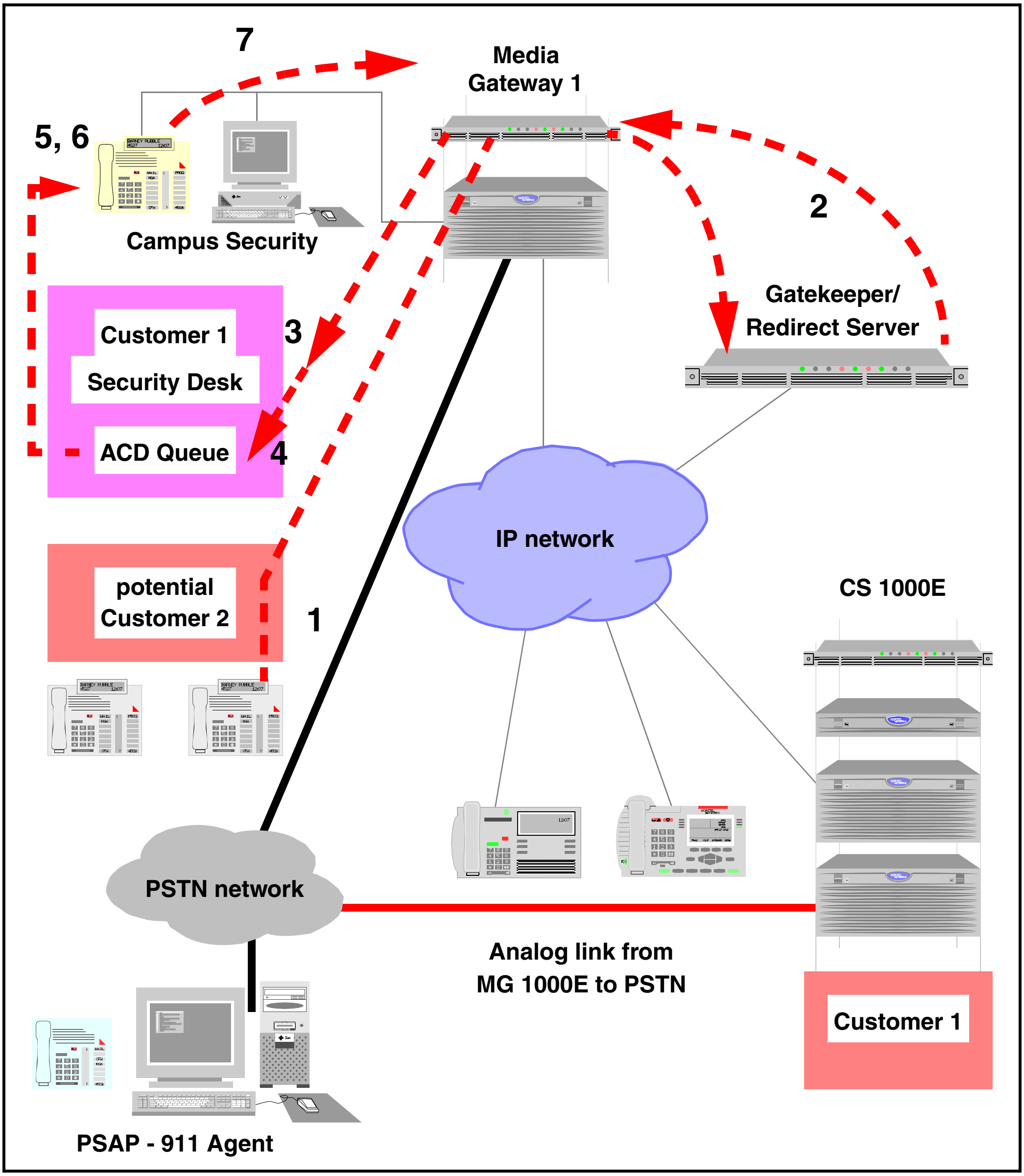
3 The call terminates to the ACD queue.

4 ACD terminates the call at an agent. If set up to do so, the ACD auxiliary modules provide extra information about the caller.

5 No OSN record is generated on the security desk customer at this time.

6 Should the answering position operator need to make a call to the external PSAP, he or she presses the "no-hold conference auto-dial" key to make the second call. Details of this are in a following flow. Refer to "Call scenario 20: User dials 911 and the security desk is available" on page 543, and the following cases.

Figure 83
Initial call — "local call" from other customer, using Virtual Trunk loop-back



The following flow applies.

1 The caller on the non-security desk customer dials 911. The ESA call is routed to the Virtual Trunk and therefore to the NRS, with the intent to terminate at the security desk, over IP. As it was sent to the IP domain, it uses a dial plan entry as per the dial plan recommendations — assume that the correct prefix and number is “61327-911”. An OSN record is generated.

2 NRS resolves to the IP address of the Trunk Gateway customer 1 Signaling Server.

3 Call terminates at the Call Server for customer 1, on the Trunk Gateway. Because the number comes in as an SPN “61327-911” and is mapped to “2020” by the LTER handling and not as the ESA DN of “911”, ESA handling is not invoked. Instead, “normal” NARS handling applies.

4 The call terminates to the ACD queue.

5 ACD terminates the call at an agent. If set up to do so, the ACD auxiliary modules provide extra information about the caller.

6 No OSN record is generated on the security desk customer at this time.

7 Should the answering position operator need to make a call to the external PSAP, he or she presses the “no-hold conference auto-dial” key (or other as applicable) to make the second call. Details of this are in a following flow. Refer to “Call scenario 20: User dials 911 and the security desk is available” on page 543, and the following cases.

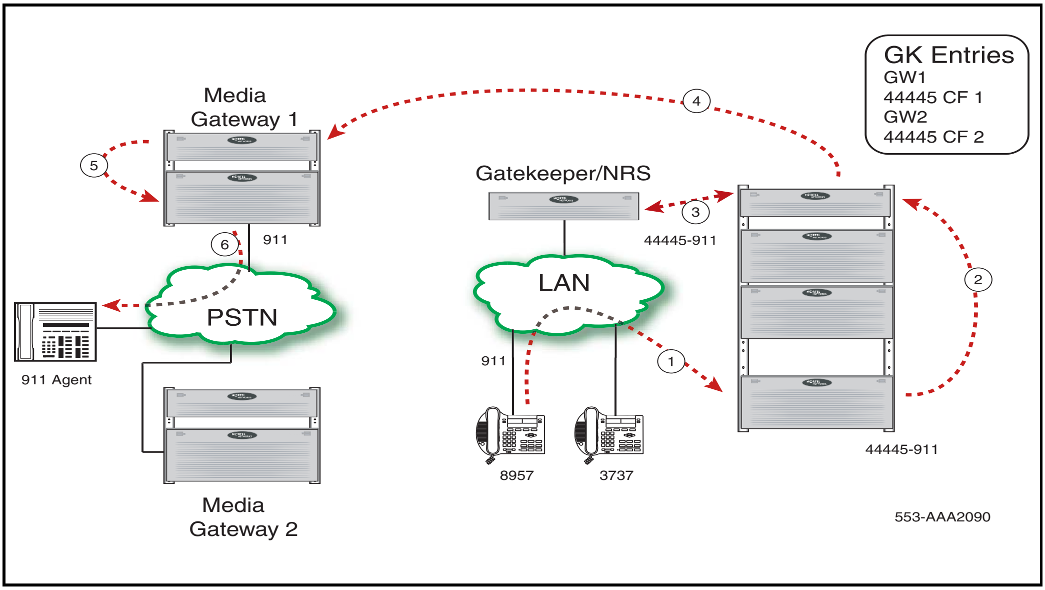
Call scenario 17: User dials 911 and the security desk gateway is available

In this scenario, the caller (DN 8957) is placing a call at the CS 1000E Call Server, over IP to a gateway with the security desk, where the call terminates.

Table 94
Call Scenario 17 Sequence

H.323 sequence	SIP sequence
The user 8957, dials 911.	
The Call Server sends the request to the Signaling Server. The Call Server does digit manipulation in the form of ZESA at the main customer and prepends 44446 to the called number 911. The transmitted digit to the Signaling Server is 44446 911. The ANI is built according to the rules pertaining to the zone (locator code present?) and the terminal CLID entry provisioning.	
The Signaling Server sends a request to Gatekeeper for address resolution. Since the NRS is able to find an entry for 44446, the call is allowed. The NRS resolves the address as the gateway with the security desk, and the gatekeeper replies to the Signaling Server. The originating Signaling Server receives the result including an ordered list of alternatives. The Security Desk is the first choice, but "in case of problems with the destination", there are alternates that go directly from the VTRK to the PSAP.	The Signaling Server sends an INVITE to the Redirect Server. (In practical terms, this is for address resolution, since the NRS and redirect server returns a list of IP addresses to try.) Since the NRS is able to find an entry for 44446, the call is allowed. The NRS resolves the address as the gateway with the security desk. The originating Signaling Server receives the result including an ordered list of alternatives. The Security Desk is the first choice, but "in case of problems with the destination", there are alternates that go directly from the VTRK to the PSAP.
The call is routed to the destination gateway. The security desk answers.	
The security desk operator determines that external support is required, and using conference auto-dial or some other feature dials 911.	
No IP routing is required. The Call Server sends the message directly to the PSTN and the PSAP using basic ESA.	

Figure 84
Setup for call scenario 17 for making ESA 911 call



Call scenario 18: User Dials 911 but the Security Desk trunking gateway is busy or congested

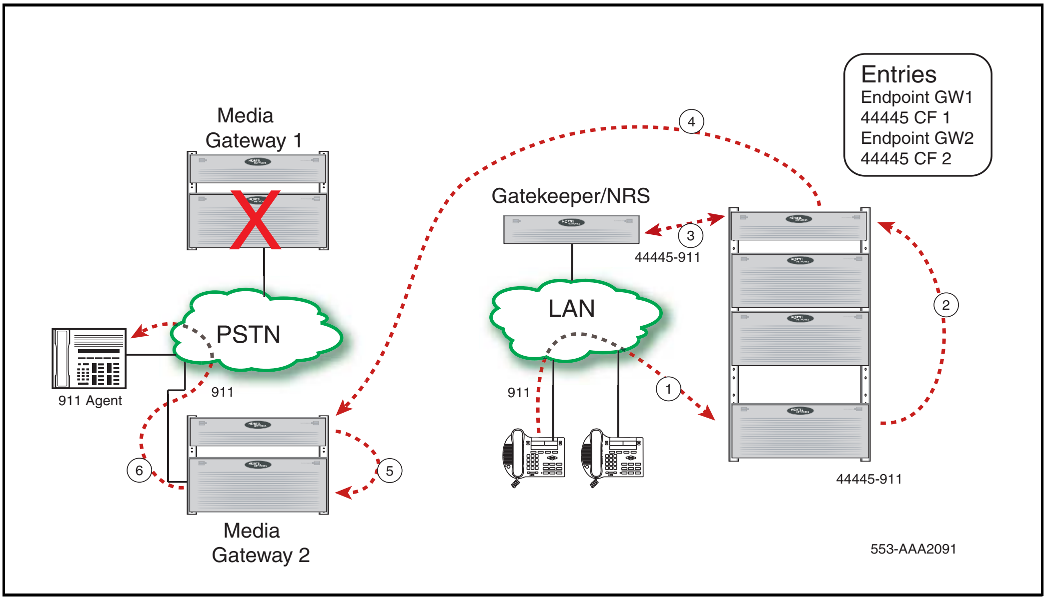
This case is somewhat different from the other “busy or congested” cases. In this situation, none of the destination Trunk Gateways with security desk capabilities are reachable; possibly they are fully utilized, or possibly they are out of service and therefore unusable. However, there is alternate routing in the least cost information, as well as a local CAMA trunk.

If the alternates are available, they is used.

Table 95
Call Scenario 18 Sequence

H.323 sequence	SIP sequence
The user 8957, dials 911.	
The Call Server sends the request to the Signaling Server. The Call Server does digit manipulation in the form of ZESA at the main customer and prepends 44446 to the called number 911. The transmitted digit to the Signaling Server is 44446 911. The ANI is built according to the rules pertaining to the zone (locator code present?) and the terminal CLID entry provisioning.	
The Signaling Server sends a request to Gatekeeper for address resolution. Since the NRS is able to find an entry for 44446, the call is allowed. The NRS resolves the address as the gateway with the security desk, and the gatekeeper replies to the Signaling Server. The originating Signaling Server receives the result including an ordered list of alternatives. The Security Desk is the first choice, but “in case of problems with the destination”, there are alternates that go directly from the VTRK to the PSAP.	The Signaling Server sends an INVITE to the Redirect Server. (In practical terms, this is for address resolution, since the NRS and redirect server returns a list of IP addresses to try.) Since the NRS is able to find an entry for 44446, the call is allowed. The NRS resolves the address as the gateway with the security desk. The originating Signaling Server receives the result including an ordered list of alternatives. The Security Desk is the first choice, but “in case of problems with the destination”, there are alternates that go directly from the VTRK to the PSAP.
The call is routed to the destination gateway. The gateway rejects the call.	
The call reroutes to another Trunk Gateway.	
If an alternate is found and the call can be placed, the Trunk Gateway sends the call to the PSAP.	

Figure 85
Setup for call scenario 11 for making ESA 911 call from CS 1000E



Call scenario 19: User Dials 911 but the Security Desk trunking gateway is busy or congested and no IP alternates available

This case is somewhat different from the other "busy or congested" cases. In this situation, not only is the security desk unreachable, but none of the destination Trunk Gateways listed for ESA can be used; possibly they are fully utilized, or possibly they are out of service and therefore unusable. The NRS may be reachable and therefore there is alternate routing in the least cost information. However, there is also a local CAMA trunk route on the CS 1000E.

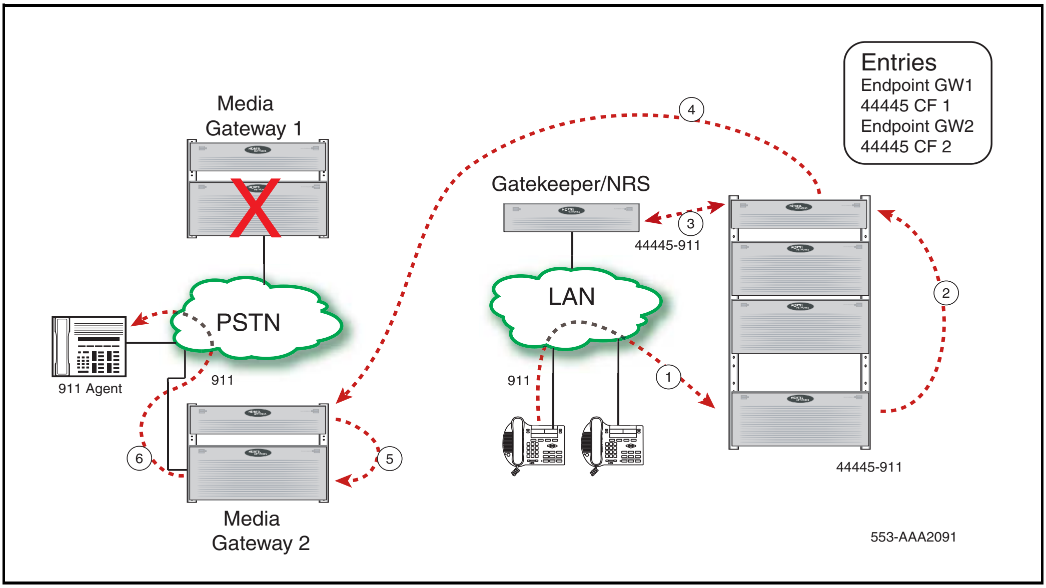
The system first tries the alternates. If the alternates are available, they are used. If not, the "STEP" capability allows the CS 1000E to revert to using a local CAMA trunk.

> ***Note:*** Note: in jurisdictions where CAMA does not exist as an option, this may be another analog trunk interface.

Table 96
Call Scenario 19 Sequence

H.323 sequence	SIP sequence
The user 8957, dials 911.	
The Call Server sends the request to the Signaling Server. The Call Server does digit manipulation in the form of ZESA at the main customer and prepends 44446 to the called number 911. The transmitted digit to the Signaling Server is 44446 911. The ANI is built according to the rules pertaining to the zone (locator code present?) and the terminal CLID entry provisioning.	
The Signaling Server sends a request to Gatekeeper for address resolution. Since the NRS is able to find an entry for 44446, the call is allowed. The NRS resolves the address as the gateway with the security desk, and the gatekeeper replies to the Signaling Server. The originating Signaling Server receives the result including an ordered list of alternatives. The Security Desk is the first choice, but “in case of problems with the destination”, there are alternates that go directly from the VTRK to the PSAP.	The Signaling Server sends an INVITE to the Redirect Server. (In practical terms, this is for address resolution, since the NRS and redirect server returns a list of IP addresses to try.) Since the NRS is able to find an entry for 44446, the call is allowed. The NRS resolves the address as the gateway with the security desk. The originating Signaling Server receives the result including an ordered list of alternatives. The Security Desk is the first choice, but “in case of problems with the destination”, there are alternates that go directly from the VTRK to the PSAP.
The call is routed to the destination gateway. The destination rejects the call.	
The call reroutes to another Trunk Gateway. This is also unavailable. This repeats until all alternates are tried.	
As the IP channels fail, the call returns to the originating node and attempts to carry out a STEP.	
If successful, the call reaches the PSAP using a local (CAMA) trunk.	

Figure 86
Setup for call scenario 11 for making ESA 911 call from CS 1000E



ESA calls with local security station on the CS 1000E

Engineering Rule 11

Avoid using the MG 1000E for a security center. If necessary, it can be done, but it is not recommended.

A brief comment on Trunk Gateways is needed to explain a little of the previous text. The CS 1000E has a Trunk Gateway intended for use on this system — the MG 1000T, which has no telephone Licenses. If the CS 1000E only uses MG 1000T Trunk Gateways, the Trunk Gateway cannot have any telephones. Therefore, the emergency desk (security desk, on-site answering position,...) must be on the CS 1000E. (Otherwise, if the emergency telephone is located on the Trunk Gateway then the emergency desk must be on a CS 1000M or CS 1000S; refer to "Security station on the CS 1000M or CS 1000S Trunk Gateway" on page 495.)

It is better to have the security desk on a CS 1000M or CS 1000S system than on the CS 1000E. However, if there are no CS 1000M or CS 1000S gateways, the CS 1000E can act as an security desk center.

System diagram

The following figure shows the CS 1000E at right, with two collocated MG 1000E systems (which may or may not have collocated H.323 or SIP to TDM trunking gateways) and a Signaling Server. The PSTN is on the left, with the destination PSAP site, and local analog trunks connect the security desk MG 1000E to the PSTN. The LAN — with the NRS and various IP Phones — is in the center. Note that one or more of the Media Gateway1 and 2 may also reside in the same location as the Call Server.

The “normal” gateways (1 and 2) are still connected to the PSTN, but have no effect on the call unless the MG 1000E of the security desk is out of service. If the call cannot reach the MG 1000E with the security desk, the call STEPs to the VTRK and out to the PSTN over these gateways.

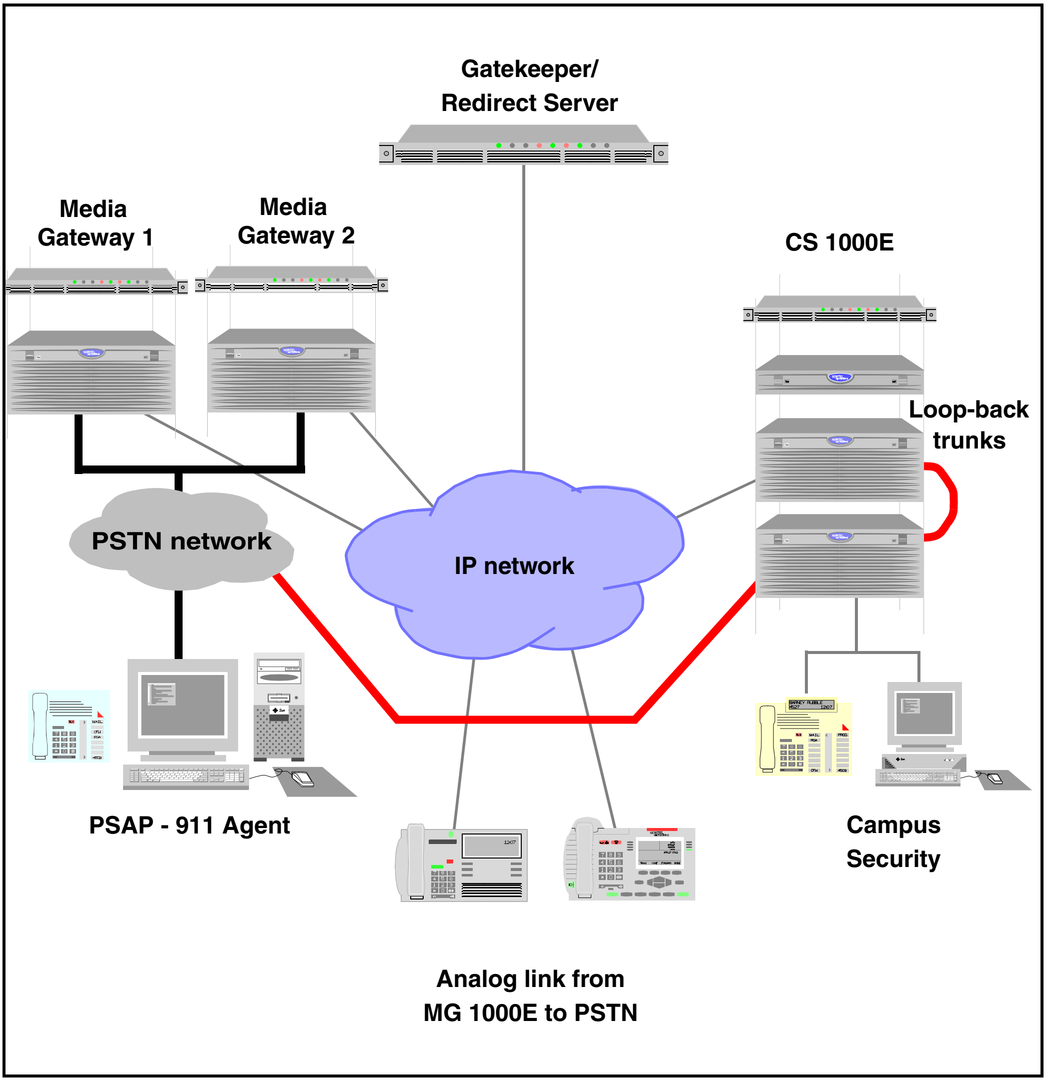
A local security desk is located on one of the MG 1000E systems; also on that node are analog trunks to the PSTN and terminating trunks of an analog loop-back (preferably, CAMA, since otherwise all calls lose the initiating ANI information). This is effectively a second customer on the system, with only CAMA trunks and the security center equipment.

Note that the CAMA (or analog) loop-back can be replaced by a Virtual Trunk loop-back, which provides originating ANI, but requires another Signaling Server and is vulnerable to WAN and LAN failures. If the call is to use Virtual Trunks to reach the security desk, it is preferable to place the security desk on a trunking gateway.

In North America, the emergency number is 911; in other countries the emergency number could be 999 or some other code.

As an example let us consider a user in North America dialing an emergency number — 911. Typically, this uses a specific variant of ESN SPN codes.

Figure 87
Setup for dialing ESA 911 (SPN) number from CS 1000E



The alternative figure shown below shows key entities (such as "customers", or more accurately, customer data blocks) within the system, as well as breaking out the physical devices somewhat more. In this figure, the trunking gateways, NRS, and the IP network are omitted; if the call has to reach them, the security desk was “out of service or unreachable”.

Note the presence of a loop-back (or hair-pin) connection between customers 1 and 2. This normally is a CAMA trunk as described in *Emergency Services Access: Description and Administration* (553-3001-313). However, in areas where CAMA is not supported, this may need to be a Virtual Trunk call to get the ANI, which means an additional Signaling Server is needed for the security desk customer. Otherwise, if analog trunks are used for the loop-back, the ANI is lost.

Engineering Rule 12

If possible, always connect two MG 1000E systems using a CAMA trunk loop-back when placing a security desk on the CS 1000E.

Engineering Rule 13

The security desk on the CS 1000E should use local CAMA trunks to the PSTN unless forced to do otherwise.

The rationale is simple. By definition, having an emergency implies that there are problems. These could include the desired trunking gateway being out of service. However, if the local security desk is still active, its CAMA trunks should also be active. Treating the call locally is the best way to ensure that an emergency call can reach the PSAP.

Figure 88
Network elements — loop-back using CAMA

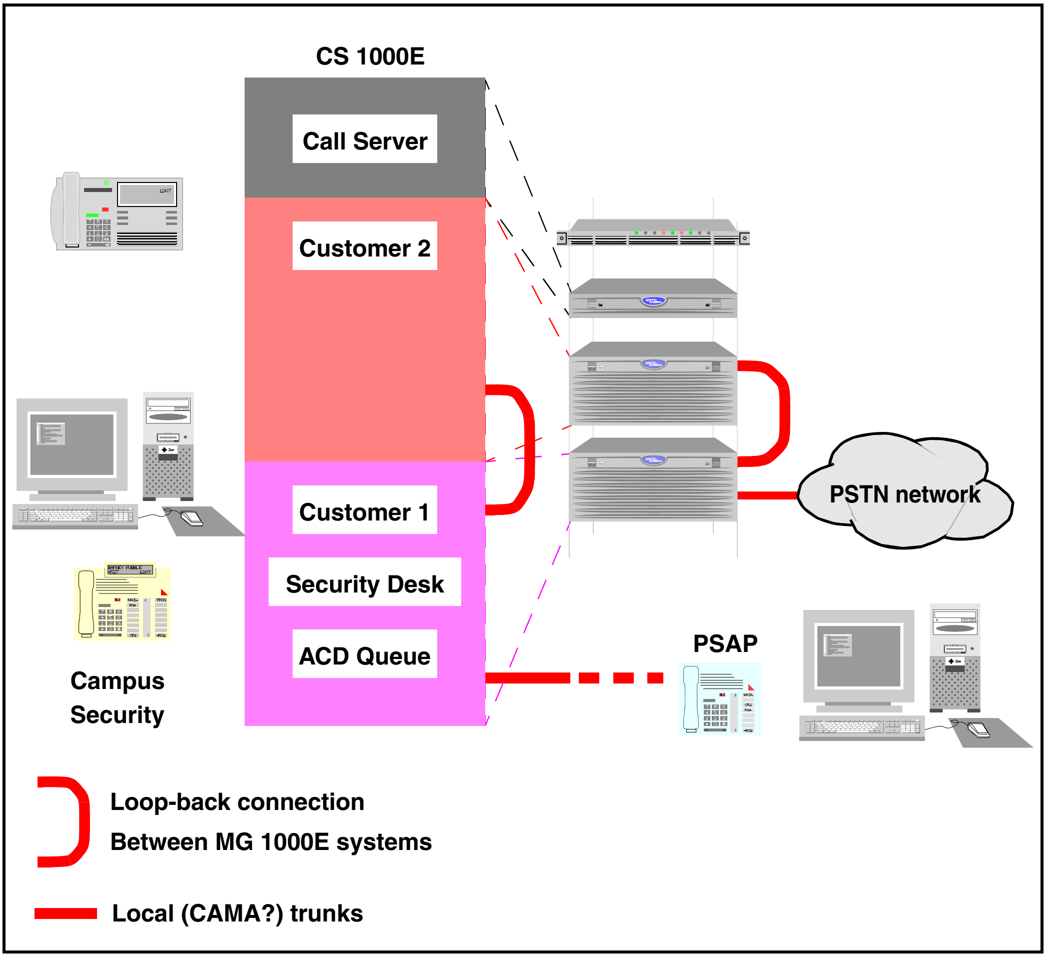
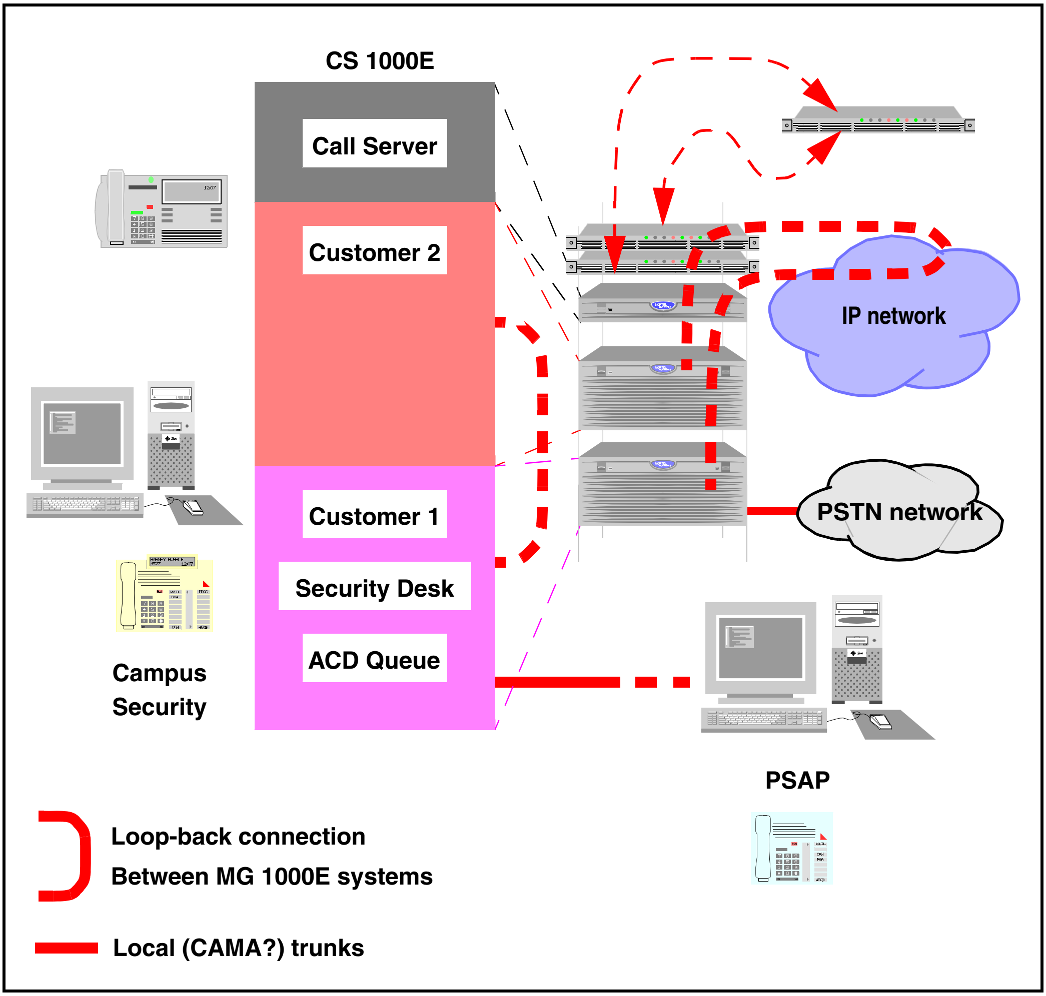


Figure 89
Network elements — loop-back using Virtual Trunks



System description

In the system shown above, the MG 1000T platforms exist, but are used only when the security desk is unavailable. The security desk uses CAMA trunks (or other permitted analog trunks) to connect to the PSTN and the PSAP. The following sections describe how to provision the numbering plan on this system for making emergency or other “special number” calls.

CAMA trunk loop-back

Because of step route limitations and issues with night call forward, ESA calls from the security desk are on CAMA. Should the security desk be unreachable (meaning the CAMA loop-back cannot process calls), the originating customer may step to a virtual route using ZESA tables, and route to a Trunk Gateway with CAMA and/or PRI calls, supported by the CS 1000E using the MG 1000T.

Since the connectivity between the Call Server and the gateway uses SIP or H.323, whenever the call steps to the Virtual Trunk route a special dialing plan is required to:

- be able to reach the correct gateway in a network, and
- be capable of notifying the correct PSAP.

In the above network, the “fail-safe” CAMA trunks and/or the PSTN PRI trunks are supported by Media Gateway1 and 2. The security desk uses a local CAMA trunk. (If it was to use a Virtual Trunk, there is no benefit to having the security desk on the CS 1000E; the advantage of placing the security desk there is that calls over H.323 and SIP could be avoided if using local services.)

Note that CAMA trunks may be provisioned on all of the MG 1000E systems, and not just the security desk MG 1000E. This provides a fail-safe in the event of network failures between the CS 1000E and its trunking gateways, with a concurrent failure at the security desk, as long as the link remains active between the Call Server and the MG 1000E. However, this would be a “step” from the Virtual Trunk, and not accessed via the Virtual Trunk.

Access to the various trunks would be as follows:

- Call placed to security desk; if CAMA trunks to reach the security desk or the desk itself are available, the desk can handle the call, but all outgoing ESA calls from the security desk use local CAMA trunks.

- Assume that the security desk is unavailable; the Call Server can step to Virtual Trunks to reach trunking gateways. If available, the gateways tandem the call out.
- Assume that the trunking gateways are unreachable; the call falls back to CS 1000E and can step to a local trunk.
- Call uses the “step” function to use the local CAMA (or other analog) trunk.

Virtual trunk loop-back

Virtual trunk loop-backs nullify any advantage of using a local security desk. The only advantage is that unless the MG 1000E loses contact with the Call Server, the CS 1000E can reach a local MG 1000E security desk. This gives it the absolute best reliability. However, as soon as the CAMA trunks looping back between customers are changed to Virtual Trunks, this advantage disappears and all the disadvantages remain.

In general, the regular form of ESA calls on CAMA and PRI calls are still supported by the CS 1000E using the MG 1000T. If the security desk MG 1000E becomes unavailable, the ESA calls can still route to a gateway. Since the connectivity between the Call Server and the gateway is via SIP or H.323, a special dialing plan is required to:

- be able to reach the correct gateway in a network, and
- be capable of notifying the correct PSAP.

In the above network, the CAMA trunks and/or the PSTN PRI trunks are supported by Media Gateway1 and 2.

Note that CAMA trunks may be provisioned on the MG 1000E systems. This provides a fail-safe in the event of network failures between the CS 1000E and its trunking gateways, as long as the link remains active between the Call Server and the MG 1000E. However, this would be a “step” from the Virtual Trunk, and not accessed via the Virtual Trunk.

Access would be as follows:

- Call placed to security desk; if Virtual Trunks to reach the security desk or the desk itself are available, the desk can handle the call, but all outgoing ESA calls from the security desk use local CAMA trunks.

- Assume that the security desk is unavailable; the Signaling Server can use least cost routing on the Virtual Trunks to reach trunking gateways. If available, the gateways tandem the call out.
- Assume that the trunking gateways are unreachable; the call falls back to CS 1000E and can step to a local trunk.
- Call uses the "step" function to use the local CAMA (or other analog) trunk.

Procedure 13
Provisioning ESA 911 (SPN) number from CS 1000E

Emergency numbers have some extra pre-work prior to provisioning the zone information; the applicable steps are:

- Ensure that the M911 package is available if using CAMA trunks; otherwise, the system cannot decode the CAMA digits.
- Create the security center customer, including provisioning. This is similar to the "Stand-alone configuration" defined in *Emergency Services Access: Description and Administration* (553-3001-313), except that instead of using CAMA or "traditional" ISDN trunks, the call uses CAMA or IP Virtual Trunks.
- Provision the Call Server ESA data
- Provision any MG 1000E systems requiring ESA data
- If needed, provision local CAMA trunks

1 Define the customer for the security desk

If using Virtual Trunks for the loop-back, a second Signaling Server is needed. Fortunately, this can help to ensure that the security center has non-blocking function. Only security center originated calls (and emergency calls, both incoming and to the PSTN) should be able to use these routes.

The provisioning steps are:

- Define the CDB.
- Define ACD capability for the customer (ACD allows the system to forward the original call information to the PSAP if the call must be

rerouted to the external emergency services). Ensure that the system is able to do a night call forward.

- Define all user terminals and equipment (ACD auxiliary devices, etc.).
- Define the virtual routes for this customer. Add the Virtual Trunks.
- Provision the ESN to handle calls coming in to the security desk. Specifically, provision an RLI to perform local termination, deleting all digits and inserting the ACD queue DN used for the security desk. Provision the Network Translations to use this RLI when the GGP and calling number type for ESA calls are detected.
- Make sure that the OSN units for the rest of the system are specifically located at the security desk associated with the security center.

2 Prepare the ESA provisioning on the Call Server

For the Call Server, the applicable steps are:

- Determine the dialing plan for ESA calls on the non-security center customer.

  This is the same as provisioning without a security desk.

- Determine the dialing plan for ESA calls on the security center customer.

  In this case, the transmitted number is different than the number for the main customer. This allows the NRS to differentiate between a call to security and a call to the PSAP.

- Configure the Virtual Trunk at Call Server.

  Readers can use either the Element Manager or command line interface for this procedure. Refer to *IP Peer Networking: Installation and Configuration* (553-3001-213) for details.

  Configure Virtual Trunks on the Call Server using the procedure given in *IP Peer Networking: Installation and Configuration* (553-3001-213).

  The Virtual Trunks must be configured and enabled from the Call Server for the emergency calls to originate from the Call Server.

- Configure ESA at the Call Server for both customers.
  - Administration for ESA in general

The administrator configures ESA in overlay 24 on the Call Server. This is the same procedure used on the CS 1000M or CS 1000S.

— Administration for digital or analog telephones located in an MG 1000E

Handled in 5 ESA data entry on the CS 1000E Call Server, using the ZESA table provisioned in overlay 117.

— Administration for IP Phones (which are within zones)

Handled in 5 ESA data entry on the CS 1000E Call Server, using the ZESA table provisioned in overlay 117.

3 Prepare the ESA provisioning on the MG 1000E

This is the same as the non-security desk example except for the split between the security desk MG 1000E and the “regular” MG 1000E systems. Note that a local CAMA trunk is required to carry out the function of sending an ESA call to the PSAP fully, although any analog trunk that cannot send the ANI could be given basic ESA handling by the PSTN.

Note that the CAMA loop-back is critical if not using Virtual Trunks. Other analog trunk types do not support the ANI. If using Virtual Trunks, Nortel recommends that the administrator provision the security desk on a CS 1000M or CS 1000S.

For the MG 1000E to function when contact is lost to the Trunk Gateways, the applicable steps are:

- Determine the dialing plan for ESA calls.

  This requires the system administrator to take a lot of care in provisioning. As an example, in many jurisdictions of the United States and Canada, the emergency number must be “911”. The call processor cannot have a DN that conflicts with these digits, but since “9” is often used for NARS AC2 (the local call Access Code), this is not usually a problem.

  The calls can only leave the MG 1000E through a trunk located within the MG 1000E; logically, this is also within the same PSTN ESZ.

- Configure ESA at the MG 1000E.

  The administrator configures ESA in overlay 24 on the Call Server. This is the same procedure used on the CS 1000M or CS 1000S.

4 GGP Planning

Note: This is only needed if using the Virtual Trunks for the loop-back. If not, do not use Virtual Trunks for calls from this CS 1000E.

This discussion assumes that CAMA trunks are not being used for the loop-back; rather, Virtual Trunks are provisioned. If CAMA trunks were used, then no Virtual Trunk provisioning (and therefore no outgoing GGP) is needed here for this function.

This is the first step unless the administrator has to execute the provisioning steps used to define ESA (from step 1, 2, and 3). If the basic requirements are configured already, provisioning starts here.

Note: Although the planning here is identical to "normal SPN" CS 1000E provisioning, ESN provisioning on the Call Server for ESA is not required. Nortel strongly recommends that the user use "conventional" ESA. None the less, the system administrator may choose to provision ESN alternates using the ESN access codes plus the ESA DN (for example, 6-911 and 9-911) to provide local termination, in case a user panics and enters the ESN access code before entering the ESN DN. In all cases, after local termination results in a normal ESA call, the NRS still looks at the call as an SPN using a GGP, so the planning is still essential.

GGP planning involves the following procedure for the "normal user" customer:

- Destination Analysis

  The call is a VTRK call only; it terminates on the other customer.

- Digit Analysis

  For the network mentioned above, assume that a unique number set "4444" is selected as a GGP. This code is unique across the whole network specified above.

- Gateway Group Selection

  The "gateway group" is the VTRK routes associated with the second customer.

- Call type Digit Set selection

  For the network, a digit string or digit (such as "6") is selected to identify the ESA and differentiate it from "true special numbers". In this example, a different code than the non-ESA SPN was used. It could be the same, but that makes provisioning more awkward. To the user it still looks the same.

GGP planning involves the following procedure for the security desk customer:

- Destination Analysis – Not required; the call is using local CAMA trunks.
- Digit Analysis – Not required; the call is using local CAMA trunks.
- Gateway Group Selection – Not required; the call is using local CAMA trunks.
- Call type Digit Set selection – Not required; the call is using local CAMA trunks.

5 ESA data entry on the CS 1000E Call Server

Engineering Rule 14

If it is on the CS 1000E, the ESA security desk needs a zone exclusively for itself.

Although ESA Zones do not belong to a specific customer, the handling of the zones on the security desk is very different than the behavior on the main node. Reserve one zone explicitly for the security desk customer, and use it for no other devices.

To enable ESA for IP zones, it is necessary for calls from IP Phones registered at the Call Server or MG 1000E systems to supply a unique identifying prefix to the Gatekeeper if the ESA calls are being routed over IP, so that the Gatekeeper can select a distinct route for each gateway. This prefix is configured with the zone data. This is done using the ZESA table provisioned in overlay 117.

- Configure an ESA zone on the Call Server.

  This only applies to IP Line or MG 1000E calls as only telephones using IP to communicate with the Call Server currently belong to zones. It is done in the Call Server via the CLI, using overlay 117.

  ```
  CHG ZESA <zone> <ESA Rte #> <AC> <ESA Prefix> <ESA Locator>
  ```

Engineering Rule 15

Always omit the ESA locator for the security desk zone.

Inserting it under certain call scenarios loses all of the information about the original caller, so assume that it corrupts all ANIs and use CLID entry blocks to handle any units that cannot provide a valid ANI. Use the locator as per the non-security center case for all other zones.

After setting the values, enable the ESA zone

ENL ZBR <Zone>

- CLID provisioning

  Either the CLID (from the CLID entry provisioned for the calling number) or the ESA Locator code is used. This depends in part on whether the locator code was provisioned; if it was not, fixed location phones use a CLID based on the CLID entry. If the locator code is defined, all phones (IP and TDM) within the zone use the locator code.

- ESN provisioning on the security center customer

  — ACD Queue provisioning

  There are multiple variants of the ACD handling. As this document is about “CS 1000E dial plan specific provisioning” and not “provisioning every feature that can exist on the CS 1000E”. See *Emergency Services Access: Description and Administration* (553-3001-313) for details.

  — Digit Manipulation provisioning

  Define a DMI to delete everything and insert the security center’s ACD queue DN.

  — RLI provisioning

  Provision an RLI to do local termination using the DMI to replace the called party number with the local security desk DN.

  — SPN provisioning

  Define an SPN based on the ESA digits sent on the call from the main customer.

  For the ESA SPN, use the RLI provisioned above with local termination.

For details, refer to *Emergency Services Access: Description and Administration* (553-3001-313).

6 ESA data entry on the MG 1000E systems

As per the non-security desk case.

7 NRS provisioning

There is one SPNs required — the one sent from the main node, and received by the security center.

Main node:

Since based on the network planning defined for this example the digit string outpulsed is 44446911, the end point in the NRS database can be a special number entry for 44446.

This step is the process of provisioning the numbering plan entries in the NRS for each of the gateways. For special number calls (such as ESA), the numbering plan entries in the NRS would vary based on the decisions made during planning about the cost factor. However, as the security desk is only over IP, only the Signaling Server of the security desk needs to be provisioned.

Since based on the network planning defined for this example the digit string outpulsed is 44446911, the end point in the NRS database can be a special number entry for 44446. (This is deleted and replaced with the security desk number when the call is received.)

For configuring this section Element Manager is required. For more details refer to *IP Peer Networking: Installation and Configuration* (553-3001-213).

8 MG 1000T provisioning

Engineering Rule 16

The number of Virtual Trunks at the security desk on the MG 1000E should be higher than the total of possible outgoing trunks, maximum number of ESA calls, and average "telephone to trunk calls over Virtual Trunks" count being handled by the security desk.

See "Engineering Rule 9" on page 471 for more details.

If using the CAMA loop-back, there is no concern about least cost routing for the gateways. However, it is possible to use Virtual Trunks for the loop-back. This is highly discouraged. Therefore, it is not discussed further here.

On the other hand, should the security desk or its MG 1000E be unreachable, the Call Server may step to routes across the IP network. In that case, provisioning at the gateway is needed.

- Configure ESN at the gateway.

A Special Number (SPN) is configured on the gateway. This SPN is for the ESA calls from the Call Server.

The SPN must use:

- A Digit Manipulation Index which deletes all the incoming digits. This may mean either all digits, or all digits except for the ESDN. In the example, since 44447911 is received, a DMI can be configured to delete the full received digit string including the 911 and insert the local ESDN in its place. This is of great utility when the ESA DN varies between locations. (Alternatively, the ESDN may be left intact. For example, in North America the ESDN is always 911; this could be left and only the 44447 deleted.)
- A RLB which has LTER (Local Termination) turned on, and using the DMI defined as deleting the prefix. This triggers re-processing of the call after the digits are removed, rather than simply tandeming the call.

When an SPN is configured, ESA determines that the call is from a trunk and forwards the correct ANI data as it tandems the call.

• Configure ESA at the gateway.

This configuration is the same as for the switch providing the outgoing side of a normal, non-IP tandem CAMA/PRI trunk ESA call. That is, if the call was PRI to ESA, provisioning the ESA side follows a specific procedure. That procedure also applies here.

ESA configuration enables the Virtual Trunk ESA call from Call Server to be tandem over to CAMA or PRI trunk.

When an ESA call is received, the gateway would recognize the incoming digits and deletes all the digits except for the ESDN left for a PRI egress (SPN configuration from Step 3), or all digits (any ESA trunk type). Then the call is routed to the local (regular) ESA processing. ESA recognizes the call as an emergency call and routes the call correctly.

ESA overrides all restrictions. So configure trunks with restrictions so that other features cannot use the same trunks. This may not be fully possible, though, if the Signaling Server may be terminating calls “for other routes” on the Call Server. To the Signaling Server, there is only one route. On the other hand, channels can be reserved for calls from the Call Server to the Signaling Server. No other calls may use these Virtual Trunks in this direction.

End of Procedure

Call scenarios

All scenarios assume an ESA DN of 911; it could just as easily be any other ESA DN. Assume a security desk DN of 2020. Further, assume that CAMA trunks (or other analog trunks) are used for the loop-back.

To invoke an ESA call, the user dials the ESA code (in the example, this is 911). The local device (in this case, the Call Server) identifies the number as being the ESA code. For CS 1000E, it matches the telephone to the corresponding ESA zone as provisioned, and uses the information in the ESA zone data to manipulate the digits and select the outgoing route.

The ZESA entry indicates a CAMA trunk route as the first choice. The prepend digits and the ESA DN are ignored; the DDGT digits are transmitted over CAMA instead.

The destination CAMA trunk terminates on the security desk MG 1000E. The incoming route directs the call to the ACD queue as per *Emergency Services Access: Description and Administration* (553-3001-313).

Two possibilities exist regarding the emergency desk customer:

- The only telephones on the security desk customer belong to the ACD queue or are telephones reached using “NCFW” from the queue.
- Other telephones may exist.

The user can theoretically have other units on the security desk customer, but this is very highly discouraged. Calls from these units will not reach the security desk, without excessively complex provisioning. Therefore, the second option is highly discouraged and is not discussed more.

If the security desk customer has only the Security Desk (Campus Security,...) and no other telephones, provisioning is simple. Only calls to and from the Security Desk use trunking resources there; as a consequence, only ESA type calls use either the CAMA trunks, or the Virtual Trunks and the Signaling Server for this customer.

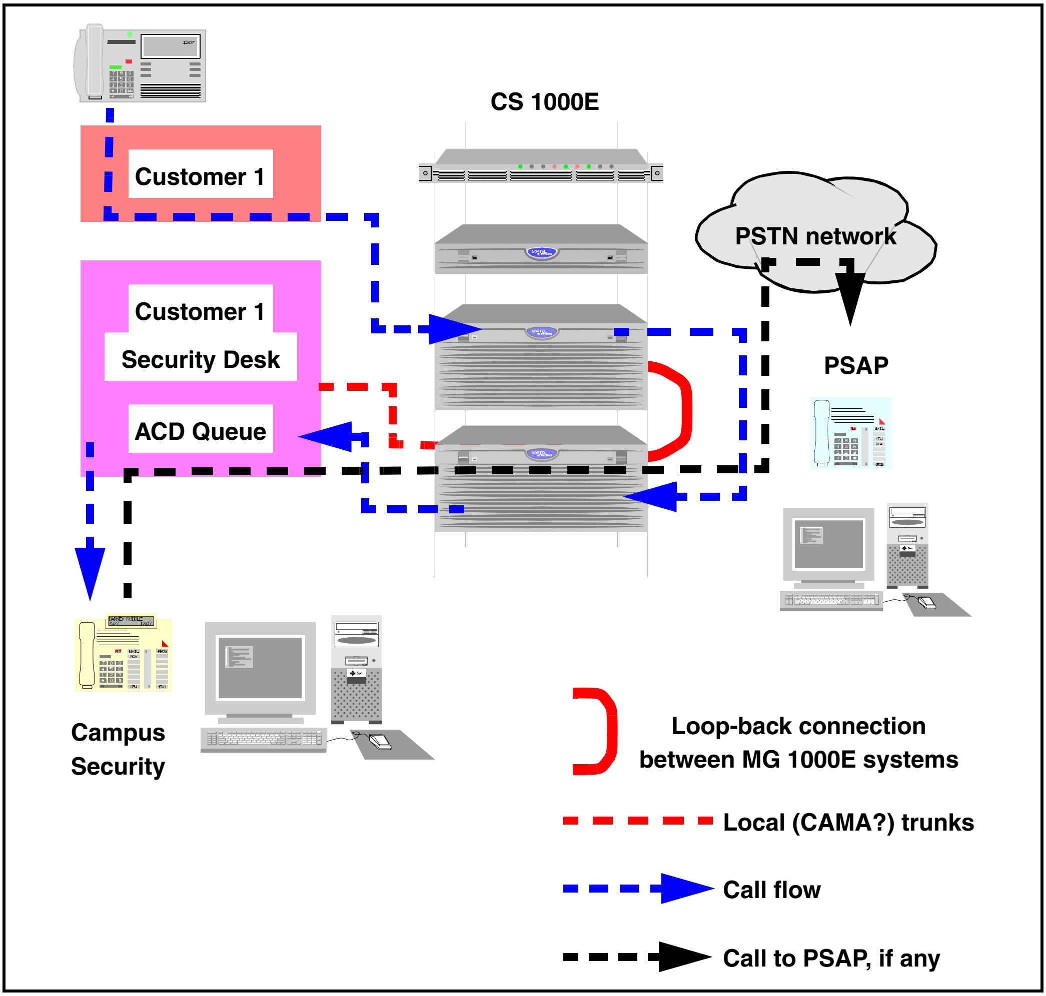
Note that the ACD agents or telephones reached from the ACD night call forward treatment must belong to a zone; they are on the MG 1000E.

Note also that the ACD agent or other telephone has a "no-hold conference/ auto-dial" key or some similar function to actually place a call to the external ESA number. This makes "an immediate" call (no digits need to be dialed) and keeps the caller in the call throughout ("no-hold conference"). Because it is a conference, the local security desk operator can provide any essential information to the PSAP, should this be required.

In jurisdictions that require the ESA caller to not be in conference, "auto-hold" and a hotline type of key operation replaces the no-hold conference auto-dial.

> ***Note:*** All scenarios show the CAMA trunks used. If necessary, the Virtual Trunk could replace the CAMA trunk. Text is included wherever the Virtual Trunk would have been used.

Figure 90
Initial call — originated from remote CS 1000E



As is shown above, the call from the user at the CS 1000E customer 2 routes through the IP network to the ACD queue on the Trunk Gateway customer 1. Here, it is sent to an ACD agent or a user terminal.

The call flow for the call placed to the security desk is as follows:

1. A caller on CS 1000E customer 2 dials 911. The ESA call is ZESA routed to the CAMA trunks (or the IP domain, using a dial plan entry as per the dial plan recommendations- assume “61327-911”). An OSN record is generated on the maintenance TTYs.
2. The call carries out the loop-back. This is either CAMA or Virtual Trunk.
3. The call lands on the ACD DN of the ACD queue used for the security desk (for example, “2020”).
4. ACD terminates the call at an agent or by NCFW to a user terminal (perhaps using a multiple appearance DN). If set up to do so, the ACD auxiliary modules and M911 capability provide extra information about the caller.
5. No OSN record is generated on the security desk customer at this time.
6. Should the answering position operator need to make a call to the external PSAP, he or she presses the “no-hold conference auto-dial” key to make the second call. Details of this are in a following flow. Refer to “Call scenario 20: User dials 911 and the security desk is available” on page 543, and the following cases.

If the security desk call is completed, the call may be as complete as it needs to get. For example, if the call was something a university security force could handle then the call might progress no further. However, if some outside agency was needed — for example, the fire department — then the security desk personnel would invoke ESA.

Because the security desk operator uses ESA, the call goes directly out over a trunk within the MG 1000E; it cannot traverse IP to use a different Trunk Gateway. Even though it is provisioned using zone ESA, it looks like “basic” ESA on another CS 1000 variant. The prepend digits could be used for an ESA attempt from the security desk but cannot be readily inserted for an ACD queue in night service — the queue has no zone. (Because there is no way for ESA to prepend the digits required, the ACD call cannot route over IP. However, because the security desk really wants to use local services, there is no need to use the VTRK.)

When the call is placed from the security desk to the PSAP, the following occurs:

1 The security desk answers the call, terminated as an LTER to the ACD agent queue.

2 The need for an external ESA call is identified; the operator handling the call presses the no-hold conference auto-dial key (or whatever was selected. See *Emergency Services Access: Description and Administration* (553-3001-313) for details. The auto-dial DN is the ESA DN (for example, 911). An OSN record is generated.

3 ESA uses the ZESA table. The system attempts to prepend the prefix but none exists ("NONE" or "~" entered) and the call goes to the CAMA trunk. The prepend attempt always comes first, because zone ESA may try to step to a Virtual Trunk; therefore, the prepend is done. The CAMA trunk then proceeds to ignore these digits.

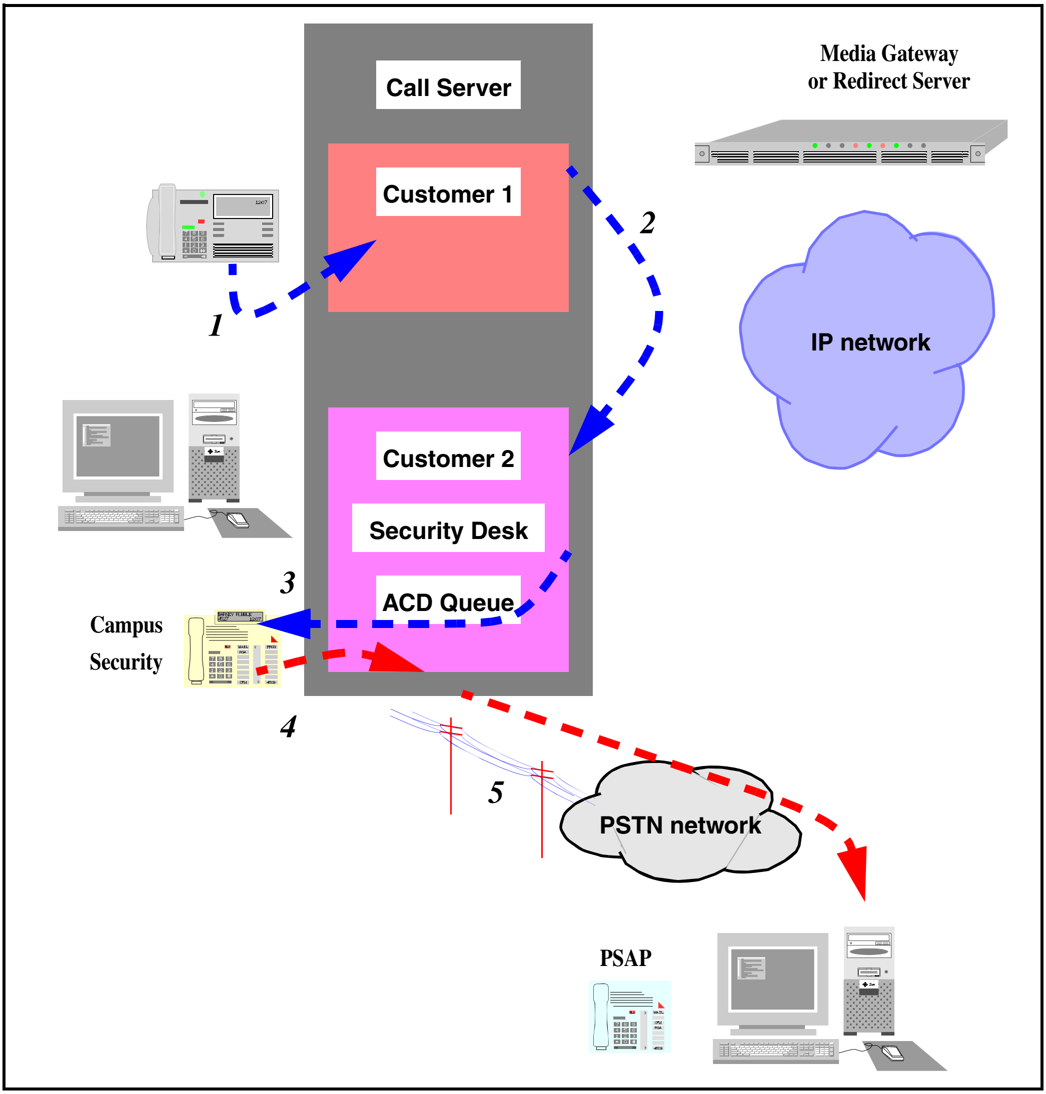
4 The CAMA trunk call reaches the PSTN. The PSTN either routes the call directly to the PSAP, or uses Selective Routing to route it to the right PSAP.

Normal case — the call reaches the PSTN via the security desk and the CAMA route

Call scenario 20: User dials 911 and the security desk is available

In this scenario, the caller (DN 8957) is placing a call at the Call Server, over CAMA to an MG 1000E with the security desk, and over CAMA to the PSTN, where the call terminates on the desired destination.

Figure 91
Setup for call scenario 20 for making ESA 911 call



The “gateway protocol” is immaterial; the Call Server uses the following sequence:

Call to the security desk:

1 The user 8957, dials 911.

2 The Call Server sends the call to the CAMA trunk.

3 It should be noted that zone ESA prepares the call to allow “STEP” within valid combinations. Since a CAMA trunk can step to a Virtual Trunk, the prepend proceeds. The Call Server does digit manipulation in the form of ZESA at the main customer and prepends 44446 to the called number 911. The ANI is built according to the rules pertaining to the zone (locator code present?) and the terminal CLID entry provisioning. However, since the call is over CAMA the prepend digits are ignored. If the CAMA trunks were busy or out of service, the call would try to route over Virtual Trunks, potentially routing to a remote Trunk Gateway. Since the CAMA trunks are available, the call uses the DDGT.

4 The destination MG 1000E detects the call, which rings on the security desk gateway. The call is answered.

Call to the external PSAP:

5 The security desk answers, determines that external support is required, and dials 911. The Call Server detects that this is for a CAMA trunk.

6 The call is routed over the CAMA trunks to the nearest PSAP.

Call scenario 21: User Dials 911 but the security desk is unreachable

This case is somewhat different from the other “busy or congested” cases. In this situation, all of the destination Trunk Gateways are usable. However, the security desk MG 1000E is down.

Table 97
Call Scenario 21 Sequence

<table>
<tr><th>H.323 sequence</th><th>SIP sequence</th></tr>
<tr><td colspan="2">The user 8957, dials 911.</td></tr>
<tr><td colspan="2">The Call Server tries the security desk trunks; it cannot reach the desk.

The Call Server does digit manipulation in the form of ZESA at the main customer and prepends 44446 to the called number 911. The ANI is built according to the rules pertaining to the zone (locator code present?) and the terminal CLID entry provisioning.

Normally, the call would proceed using CAMA trunks. However, since the call cannot route over CAMA, for this step the prepend digits are needed.</td></tr>
<tr><td colspan="2">The Call Server sends the request to the Signaling Server.

The Call Server uses the digits with the prepend.</td></tr>
<tr><td>The Signaling Server sends a request to Gatekeeper for address resolution.

Since the gatekeeper is able to find an entry for 44446 with a cost factor of 1 on Media Gateway 1, it send the IP address of Media Gateway 1 to the requesting Signaling Server. Media Gateway 2 is indicated as an alternate endpoint if least cost routing is available.</td><td>The call is then routed to the redirect server for address resolution.

Since an entry with cost factor “1” is found for 44446, the IP address of the endpoint — Media Gateway 1 — used to forward the INVITE. Media Gateway 2 is indicated as an alternate endpoint if least cost routing is available.</td></tr>
<tr><td colspan="2">The originating Signaling Server then transmits the H.225.0 SETUP to the gateway. The call is sent from the Signaling Server to the gateway Call Server to route the call.</td></tr>
<tr><td colspan="2">The call completes as though there was no security desk attempt.</td></tr>
</table>

Call scenario 22: User Dials 911 but the security desk is unavailable and all trunking gateways are busy or congested

This case is somewhat different from the other "busy or congested" cases. In this situation, the security desk cannot be reached, and none of the destination Trunk Gateways are usable. However, there is a local CAMA trunk.

Table 98
Call Scenario 21 Sequence (Part 1 of 2)

H.323 sequence	SIP sequence
The user 8957, dials 911.	
The Call Server tries the security desk trunks; it cannot reach the desk. The Call Server does digit manipulation in the form of ZESA at the main customer and prepends 44446 to the called number 911. The ANI is built according to the rules pertaining to the zone (locator code present?) and the terminal CLID entry provisioning. Normally, the call would proceed using CAMA trunks. However, since the call cannot route over CAMA, for this step the prepend digits are needed.	
The Call Server sends the request to the Signaling Server. The Call Server uses the digits with the prepend.	
The Signaling Server sends a request to Gatekeeper for address resolution. Since the gatekeeper is able to find an entry for 44446 with a cost factor of 1 on Media Gateway 1, it send the IP address of Media Gateway 1 to the requesting Signaling Server. Media Gateway 2 is indicated as an alternate endpoint if least cost routing is available.	The call is then routed to the redirect server for address resolution. The INVITE arrives at the NRS. Since the redirect server is able to find an entry for 44446, the IP address of the endpoint — Media Gateway 1 — is returned and used by the originator to forward the INVITE. Media Gateway 2 is indicated as an alternate endpoint if least cost routing is available.
The security desk Signaling Server then transmits the H.225.0 SETUP to the gateway. The call is sent from the Signaling Server to the Call Server on the gateway for routing the call.	The originating Signaling Server then transmits the SIP INVITE to the gateway. The call is sent from the Signaling Server to the Call Server on the gateway for routing the call.

Table 98
Call Scenario 21 Sequence (Part 2 of 2)

H.323 sequence	SIP sequence
All trunking gateways are unavailable, the call is rejected as "no trunks available". The RELEASE COMPLETE message is sent to the security desk Signaling Server.	All trunking gateways are unavailable, the call is rejected as "no trunks available". The SIP clearing message is sent to the security desk Signaling Server.
The security desk Signaling Server checks for another "least cost routing" entry. If it finds one, it retransmits the H.225.0 SETUP to the next gateway in the least cost list. The call is sent from the Signaling Server to the Call Server on the gateway for routing the call.	The originating Signaling Server checks the "least cost route", and finding one, then transmits the SIP INVITE to the gateway. The call is sent from the Signaling Server to the Call Server on the gateway for routing the call.
All trunking gateways are unavailable, the call is rejected as "no trunks available". The RELEASE COMPLETE message is sent to the security desk Signaling Server.	All trunking gateways are unavailable, the call is rejected as "no trunks available". The SIP clearing message is sent to the security desk Signaling Server.
The security desk Signaling Server finds no more options. The rejection returns to the Call Server.	
The Call Server steps to the CAMA trunk route, and as long as one or more trunks is/are free, the call is placed to the PSTN.	

Provisioning procedures

Provisioning is approached as a “step by step” operation to complete a specific task. This should simplify data entry for the user.

Refer to the following procedures to provision the listed call types:

Table 99
Procedure to use based on call type

Call Type	See Procedure	On Page
NXX	14	550
Local SPN, or all SPN types to the PSTN except national numbers	15	552
NPA	16	555
National SPN	17	558
International calls	18	561
GDP — Location code (LOC) dialing	21	571
UNP (CDP dialing)	22	572
Incoming DID calls	23	573
Incoming GDP calls	24	574
Incoming UNP calls	25	575
ESA	26	576

Data prerequisites

The user is expected to have already provisioned all of the CDB and RDBs required, as well as the ESN data blocks. This implies provisioning ISDN, IP Peer Virtual Trunks, and so forth.

Outgoing calls

Procedure 14
Provisioning required for placing NXX calls

Note that “NXX” refers explicitly to the North American variant of E.164 “local” or “subscriber” numbers. Note also that in prior descriptions the GGP (ggp) was “4444” and the call type digit was 1.

1 Carry out preliminary analysis, if it has not already been done.

Determine where this call will land. Does it land on one or more than one gateway? Are there different costs for each gateway?

Select the GGP for this gateway or set of gateways. This code must be unique across the whole network. Record this code for use in creating Digit Manipulation Indices.

Select the call type digit for the NXX.

2 Carry out Digit Manipulation Index (DMI) provisioning for this destination.

If the DMI was provisioned in an earlier cycle defining another NXX, this step may be skipped. However, Nortel recommends that the user confirm that the step is not required before proceeding.

Define the DMI to insert the digit string made up of the GGP (ggp) and call type digit. The DMI maps the call type to “SPN”, and has “ISPN” set to YES to force the system to build the CLID as an NXX, and not as an SPN.

The entries requiring input in the DMI configurations are shown below.

```
REQ NEW
CUST <as applicable>
FEAT DGT
DMI <as applicable>
DEL
INST <ggp><ctd>
CTYP SPN
ISPN YES
```

The INST includes the concatenated GGP and the call type digit. CTYP is set to SPN.

In addition, this DMI also handles the CLID provisioning. Setting ISPN to YES means that the CLID is built as an NXX.

Based on the example and scenarios in the description, this would be:

```
REQ NEW
CUST <as applicable>
FEAT DGT
DMI <as applicable>
DEL
INST 44441
CTYP SPN
ISPN YES
```

For more details on provisioning of Digit Manipulation, please refer to the Appendix section.

3 Provision the RLI

Define the RLI to be used for the NXXs terminating on this gateway group. The RLI includes all ESN data as applicable, and uses the DMI defined in the previous step.

```
REQ NEW
CUST <as applicable>
FEAT RLB
RLI <as applicable>
NTR <as applicable>
.....
ROUT <as applicable>
.....
DMI <as defined in the previous step>
.....
```

For most networks, routes for a specific call type to a single gateway group can be handled by having a single RLI. Normally, it is not necessary to have more than one route for NXX entries to a specific destination.

4 Provision the NXX

Configure the local exchange number as an NXX in the Call Server and associate the prefix with the respective RLI created in the preceding step. This configuration procedure is same as that of a CS 1000M or CS 1000S system.

5 NRS provisioning

Provision the entries associated with that SPN prefix on the gatekeeper.

For local calls using the steering code prefix defined above, the numbering plan entries in the NRS would be as below:

```
numbertype.Special.Private (SPN)
```

```
xxxxx on gateway1 cost factor 1
```

```
xxxxx on gateway2 cost factor 2
```

where “xxxxx” was the combined GGP and possibly the call type digit. (If all call types using the GGP are to use the same entry, this may be the GGP alone.)

6 Destination gateway provisioning

Create the destination DMI and RLB to strip off the prefix and change the number to the correct call type.

The number of digits to be deleted includes both the GGP length and the length of the call type digits. Removing both returns the number to its original NXX format.

The DMI provisioning is as follows:

```
REQ NEW
CUST <as applicable>
FEAT DGT
DMI <as applicable>
DEL <length of ggp and ctd>
INST
CTYP NXX
ISPN NO
```

The DMI is used in the outgoing RLI. The RLI is accessed by provisioning the SPN in the ESN data, using the RLI configured for this use.

For more details about provisioning the destination refer to the appendix section of this document.

End of Procedure

Procedure 15
Provisioning required for placing local PSTN SPN calls

This includes local exchange numbers for systems outside North America and local exchange numbers used for assistance such as 411 (directory assistance) inside North America. Note that in prior descriptions the GGP (ggp) was “4444” and the call type digit was 1.

1 Carry out preliminary analysis, if it has not already been done.

Determine where this call will land. Does it land on one or more than one gateway? Are there different costs for each gateway?

Select the GGP for this gateway or set of gateways. This code must be unique across the whole network. Record this code for use in creating Digit Manipulation Indices.

Select the call type digit for the local number.

2 Carry out Digit Manipulation Index (DMI) provisioning for this destination.

If the DMI was provisioned in an earlier cycle defining another SPN, this step may be skipped. However, Nortel recommends that the user confirm that the step is not required before proceeding.

Define the DMI to insert the digit string made up of the GGP (ggp) and call type digit. The DMI maps the call type to "SPN", and has "ISPN" set to YES.

The entries requiring input in the DMI configurations are shown below.

```
REQ NEW
CUST <as applicable>
FEAT DGT
DMI <as applicable>
DEL
INST <ggp><ctd>
CTYP SPN
ISPN YES
```

The INST includes the concatenated GGP and the call type digit. CTYP is set to SPN.

In addition, this DMI also handles the CLID provisioning. Setting ISPN to YES means that the CLID is built correctly.

For more details on provisioning of Digit Manipulation, please refer to the Appendix section.

3 Provision the RLI

Define the RLI to be used for the NXXs terminating on this gateway group. The RLI includes all ESN data as applicable, and uses the DMI defined in the previous step.

```
REQ NEW
CUST <as applicable>
FEAT RLB
RLI <as applicable>
ENTR <as applicable>
.....
ROUT <as applicable>
.....
DMI <as defined in the previous step>
.....
```

For most networks, routes for a specific call type to a single gateway group can be handled by having a single RLI. Normally, it is not necessary to have more than one route for national number entries to a specific destination.

4 Provision the SPN

Configure the digit string as an SPN in the Call Server and associate the prefix with the respective RLI created in the preceding step. This configuration procedure is same as that of a CS 1000M or CS 1000S system.

5 NRS provisioning

Provision the entries associated with that SPN prefix on the gatekeeper.

For local calls using the steering code prefix defined above, the numbering plan entries in the NRS would be as below:

```
numbertype.Special.Private (SPN)

xxxxx on gateway1 cost factor 1

xxxxx on gateway2 cost factor 2
```

where “xxxxx” was the combined GGP and possibly the call type digit. (If all call types using the GGP are to use the same entry, this may be the GGP alone.)

6 Destination gateway provisioning

Create the destination DMI and RLB to strip off the prefix and change the number to the correct call type.

The number of digits to be deleted includes both the GGP length and the length of the call type digits. Removing both returns the number to its original format. If the call is exiting to the public network and the scenario allows the CTYP to be set as NXX, then this may also be done. Otherwise, map it to the correct call type as per the local requirements.

(Many to most non-North American PSTNs expect “E.164 local” — NXX in North America — as the call type, which can be obtained by using CTYP as NXX. This does not affect overlap signaling calls, provided the far side of the call treats the number as per the local country procedures. Do not convert to an NXX if the next switch is a Meridian 1 or CS 1000; let the final Call Server handle the manipulation prior to sending the call to the PSTN.)

The DMI provisioning is as follows:

```
REQ NEW
CUST <as applicable>
FEAT DGT
DMI <as applicable>
DEL <length of ggp and ctd>
INST
CTYP NXX or as applicable
ISPN NO
```

The DMI is used in the outgoing RLI. The RLI is accessed by provisioning the SPN in the ESN data, using the RLI configured for this use.

For more details about provisioning the destination refer to the appendix section of this document.

End of Procedure

Procedure 16
Provisioning required for placing NPA calls

Note that “NPA” refers explicitly to the North American variant of E.164 “national” numbers. Note also that in prior descriptions the GGP (ggp) was “4444” and the call type digit was 2.

1 Carry out preliminary analysis, if it has not already been done.

Determine where this call will land. Does it land on one or more than one gateway? Are there different costs for each gateway?

Select the GGP for this gateway or set of gateways. This code must be unique across the whole network. Record this code for use in creating Digit Manipulation Indices.

Select the call type digit for the NPA.

2 Carry out Digit Manipulation Index (DMI) provisioning for this destination.

If the DMI was provisioned in an earlier cycle defining another NPA, this step may be skipped. However, Nortel recommends that the user confirm that the step is not required before proceeding.

Define the DMI to insert the digit string made up of the GGP (ggp) and call type digit. The DMI maps the call type to “SPN”, and has “ISPN” set to YES to force the system to build the CLID as an NPA, and not as an SPN.

The entries requiring input in the DMI configurations are shown below.

```
REQ NEW
CUST <as applicable>
FEAT DGT
DMI <as applicable>
DEL
INST <ggp><ctd>
CTYP SPN
ISPN YES
```

The INST includes the concatenated GGP and the call type digit. CTYP is set to SPN.

In addition, this DMI also handles the CLID provisioning. Setting ISPN to YES means that the CLID is built as an NPA.

For more details on provisioning of Digit Manipulation, please refer to the Appendix section.

3 Provision the RLI

Define the RLI to be used for the NPAs terminating on this gateway group. The RLI includes all ESN data as applicable, and uses the DMI defined in the previous step.

```
REQ NEW
CUST <as applicable>
FEAT RLB
RLI <as applicable>
ENTR <as applicable>
.....
ROUT <as applicable>
.....
DMI <as defined in the previous step>
.....
```

For most networks, routes for a specific call type to a single gateway group can be handled by having a single RLI. Normally, it is not necessary to have more than one route for NPA entries to a specific destination.

4 Provision the NPA

Configure the correct area code (typically with the long distance digit; normally, if it isn't a long distance toll call the users don't need the area code, but some areas overlap or allow local calls across adjacent boundaries) as an NPA in the Call Server and associate the prefix with the respective RLI created in the preceding step. This configuration procedure is same as that of a CS 1000M or CS 1000S system.

5 NRS provisioning

Provision the entries associated with that SPN prefix on the gatekeeper.

For national calls using the steering code prefix defined above, the numbering plan entries in the NRS would be as below:

```
numbertype.Special.Private (SPN)

xxxxx on gateway1 cost factor 1

xxxxx on gateway2 cost factor 2
```

where "xxxxx" was the combined GGP and possibly the call type digit. (If all call types using the GGP are to use the same entry, this may be the GGP alone.)

6 Destination gateway provisioning

Create the destination DMI and RLB to strip off the prefix and change the number to the correct call type.

The number of digits to be deleted includes both the GGP length and the length of the call type digits. Removing both returns the number to its original NPA format.

The DMI provisioning is as follows:

```
REQ NEW
CUST <as applicable>
FEAT DGT
DMI <as applicable>
DEL <length of ggp and ctd>
INST
CTYP NPA
ISPN NO
```

The DMI is used in the outgoing RLI. The RLI is accessed by provisioning the SPN in the ESN data, using the RLI configured for this use.

For more details about provisioning the destination refer to Appendix section of this document.

End of Procedure

Procedure 17
Provisioning required for placing National SPN calls

Note that in prior descriptions the GGP (ggp) was “4444” and the call type digit was 2.

1 Carry out preliminary analysis, if it has not already been done.

Determine where this call will land. Does it land on one or more than one gateway? Are there different costs for each gateway?

Select the GGP for this gateway or set of gateways. This code must be unique across the whole network. Record this code for use in creating Digit Manipulation Indices.

Select the call type digit for the national number.

2 Carry out Digit Manipulation Index (DMI) provisioning for this destination.

If the DMI was provisioned in an earlier cycle defining another national number, this step may be skipped. However, Nortel recommends that the user confirm that the step is not required before proceeding.

Define the DMI to insert the digit string made up of the GGP (ggp) and call type digit. The DMI maps the call type to “SPN”, and has “ISPN” set to YES to force the system to build the CLID correctly.

The entries requiring input in the DMI configurations are shown below.

```
REQ NEW
CUST <as applicable>
FEAT DGT
DMI <as applicable>
DEL
INST <ggp><ctd>
CTYP SPN
ISPN YES
```

The INST includes the concatenated GGP and the call type digit. CTYP is set to SPN.

For more details on provisioning of Digit Manipulation, please refer to the Appendix section.

3 Provision the RLI

Define the RLI to be used for the national number SPNs terminating on this gateway group. The RLI includes all ESN data as applicable, and uses the DMI defined in the previous step.

```
REQ NEW
CUST <as applicable>
FEAT RLB
RLI <as applicable>
ENTR <as applicable>
.....
ROUT <as applicable>
.....
DMI <as defined in the previous step>
.....
```

For most networks, routes for a specific call type to a single gateway group can be handled by having a single RLI. Normally, it is not necessary to have more than one route for NPA entries to a specific destination.

4 Provision the SPN

Configure the dialed digit string for the national number as an SPN in the Call Server and associate the prefix with the respective RLI created in the preceding step. This configuration procedure is same as that of a CS 1000M or CS 1000S system.

5 NRS provisioning

Provision the entries associated with that SPN prefix on the gatekeeper.

For national calls using the steering code prefix defined above, the numbering plan entries in the NRS would be as below:

```
numbertype.Special.Private (SPN)

xxxxx on gateway1 cost factor 1

xxxxx on gateway2 cost factor 2
```

where "xxxxx" was the combined GGP and possibly the call type digit. (If all call types using the GGP are to use the same entry, this may be the GGP alone.)

Destination gateway provisioning

Create the destination DMI and RLB to strip off the prefix and change the number to the correct call type.

The number of digits to be deleted includes both the GGP length and the length of the call type digits. Removing both returns the number to its original digit string format.

In addition, if the call scenario allows and the network permits, the call type can be mapped into "NPA" (even though the Call Server would treat this as a North American call if it received this, it is sending it to a PSTN that expects it). Alternatively, use the call type as is used for normal national number calls over ISDN.

(Many to most non-North American PSTNs expect "E.164 national number" — NXX in North America — as the call type, which can be obtained by using CTYP as NPA. This does not affect overlap signaling calls, provided the far side of the call treats the number as per the local country procedures. Do not convert to an NPA if the next switch is a Meridian 1 or CS 1000; let the final Call Server handle the manipulation prior to sending the call to the PSTN.)

The DMI provisioning is as follows:

```
REQ NEW
```

```
CUST <as applicable>
FEAT DGT
DMI <as applicable>
DEL <length of ggp and ctd>
INST
CTYP NPA or as applicable
ISPN NO
```

The DMI is used in the outgoing RLI. The RLI is accessed by provisioning the SPN in the ESN data, using the RLI configured for this use.

For more details about provisioning the destination refer to Appendix section of this document.

End of Procedure

Procedure 18
Provisioning required for placing International calls

Note that in prior descriptions the GGP (ggp) was “4444” and the call type digit was 3.

1 Carry out preliminary analysis, if it has not already been done.

Determine where this call will land. Does it land on one or more than one gateway? Are there different costs for each gateway?

Select the GGP for this gateway or set of gateways. This code must be unique across the whole network. Record this code for use in creating Digit Manipulation Indices.

Select the call type digit for the INTL.

2 Carry out Digit Manipulation Index (DMI) provisioning for this destination.

If the DMI was provisioned in an earlier cycle defining another international number, this step may be skipped. However, Nortel recommends that the user confirm that the step is not required before proceeding.

Define the DMI to insert the digit string made up of the GGP (ggp) and call type digit. The DMI maps the call type to “SPN”, and has “ISPN” set to YES to force the system to build the CLID as an international, and not as an SPN.

The entries requiring input in the DMI configurations are shown below.

```
REQ NEW
CUST <as applicable>
FEAT DGT
DMI <as applicable>
DEL
INST <ggp><ctd>
CTYP SPN
ISPN YES
```

The INST includes the concatenated GGP and the CDT. CTYP is set to SPN.

In addition, this DMI also handles the CLID provisioning. Setting ISPN to YES means that the CLID is built as an INTL.

For more details on provisioning of Digit Manipulation, please refer to the Appendix section.

3 Provision the RLI

Define the RLI to be used for the SPNs terminating on this gateway group. The RLI includes all ESN data as applicable, and uses the DMI defined in the previous step.

```
REQ NEW
CUST <as applicable>
FEAT RLB
RLI <as applicable>
ENTR <as applicable>
```

```
.....
ROUT <as applicable>
.....
DMI <as defined in the previous step>
.....
```

For most networks, routes for a specific call type to a single gateway group can be handled by having a single RLI. Normally, it is not necessary to have more than one route for international entries to a specific destination.

4 Provision the International SPN

Configure 011 as an SPN in the Call Server and associate the prefix with the respective RLI created in the preceding step. This configuration procedure is same as that of a CS 1000M or CS 1000S system.

5 NRS provisioning

Provision the entries associated with that SPN prefix on the gatekeeper.

For national calls using the steering code prefix defined above, the numbering plan entries in the NRS would be as below:

```
numbertype.Special.Private (SPN)

xxxxx on gateway1 cost factor 1

xxxxx on gateway2 cost factor 2
```

where “xxxxx” was the combined GGP and possibly the CDT. (If all call types using the GGP are to use the same entry, this may be the GGP alone.)

6 Destination gateway provisioning

Create the destination DMI and RLB to strip off the prefix and change the number to the correct call type.

The number of digits to be deleted includes both the GGP length and the length of the CDTs. Removing both returns the number to its original INTL format.

The DMI provisioning is as follows:

```
REQ NEW
CUST <as applicable>
FEAT DGT
DMI <as applicable>
DEL <length of ggp and ctd>
INST
CTYP INTL
ISPN NO
```

The DMI is used in the outgoing RLI. The RLI is accessed by provisioning the SPN in the ESN data, using the RLI configured for this use.

For more details about provisioning the destination refer to Appendix section of this document

End of Procedure

Procedure 19
Provisioning required for placing ESA 911 calls

1 Carry out all pre-provisioning, if it has not already been done.

Configure the Virtual Trunk route on the Call Server using the procedure given in *IP Peer Networking: Installation and Configuration* (553-3001-213). Either Element Manager or the system CLI is acceptable.

To ensure that VTRKs are available when needed for ESA calls, this route must be for outgoing calls only; that is, it must be reserved for ESA. This may be done via ICOG of OGT and putting the trunks in an ESA only route, or by TGAR. (ICOG prevents incoming calls from the Signaling Server; TGAR rejects calls from the Signaling Server.)

Configure ESA on the originating Call Server. This is used for all non-IP Phones.

Configure the Zone that is used for ESA on the Call Server. This is done in LD 117.

CHG ZESA <zone> <ESA Route #> <AC> <ESA Prefix> <ESA Locator>

Define the ESA parameters for the zone, where:

- Zone = Zone number for ESA calls. This is typically at least the size of the local gateway BWZ.
- ESA Route # = Virtual Trunk route to gateway. Reserved for ESA calls.
- AC = Access Code to add to dialed digits. If no AC is required, AC0 is to be entered in place of AC1 or AC2.
- ESA Prefix = mandatory digit string added to start of ESDN (ESA DN).

This looks like an ESN special number when sent to NRS, and is used to uniquely identify the gateway.

- ESA Locator = the full Direct Inward Dial telephone number to be sent as the CLID or ANI, for use by the PSAP to locate the source of the call.
  - If not present, the system uses the CLID and CLID entry to build the CLID or ANI; if unable to build this number, the ESA "default number" is used instead.

— If the locator number is present, all calls use this locator number. This allows the system to guarantee a return call to the same site.

— As a consequence, the ESA Locator must be a set physically within the same zone as the ESA caller.

Enable the ESA zone

ENL ZBR <Zone>

2 Carry out preliminary analysis, if it has not already been done.

Determine where this call will land. Does it land on one or more than one gateway? Are there different costs for each gateway?

Select the GGP for this gateway or set of gateways. This code must be unique across the whole network. Record this code for use in creating Digit Manipulation Indices.

Select the CDT for the "SPN" (the GGP and this digit form the ESA Prefix, and are treated by the NRS as an SPN).

3 Carry out Digit Manipulation Index (DMI) provisioning for this destination.

The digit manipulation is done using ZESA configuration, above. No more is needed.

For example for zone 7, using an ESA route 100, not using ESN access codes, adding the gateway group, prefix 44445, and having the DID locator as 967-5000 the configuration is as follows

chg ZESA 7 100 ac0 44445 9675000

For more details on provisioning ESA, please refer to the Appendix section.

4 Provision the RLI

Not required; part of provisioning the zone ESA.

5 Gatekeeper provisioning

For configuring this section, Element Manager is required. For more details refer to *IP Peer Networking: Installation and Configuration* (553-3001-213).

6 Provision the entries associated with that SPN prefix on the gatekeeper.

For E911 calls using steering code 44445 the numbering plan entries in the NRS would be as below:

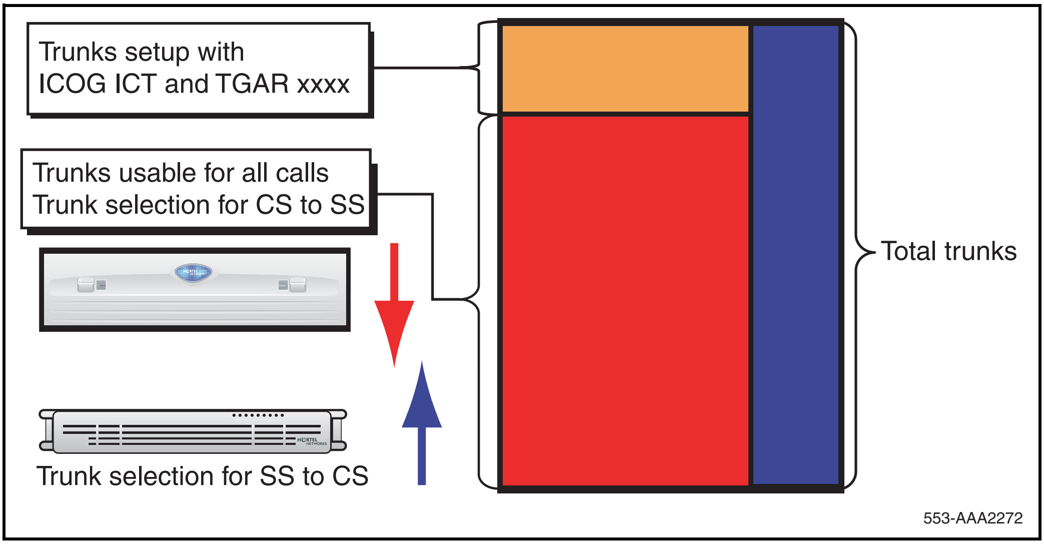
```
numbertype.Special.Private (SPN)

44445 on gateway1 cost factor 1

44445 on gateway2 cost factor 2
```

7 Destination gateway provisioning

ESA overrides all restrictions. So configure trunks with restrictions so that other features cannot use the same trunks.

The route which is associated with this ESA zone should have access to only incoming calls. This can be achieved by setting the ICOG of the ESA trunk route to ICT and the TGAR such that under normal circumstances no calls can complete. This would ensure that these Virtual Trunks are not used for outgoing calls. Note, though, that unless the TGAR is blocking normal incoming calls that other incoming calls may still end up using up all the trunks.

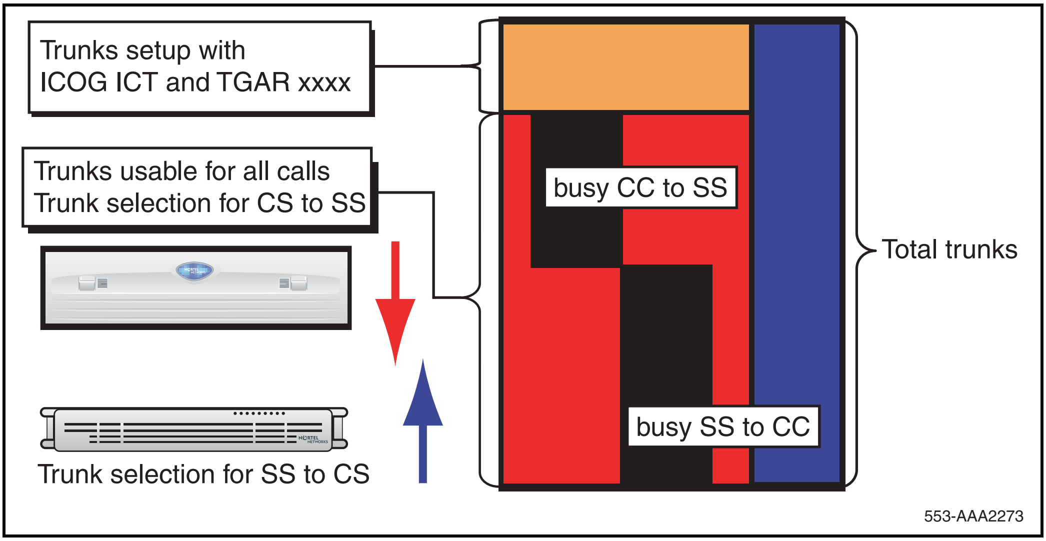
Figure 92
Trunk reservation



In this figure, the block of trunks at the top are a subset of the total belonging to one route (for example, route 911), and are incoming only, with TGAR xxxx. This blocks all normal calls. The lower block is the subset of trunks available for all calls.

Normal trunk selection selects from the ends and eventually meets in the middle. If at that time all trunks are in use, no more outgoing calls are possible, but so far the reserved telephones are not used.

Figure 93
Trunk reservation when all "any call" trunks are in use



At this time, only the telephones reserved for the ESA calls are free; these can only be used for Signaling Server to Call Server calls, but as they are the farthest from the start point for trunk selection, the Signaling Server selects them last.

Assume that a non-ESA call comes from the Signaling Server. Since it does not over-ride the TGAR, the Call Server rejects the call.

Assume that an ESA call comes from the Signaling Server. As it is ESA, it over-rides the TGAR and allows the call.

End of Procedure

Procedure 20
Configuring the gateway

1 Configure an emergency trunk (CAMA or PRI)

2 Configure Virtual Trunks

Before a call can come on the Virtual Trunks, the trunks must be configured. This should be ICOG ICT and use a TGAR value for all trunks that blocks any non-ESA calls.

3 Configure ESN

- Provision the “standard” ESN data blocks required as per *Emergency Services Access: Description and Administration* (553-3001-313).
- Provision a DMI:
  - — to delete all received digits and insert the new ESA DN, or
  - — to delete all GGP and CDTs, leaving only the ESA DN.
- Provision an RLI with local termination.
- Provision a Special Number (SPN) on the gateway. This SPN is for the ESA calls from the Call Server.

The SPN must use

- — The digit Manipulation Index provisioned above, which deletes all the incoming digits (possibly, except for the ESDN, but this is PRI ESA destination specific. All ESA trunks can delete the full string.). In the example since 44445911 is received, a DMI can be configured to delete 44445911.
- — A RLB which has LTER (Local Termination) turned on.

When an SPN is configured, ESA determines that the call is from a trunk and forwards the correct ANI data as it tandems the call.

4 Configure ESA

ESA configuration enables the Virtual Trunk ESA call from Call Server to be tandem over to CAMA or PRI trunk.

5 Configure the gateway zone

Use the same zone number between the Call Server and the gateway.

6 Configure ESA ESN

This configuration is for normal CAMA/PRI trunk ESA call.

When an ESA call is received, the gateway would recognizes the incoming digits and deletes all the digits except for the ESDN (SPN configuration from Step 3). Then the call is routed to the local termination. ESA recognizes the call as an emergency call and routes the call correctly.

For more details on the provisioning, please refer to the appendix section of this document.

End of Procedure

Procedure 21
Provisioning required for placing GDP (LOC) calls

1 Carry out preliminary analysis, if it has not already been done.

Determine where this call will land. What kind of trunks it is supposed to take? Does it land on one or more than one gateway? Are there different costs for each gateway?

2 Provision the RLI

Define the RLI to be used for the LOC for routing the call to the correct gateway. The RLI includes all ESN data as applicable.

```
REQ NEW
CUST <as applicable>
FEAT RLB
RLI <as applicable>
ENTR <as applicable>
.....
ROUT <as applicable>
.....
```

For most networks, routes for a specific call type to a single gateway group can be handled by having a single RLI.

3 Provision the LOC for reaching the remote node

Configure 501 as a LOC and associate the RLI created in the previous step. This configuration procedure is same as that of a CS 1000M or CS 1000S system.

4 Gatekeeper provisioning

Provision the entries associated with that LOC prefix on the gatekeeper.

In the example network, Level 1 entry is created on Node B.

5 Destination gateway provisioning

Not applicable. The site is remote.

But a normal configuration is to have a HLOC to terminate the calls on Node B.

For more details about provisioning the destination. Refer to Appendix section of this document

End of Procedure

Procedure 22
Provisioning required for placing UNP (CDP) calls to remote sites

1 Carry out preliminary analysis, if it has not already been done.

Determine which telephones need the functionality of being able to transfer across sites and plan the numbering plan accordingly.

2 Provision the RLI

Define the RLI for vacant number routing. This RLI is used to route the call for those numbers which are not available on the current node. The RLI includes all ESN data as applicable:

```
LD 86
REQ NEW
CUST <as applicable>
FEAT RLB
RLI <as applicable>
ENTR <as applicable>
.....
ROUT <as applicable>
.....
```

3 Provision the VNR

Configure VNR on the Call Server to route the calls to unavailable numbers to the Signaling Server. The Signaling Server in turn routes the call according to the numbering plan entry on the GK. The provisioning procedure is the same as in CS 1000M or CS 1000S systems.

4 NRS provisioning

Provision the CDP entries as Level 0 on the GK with the numbers which were moved out of one system and into another.

End of Procedure

Incoming calls

The next category of call is the incoming calls to CS 1000E. For incoming calls it is assumed that the CS 1000E and the MG 1000T are in the same CDP domain.

Procedure 23
Provisioning required to receive incoming DID calls

For CS 1000E, the MG 1000T would be interfacing between the PSTN and SIP/H.323. So for a typical scenario consider the following setup.

Scenario: A PSTN user dials a DID number (967-8971) on the CS 1000E

The can be addressed on CS 1000E using several options, of which the preferred two are shown:

- Option A

  For routing the calls to the CS 1000E CS, VNR can be used. VNR is configured on the MG 1000T which on receiving the DID call performs a VNR, and routes the call to CS 1000E.

- Option B

  In this option, Incoming DID Digit conversion is used to convert the digits to various extensions in the network. The conversion is accomplished using translation table dedicated to a DID route. The digit conversion table is set up to map the received DID digits into the local DN.

Mapping of incoming number can be done by one of the following ways

- Full Digit conversion

  All the digits received are converted to another string of digits as specified in the conversion table.

- Partial Digit conversion.

  Not all of the digits received from the Central Office (CO) are converted.

This operation of IDC is same as in prior releases of software, such as Succession 1000 release 3.0, Meridian 1 X11 release 25.40, and so forth.

> ***Note:*** There are provisioning concerns at the MG 1000T where the call enters the CS 1000E network. You must provision the TDM Trunk Gateway customer data block for the customer with the Virtual Trunk route at the node where the DID call enters the IP network as having "DITI" set to YES. "DITI" is used to enable or disable making a DID call tandem to a TIE trunk. DITI set to NO means that the call cannot even reach the CS 1000E node.

Procedure 24
Provisioning required for receiving GDP (LOC) calls

This procedure is different from that of Outgoing GDP calls as this is the terminating Node for the GDP call.

Here the only change to the configuration would be changing the LOC configured to HLOC. So when a call comes to the Node, the Home location code is stripped and the call is terminated on the CDP which remains after the home location code is stripped.

For example consider a network where a CS 1000E is deployed. Other nodes reach this node using a LOC of 501. In this case, the CS 1000E has a HLOC configured as 501, and the remaining digits can terminate locally on a telephone.

1 Carry out preliminary analysis, if it has not already been done.

Determine how CS 1000E is going to be connected to the network.

2 Provision the HLOC

Provision the HLOC on the Call Server or on the gateway depending on how the CS 1000E is connected to the network.

Consider that the CS 1000E is connected to the network via a gateway. In that case, the HLOC is configured on the gateway and the stripped digits is equal to a CDP number on the Call Server.

3 Provision the CDP

Configure CDP with the RLI to route the call to Call Server.

4 NRS provisioning

Provision the CDP entries as Level 0 on the GK with the number on the Call Server.

End of Procedure

Procedure 25
Provisioning required for receiving UNP (CDP) calls from remote sites

No special provisioning procedure required for this setup. The key to TNDN is to have a numbering plan which is flexible.

1 Carry out preliminary analysis, if it has not already been done.

If the change is a “move”, determine which telephone has moved to CS 1000E.

If this is a newly commissioned switch, determine which telephones belong on this CS 1000E.

2 Provision the RLI

Since this is done on the remote node, this is not covered in this section.

3 Provision the CDP

Since this is done on the remote node, this is not covered in this section.

4 NRS provisioning

Provision the moved number entries as Level 0 on the GK.

5 Call Server Provision

Since a new CDP number has moved to the Call Server, a LSC can be provisioned to delete the leading digits and terminate the call on the desired telephone. This is provisioned only when the CDP number includes a prefix intended for network routing purposes only.

End of Procedure

ESA calls

> **IMPORTANT!**
>
> Do not route ESA calls to a node that has no direct ESA trunks.

Ideally, route ESA calls directly over Central Office (CO) trunks to the Public Safety Answering Point (PSAP). In those cases where this is not possible, do not route ESA calls to nodes that have no direct ESA trunks.

The implications of routing calls to nodes without direct ESA trunks are as follows:

- At the node without the direct ESA trunks, the node cannot route the ESA call directly to the PSAP. Instead, that node must re-route the call to another node. This re-routing is an unnecessary use of resources.
- If the node is a CS 1000E node, the only tandem trunks are IP Peer trunks. There is no way to specify the appropriate rerouting digits (that is, Prepend Digits) to re-route the ESA call to another node with direct ESA trunks.

Therefore, if you are unable to route ESA calls directly to the PSAP, the next best practice is to route ESA calls to nodes with direct ESA trunks.

Procedure 26
Provisioning required for placing ESA 911 calls

This procedure assumes that all the zones and at least most of the units belonging to them have been defined.

1 If using a security center, provision the security center

ESA provisioning varies based on whether the security center is collocated with the CS 1000E on one of its MG 1000E systems, or is on another system (such as a CS 1000M or CS 1000S). In all cases, the system must be provisioned with the security desk customer, with trunks to receive calls from the CS 1000E, and with the capability of providing outgoing emergency calls to the PSAP.

If a jurisdiction or country does not support CAMA trunks, the security desk should be on the CS 1000M or CS 1000S Trunk Gateway.

- Security desk on the CS 1000E

  The security desk MG 1000E must be in a zone without any non-security units.

  If the security center is on an MG 1000E of the CS 1000E the trunks to receive the ESA call from the other MG 1000E systems are CAMA by preference; any other analog trunks loses the ANI. The CAMA trunks may “step” to Virtual Trunks to provide overflow capability.

  The outgoing ESA trunks is CAMA. Stepping to other trunk types is not recommended; ISDN trunks are not supported on the MG 1000E, and night call forward to ESA stepping to a Virtual Trunk fails.

  Provision the Zone ESA entry for this zone to use no prepend digits. Do not step from the CAMA trunks to the Virtual Trunks, as this permits stepping when not using ZESA.

  Provision the ESA data block to use the CAMA trunks. This is used by the ACD night call forward, as the queue does not have an associated zone. Do not step to Virtual Trunks, as it is impossible to get the prepend digits.

  The security desk customer must have ACD defined to route the calls to the ACD agents — in this case, the security desk unit(s). It must also have night call forward capability, allowing the calls to route directly to the PSAP when the center is vacant.

- Security desk on the CS 1000M or CS 1000S

  The security desk cannot be in a zone; only the CS 1000E has zones for this purpose.

  When the security desk is on a trunking gateway, do not step back to the Virtual Trunks. STEP works between CAMA and Virtual Trunks if using zone ESA, but zone ESA is not supported on the CS 1000M or CS 1000S.

  STEP works well between CAMA and all non-Virtual Trunks for basic ESA using overlay 24. STEP does not work properly between Virtual Trunks and non-CAMA in either direction; it is not possible to use the prepend digits for Virtual Trunks and omit them for all others, and only the ZESA provisioning allows prepend digits. Note that failure to get one of the permitted trunks triggers call clearing, which in turn triggers use of the next entry in the least cost routing table.

The security desk customer must have ACD defined to route the calls to the ACD agents — in this case, the security desk unit(s). It must also have night call forward capability, allowing the calls to route directly to the PSAP when the center is vacant.

When the On Site Notification units are defined, these are physically located at the security center and accessible to the operators at the ACD agents. The OSN units for calls from the security center to the PSAP are also collocated with the security center ACD agents.

For details, refer to *Emergency Services Access: Description and Administration* (553-3001-313).

2 Carry out all pre-provisioning, if it has not already been done.

Configure the Virtual Trunk route on the Call Server "reserved for ESA use" using the procedure given in the *IP Peer Networking: Installation and Configuration* (553-3001-213). Note that the route typically does not require a large number of channels, as the calls can use channels not reserved for ESA, too. Either Element Manager or the system CLI is acceptable.

To ensure that CAMA or Virtual Trunks are available when needed for ESA calls, this route must be for outgoing calls only, and it must be reserved for ESA. This may be done by using the response to the route ICOG prompt of OGT ("Out Going Trunk) and using the trunks in an ESA only route. (An ICOG value of OGT prevents incoming calls from the Signaling Server.)

Nortel recommends that CDR — if used for this route — not use "OPD", or "Outpulsed Digits" in the CDR record if the digit string — including prefix — exceeds 12 digits. It must not be used if the number of digits exceeds the limits of the downstream processor accepting CDR data.

Configure ESA on the originating Call Server. Configure ESA on all MG 1000E systems and TDM trunking gateways that is able to continue to provide local ESA service if the Call Server fails. Refer to *Emergency Services Access: Description and Administration* (553-3001-313) for details.

3 Carry out all pre-provisioning on the security desk (if needed), if it has not already been done.

Configure the Virtual Trunk route on the Call Server “reserved for ESA use” using the procedure given in the *IP Peer Networking: Installation and Configuration* (553-3001-213). Note that the route typically does not require a large number of channels, as the calls can use channels not reserved for ESA, too. Either Element Manager or the system CLI is acceptable.

To ensure that CAMA or Virtual Trunks are available when needed for ESA calls, this route must be for incoming calls only; however, it cannot be otherwise reserved for ESA. This may be done via ICOG of ICT and putting the trunks in an ESA only route. It is also necessary to ensure that enough Virtual Trunks are available to allow calls to every non-Virtual Trunk, plus the maximum number of security desk agents, plus a safety factor to cover cases of calls that are trying to use external trunks that are already in use. These calls fail, but in the interim they still consume Virtual Trunk resources.

Nortel recommends that CDR — if used for this route — not use “OPD”, or “Outpulsed Digits” in the CDR record if the digit string — including prefix — exceeds 12 digits. It must not be used if the number of digits exceeds the limits of the downstream processor accepting CDR data.

Configure ESA on the security desk Call Server. Configure ESA on all MG 1000E systems and TDM trunking gateways that is able to continue to provide local ESA service if the Call Server fails. Refer to *Emergency Services Access: Description and Administration* (553-3001-313) for details.

4 Carry out preliminary analysis, if it has not already been done.

Determine where this call will land. Does it land on one or more than one gateway? Are there different costs for each gateway? Is there a local security center, and therefore two different choices — the general destination terminating on the security desk CAMA and Virtual Trunk route, and the destination reached from the security center?

Select the GGP for this gateway or set of gateways. This code must be unique across the whole network. Record this code (or, with a security center on the CS 1000E, these codes) for use in creating ZESA prefixes.

Select the CDT for the “SPN” (the GGP and this digit form the ESA Prefix, and are treated by the NRS as an SPN).

5 Provision CLID entries and assign them to terminals, routes, ...

The CLID entry is a part of the customer data block provisioning. Each entry includes several values, of which the crucial ones are:

- ESA_HLCL — the digit string or prefix used to allow the PSAP operator to call back in event of disconnection.
- ESA_APDN — a “yes/no” prompt controlling whether the DN associated with this entry is to be added to the end of the ESA_HLCL digits. If “yes”, the ESA_HLCL plus the DN must be DID dialable, and must terminate on this telephone.
- DIDN — a “yes/no” prompt indicating whether this is a DID DN.

Also important under certain circumstances are the “national number” prefix. (In North America, this is the area code.) In certain jurisdictions, the ANI must start with the national number prefix, so this must be provisioned and enabled:

- HNTN — the home national number prefix.
- ESA_INHN — a “yes/no” prompt indicating whether to insert the HNTN (yes) or to not insert it (no).

Assign these to telephones and IP Lines, as per the general administration overlay NTPs.

6 Provision zone data on the Call Server

The “Primary Zone” (or zones) on the CS 1000E is the zone (or zones) where the default handling is to use the CLID entry block for DID capable numbers. By definition, this means that the locator code cannot be used, as it over-rides all other ANI data.

If the security desk is on the CS 1000E, the first choice route is the CAMA link between the MG 1000E of the security desk and an MG 1000E of the main CS 1000E CDB. As a fail-safe (in case all of these are in use), the Virtual Trunk route may be used as a STEP route (always step from CAMA to Virtual Trunk and never in the opposite direction). This requires prepend digits, and requires an additional Signaling Server that is not needed otherwise.

Configure the zone data for the Primary Zone that is used for ESA on the Call Server. This is done in LD 117.

CHG ZESA <zone> <ESA Route #> <AC> <ESA Prefix> *<ESA Locator>*

Define the ESA parameters for the zone, where:

- Zone = Zone number for ESA calls. This is typically at least the size of the local gateway BWZ.
- ESA Route # = Virtual Trunk route to gateway. Reserved for ESA calls.
- AC = Access Code to add to dialed digits. If no AC is required, AC0 is to be entered in place of AC1 or AC2.
- ESA Prefix = mandatory digit string added to start of ESDN (ESA DN).

  This looks like an ESN special number when sent to NRS, and is used to uniquely identify the gateway.
- ESA Locator: Not usually used for this zone; always used for other zones. Mandatory if using the Emergency Call Services Management System (ECSMS) for mobility. This provides the full Direct Inward Dial telephone number to be sent as the CLID or ANI, for use by the PSAP to locate the source of the call. Omitting it allows the Call Server to build the CLID pr ANI using the DID numbers of

any DID units, or using the “floor security desk” or other local call-back sites closer to the caller than the main site.

For example, if zone 5 is the primary zone, then for zone 5, using an ESA route 100, not using ESN access codes, adding the GGP 44447, and not having a locator the configuration is as follows:

`chg ZESA 5 100 ac0 44447`

Configure the zone data for all other zones that is used for ESA on the Call Server. This is done in LD 117.

`CHG ZESA <zone> <ESA Route #> <AC> <ESA Prefix> <ESA Locator>`

Define the ESA parameters for the zone, where:

- Zone = Zone number for ESA calls. This is typically at least the size of the local gateway BWZ.
- ESA Route # = Virtual Trunk route to gateway. Reserved for ESA calls.
- AC = Access Code to add to dialed digits. If no AC is required, AC0 is to be entered in place of AC1 or AC2.
- ESA Prefix = mandatory digit string added to start of ESDN (ESA DN).

  This looks like an ESN special number when sent to NRS, and is used to uniquely identify the gateway.
- ESA Locator = the full Direct Inward Dial telephone number to be sent as the CLID or ANI, for use by the PSAP to locate the source of the call.
  - If not present, the system uses the CLID and CLID entry to build the CLID or ANI; if unable to build this number, the ESA “default number” is used instead.
  - If the locator number is present, all calls use this locator number. This allows the system to guarantee a return call to the same site.

— As a consequence, the ESA Locator must be a set physically within the same zone as the ESA caller.

For example, for non-primary zone 7, using an ESA route 100, not using ESN access codes, adding the GGP 44447, and having the DID locator as 967-5000 the configuration is as follows

chg ZESA 7 100 ac0 44447 9675000

Enable the ESA zones; repeat the following command for all zones.

ENL ZBR <Zone>

7 If the security center is on an MG 1000E of the CS 1000E, provision zone data on the Call Server

Execute this step only if there is a security center on the CS 1000E.

Ensure that the security desk is on a dedicated MG 1000E as a separate customer. It cannot share an MG 1000E with a second CDB, and it cannot share its CDB with the other MG 1000E systems. Use a zone dedicated to the security desk MG 1000E.

Ensure that the “back to back” CAMA trunks are provisioned. Ensure that the CAMA trunks to the PSAP are provisioned for the ESA route.

Ensure that the ESA data uses the ESA CAMA route to the PSAP as the route number. Ensure that this route does not step to Virtual Trunks.

Configure the zone data for the security center zone that is used for ESA on the Call Server. This is done in LD 117.

CHG ZESA <zone> <ESA Route #> <AC> <ESA Prefix> *<ESA Locator>*

Define the ESA parameters for the zone, where:

- Zone = Zone number for ESA calls. This is typically at least the size of the local gateway BWZ.
- ESA Route # = Virtual Trunk route to gateway. Reserved for ESA calls.
- AC = Access Code to add to dialed digits. If no AC is required, AC0 is to be entered in place of AC1 or AC2.
- ESA Prefix = mandatory digit string added to start of ESDN (ESA DN).
- This looks like an ESN special number when sent to NRS, and is used to uniquely identify the gateway.
- ESA Locator: **DO NOT USE.**

For example, if zone 2 is the security center zone, then for zone 2, using an ESA route 100, not using ESN access codes, adding the GGP 44446, and not having a locator the configuration is as follows:

chg ZESA 2 100 ac0 44446

For more details on provisioning ESA, please refer to *Emergency Services Access: Description and Administration* (553-3001-313).

8 Gatekeeper provisioning

For configuring this section, Element Manager is required. For more details refer to the *IP Peer Networking: Installation and Configuration* (553-3001-213).

Provision the entries associated with that SPN prefix on the gatekeeper.

When there is no security center, for ESA calls using steering code 44447 the numbering plan entries in the NRS would be as below:

```
numbertype.Special.Private (SPN)

44447 on gateway1 cost factor 1

44447 on gateway2 cost factor 2
```

For ESA calls from the security center, using steering code 44446, the numbering plan entries in the NRS would be as below:

```
numbertype.Special.Private (SPN)

44447 on securityCenter cost factor 1

44447 on anyOthergatewayToPsap cost factor 2
```

This applies whether the security center is on the CS 1000E or on a Trunk Gateway. However, if it is on the CS 1000E, an additional Signaling Server is needed for this customer.

For ESA calls from the security center, none reach the IP network, since there are problems mixing “prepend” routes with “can’t prepend” routes. Therefore, no NRS provisioning is needed.

9 Destination gateway provisioning

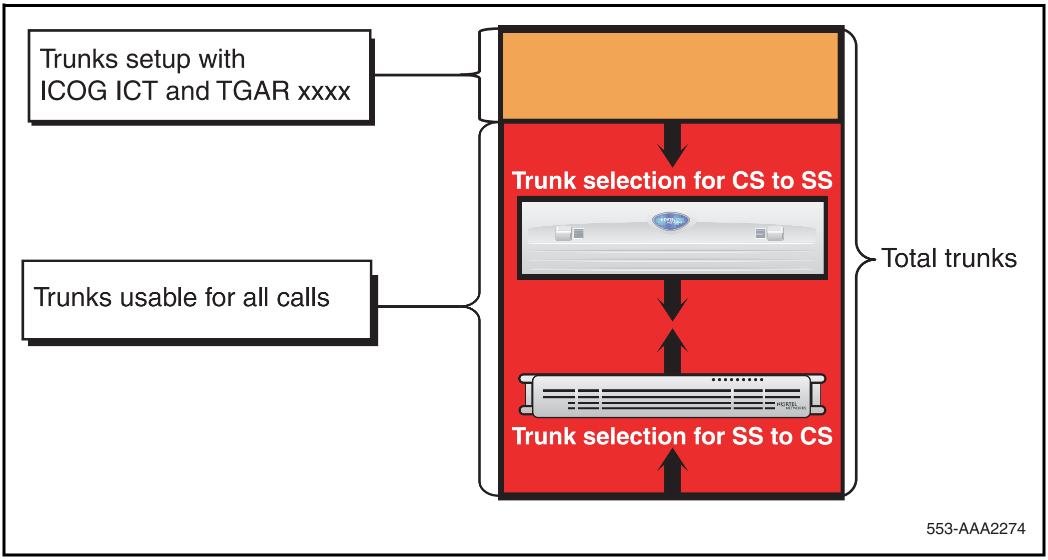
ESA overrides all restrictions. To ensure that trunks are always available for ESA, configure trunks with direction restrictions (incoming only) so that other calls cannot use the same trunks. Also, over provision the system to ensure that trunks is available on the IP side of the gateway.

The route which is associated with this ESA zone should have access to only incoming calls. This can be achieved by setting the ICOG of the ESA trunk route to ICT. This would ensure that these Virtual Trunks are not used for outgoing calls. Note that other incoming calls may still end up using up all the trunks.

Furthermore, note that ESA can also use “regular” trunks, so reserving a small number on the system for the ESA specific route and using the rest generically will suffice.

Refer to the following illustration. In it are shown the trunks as visible from the Call Server (to the Signaling Server, they are one solid block).

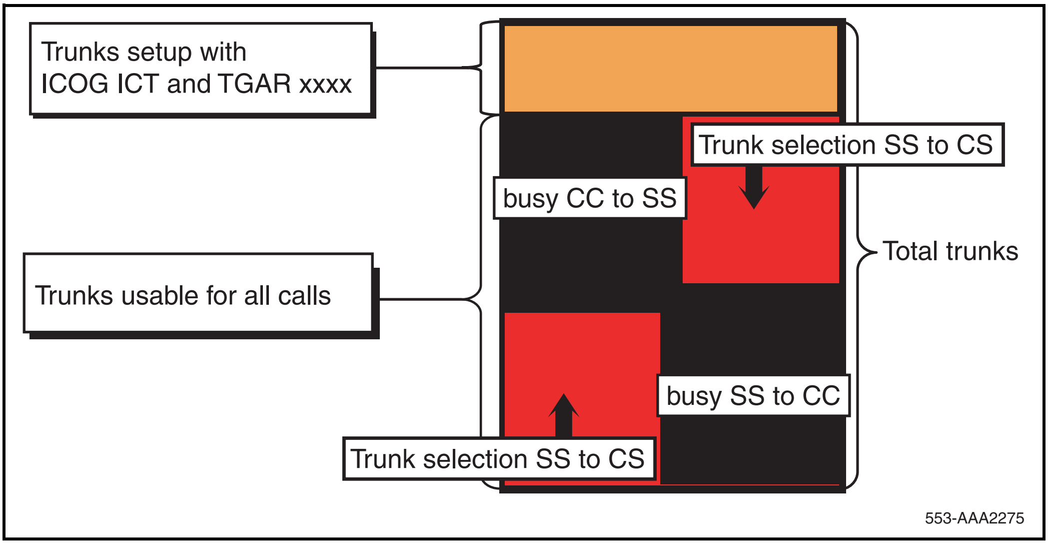
Figure 94
Trunk reservation



In this figure, the block of trunks at the top are a subset of the total available. These trunks belong to one route (for example, route 123), and are incoming only, with TGAR xxxx. This blocks all normal calls. The lower block is the subset of trunks available for all calls, available as an independent route on the Call Server.

Normal trunk selection selects from the ends and eventually meets in the middle. If at that time all trunks are in use, no more outgoing calls are possible, but so far the reserved set are not used.

Figure 95
Trunk reservation when all “any call” trunks are in use



At this time, only the set reserved for the ESA calls are free; these can only be used for Signaling Server to Call Server calls, but as they are the farthest from the start point for trunk selection, the Signaling Server selects them last.

End of Procedure

Procedure 27
Configuring the gateway

1 Configure an emergency trunk (preferably CAMA or PRI, but others supported by the ESA feature may be used) as per *Emergency Services Access: Description and Administration* (553-3001-313).

2 Configure Virtual Trunks

Before a call can come on the Virtual Trunks, the trunks must be configured. A subset of the total virtual calls should be reserved in an RDB with ICOG ICT.

Make sure that the total number of trunks on the IP side is higher than the total count of TDM trunks. This ensures that temporarily seized Virtual Trunks that are going to clear as “no resources” do not block ESA calls that can still complete.

3 Configure ESN

- Provision the “standard” ESN data blocks required as per *Electronic Switched Network: Signaling and Transmission Guidelines* (553-3001-180).
- Provision a DMI:
  - — to delete all digits that have been received and insert the new ESA DN, or
  - — to delete all GGP and CDTs, leaving only the ESA DN.
- Provision an RLI with local termination, using the DMI provisioned in the previous substep.
- Provision a Special Number (SPN) on the gateway. This SPN is for the ESA calls from the Call Server.

The SPN must use:

- The RLB defined above which has LTER (Local Termination) turned on and the selected DMI.
- Note that the Digit Manipulation Index provisioned above may delete all the incoming digits and insert the local ESDN. Otherwise, it may delete all except for the received ESDN. If 44445911 is received, a DMI can be configured to delete 44445911 and insert a different ESA DN, or it can delete the 44445.

  When an SPN is configured, ESA determines that the call is from a trunk and forwards the correct ANI data as it tandems the call.

4 Configure ESA

ESA configuration enables the Virtual Trunk ESA call from Call Server to be tandem over to CAMA or PRI trunk.

5 5. Configure the security desk if not already done

This requires:

- Local termination of the SPN to an ACD queue.
- ACD agents or a night call forward to a MADN for non-ACD units.
- ESA to allow the security agents to send an ESA request to the PSAP.

For more details on the provisioning, please refer to the appendix section of this document.

End of Procedure

Overlay configuration tutorial

Configuring Emergency Service Access

Table 100
LD 24

Prompt	Response	Description
REQ	NEW CHG	New or Change
TYPE	ESA	Emergency Services Access data block
CUST	xx	Customer number, as defined in LD 15
ESDN	xxxx	Emergency Services DN (for example, 911). Up to four digits are accepted.
ESRT	0-511	ESA route number
DDGT	x...x	Directing Digits. Up to four digits are accepted. This prompt only applies to CAMA trunks.
DFCL	x...x	Default ESA Calling Number. This only is used if the system has configuration errors. It provides a “last chance” to generate a valid CLID or ANI. The input must be the following lengths: On a system that is not FNP equipped, 8 or 11 digits are accepted if the first digit of the input is 1; otherwise the input must be 7 or 10 digits. On a system that is FNP equipped, up to 16 digits are allowed.
OSDN	x...x	On-Site Notification station DN (optional). The input must be a valid single appearance internal DN.

Refer also to *Emergency Services Access: Description and Administration* (553-3001-313).

Configuring the ESA Zone

There are no "traditional" data entry prompt sequences for zone ESA such as is used for LD 24. Instead, a single command is used to provision a zone for ESA.

Configure the zone data in LD 117.

CHG ZESA <zone> <ESA Route #> <AC> <ESA Prefix> <ESA Locator>

Table 101
ZESA data entry in LD 117

Prompt	Response	Comments
Zone	x...x	Zone number for ESA calls. This is typically at least the size of the local gateway BWZ.
ESA Route #	0-max route number	Virtual Trunk route to gateway, reserved for ESA calls.
AC	AC0, AC1, AC2	Access Code to add to dialed digits. If no AC is required, AC0 is to be entered in place of AC1 or AC2.

Table 101
ZESA data entry in LD 117

Prompt	Response	Comments
ESA Prefix	xxxxx...x	This looks like an ESN special number when sent to NRS, and is used to uniquely identify the gateway. mandatory digit string added to start of ESDN (ESA DN).
ESA Locator	xxxxx...x	This provides the full Direct Inward Dial telephone number to be sent as the CLID or ANI, for use by the PSAP to locate the source of the call. Omitting it allows the Call Server to build the CLID or ANI using the DID numbers of any DID units, or using the “floor security desk” or other local call-back sites closer to the caller than the main site. The following conditions apply: If not present, the system uses the CLID and CLID entry to build the CLID or ANI; if unable to build this number, the ESA “default number” is used instead. If the locator number is present, all calls use this locator number. This allows the system to guarantee a return call to the same site. As a consequence, the ESA Locator must be a set physically within the same zone as the ESA caller.

Enable the ESA zones; repeat the following command for all zones:

ENL ZBR <Zone>

Configuring Digit Manipulation Index

Table 102
LD 86

Prompt	Response	Description
REQ	NEW	Create new data block
CUST	xx	Customer number, as defined in LD 15
FEAT	DGT	Digit manipulation data block
DMI		Digit Manipulation Index numbers
	(0)	No digit manipulation required
	(0)-31	CDP
	(0)-255	NARS and BARS
	(0)-999	NARS and BARS with FNP
		DMI is only prompted when the Directory Number Expansion (DNXP) package 150 is equipped and SDRR = LDID. The maximum number of Digit Manipulation tables is defined by prompt MXDM.
DEL	(0)-19	Number of leading digits to be deleted
ISPN	YES/NO	Generates CLID on the original called type.
INST	x...x	Insert. Up to 31 leading digits can be inserted.
CTYP		Call Type to be used by the manipulated digits. This call type must be recognized by the far-end switch.

Configuring Route List Index

Table 103
LD 86

Prompt	Response	Description
REQ	NEW	Create new data block
CUST	xx	Customer number, as defined in LD 15
FEAT	RLB	Route List data block
RLI		Route List Index to be accessed
	0-127	CDP and BARS
	0-255	NARS
	0-999	FNP
ENTR	0-63	Entry number for NARS/BARS Route List
	0-6	Route List entry number for CDP
	X	Precede with X to remove
LTER	YES/NO	Local Termination entry
ROUT	0-511	Route number
DMI	(0)-999	Digit Manipulation Index number

Configuring SPN

Table 104
LD 90 (Part 1 of 3)

Prompt	Response	Description
REQ	NEW	Create new data block
CUST	xx	Customer number, as defined in LD 15

Table 104
LD 90 (Part 2 of 3)

Prompt	Response	Description
FEAT	NET	Network translation tables
TRAN		Translator
	AC1	Access Code 1 (NARS/BARS)
	AC2	Access Code 2 (NARS)
SPN	x...x	Special Number translation Enter the SPN digits in groups of 3 or 4 digits, separated by a space (for example, xxxx xxx xxxx). The SPN can be up to 19 digits long. The maximum number of groups allowed is 5.
- FLEN	(0)-24	Flexible Length The number of digits the system expects to receive before accessing a trunk and outpulsing these digits.
...		
- RLI		Route List Index to be accessed
	0-127	CDP and BARS
	0-255	NARS
	0-999	FNP
...		

Table 104
LD 90 (Part 3 of 3)

Prompt	Response	Description
- SDRR		Supplemental Digit Restriction or Recognition
	ALOW	Allowed codes
	ARRN	Alternate Routing Remote Number
	DDD	Recognized remote Direct Distance Dial codes
	DENY	Restricted codes
	DID	Recognized remote Direct Inward Dial codes
	ITED	Incoming Trunk group Exclusion Digits
	LDDD	Recognized Local Direct Distance Dial codes
	LDID	Recognized Local Direct Inward Dial codes
	STRK	For ADM/MDM trunk groups
	<cr>	Return to SPN
- - DMI	1-255	Digit Manipulation Index
	1-999	Digit Manipulation Index with FNP
		DMI is only prompted when the Directory Number Expansion (DNXP) package 150 is equipped and SDRR = LDID.

Configuring the CLID (Calling Line ID)

Background

Reverse IDC (“SDID”, or Send DID number”) is for further discussion.

CLID tables (or entries) are configured as part of NET_DATA configuration for a customer data block (LD 15). It consists of several data blocks or fields:

- ENTRY -> CLID entry #

  Edit the data for this specific CLID data block.

- INTL -> Country Code

  This data can be added to the CLID if the call type is international.

- HNTN -> National code for home national number

  This data can be added to the CLID if the call type is national.

- ESA_HLCL -> Home Local Number for ESA calls

  This data can be added to the CLID if the call type is a local call, but is only used for an emergency call. (For North America, is usually the prefix of the number — the NXX plus any other digits to convert the number to a 7 digit format.)

  See *Emergency Services Access: Description and Administration* (553-3001-313) for details and examples.

- ESA_INHN -> Insert HNTN — Yes/No

  Is the system to insert the Home National Number in front of the Home Local Number for Emergency ESA calls?

  See *Emergency Services Access: Description and Administration* (553-3001-313) for details and examples.

- ESA_APDN -> Append the DID DN — Yes/No

  Is the system to append the originating DID capable Directory Number (if there is one) after the Home Local Number for ESA calls?

  See *Emergency Services Access: Description and Administration* (553-3001-313) for details and examples.

- HLCL -> Local exchange code

  This data can be added to the CLID if the call type is a local call, added to the CLID as part of any public number.

- DIDN -> Indicates if the numbers are DID or not.

  — YES: Precede the DN of the active DN key with the digits in HLCL

  — NO: Use digits in HLCL only

- SRCH: Find a DN key of the set starting from key 0, which has DIDN of a CLID entry set to YES

- HLOC -> the prefix that is used for UDP calls

  This is the Home Location Code (ESN) as defined in LD 90. Its length can be up to 7 digits with extended code. It is prompted when ISDN=YES, or with Digital Private Network Signaling System 1 (DPNSS) package 123.

- LSC -> the prefix that is used for CDP calls

  The Local Steering Code (LSC) can be one to seven digits. LSCs are required if the CDP DNs are longer than the local Prime DNs. The CLID sent for a CDP call is composed of the LSC defined in LD 15 plus the PDN of the calling telephone.

- CLASS_FMT -> format used for a Custom Local Area Signaling Service (CLASS) set. Options:

  - (DN) Send internal Directory Number to a CLASS telephone as the calling number.
  - LCL Send Local Number to a CLASS telephone as the calling number.
  - NTN Send National Number to a CLASS telephone as the calling number.

  A CLASS telephone is, by definition, any non-proprietary analog telephone with an integrated display and a Frequency Shift Key (FSK) modem receiver, or with a FSK modem receiver built-in display attachment. The CLASS telephones are configured on the Meridian 1 as analog (500/2500 type) telephones using LD 10, and are supported by the existing 500/2500 type peripheral line cards.

By default, there is always a CLID entry 0 with default values.

Associating telephones with a CLID entry number

Telephones can be associated with a CLID entry number on a per DN key basis. If a multiple line telephone has many different DNs, it could have different CLID entry numbers assigned for each DN key.

OVL 11 KEY prompt:

`KEY xx aaa yyyy (cccc or D) zz...z`

Where:

- xx = key number
- aaa = key name or function
- yyyy = additional information required for the key
- zz...z = additional information required for the key aaa.
- cccc or D == deals specifically with the CLID feature, where:
  - — cccc = CLID table entry of (0)-N, where N = the value entered at the SIZE prompt in LD 15 minus 1.
  - — D = the character “D”. When the character “D” is entered, the system searches the DN keys from key 0 and up, to find the first DN key with a defined “non-D” CLID table entry. The CLID associated with the found DN key is then used.

Note 1: If an invalid CLID entry # is entered during a DN key assignment, SCH6710 warning message is presented. With an invalid CLID entry # associated with a DN key, dialing from that key results CLID be the internal DN only.

Note 2: Do not configure a multiple appearance DN with a CLID entry other than D if that TN is not the MARP (Multiple Appearance Redirection Prime) DN. Only that set should have a value entered here. Alternatively, use the CLID entry to build a full DID capable number (the “zone ANI” analogous to the ESA Locator number from the zone provisioning, an LDN, or some other dialable number).

Details and LD data

The CLID is based on the call type. Given a specific call type, the data for the CLID (the called party number) is built.

The key elements of a called party number are the prefixes and the telephone DN. The prefixes are:

- INTL — Country Code

- HNTN — Home National Code
- HLCL — Home Local Code
- HLOC — ESN Home Location Code
- LSC — ESN Local Steering Code

In addition, not all numbers have meaning in other networks. If a number is DID capable, it can be thought of as a DID DN, leading to:

- DIDN — When constructing a national or local number, use the DN as DID.

The mechanism of constructing a CLID for different call types is as follows:

- If a DN is not a DID number, the DN is not included in the CLID.
- International number = INTL + HNTN + HLCL + DN
- National number = HNTN + HLCL + DN
- Local (subscriber) number = HLCL + DN; if DIDN = NO, then only the digits in HLCL are used to form a local number.
- ESN UDP number = HLOC + DN
- ESN CDP number = LSC + DN
- For ESA:
  - — If the telephone is IP, use the ESA Locator code. Otherwise, zone ESA does not apply.

— Else, cycle through the keys to find a DN which has a non-"D" CLID entry. If a CLID entry other than "D" exists for a DN on a phone, use that DN and CLID entry.

— Else, use the DFCL from LD 24.

Table 105
LD 15

Prompt	Response	Description
REQ	NEW/CHG	
TYPE	CDB	Customer Data Block
.....	......	......
NET_DATA	YES/NO	Net gateway
.....	......	......
ISDN	YES/NO	Change ISDN options
PNI	1-32700	Private Network Identifier
CLID	YES, (NO)	CLID option
SIZE	0-4000 (256)	CLID entry size. If <CR> is entered when REQ=NEW, it defaults to 256.
INTL	0-9999 X	Country code, 1 to 4 digits. Delete digits.
ENTRY	aa, Xaa, Xaa Xbb	CLID entry to be configured. CLID entry to be deleted. CLID entries (aa-bb) to be deleted. CLID entries must be between 0 and (SIZE-1). This prompt is repeated until <CR> is entered as response.

Table 105
LD 15

Prompt	Response	Description
HNTN	0-999999	National code for home national number, 1 to 6 digits.
	X	Delete digits.
HLCL	0-99......99	Local code for home local number or Listed directory number, 1 to 12 digits.
	X	Delete digits.
DIDN	(YES)	Precede the DN of the active DN key with the digits in HLCL.
	NO	Use digits in HLCL.
	SRCH	Find a DN key of the set from key 0 which has DIDN of a CLID entry set to YES.
HLOC	0-9999999	Home location code (ESN), 1 to 7 digits
	X	Delete digits.
LSC	0-9999999	Local steering code, 1 to 7 digits
	X	Delete digits.
PINX_DN	xx...xx	Node DN, up to 7 digits with DN expansion
		X to remove
.....	....	

GGP tables

The GGP may be planned by using a table such as the following.

Procedure 28
Planning a GGP

1 Identify the destination gateways that is allowed to break out to the PSTN. No other gateways should be used for PSTN break-out. Table 106 on page 604 may be useful, but is not mandatory.

2 Match the gateway to the PSTN numbers using one of the following three procedures:

- **a.** Cycle through all PSTN numbers to identify numbers allowed to terminate at this gateway, recording the numbers as “belonging to this gateway”, or
- **b.** Cycle through the gateways, identifying the specific numbers that is allowed to terminate here.
- **c.** Assign cost factors to each gateway for each PSTN number. This allows setting a precedence for a destination, such that “Media Gateway 1" is normally used, and “Media Gateway 2" used if Media Gateway 1 has no remaining resources.

This creates the “gateway groups”. Table 107 on page 604 may be useful, but is not mandatory.

3 Select a GGP for this gateway group.

4 Decide on the digits indicating which call type is being carried within this call. Table 108 on page 605 may be useful, but is not mandatory.

Table 106
Gateways permitting PSTN break-out

Destination gateway (optional IP address)	Destination Location for PSTN Break-out
Sample_site_name	Country:City Country:City ...

Table 107
GGP determination

Destination	Destination gateway and IP address	PSTN numbers using this gateway	Cost
Group steering code:			
Country:City	Sample_site 11.22.33.44	INTL CC-City1 INTL CC-City2 ...	128 256 ...
Country:City	Sample_site 11.22.33.45	INTL CC-City1 INTL CC-City2 ...	128 64 ...

Table 108
CDT identifiers

Numbering plan	Type of number	Selected code
Public E.164	International	
Public E.164	National (NPA)	
Public E.164	Subscriber/Local (NXX)	
Private	Location Codes (LOC)	
Private	Special numbers (SPN)	
Private	Coordinated dialing plan (CDP)	
Unknown		

End of Procedure

Remote gateways

Gateways supported

The CS 1000E typically has a collocated MG 1000T to the PSTN, for local calls. This gateway (or, if redundant gateways are provided for robustness, these gateways) may also be used by remote CS 1000E systems (or others) for calls breaking out to the PSTN, that use the private IP network to reach this location. This is a CS 1000E gateway by definition.

In addition, the CS 1000E can use remote gateways to provide access to remote PSTNs. The user may use the provisioning scheme within this document to provide a flexible least cost routing mechanism, allowing the user to select the remote gateways as first (and possibly second) choice, but after any tries to get remote resources fail, falling back to local PSTN resources.

These gateways do not need to be on a CS 1000E system. In fact, they do not need to be on a CS 1000 system at all; however, the feature set supported with CS 1000E to and from compatible Nortel systems (such as CS 1000M or

CS 1000S, CS 1000E, BCM, or Meridian 1 over H.323 IP Trunks) is much larger than the feature set available with calls to and from third party gateways.

Nortel gateways as Remote gateways

The CS 1000E can use both enterprise and carrier gateways, based on interoperability and interworking compliance testing. This can be broken into three main groups — CS 1000 and Meridian 1 gateways, other enterprise gateways, and carrier gateways.

- "CS 1000 and Meridian 1"

  For all practical purposes, there are no real limitations on the capabilities of these gateways, with the exception of ones based on features present in "release A" that do not exist in "release B". As an example, H.323 Overlap Signaling is supported on all CS 1000 Release 4.5 systems, but is not supported on prior releases, or on IP Trunk. These feature compatibility constraints are common across the full CS 1000 line, though, and because of that are not discussed here.

The CS 1000 and Meridian 1 gateways can be:

- CS 1000E

  A remote CS 1000E gateway behaves the same as a local one, provided that they are provisioned the same at the NRS (the route selector at the heart of the CS 1000 H.323 gatekeeper or CS 1000 SIP redirect server).

- CS 1000M or CS 1000S

  This system appears an originating CS 1000E system to be the same as a local MG 1000T to the originating CS 1000E. However, it usually is not set up to provide the MG 1000T handling as per this document, as calls from non-CS 1000E systems will not use the GGPs.

  Therefore, the following two options apply:

- Provision the CS 1000M or CS 1000S to accept the call with the GGP and handle it as per the CS 1000E trunking gateways.
- Provision the CS 1000E as though it was a CS 1000M or CS 1000S for these calls.

  Either approach is acceptable. The first allows the CS 1000E to maintain its flexible originator specific gateway selection approach but is more complex to provision; the second loses this capability, but is simpler to provision. The user must decide on which approach suits their needs best.

- Meridian 1 with IP Trunk release 3.0 or higher

  Meridian 1 and IP Trunk supports H.323 protocol only. Therefore, SIP calls cannot terminate on this destination. However, as a migration approach, existing systems upgraded to IP Trunk 3.0 or IP Trunk 3.01 can interoperate with the CS 1000E, provided the CS 1000E has been configured to support H.323.

  Note that the CS 1000E Signaling Server can do either SIP or H.323 alone, or combine the two on the same Signaling Server. If the network is to use Meridian 1 and IP Trunk, the calls for IP Trunk destinations must use the H.323 route on the CS 1000E only.

- Other Enterprise gateways

  Other Nortel Enterprise gateways, such as BCM (at releases compatible with CS 1000 in general), are also compatible. The CS 1000E list is subject to additions based on interoperability tests, but is expected to be exactly the same as with CS 1000M or CS 1000S interoperability.

  Note that some capabilities may remain “subject to provisioning capabilities”. If, for example, the gateway does not do the necessary digit manipulation to carry out the deletion of the SPN “header” in the called party number, then the calls should be placed as per CS 1000M or CS 1000S. On the other hand, if the gateway can support a “DMI equivalent” and delete the GGP, then the CS 1000E may place calls to that gateway identically to calls to a CS 1000E gateway.

Note: Gateway compatibility is considered as "unconfirmed" until interoperability testing has been done. The standards have several areas where interpretation can cause issues, and these must be checked on a case by case basis.

- Other Nortel gateways

  Other Nortel gateways (such as carrier network gateways) are also compatible, subject to confirmation in testing with the CS 1000 as a whole. The CS 1000 list receives additions based on interoperability tests, and it is possible (although improbable) that a gateway that can interwork with CS 1000M or CS 1000S may not work with CS 1000E. However, it is expected that the CS 1000E interoperability behavior is exactly the same with regard to carrier networks gateways as with CS 1000M or CS 1000S to carrier interoperability.

  Again, some capabilities may remain "subject to provisioning capabilities". If, for example, the gateway (or, because they do a "tandem signaling" message handling, for most carrier networks the carrier gatekeeper or redirect server) does not do the necessary digit manipulation to carry out the deletion of the SPN "header" in the called party number, then the calls should be placed as per CS 1000M or CS 1000S. On the other hand, if the gateway (or carrier gatekeeper or redirect server) can support a "DMI equivalent" and delete the GGP, then the CS 1000E may place calls to that gateway identically to calls to a CS 1000E gateway.

Non-Nortel gateways

Gateways other than Nortel probably do not have the DMI equivalent. Even if they do, they are very unlikely to support SPNs, and, barring violation of Intellectual Property Rights, do not support MCDN (as it is a proprietary Nortel protocol).

With that said, a third party gateway that interoperates with CS 1000M or CS 1000S can also interoperate with CS 1000E at exactly the same level. It must be provisioned on the CS 1000E in the same way it was provisioned on the other CS 1000 systems, and has no added capabilities above and beyond what it has for "gateway to and from generic CS 1000". However, it also has "no less".

GGP planning implications

For gateways capable of being provisioned in this manner, the remote gateway may be provisioned identically to the gateway in a CS 1000E system. This allows the optimum performance as per the CS 1000E gateway group handling. However, this is not mandatory for these systems.

If the user is willing to accept the exact gateway selection handling by the gatekeeper or redirect server provided for all other gateways in the network, they do not need to provision any additional values beyond the normal CS 1000M or CS 1000S entries for IP Peer. In this case, there is no "customization" of the call handling; everyone uses the same ordered list.

Only when the user wants to have specific handling for this system is the full provisioning as per this document required. This permits the user to customize the route costing based on the originating site.

To compare and contrast, if a network does not want local break-out from IP to the PSTN for certain call types (potentially, for long distance calls), the user can provision a single entry in the NRS database, for the true number (for example, national number 543-1234-xxxxx may be provisioned as national number type, "5431234"). All calls using this number at the NRS (whether SIP or H.323) terminate on the same ordered list. Access to the PSTN locally is via TDM trunks on the local Call Server, as long as it isn't CS 1000E.

For cases where allowing local break-out from an MG 1000E (or the CS 1000E that didn't have an IPE shelf with TDM trunk resources), use the CS 1000E approach. Assume that the user wants to dial national number 543-1234-xxxxx as per the prior paragraph. If a prefix such as 44245 is defined, and a call type code of 7 is defined for the given number, the NRS can be provisioned by the user to select the same entries as 5431234, but add the CS 1000E local trunking gateway as an option.

The second option is the only possible alternative for a CS 1000E to get access to the local PSTN, so it acts as the only choice that the user should select. All other Call Servers may do the same, or may use one "default" entry without any manipulation anywhere. This choice is up to the user. However, if in non-North American countries using SPNs to place the calls, the user must plan carefully; any codes used to access the national or international numbers from any CS 1000 switch cannot be used by any other switches to resolve the call to a different destination.

As an example, assume that the caller wants to be able to call London, England. One of the city codes is 207. If any national number 2071, 2072, 2073, or 2077 is to used "gateway A", the 2071 (etc.) is provisioned in NRS as an SPN. If the user also wants to use 2071 as a group prefix in Paris to reach Cannes, but there is only a single NRS database in the European network, there is confusion; is SPN 2071 London, or Cannes? There is no conflict with the North American NPA, the international numbers to Egypt (country code 20), CDP calls to DN 2071 or 2071x, or Location code calls to 207-1xxx. Conflicts are limited to the same plan and type.

Key terminology

A glossary defining important terms used throughout this appendix is provided in Table 109 on page 610. Common acronyms used throughout this appendix are also provided in Table 110 on page 613.

Glossary of terms

The following table is sorted alphabetically by the terms entered.

Table 109
Important terms (Part 1 of 3)

Term	Definition
Automatic Location Identification	The determination of the location of a caller through a database linking the caller's Automatic Number Identification data or the Calling Party Number (based on trunk type). This allows the call to be routed to the correct Public Safety Answering Position.
Automatic Number Identification	The digit string either assigned by the PSTN to a trunk used for ESA calls (typically, the billing number or Listed Directory Number) or the digit string sent by the PBX to provide the number of the user. This number must be able to receive incoming calls and ideally terminates on the specific user device placing the call.

Table 109
Important terms (Part 2 of 3)

Term	Definition
Bandwidth Zone	A number of IP Phones that are usually located in the same small geographical area, and have the same bandwidth attributes, are placed in the same bandwidth zone. Bandwidth zones are a complex topic; a reasonable first approximation is used here to “set the stage” for further discussions of how bandwidth zones interact with ESA.
Call Type Digit	Using the dialing plan to get off-net access requires changing the number type to an SPN. This digit or set of digits allows the call to be correctly converted back to the original call type.
DID unit	This is a unit — telephone, soft client, and so forth — that has a DID DN assigned, and this unit is the prime for this DN. That is, if the DN is multiple appearance, this unit acts as the Multiple Appearance Redirection Prime and therefore the PSAP is able to select this unit as the site for any received alarm. (All other units using this DN will either associate the CLID (etc.) with another DN or build the CLID from the default information.)
Emergency Services Access	The Emergency Service Access feature on the Call Server routes calls to trunks to the public network to contact the PSAP. The Call Server ensures that the correct Calling Party Number (or Automatic Number Identification) is built for the call, to allow the public network to select the right Public Safety Answering Position. This Calling Party Number also allows callback from the Public Safety Answering Position, in case of disconnection, need for more information, or any other reason that the Public Safety Answering Position personnel may identify.
Emergency Services Directory Number	The Emergency Services Directory Number
Emergency Services Zone	The public network defines Emergency Service Zones as the area serviced by a specific Public Safety Answering Position.

Table 109
Important terms (Part 3 of 3)

Term	Definition
Gateway Group	A grouping of destination gateways (typically, a list ordered by preference as to “the best place to re-enter the TDM domain) used for a specific call scenario. The group allows a specific Call Server to uniquely identify a preferred sequence of destinations for least cost routing when using the NRS to control destination selection. Note, though, that this does not mean that a gateway group can only be used by a single Call Server. Rather, it means that the granularity of precedence is such that a single originating Call Server can uniquely specify the destination selection according to its own “best sequence”.
Group Gateway Prefix	A digit string used to allow the gatekeeper to resolve a destination based on a prioritized list of alternates, that is intended to be unique within the network. That is, if the digit string prefix is discovered, it means that the call must exit the IP network at the “most preferred” gateway available from the ordered list.
Primary Zone	The CS 1000E zone which has the largest number of TDM units, which behaves like the main office in a main office and branch office setup, or like the core system for the CS 1000M or CS 1000S. That is, the branch office configuration has the “Main Office”; this is the equivalent “main zone”.
Public Safety Answering Position	The public network uses a specific Public Safety Answering Position to answer the emergency calls from a specific geographical area. This is based on the incoming trunk group (therefore, a direct physical link) or on the Calling Party Number.

Acronyms

The following table is sorted alphabetically by the terms entered.

Table 110
Important acronyms

Acronym	Term
ALI	Automatic Location Identification
ANI	Automatic Number Identification
BWZ	Bandwidth Zone
CAMA	Centralized Automatic Message Accounting
CLID	Calling Line ID
CNI	Calling Number Identification for MFC
CTD	Call Type Digit
DID	Direct Inward Dialing
ESA	Emergency Services Access
ESZ	Emergency Services Zone
GGP	Gateway Group Prefix
MFC	Multi-Frequency Compelled
PSAP	Public Safety Answering Position
ZESA	Zone ESA data block

Appendix C: Reference tables

List of tables

Trunk traffic – Erlang B with P.01 Grade-of-Service

Reference Table 1
Trunk traffic – Erlang B (P.01) (Part 1 of 2)

Trunks	CCS	Trunks	CCS	Trunks	CCS	Trunks	CCS	Trunks	CCS
1	0.4	21	462	41	1076	61	1724	81	2387
2	5.4	22	491	42	1108	62	1757	82	2419
3	16.6	23	521	43	1140	63	1789	83	2455
4	31.3	24	550	44	1171	64	1822	84	2488
5	49.0	25	580	45	1203	65	1854	85	2520
6	68.8	26	611	46	1236	66	1886	86	2552
7	90.0	27	641	47	1268	67	1922	87	2588
8	113	28	671	48	1300	68	1955	88	2621
9	136	29	702	49	1332	69	1987	89	2653
10	161	30	732	50	1364	70	2020	90	2689
11	186	31	763	51	1397	71	2052	91	2722
12	212	32	794	52	1429	72	2088	92	2758
13	238	33	825	53	1462	73	2120	93	2790
14	265	34	856	54	1494	74	2153	94	2822
15	292	35	887	55	1526	75	2185	95	2858
16	319	36	918	56	1559	76	2221	96	2891
17	347	37	950	57	1591	77	2254	97	2923
18	376	38	981	58	1624	78	2286	98	2959
19	404	39	1013	59	1656	79	2318	99	2992
20	433	40	1044	60	1688	80	2354	100	3028

Reference Table 1
Trunk traffic – Erlang B (P.01) (Part 2 of 2)

Trunks	CCS	Trunks	CCS	Trunks	CCS	Trunks	CCS	Trunks	CCS
101	3060	121	3740	141	4424	161	5119	181	5810
102	3092	122	3776	142	4460	162	5155	182	5843
103	3128	123	3809	143	4493	163	5188	183	5879
104	3161	124	3845	144	4529	164	5224	184	5915
105	3197	125	3877	145	4561	165	5260	185	5974
106	3229	126	3913	146	4597	166	5292	186	5983
107	3265	127	3946	147	4630	167	5328	187	6019
108	3298	128	3982	148	4666	168	5360	188	6052
109	3330	129	4014	149	4702	169	5396	189	6088
110	3366	130	4050	150	4738	170	5429	190	6124
111	3398	131	4082	151	4770	171	5465	191	6156
112	3434	132	4118	152	4806	172	5501	192	6192
113	3467	133	4151	153	4842	173	5533	193	6228
114	3503	134	4187	154	4874	174	5569	194	6260
115	3535	135	4219	155	4910	175	5602	195	6296
116	3571	136	4255	156	4946	176	5638	196	6332
117	3604	137	4288	157	4979	177	5670	197	6365
118	3640	138	4324	158	5015	178	5706	198	6401
119	3672	139	4356	159	5051	179	5738	199	6433
120	3708	140	4392	160	5083	180	5774	200	6469

Note: For trunk traffic greater than 6469 CCS, allow 32.35 CCS per trunk.

Trunk traffic – Poisson 1% blocking

Reference Table 2
Trunk traffic – Poisson 1% blocking (Part 1 of 2)

Trunks	CCS	Trunks	CCS	Trunks	CCS	Trunks	CCS	Trunks	CCS
1	0.4	21	426	41	993	61	1595	81	2215
2	5.4	22	453	42	1023	62	1626	82	2247
3	15.7	23	480	43	1052	63	1657	83	2278
4	29.6	24	507	44	1082	64	1687	84	2310
5	46.1	25	535	45	1112	65	1718	85	2341
6	64	26	562	46	1142	66	1749	86	2373
7	84	27	590	47	1171	67	1780	87	2404
8	105	28	618	48	1201	68	1811	88	2436
9	126	29	647	49	1231	69	1842	89	2467
10	149	30	675	50	1261	70	1873	90	2499
11	172	31	703	51	1291	71	1904	91	2530
12	195	32	732	52	1322	72	1935	92	2563
13	220	33	760	53	1352	73	1966	93	2594
14	244	34	789	54	1382	74	1997	94	2625
15	269	35	818	55	1412	75	2028	95	2657
16	294	36	847	56	1443	76	2059	96	2689
17	320	37	876	57	1473	77	2091	97	2721
18	346	38	905	58	1504	78	2122	98	2752
19	373	39	935	59	1534	79	2153	99	2784
20	399	40	964	60	1565	80	2184	100	2816

Reference Table 2
Trunk traffic – Poisson 1% blocking (Part 2 of 2)

Trunks	CCS	Trunks	CCS	Trunks	CCS	Trunks	CCS	Trunks	CCS
101	2847	121	3488	141	4134	161	4786	181	5442
102	2879	122	3520	142	4167	162	4819	182	5475
103	2910	123	3552	143	4199	163	4851	183	5508
104	2942	124	3594	144	4231	164	4884	184	5541
105	2974	125	3616	145	4264	165	4917	185	5574
106	3006	126	3648	146	4297	166	4549	186	5606
107	3038	127	3681	147	4329	167	4982	187	5639
108	3070	128	3713	148	4362	168	5015	188	5672
109	3102	129	3746	149	4395	169	5048	189	5705
110	3135	130	3778	150	4427	170	5081	190	5738
111	3166	131	3810	151	4460	171	5114	191	5771
112	3198	132	3843	152	4492	172	5146	192	5804
113	3230	133	3875	153	4525	173	5179	193	5837
114	3262	134	3907	154	4557	174	5212	194	5871
115	3294	135	3939	155	4590	175	5245	195	5904
116	3326	136	3972	156	4622	176	5277	196	5937
117	3359	137	4004	157	4655	177	5310	197	5969
118	3391	138	4037	158	4686	178	5343	198	6002
119	3424	139	4070	159	4721	179	5376	199	6035
120	3456	140	4102	160	4754	180	5409	200	6068

Note: For trunk traffic greater than 6068 CCS, allow 30.34 CCS per trunk.

Trunk traffic – Poisson 2% blocking

Reference Table 3
Trunk traffic – Poisson 2% blocking (Part 1 of 2)

Trunks	CCS	Trunks	CCS	Trunks	CCS	Trunks	CCS	Trunks	CCS
1	0.4	31	744	61	1659	91	2611	121	3581
2	7.9	32	773	62	1690	92	2643	122	3614
3	20.9	33	803	63	1722	93	2674	123	3647
4	36.7	34	832	64	1752	94	2706	124	3679
5	55.8	35	862	65	1784	95	2739	125	3712
6	76.0	36	892	66	1816	96	2771	126	3745
7	96.8	37	922	67	1847	97	2803	127	3777
8	119	38	952	68	1878	98	2838	128	3810
9	142	39	982	69	1910	99	2868	129	3843
10	166	40	1012	70	1941	100	2900	130	3875
11	191	41	1042	71	1973	101	2931	131	3910
12	216	42	1072	72	2004	102	2964	132	3941
13	241	43	1103	73	2036	103	2996	133	3974
14	267	44	1133	74	2067	104	3029	134	4007
15	293	45	1164	75	2099	105	3051	135	4039
16	320	46	1194	76	2130	106	3094	136	4072
17	347	47	1225	77	2162	107	3126	137	4105
18	374	48	1255	78	2194	108	3158	138	4138
19	401	49	1286	79	2226	109	3190	139	4171
20	429	50	1317	80	2258	110	3223	140	4204

Note: For trunk traffic greater than 4533 CCS, allow 30.2 CCS per trunk.

Reference Table 3
Trunk traffic – Poisson 2% blocking (Part 2 of 2)

Trunks	CCS	Trunks	CCS	Trunks	CCS	Trunks	CCS	Trunks	CCS
21	458	51	1348	81	2290	111	3255	141	4237
22	486	52	1374	82	2322	112	3288	142	4269
23	514	53	1352	83	2354	113	3321	143	4302
24	542	54	1441	84	2386	114	3353	144	4335
25	571	55	1472	85	2418	115	3386	145	4368
26	562	56	1503	86	2450	116	3418	146	4401
27	627	57	1534	87	2482	117	3451	147	4434
28	656	58	1565	88	2514	118	3483	148	4467
29	685	59	1596	89	2546	119	3516	149	4500
30	715	60	1627	90	2578	120	3548	150	4533

Note: For trunk traffic greater than 4533 CCS, allow 30.2 CCS per trunk.

Digitone receiver requirements – Model 1

Reference Table 4
Digitone receiver requirements – Model 1

Number of DTRs	Max. number of Digitone lines	DTR load (CCS)	Number of DTRs	Max. number of Digitone lines	DTR load (CCS)
2	7	2	17	1181	319
3	33	9	18	1244	336
4	69	19	19	1348	364
5	120	33	20	1455	393
6	179	49	21	1555	420
7	249	68	22	1662	449
8	332	88	23	1774	479
9	399	109	24	1885	509
10	479	131	25	1988	537
11	564	154	26	2100	567
12	659	178	27	2211	597
13	751	203	28	2325	628
14	848	229	29	2440	659
15	944	255	30	2555	690
16	1044	282			

Note: See “Step 5: Calculate Digitone receiver requirements” for Model 1 assumptions.

Digitone receiver requirements – Model 2

Reference Table 5
Digitone receiver requirements – Model 2

Number of DTRs	Max. number of Digitone lines	DTR load (CCS)	Number of DTRs	Max. number of Digitone lines	DTR load (CCS)
2	2	2	17	843	253
3	21	7	18	920	276
4	52	15	19	996	299
5	90	27	20	1076	323
6	134	40	21	1153	346
7	183	55	22	1233	370
8	235	71	23	1316	395
9	293	88	24	1396	419
10	353	107	25	1480	444
11	416	126	26	1563	469
12	483	145	27	1650	495
13	553	166	28	1733	520
14	623	187	29	1816	545
15	693	208	30	1903	571
16	770	231			

Note: See “Step 5: Calculate Digitone receiver requirements” for Model 2 assumptions.

Digitone receiver requirements – Model 3

Reference Table 6
Digitone receiver requirements – Model 3

Number of DTRs	Max. number of Digitone lines	DTR load (CCS)	Number of DTRs	Max. number of Digitone lines	DTR load (CCS)
2	5	2	17	862	319
3	22	9	18	908	336
4	50	19	19	983	364
5	87	33	20	1062	393
6	132	49	21	1135	420
7	180	68	22	1213	449
8	234	88	23	1294	479
9	291	109	24	1375	509
10	353	131	25	1451	537
11	415	154	26	1532	567
12	481	178	27	1613	597
13	548	203	28	1697	628
14	618	229	29	1781	659
15	689	255	30	1864	690
16	762	282			

Note: See “Step 5: Calculate Digitone receiver requirements” for Model 3 assumptions.

Digitone receiver requirements – Model 4

Reference Table 7
Digitone receiver requirements – Model 4

Number of DTRs	Max. number of Digitone lines	DTR load (CCS)	Number of DTRs	Max. number of Digitone lines	DTR load (CCS)
2	4	2	17	683	253
3	18	7	18	745	276
4	41	15	19	808	299
5	72	27	20	872	323
6	109	40	21	935	346
7	148	55	22	1000	370
8	193	71	23	1067	395
9	240	88	24	1132	419
10	291	107	25	1200	444
11	340	126	26	1267	469
12	391	145	27	1337	495
13	448	166	28	1405	520
14	505	187	29	1472	545
15	562	208	30	1543	571
16	624	231			

Note: See “Step 5: Calculate Digitone receiver requirements” for Model 4 assumptions.

Digitone receiver load capacity – 6 to 15 second holding time

Reference Table 8
Digitone receiver load capacity – 6 to 15 second holding time (Part 1 of 3)

Number of DTRs	Average holding time in seconds									
	6	7	8	9	10	11	12	13	14	15
1	0	0	0	0	0	0	0	0	0	0
2	3	2	2	2	2	2	2	2	2	2
3	11	10	10	9	9	9	9	8	8	8
4	24	23	22	21	20	19	19	19	18	18
5	41	39	37	36	35	34	33	33	32	32
6	61	57	55	53	52	50	49	49	48	47
7	83	78	75	73	71	69	68	67	66	65
8	106	101	97	94	91	89	88	86	85	84
9	131	125	120	116	113	111	109	107	106	104
10	157	150	144	140	136	133	131	129	127	126
11	185	176	170	165	161	157	154	152	150	148
12	212	203	196	190	185	182	178	176	173	171
13	241	231	223	216	211	207	203	200	198	196
14	270	259	250	243	237	233	229	225	223	220
15	300	288	278	271	264	259	255	251	248	245
16	339	317	307	298	292	286	282	278	274	271
17	361	346	335	327	320	313	310	306	302	298
18	391	377	365	356	348	342	336	331	327	324
Note: Load capacity is measured in CCS.										

Reference Table 8
Digitone receiver load capacity – 6 to 15 second holding time (Part 2 of 3)

Number of DTRs	Average holding time in seconds									
	6	7	8	9	10	11	12	13	14	15
19	422	409	396	386	378	371	364	359	355	351
20	454	438	425	414	405	398	393	388	383	379
21	487	469	455	444	435	427	420	415	410	406
22	517	501	487	475	466	456	449	443	438	434
23	550	531	516	504	494	487	479	472	467	462
24	583	563	547	535	524	515	509	502	497	491
25	615	595	579	566	555	545	537	532	526	521
26	647	628	612	598	586	576	567	560	554	548
27	680	659	642	628	618	607	597	589	583	577
28	714	691	674	659	647	638	628	620	613	607
29	746	724	706	690	678	667	659	651	644	637
30	779	758	738	723	709	698	690	682	674	668
31	813	792	771	755	742	729	719	710	703	696
32	847	822	805	788	774	761	750	741	733	726
33	882	855	835	818	804	793	781	772	763	756
34	913	889	868	850	836	825	812	803	795	787
35	947	923	900	883	867	855	844	835	826	818
36	981	957	934	916	900	886	876	866	857	850
37	1016	989	967	949	933	919	909	898	889	881
38	1051	1022	1001	982	966	951	938	928	918	912

Note: Load capacity is measured in CCS.

Reference Table 8
Digitone receiver load capacity – 6 to 15 second holding time (Part 3 of 3)

Number of DTRs	Average holding time in seconds									
	6	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
39	1083	1055	1035	1015	999	984	970	959	949	941
40	1117	1089	1066	1046	1029	1017	1002	990	981	972

Note: Load capacity is measured in CCS.

Digitone receiver load capacity – 16 to 25 second holding time

Reference Table 9
Digitone receiver load capacity – 16 to 25 second holding time (Part 1 of 3)

Number of DTRs	Average holding time in seconds									
	16	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**
1	0	0	0	0	0	0	0	0	0	0
2	2	2	2	2	2	2	2	2	2	2
3	8	8	8	8	8	8	8	8	8	8
4	18	18	18	18	18	17	17	17	17	17
5	31	31	31	30	30	30	30	30	30	29
6	47	46	46	45	45	45	45	44	44	44
7	64	63	63	62	62	62	61	61	61	60
8	83	82	82	81	80	80	79	79	79	78
9	103	102	101	100	100	99	99	98	98	97
10	125	123	122	121	121	120	119	119	118	118
11	147	145	144	143	142	141	140	140	139	138
12	170	168	167	166	165	164	163	162	161	160
13	193	192	190	189	188	186	185	184	184	183
14	218	216	214	213	211	210	209	208	207	206
15	243	241	239	237	236	234	233	232	231	230
16	268	266	264	262	260	259	257	256	255	254
17	294	292	290	288	286	284	283	281	280	279
18	322	319	317	314	312	311	309	308	306	305

Note: Load capacity is measured in CCS.

Reference Table 9
Digitone receiver load capacity – 16 to 25 second holding time (Part 2 of 3)

Number of DTRs	Average holding time in seconds									
	16	17	18	19	20	21	22	23	24	25
19	347	344	342	339	337	335	334	332	331	329
20	374	371	368	366	364	361	360	358	356	355
21	402	399	396	393	391	388	386	385	383	381
22	431	427	424	421	419	416	414	412	410	409
23	458	454	451	448	445	442	440	438	436	434
24	486	482	478	475	472	470	467	465	463	461
25	514	510	506	503	500	497	495	492	490	488
26	544	539	535	532	529	526	523	521	518	516
27	573	569	565	561	558	555	552	549	547	545
28	603	598	594	590	587	584	581	578	576	573
29	631	626	622	618	614	611	608	605	602	600
30	660	655	651	646	643	639	636	633	631	628
31	690	685	680	676	672	668	665	662	659	656
32	720	715	710	705	701	698	694	691	688	686
33	751	745	740	735	731	727	724	721	718	715
34	782	776	771	766	761	757	754	750	747	744
35	813	807	801	796	792	788	784	780	777	774
36	841	835	829	824	820	818	814	810	807	804
37	872	865	859	854	849	845	841	837	834	831
38	902	896	890	884	879	875	871	867	863	860

Note: Load capacity is measured in CCS.

Reference Table 9
Digitone receiver load capacity – 16 to 25 second holding time (Part 3 of 3)

Number of DTRs	Average holding time in seconds									
	16	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**
39	934	927	921	914	909	905	901	897	893	890
40	965	958	952	945	940	936	931	927	923	920
Note: Load capacity is measured in CCS.										

Digitione receiver requirement – Poisson 0.1% blocking

Reference Table 10
Digitone receiver requirements – Poisson 0.1% blocking (Part 1 of 2)

Number of DTRs	DTR load (CCS)	Number of DTRs	DTR load (CCS)
1	0	26	469
2	2	27	495
3	7	28	520
4	15	29	545
5	27	30	571
6	40	31	597
7	55	32	624
8	71	33	650
9	88	34	676
10	107	35	703
11	126	36	729
12	145	37	756
13	166	38	783
14	187	39	810
15	208	40	837
16	231	41	865
17	253	42	892
18	276	43	919
19	299	44	947
20	323	45	975
21	346	46	1003

Reference Table 10
Digitone receiver requirements – Poisson 0.1% blocking (Part 2 of 2)

Number of DTRs	DTR load (CCS)	Number of DTRs	DTR load (CCS)
22	370	47	1030
23	395	48	1058
24	419	49	1086
25	444	50	1115

Conference and TDS loop requirements

Reference Table 11
Conference and TDS loop requirements

Network loops required at 2 years	TDS loops required	Conference loops required
1–12	1	1
13–24	2	2
25–36	3	3
37–48	4	4
49–60	5	5
61–72	6	6
73–84	7	7
85–96	8	8
97–108	9	9
109–120	10	10

Digitone receiver provisioning

Reference Table 12
Digitone receiver provisioning (Part 1 of 3)

DTR CCS	DTR ports	DTR CCS	DTR ports
1–2	2	488–515	24
3–9	3	516–545	25
10–19	4	546–576	26
20–34	5	577–607	27
35–50	6	608–638	28
51–69	7	639–667	29
70–89	8	668–698	30
90–111	9	699–729	31
112–133	10	730–761	32
134–157	11	762–793	33
158–182	12	794–825	34
183–207	13	826–856	35
208–233	14	857–887	36
234–259	15	888–919	37
260–286	16	920–951	38
287–313	17	952–984	39
314–342	18	985–1017	40
343–371	19	1018–1050	41
372–398	20	1051–1084	42
399–427	21	1085–1118	43
428–456	22	1119–1153	44
457–487	23	1154–1188	45

Reference Table 12
Digitone receiver provisioning (Part 2 of 3)

DTR CCS	DTR ports	DTR CCS	DTR ports
1189–1223	46	1961–1995	68
1224–1258	47	1996–2030	69
1259–1293	48	2031–2065	70
1294–1329	49	2066–2100	71
1330–1365	50	2101–2135	72
1366–1400	51	2136–2170	73
1401–1435	52	2171–2205	74
1436–1470	53	2206–2240	75
1471–1505	54	2241–2275	76
1506–1540	55	2276–2310	77
1541–1575	56	2311–2345	78
1576–1610	57	2346–2380	79
1611–1645	58	2381–2415	80
1646–1680	59	2416–2450	81
1681–1715	60	2451–2485	82
1716–1750	61	2486–2520	83
1751–1785	62	2521–2555	84
1786–1802	63	2556–2590	85
1821–1855	64	2591–2625	86
1856–1890	65	2626–2660	87
1891–1926	66	2661–2695	88
1926–1960	67	2696–2730	89

Reference Table 12
Digitone receiver provisioning (Part 3 of 3)

DTR CCS	DTR ports	DTR CCS	DTR ports
2731–2765	90	2941–2975	96
2766–2800	91	2976–3010	97
2801–2835	92	3011–3045	98
2836–2870	93	3046–3080	99
2871–2905	94	3081–3115	100
2906–2940	95	3116–3465	101
Note: Provisioning assumes an 11-second holding time.			

Nortel Communication Server 1000

Communication Server 1000E

Planning and Engineering

Publication number: 553-3041-120
Document release: Standard 6.00
Date: December 2006

Sourced in Canada

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

NORTEL