Nortel Communication Server 1000

Branch Office Installation and Commissioning

Release: 7.0
Document Revision: 04.02

www.nortel.com

NN43001-314

Nortel Communication Server 1000
Release: 7.0
Publication: NN43001-314
Document release date: 11 June 2010

Contents

New in this release 11
Features 11
Co-resident Call Server and Signaling Server 11
Common Processor Dual Core (CP DC) card 11
Common Processor Media Gateway (CP MG) card 12
128-port DSP daughterboard 12
Branch Office capacity 12
RLI and DMI enhancement 13
Other changes 13
Revision history 13

How to get help 15
Getting help from the Nortel web site 15
Getting help over the telephone from a Nortel Solutions Center 15
Getting help from a specialist by using an Express Routing Code 16
Getting help through a Nortel distributor or re-seller 16

Introduction 17
Subject 17
Note on legacy products and releases 17
Applicable systems 18
System migration 18
Intended audience 18
Conventions 18
Related information 20
Technical documentation 20
Online 20
CD-ROM 20

Overview 21
Contents 21
What is Branch Office? 21
Main Office and Branch Office Migration 23
Media Gateway 1000B 24
Co-resident Call Server and Signaling Server 25

SIP Line Service 26
S1/S2 solution mode 28
Local Mode 37
UEXT configuration 37
IP Telephony node 37
IP Telephony Node Management 37
IP Telephony Node Management 38
Zone Based Dialing 38
Gateway Controller serial ports 39
Single CPU Implications 39
Gateway Controller serial port default configuration 39
Gateway Controller serial ports configuration change in Overlay 17 40
CEMux Support 40
Clock References 41
Main office hardware description 41
MG 1000B platform hardware description 41
MG 1000B Core 45
MG 1000B Expander 49
Signaling Server 49
Network Routing Service (NRS) 50
Telephones 51
Voice Gateway Media Card 52
Analog or digital trunk cards 52
Analog or digital line cards 52
MG 1000B Data Networking 53
Gateway Controller network connections 55
MG 1000B platform configuration overview 57
MG 1000B platform without a chassis expander 58
MG 1000B platform with a chassis expander 60
Capacity 60
Voice Gateway Media Card DSP capacity 61
Software requirements 62
Main and Branch Office running the same release 62
Main and Branch Office running different releases 62
Package Combinations 64
Supported applications 64
Survivability 64
Active Call Failover 66
Configuring S2 IP Address to point to the main office TPS 67
Patch Management Enhancements 68

How the Branch Office feature works 69
Contents 69
Introduction 69

Normal Mode and Local Mode operation 69
Normal Mode 69
Local Mode 70
Virtual Trunks 74
IP Phone calls 74
MCDN ALTernate Routing and Vacant Number Routing 74
IP Phone to analog (500/2500-type) or digital telephone calls 76
Conference calls 76
Group Call 77
Survivability of IP Phones 77
Configuring non-zero S2 IP Addresses for UNIStim phones 78
Points to remember 79
Configuring the S2 IP Address parameter 80
Multiple Appearance DN (MADN) 80
IP Phones with the same DN at the Branch Office 80
IP Phones with the same DN at the main office 81
Emergency services 81
Configuring ESA for emergency services 82
Configuring SPN for emergency services 82
MG 1000B Core interoperability 83
Network Wide Redundancy Phase II and Network Music 83

Planning and management **87**
Contents 87
Branch Office dialing plan 87
Emergency Services 88
Zone Based Dialing 88
Zones 89
Music on Hold 89
ESN Access Codes 89
Provisioning the IP Phones 89
Configuration example for PSTN resources at the Branch Office 90
Management 92
Remote Access 92
Element Manager 92
Traffic measurement 93
Call Detail Recording (CDR) 93
System security 94

Adding a Branch Office **97**
Contents 97
Introduction 97
Main office requirements 98
Optional features 99
Branch Office requirements 99

Implementation summary 100
Adding a Communication Server 1000 Release 7.0 Branch Office to a Main Office with a previous software release 102
Upgrade the entire network to Communication Server 1000 Release 7.0 102
Upgrade only the Main Office to Communication Server 1000 Release 7.0 103

Converting a small system to a Branch Office 107
Contents 107
Introduction 107
Requirements 107
Conversion 108
Implementation summary 109

Upgrading to Communication Server 1000 Release 7.0 113
Contents 113
Introduction 113
Upgrading to Communication Server 1000 Release 7.0 113

Main office configuration 115
Contents 115
Introduction 115
IP Telephony Nodes 115
Importing an IP Telephony Node file 117
Exporting an IP Telephony Node file 118
Adding Linux servers to a Node 120
SIP Client configuration 120
Proxy Server 1 and Server 2 solution 120
Zone Based Dialing 124
UNIStim LTPS 125
Gateway application services 125
IP Phone passwords and parameters 125
MG 1000B IP Phone configuration 128
MG 1000B IP Phone configuration using LD 11 128

MG 1000B platform hardware installation 131
Contents 131
Installing an MG 1000B Core 131
Readiness checklist 132
Rack-mounting an MG 1000B 133
Installing cards 137
Upgrading the MG 1000B hardware 138
Perform a customer backup data dump (installation release) 139
Installing the cards 140
Installing a DSP Daughterboard 140
Gateway Controller installation 141
Server card installation 144

Upgrading the CP PM software 148
Installing a Signaling Server 149
Hardware installation 149

MG 1000B software installation 155
Contents 155
Installing MG 1000B software 156
Connecting the MG 1000B Core to the network 157
Connecting the MG 1000B Core to the network 157
Using Element Manager to configure the node 161
Signaling Server software installation 164
Co-resident Call Server and Signaling Server software installation 165
Preinstallation checklist 165
Nortel Linux Base installation 170
Call Server and Signaling Server software installation 171

Branch Office configuration 173
Contents 173
Configuring the Branch Office 173
Summary of steps 173
Configuring the Zone Based Dialing 174
Configuring the Voice Gateway Media Cards 174
Configuring the trunks and lines 175
Adding the Branch Office endpoints to the NRS database 175

MG 1000B telephones 177
Contents 177
Overview 177
Installing and configuring IP Phones 177
Password requirements 178
Installing an IP Phone using the keypad 179
Branch User Config 181
Survivability test 186
Installing IP Phones through LD 11 189
Using the IP Phones 191
Telephone Options 192
Virtual Office Login on the Branch Office 193
Test Local Mode 195
Personal Directory, Callers List, Redial List 196
Set-Based Removal 197
Analog and digital devices in the Branch Office 197
Analog devices 197
Digital devices 198

Emergency Services configuration 199
Contents 199

Overview 199
Emergency Services Access (ESA) 199
Routing ESA calls 199
Configuring ESA for the Branch Office 201
Configuring ESA in Element Manager 210
Provisioning ESA calls for a central deployment 210
Emergency Service using Special Numbers (SPN) 211
CLID verification (CLIDVER) 212
Networked M911 212

Maintenance and diagnostics 215
Contents 215
Firmware downloads 215
Enhanced UNIStim Firmware Download for IP Phones 215
Troubleshooting 218
Signaling Server CLI commands 223
isetShow 224
clearLockout TN or IP 224
Call Server commands 224
Verify CLID 224
Print Branch Office zone information 225
Enable and disable Branch Office zone features 226
View status of Branch Office zone at main office Call Server 226
Change and print PVQ notification levels 227
Print PVQ statistics 227
Print inventory 228
Co-resident Call Server and Signaling Server restart commands 228

Preprogrammed data 231
Contents 231
Introduction 231
Passwords and codes 231
Default numbering plan 232
First digits 232
Important extension numbers 233
Flexible Feature Codes 233
SDI ports 234
Modem port 235
ESDI settings 235
Telephone tones 235
Trunk routes 236
System parameters 236
Customer data 237
Trunk models 237

Branch Office engineering example **241**
Introduction 241
Assumptions 241
Equipment characteristics 241
Traffic characteristics 241
Calculations 242
Traffic 242
DSP requirements 244
Virtual Trunk requirements 245
Call Server Real-time usage 246
MG 1000B Core and MG 1000B Expander requirements 247
Bandwidth requirement for Branch Office LAN/WAN 248

New in this release

The following sections detail what's new in *Branch Office Installation and Commissioning* (NN43001-314) for Release 7.0.

- "Features" (page 11)
- "Other changes" (page 13)

Features

The following sections describe new features or hardware for Communication Server 1000 Release 7.0.

Co-resident Call Server and Signaling Server

Communication Server 1000 Release 7.0 Co-resident Call Server and Signaling Server (Co-res CS & SS) can run the Call Server software, the Signaling Server software, and the System Management software on one hardware platform running the Linux base Operating System. Co-residency of the Call Server and the Signaling Server provides a cost-effective solution for Communication Server 1000 installations.

For Communication Server 1000 Release 7.0, various hardware platforms can support the Co-res CS and SS configuration, see Table 2 "Hardware platform supported roles" (page 20). For more information about the supported hardware, see *Circuit Card Reference* (NN43001-311).

Common Processor Dual Core (CP DC) card

The Common Processor Dual Core (CP DC) card is introduced. The CP DC is a Server card for use in a Communication Server 1000 system. The CP DC card contains a dual core AMD processor and upgraded components which can provide improvements in processing power and speed over existing Server cards.

The CP DC card is available in two versions:

- NTDW53AAE6 - single slot metal faceplate CP DC card for CS 1000E systems
- NTDW54AAE6 - double slot metal faceplate CP DC card for CS 1000M systems

The CP DC card requires the Linux Base Operating System, and supports Co-resident Call Server and Signaling Server, or stand-alone Signaling Server configurations. The CP DC card does not support the standard or high availability Call Server configuration.

Common Processor Media Gateway (CP MG) card

The Common Processor Media Gateway (CP MG) card is introduced. The hardware for the CP MG card consists of integrating a Common Processor, a Gateway Controller, and non-removable Digital Signal Processor (DSP) resources into a single card for use in a Communication Server 1000E system.

The CP MG card is available in two versions:

- NTDW56BAE6 - CP MG card with 32 DSP ports
- NTDW59BAE6 - CP MG card with 128 DSP ports

The CP MG card provides improvements in port density and cost reductions by functioning as a Call Server or Application Server and a Gateway Controller with DSP resources while occupying slot 0 in a Media Gateway. The CP MG card requires the Linux Base Operating System, and supports the Co-resident Call Server and Signaling Server, and CS 1000E TDM configurations. The CP MG card does not support the standard or high availability Call Server configuration.

128-port DSP daughterboard

The 128-port Digital Signal Processor (DSP) daughterboard (DB-128) for the Media Gateway Controller (MGC) card is introduced. An MGC card populated with one NTDW78 DB-128 can provide 128 DSP ports.

The CS 1000E Peripheral Rate Interface (PRI) Media Gateway (PRI Gateway) can support a MGC card populated with two DB-128 for a maximum of 256 DSP ports. The Extended Media Gateway PRI (MGP) package 418 is required to support MGC cards populated with two DB-96 or two DB-128.

Branch Office capacity

Each Communication Server 1000 Main Office (SA or HA) can support up to 1000 Branch Offices, consisting of combinations of SRGs, MG 1000Bs, SIP Media Gateways, and Geographically Redundant Survivable Media

Gateways (GR-SMG). The SRGs, MG 1000Bs, SIP Media Gateways, and GR-SMGs can be deployed in various combinations but the total cannot exceed 1000.

RLI and DMI enhancement

For Communication Server 1000 Release 7.0, the range of allowable Route List Index (RLI) and Digit Manipulation Index (DMI) values is increased from 0–999 to 0–1999. For more information about RLI and DMI values, see “Emergency Services configuration” (page 199).

Other changes

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

Revision history

June 2010	Standard 04.02. This document is up-issued to reflect changes in the Branch Office task flow graphic and to include CP PM version 2 content.
June 2010	Standard 04.01. This document is issued to support Communication Server 1000 Release 7.0.
December 2009	Standard 03.09. This document is up-issued to reflect changes in the section Converting a small system to a Branch Office.
November 2009	Standard 03.08. This document is up-issued to reflect changes in the section Trunk models.
October 2009	Standard 03.07 This document is up-issued to reflect changes in technical content found in “IP Telephony Node Management” (page 37).
September 2009	Standard 03.06. This document is up-issued to support Nortel Communication Server 1000 Release 6.0.
May 2009	Standard 03.05. This document is up-issued to support Nortel Communication Server 1000 Release 6.0.
July 2008	Standard 02.05. This document is up-issued to reflect changes in technical content. Sections relating to Bandwidth Management have been moved to *Converging the Data Network with VoIP Fundamentals* (NN43001-260).
May 2008	Standard 02.04. This document is up-issued to reflect changes in technical content for CR Q01870816.
February 2008	Standard 02.03. This document is up-issued to support Communication Server 1000 Release 5.5. Obsolete references and images have been removed.
December 2007	Standard 02.01. This document is up-issued to support Communication Server 1000 Release 5.5.

June 2007	Standard 01.02. This document has been up-issued to reflect changes in alternate call routing.
May 2007	Standard 01.01. This document is issued to support Communication Server 1000 Release 5.0. This document contains information previously contained in the following legacy document, now retired: *Branch Office* (553-3001-314).

How to get help

This chapter 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:

http://www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. From this site, you can:

- 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 do not find the information you require on the Nortel Technical Support web site, and you have a Nortel support contract, you can also get help over the telephone 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 telephone number for your region:

http://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:

http://www.nortel.com/erc

Getting help through a Nortel distributor or re-seller

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

Introduction

This document contains the following topics:

- “Overview” (page 21)
- “How the Branch Office feature works” (page 69)
- “Planning and management” (page 87)
- “Adding a Branch Office” (page 97)
- “Converting a small system to a Branch Office” (page 107)
- “Main office configuration” (page 115)
- “MG 1000B platform hardware installation” (page 131)
- “MG 1000B software installation” (page 155)
- “Branch Office configuration” (page 173)
- “MG 1000B telephones” (page 177)
- “Emergency Services configuration” (page 199)
- “Maintenance and diagnostics” (page 215)

Subject

This document describes the Branch Office and how to install and configure Branch Office as part of your system.

Note on legacy products and releases

This NTP contains information about systems, components, and features that are compatible with Nortel Communication Server 1000 Release 7.0 (or later) software. For more information about 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 following systems:

- Communication Server 1000M Single Group (CS 1000M SG)
- Communication Server 1000M Multi Group (CS 1000M MG)
- Communication Server 1000E (CS 1000E)
- Meridian 1 PBX 61C
- Meridian 1 PBX 81C

System migration

When particular Meridian 1 systems are upgraded to run Communication Server 1000 Release 7.0 software and configured to include a Signaling Server, they become Communication Server 1000 systems.Table 1 "Meridian 1 systems to CS 1000 systems" (page 18) lists each Meridian 1 system that supports an upgrade path to a Communication Server 1000 system.

Table 1
Meridian 1 systems to CS 1000 systems

This Meridian 1 system	Maps to Communication Server 1000 system
Meridian 1 PBX 11C Chassis	Communication Server 1000E
Meridian 1 PBX 11C Cabinet	Communication Server 1000E
Meridian 1 PBX 61C	Communication Server 1000M Single Group
Meridian 1 PBX 81C	Communication Server 1000M Multi Group

For more information, see *Communication Server 1000M and Meridian 1 Large System Upgrades Overview* (NN43021-458), *Communication Server 1000E Upgrades* (NN43041-458), and *Communication Server 1000E Upgrade — Hardware Upgrade Procedures* (NN43041-464).

Intended audience

This document is intended for individuals responsible for administering Communication Server 1000 and Meridian 1 systems.

Conventions

In this document, the following systems are referred to generically as system:

- Communication Server 1000E (CS 1000E)
- Communication Server 1000M (CS 1000M)
- Meridian 1

Unless specifically stated otherwise, the term Element Manager refers to the Communication Server 1000 Element Manager.

In this document, the Branch Office Media Gateway systems are referred to generically as Media Gateway 1000B (MG 1000B).

The following hardware is referred to generically as Media Gateway:

- Option 11C Mini Chassis (NTDK91) and Expander chassis (NTDK92) - legacy hardware
- Option 11C Cabinet (NTAK11) - legacy hardware
- MG 1000E Chassis (NTDU14) and Expander chassis (NTDU15)
- MG 1010 Chassis (NTC310)

In this document, the following hardware platforms are referred to generically as Server.

- Common Processor Pentium Mobile (CP PM) card
- Common Processor Media Gateway (CP MG) card
- Common Processor Dual Core (CP DC) card
- Commercial off-the-shelf (COTS) servers
  - IBM x360m server (COTS1)
  - HP DL320 G4 server (COTS1)
  - IBM x3350 server (COTS2)
  - Dell R300 server (COTS2)

In this document, the generic term COTS refers to all COTS servers. The term COTS1 or COTS2 refers to the specific servers in the preceding list.

In this document, following cards are referred to generically as Gateway Controller.

- Media Gateway Controller (MGC) card (NTDW60 and NTDW98)
- Media Gateway Extended Peripheral Equipment Controller (MG XPEC) card (NTDW20)
- Common Processor Media Gateway (CP MG) card (NTDW56 and NTDW59)

The following table shows CS 1000 Release 7.0 supported roles for common hardware platforms

Table 2
Hardware platform supported roles

Hardware platform	VxWorks Server	Linux Server	Co-res CS and SS	Gateway Controller
CP PIV	yes	no	no	no
CP PM	yes	yes	yes	no
CP DC	no	yes	yes	no
CP MG	no	no	yes (see note)	yes (see note)
MGC	no	no	no	yes
MG XPEC	no	no	no	yes
COTS	no	yes	no	no
COTS2	no	yes	yes	no

Note: The CP MG card functions as the Co-res CS and SS, and the Gateway Controller while occupying slot 0 in a Media Gateway.

Related information

This section lists information sources that relate to this document.

Technical documentation

This document references the following technical documents:

- *Features and Services Fundamentals* (NN43001-106)
- *Unified Communications Management Common Services Fundamentals* (NN43001-116)
- *IP Peer Networking Installation and Commissioning* (NN43001-313)
- *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315)
- *Hospitality Features Fundamentals* (NN43001-553)

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

Contents

This chapter contains the following topics:

"What is Branch Office?" (page 21)
"Main Office and Branch Office Migration" (page 23)
"Media Gateway 1000B " (page 24)

"Co-resident Call Server and Signaling Server" (page 25)
"SIP Line Service" (page 26)

"IP Telephony node" (page 37)
"Zone Based Dialing" (page 38)
"Gateway Controller serial ports" (page 39)
"Main office hardware description" (page 41)
"MG 1000B platform hardware description" (page 41)
"MG 1000B Data Networking" (page 53)
"MG 1000B platform configuration overview" (page 57)
"Capacity" (page 60)
"Software requirements" (page 62)
"Package Combinations" (page 64)
"Supported applications" (page 64)
"Survivability" (page 64)
"Patch Management Enhancements" (page 68)

What is Branch Office?

The Branch Office feature extends Communication Server 1000 features from a main office to one or more remote offices.

The Branch Office feature is implemented on a Branch Office Media Gateway platform (MG 1000B). The MG 1000B platform includes a MB 1000B Core connected to an IP PBX at the main office over a LAN or a WAN. This configuration enables a secondary location to centralize the call processing of its IP-based communication network. The Call Server at the main office provides the call processing for the IP Phones in both the main office and Branch Office locations. The MG 1000B Core provides call processing functionality to local digital telephones and analog devices. The MG 1000B Core also provides digital and analog trunk access to the local Public Switched Telephone Network (PSTN).

The MG 1000B platform connects to the Main Office over Virtual Trunks on a LAN/WAN. The Main Office transmits and controls IP Phone calls and IP network connections. If the Main Office fails to function, or if there is a network outage, the Server in MG 1000B Core provides service to the telephones located at the Branch Office location. This enables the IP Phones to survive the outage between the Branch Office and the Main Office.

You can configure the Media Gateway 1000B Branch Office with the following hardware configurations:

- A Server and a Gateway Controller in a Media Gateway
- Co-resident Call Server and Signaling Server (Co-res CS and SS)
- VxWorks CP PM with a Linux Signaling Server

For both hardware platforms the Main Office must use a Communication Server 1000E system, or a Communication Server 1000M CP PIV or CP PM system. The Main Office can support a combination of up to 255 of the two Branch Office hardware platforms.

You can implement the Branch Office feature as a new hardware configuration. You can also create it by converting an existing Small System to an MG 1000B platform (see “Converting a small system to a Branch Office” (page 107)). The functionality is the same in both configurations.

ATTENTION
If you have a Co-resident Call Server and Signaling Server, converting to a Branch Office is different. The procedure is the same for a CP PM VxWorks-based Calling Server migration but the Signaling Server installation is not. For more information about installing a Signaling Server, see *Signaling Server IP Line Applications Fundamentals* (NN43001-125)

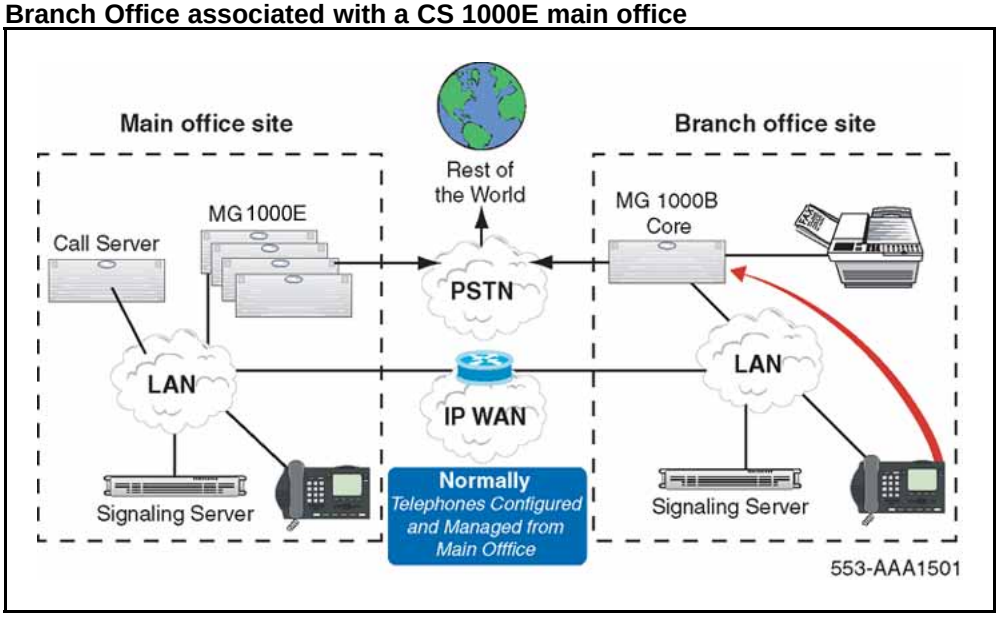
A Branch Office works with a main office only if the two offices use a common dialing plan. Any other configuration is not guaranteed to work properly. For example, as seen with the following Dialed Numbers (DN), Branch User ID is different from a DN.

31415 as DN on BO
27181 as DN on MO

Vacant number routing for Branch Office calls does not route to the Main Office properly because 31415 is sent to the network, and 27181 is not because it is configured at the Main Office. This is why it is important to have the same extensions on a phone in normal and local mode.

Figure 1 "Branch Office associated with a CS 1000E main office" (page 23) shows a Branch Office network.

Figure 1
Branch Office associated with a CS 1000E main office



Main Office and Branch Office Migration

All Main Office Call Servers in Communication Server 1000 are large system software stream based. The Main Office TN (MOTN) in a Branch Office is always set to the large system software stream MOTN.

In a Branch Office where you migrated the Main Office from an SSC to a Server, the LD 20 PRT on the branch may incorrectly display the MOTN using the small system TN format until you reenter the MOTN using the large system TN format. You must manually correct the MOTN. Therefore, you must manually change the Branch User ID, 63.20, to 96-0-3-20.

Media Gateway 1000B

The Media Gateway with Gateway Controller has a number of differences in hardware capability compared with older Branch Offices. You can use an MGC card or a CP MG card as the Gateway Controller.

The has six external Ethernet interfaces, and the CP MG has external four Ethernet interfaces. The Ethernet ports are for connecting to The ELAN and TLAN subnets of the CS 1000E system. The Ethernet interfaces on the Gateway Controller are configured to Autonegotiate mode by default. You can change the settings for ports to 100 Mbps full duplex by using the **`setup`** command.

With a properly designed data network, you can use the multiple ELAN and TLAN interfaces to implement a dual-home configuration for the MG 1000B

For the card, four Ethernet ports are accessible by using RJ-45 connectors on the faceplate. Two are reserved for ELAN and two are reserved for TLAN. For the CP MG card, two Ethernet ports are accessible by using the RJ-45 connectors on the faceplate.

Two additional Ethernet connections are available if you use a cabinet. One is reserved for ELAN and one is reserved for TLAN.

For the cabinets to break out the two additional 100BaseT Ethernet connections, you must use the 100BT Adapter (NTDW63AAE5) backplane adapter. This adapter replaces the MDF-to-AUI cable used for the 10BaseT Ethernet connection on the existing system.

One use for the additional LAN connections is to allow network redundancy, previously known as dual-homing on older Branch Offices. The Gateway Controller Ethernet interface failover occurs with the embedded Ethernet switch. The Ethernet interface failover feature requires no special network configuration to function. The customer decides if two Layer 2 switches are used to implement the feature to minimize the service outage. For more information see the *Communication Server 1000E Installation and Commissioning* (NN43041-310).

In addition, certain debug features use the LAN connections (for example, port mirroring.)

The Gateway Controller has two conference loops with thirty units each. The maximum number of participants in a conference is thirty.

The Gateway Controller has a four-character alphanumeric LED display on the faceplate. The boot and application software use the display to show diagnostic information.

The Gateway Controller has a clock reference input/output to support the requirements of the Digital Enhanced Cordless Telecommunications (DECT) standard. The DECT product requires a tight clock tolerance between cabinets with interconnected radio equipment of ±5ppm. To accommodate the tight clock tolerance, the Gateway Controller is equipped with a clock reference input/output. The clock reference input and output connections and cable detect are provided through a 15-pin DSUB connector.

Co-resident Call Server and Signaling Server

You can deploy the Co-resident Call Server and Signaling Server (Co-res CS and SS) as a Main Office or Branch Office. The Co-res CS and SS is supported on various hardware platforms, see Table 3 "Co-res CS and SS hardware platforms" (page 25).

Table 3
Co-res CS and SS hardware platforms

Co-res CS and SS hardware platform	System type
CP PM	4121
CP DC	4221
CP MG 32	4321
CP DC 128	4421
COTS	4521

The Co-res CS and SS can run on the CP PM hardware introduced in Release 5.0, however upgrades to the hardware and software are required. The CP PM card, when populated with the required 2 Gigabyte (GB) memory and 40 GB disk drive, becomes the hardware platform for the CP PM Co-res CS and SS.

The following tables show the existing Communication Server 1000 Call Server packages that are required for the Co-res CS and SS.

Table 4
MG1000B Feature Package Requirements

Package mnemonic	Package number	Package description
SOFTSWITCH	402	Soft Switch Package
Media Gateway	402	Media Gateway Package
CPP_CNI	368	CP Pentium Backplane for Intel Machine

Table 4
MG1000B Feature Package Requirements (cont'd.)

Package mnemonic	Package number	Package description
CORENET	299	CP Network
SBO	390	Branch Office Package

The Co-resident Call Server and Signaling Server supports the existing and current release call processing on a small scale. Similarly, the Signaling Server applications running on a Co-resident Call Server and Signaling Server provide the same functionality as stand–alone Signaling Server on a smaller scale. For more information about the Co-resident Call Server and Signaling Server, refer to *Co-resident Call Server and Signaling Server Fundamentals* (NN43001-509).

SIP Line Service

Geographic Redundancy (GR) and Survivable Branch Office (BO) use the Geographic Redundancy N-Way data replication model. Therefore, all Call Servers including the Main Office (MO), Geographically Redundant Main Office (GRMO), and Branch Office have the same data stored. BO SIP clients can register through the BO, MO, or GRMO depending on the failover case.

SIP Line supports both of the following configurations:

- Main Office and Branch Office configuration
- Primary Call Server (PCS), Secondary Call Server (SCS), and Survivable Media Gateway (SMG) configuration
  - — The Primary Call Server is where the Main Office is in GR/BO configuration.
  - — The Secondary Call Server is where the GR office is located.
  - — The Survivable Media Gateway is the local server in a GR N-way configuration.

The Geographically Redundant Main Office (GRMO) and the Branch Office SLGs regularly send keepalive messages. These messages are critical decision makers if incoming registrations or calls are based on the background keepalive mechanism.

Unlike UNIStim telephones, the SIP clients in the Branch Office are always redirected to the Main Office when the Main Office is available. The Branch Office SIP client cannot be forced to switch back to Local Mode. Local Mode is not displayed on SIP Line clients when they are registered locally on Branch Office.

A Proxy S1/S2 configuration mode is available to support GR/BO for SIP Line clients. For more information about the S1/S2 configuration for SIP clients, see “SIP Client configuration” (page 120).

The following sections summarize the Geographic Redundant and Branch Office operation and configuration, including normal operation and abnormal operations (for example, a given system is out of service).

Any system (X-System) is down in the following scenarios:

- The SLG proxy X-SLG is down.
- The Call Server belonging to the X-SLG is down.
- Either the ELAN or TLAN cable (or both) of the X-SLG is not plugged in.
- The ELAN cable of the Call Server belonging to the X-SLG is not plugged in.
- The PBXLink between the Call Server and the X-SLG is down.

If the Main Office system and the Branch Office system are down, any combination of the following scenario items are possible.

Scenario A: The Main Office system is down.

- The Main Office SLG is down.
- The Primary Call Server (PCS) is down.
- Either the ELAN or TLAN cable (or both) of the Main Office SLG is not plugged in.
- The ELAN cable of the PCS is not plugged in.
- The PBXLink between the PCS and the Main Office SLG is down.

Scenario B: The Branch Office system is down

- The Branch Office SLG is down.
- The Survivable Media Gateway (SMG) is down.
- Either the ELAN or TLAN cable (or both) of the Branch Office SLG is not plugged in.
- The ELAN cable of the SMG is not plugged in.
- The PBXLink between the SMG and the Branch Office SLG is down.

S1/S2 solution mode

The S1/S2 solution mode includes the following requirements for the SIP clients:

1. The SIP client must support two proxies in their outbound proxy configuration.
2. The SIP client must be able to redirect registrations (Handling “302 Moved Temporarily”).
3. The SIP client must support keepalive messages in the form of SIP PINGs. (SIP PINGs are sent from the SIP client every minute.)
4. The SIP client must be able to send the REGISTER message even though the PINGs are not responded to. (This requirement applies only to the MO-GRMO-BO deployment case.)
5. The SIP client must be able to switch to an alternate proxy in case of a PING/REGISTER timeout.

“SIP client support for S1/S2 solution mode” (page 36) shows the SIP clients and the requirements that they meet.

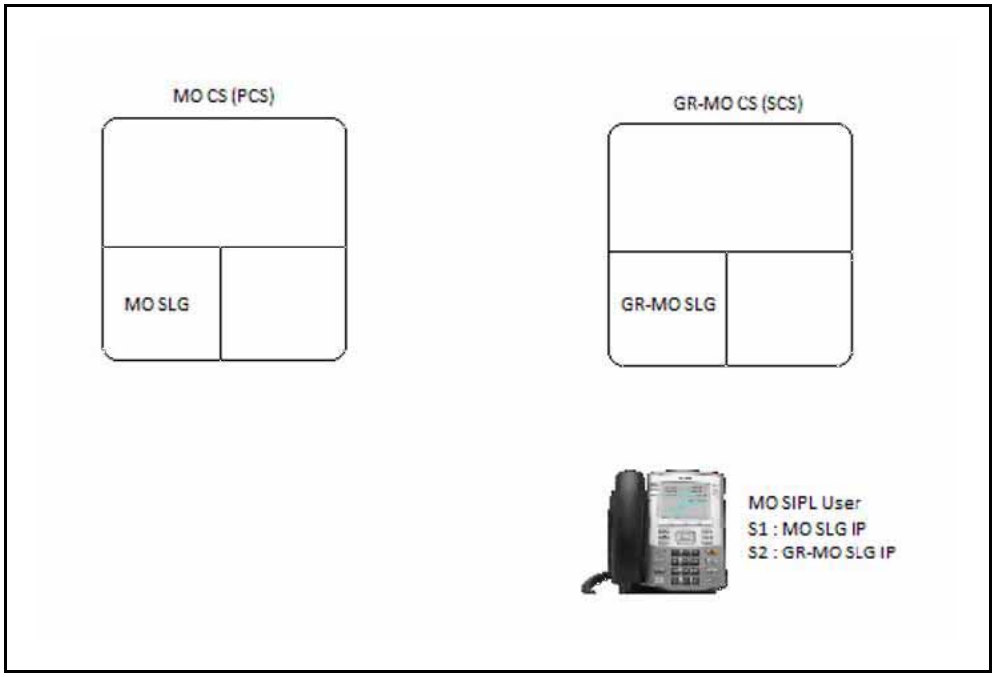
If the above requirements are met, the following redundancy deployments are available:

- “MO-GRMO or PCS-SCS deployment” (page 28)
- “MO-BO or PCS-SMG deployment” (page 31)
- “MO-GRMO-BO or PCS-SCS-SMG or GR N-way deployment” (page 32)

MO-GRMO or PCS-SCS deployment

Figure 2 "MO-GRMO or PCS-SCS deployment" (page 29) shows that the SIP client is configured with the S1 IP address pointing to the Main Office SIP Line Gateway (MO SLG) and the S2 IP address pointing to Geographically Redundant Main Office SIP Line Gateway (GRMO SLG).

Figure 2
MO-GRMO or PCS-SCS deployment



Scenario 1 (SIP client reset scenario)

The SIP client is registering to the system for the first time (that is, client power up). Both the MO and GRMO systems are up and running. (This use case also applies to the scenario where the GRMO system is down.)

1. On the SIP client reset, the client sends PING and REGISTER requests to the S1 IP address (that is, the MO SLG IP address).
2. Because the MO SLG is up and running, the MO SLG sends a 200 OK response for the PING request.
3. The MO SLG sends a 200 OK response for the REGISTER request after the authentication process.
4. The SIP client configures the MO SLG as its active proxy. After this configuration, incoming requests are received from this active proxy and any outgoing responses are sent to this active proxy.
5. The SIP client maintains regular keepalive messages with the active proxy in the form of PING requests.
6. The SIP client maintains registration refreshes with the active proxy before registration timer expiry.

Scenario 2 (SIP client reset scenario)

The SIP client is registering to the system for the first time (that is, client power up). The MO system is down; however, the GRMO SLG is up and running.

1. On the SIP client reset, the client sends a PING/REGISTER request to the S1 IP address (that is, the MO SLG IP address).
2. The MO SLG is down. No response is sent back to the client for the PING/REGISTER request.
3. The SIP client times out on the PING request. The client then switches to alternate proxy S2 IP address (that is, the GRMO SLG IP address) and sends a PING/REGISTER request to the S2 IP address.
4. The GRMO SLG is aware that MO SLG is down, so it sends a 200 OK response for the PING request.
5. The GRMO SLG sends a 200 OK response for the REGISTER request after the authentication process.
6. The SIP client configures the GRMO SLG as its active proxy. After this configuration, incoming requests are received from this active proxy and any outgoing responses are sent to this active proxy.
7. The SIP client maintains regular keepalive message with the active proxy in the form of PING requests.
8. The SIP client maintains registration refreshes with the active proxy before registration timer expiry.

Scenario 3

The SIP client is currently registered to the MO SLG but the MO system goes down. GRMO system is up and running.

1. The SIP client sends a PING/REGISTER request to the S1 IP address (that is, MO SLG IP address) at regular intervals.
2. When MO SLG goes down, no response is sent back to client for the PING/REGISTER request.
3. The SIP client times out on the PING request. The client then switches to the alternate proxy S2 IP address (that is, the GRMO SLG IP address) and sends a PING/REGISTER request to the S2 IP address.
4. The GRMO SLG is aware that MO SLG is down, so it sends a 200 OK response for the PING request.
5. The GRMO SLG sends a 200 OK response for the REGISTER request after the authentication process.

6. The SIP client configures the GRMO SLG as its active proxy. After this configuration, incoming requests are received from this active proxy and any outgoing responses are sent to this active proxy.
7. The SIP client maintains regular keepalive messages with the active proxy in the form of PING requests.
8. The SIP client maintains registration refreshes with the active proxy before registration timer expiry.

Scenario 4

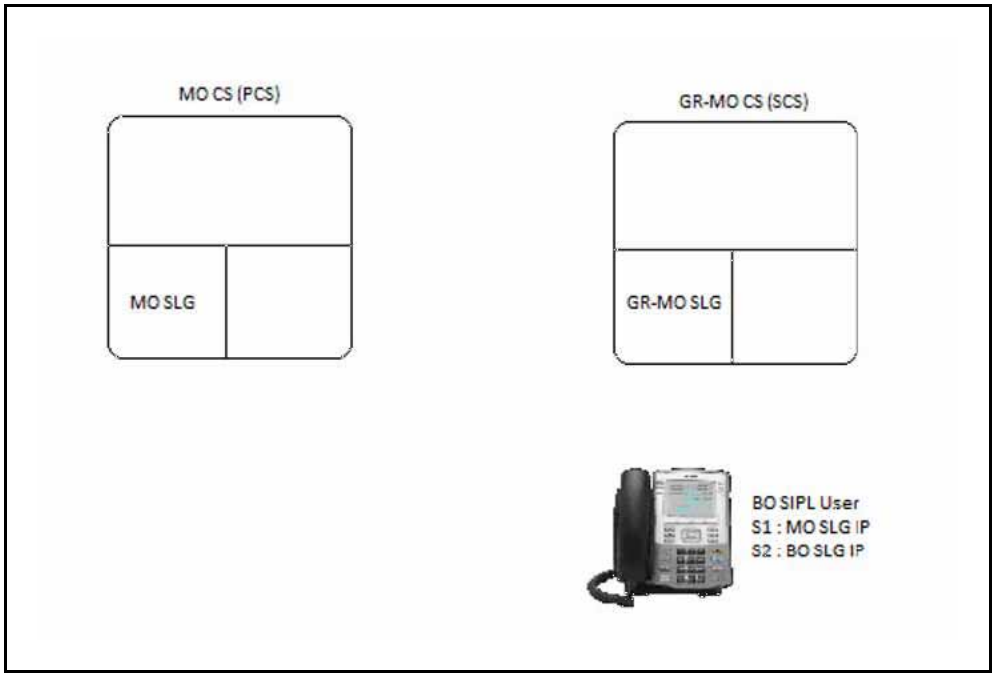
The SIP client is currently registered to GRMO SLG. The MO system comes back into service. The GRMO system is up and running.

1. The SIP client sends a PING/REGISTER request to the S2 IP address (that is, the GRMO SLG IP address) at regular intervals.
2. When the MO SLG is up, GRMO SLG starts ignoring the PING requests.
3. The GRMO SLG sends a 302 Moved Temporarily response for the REGISTER request from the client. This SIP message contains the contact header set to MO SLG IP address (for redirecting).
4. The SIP client receives the 302 Moved Temporarily and redirects the REGISTER request to MO SLG.
5. The MO SLG sends a 200 OK response for the REGISTER request after the authentication process.
6. The SIP client configures the MO SLG as its active proxy. After this configuration, incoming requests are received from this active proxy and any outgoing responses are sent to this active proxy.
7. The SIP client maintains regular keepalive messages with the active proxy in the form of PING requests.
8. The SIP client maintains registration refreshes with the active proxy before registration timer expiry.

MO-BO or PCS-SMG deployment

Figure 3 "MO-BO or PCS-SMG deployment" (page 32)shows that the SIP client is configured with the S1 IP address pointing to the Main Office SIP Line Gateway (MO SLG) and the S2 IP address pointing to Geographically Redundant Main Office SIP Line Gateway (GRMO SLG).

Figure 3
MO-BO or PCS-SMG deployment

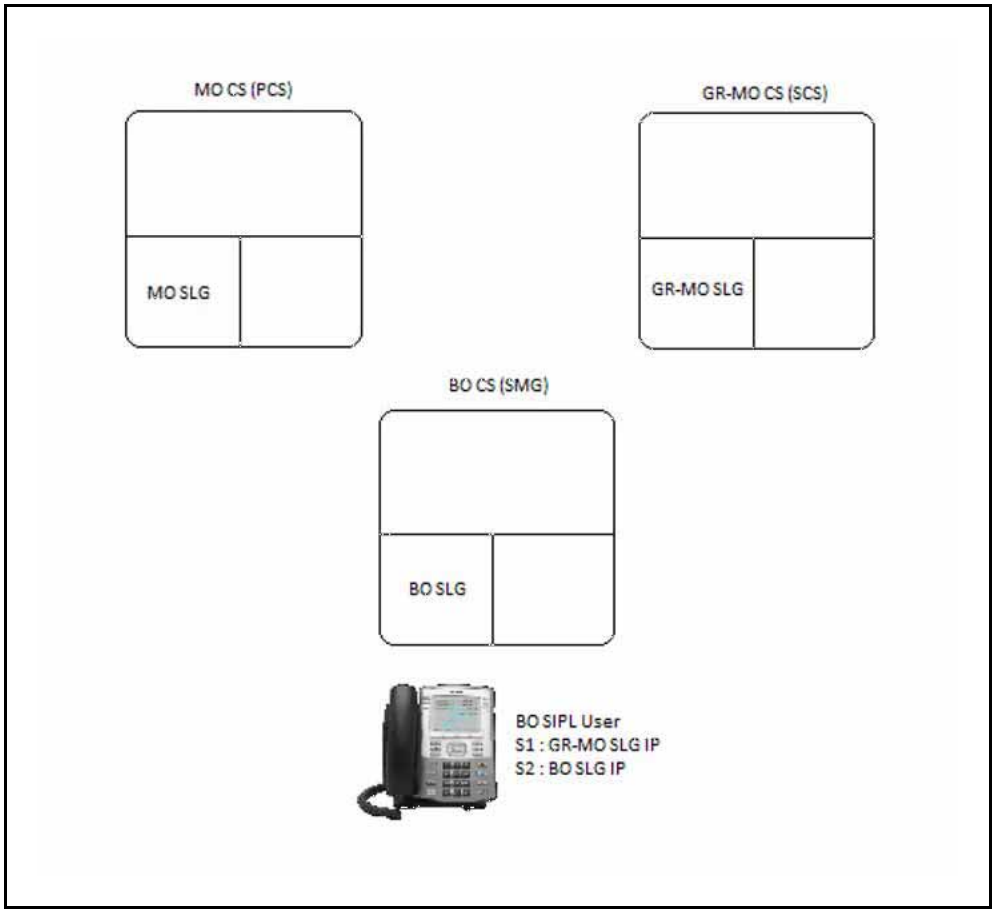


Note: The use cases for the MO-BO deployment are exactly the same as that of MO-GRMO deployment.

MO-GRMO-BO or PCS-SCS-SMG or GR N-way deployment

Figure 4 "MO-GRMO-BO or PCS-SCS-SMG or GR N-way deployment" (page 33) shows that the SIP client is configured with the S1 IP address pointing to Geographically Redundant Main Office SIP Line Gateway (GRMO SLG) and the S2 IP address pointing to the Branch Office SIP Line Gateway (BO SLG).

Figure 4
MO-GRMO-BO or PCS-SCS-SMG or GR N-way deployment



In this deployment, there is a limitation that the GRMO and BO system cannot be down at the same time. At least one system must be up and running to facilitate redirection (since the purpose of geographic redundancy is to handle network outage, not server failures). Single server failures must be handled using the server redundancy feature. As a result, this limitation can be overcome by implementing both server redundancy and geographic redundancy.

Scenario 1 (SIP client reset)

The SIP client is registering to the system for the first time. The BO system is down.

1. The SIP client sends a PING/REGISTER request to the GRMO SLG.
2. The GRMO SLG is aware that MO-SLG is up, so the GRMO SLG ignores the PING request.

3. The GRMO SLG responds with a 302 Moved Temporarily for the REGISTER request. The contact header of this SIP message contains the redirection IP address (that is, the MO SLG).
4. The SIP client redirects the REGISTER message to the MO SLG.
5. The MO SLG responds back with a 200 OK for the REGISTER request after the authentication process.
6. The SIP client configures the MO SLG as its active proxy. After this configuration, incoming requests are received from this active proxy and any outgoing responses are sent to this active proxy.
7. The SIP client maintains regular keepalive message with the active proxy in the form of PING requests.
8. The SIP client maintains registration refreshes with the active proxy before registration timer expiry.

Scenario 2 (SIP Client reset)

The SIP client is registering to the system for the first time. The GRMO system is down.

1. The SIP client sends a PING/REGISTER request to the GRMO SLG.
2. The GRMO SLG is down, so no response is sent back to the client for PING/REGISTER request.
3. The SIP client times out on the PING request. The client then switches to the alternate proxy (that is, the BO SLG) and sends a PING/REGISTER request to the BO SLG.
4. The BO SLG is aware that MO-SLG is up, so it ignores the PING request.
5. The BO SLG responds with a 302 Moved Temporarily for the REGISTER request. The contact header of this SIP message contains the redirection IP address (that is, the MO SLG).
6. The SIP client redirects the REGISTER message to the MO SLG.
7. The MO SLG responds with a 200 OK for the REGISTER request after the authentication process.
8. The SIP client configures the MO SLG as its active proxy. After this configuration, incoming requests are received from this active proxy and any outgoing responses are sent to this active proxy.
9. The SIP client maintains regular keepalive messages with the active proxy in the form of PING requests.
10. The SIP client maintains registration refreshes with the active proxy before registration timer expiry.

Scenario 3 (SIP Client reset)

The SIP client is registering to the system for the first time. The MO system is down. (This use case scenario also applies to when the MO and BO systems are down.)

1. The SIP client sends a PING/REGISTER request to the GRMO SLG.
2. The GRMO SLG is aware that MO SLG is down, so it sends a 200 OK response for the PING request.
3. The GRMO SLG responds with a 200 OK for the REGISTER request after the authentication process.
4. The SIP client sets the GRMO SLG as its active proxy. After this configuration, incoming requests are received from this active proxy and any outgoing responses are sent to this active proxy.
5. The SIP client maintains regular keepalive messages with the active proxy in the form of PING requests.
6. The SIP client maintains registration refreshes with the active proxy before registration timer expiry.

Scenario 4 (SIP client reset)

The SIP client is registering to the system for the first time . The MO and GRMO systems are down.

1. The SIP client sends a PING/REGISTER request to GRMO SLG.
2. The GRMO SLG is down so no response is sent back to the client for the PING/REGISTER request.
3. The SIP client times out on the PING request. The client then switches to the alternate proxy (that is, the BO SLG) and sends a PING/REGISTER request to the BO SLG.
4. The BO SLG is aware that MO SLG is down so it sends a 200 OK response for the PING request.
5. The BO SLG responds with a 200 OK for the REGISTER request after the authentication process.
6. The SIP client configures the BO SLG as its active proxy. After this configuration, incoming requests are received from this active proxy and any outgoing responses are sent to this active proxy.
7. The SIP client maintains regular keepalive messages with the active proxy in the form of PING requests.
8. The SIP client maintains registration refreshes with the active proxy before registration timer expiry.

Other scenarios

Use cases for the following scenarios are similar:

- The SIP client is currently registered on the MO SLG and the MO SLG goes down. The SIP client registers to the GRMO SLG.
- The SIP client is currently registered on the GRMO SLG and the GRMO SLG goes down. The SIP client registers to the BO SLG.
- The SIP client is currently registered on the BO SLG and the GRMO SLG comes back in service. The SIP client registers to the GRMO SLG.
- The SIP client is currently registered on GRMO SLG and the MO SLG comes back in service. The SIP client registers to the MO SLG.

SIP client support for S1/S2 solution mode

Table 5 "SIP client support for S1/S2 solution mode" (page 36) shows the features supported by the SIP clients.

Table 5
SIP client support for S1/S2 solution mode

Feature \ Client	Nortel IP Phone 1120E and 1140E	ipDialog (SIPTone V)	Teledex 4200 (with display)	Nortel IP Softphone 3456
Support for S1/S2 solution mode	Yes	Yes	No	No
Support for registration redirection	Yes	Yes	No	No
Registration timer	1 hour to 31 days	1 second to unlimited	300 seconds to 1 hour	Unlimited
Transport	UDP	TLS/UDP	TCP/UDP (TLS option can be selected from the Web user interface; however, TLS support is not yet available.)	TLS/TCP/UDP

Local Mode

Unlike the operation of UNIStim telephones, SIP Line does not support the force switch to Local Mode operation. If the Main Office is active, SIP Line remains registered at the Main Office. There is no Local Mode display on SIP Line client when it is registered locally at Branch Office.

UEXT configuration

The SIP Line operation in the Main Office and Branch Office (MO/BO) configuration and the Primary Call Server, Secondary Call Server, and Survivable Media Gateway (PCS/SCS/SMG) configuration relies on Geographic Redundancy N-Way data replication model. No extra configuration is required for clients on the Branch Office or Survivable Media Gateway. Although the Branch User ID (BUID) and Main Office TN (MOTN) are prompted in LD 11, they are used by SIP Line.

IP Telephony node

The node represents a group of physical servers that share the same configuration properties. The same set of services are configured and enabled on all physical servers within a node.

IP Telephony Node Management

A node is defined as a collection of Signaling Servers. Each node in the network has a unique Node ID. This Node ID is an integer value. A node has only one Primary Signaling Server. All other Signaling Servers are defined as Followers. Node management introduces the cluster concept where a cluster represents a group of physical servers that share the same configuration properties. The same set of services are configured and enabled on all physical servers within a cluster (node).

The nodes provide scalability by deploying multiple nodes and optionally load sharing by distributing processing to other node members. Each node belongs to a Call Server and has a one-to-many relationship with the Call Server. The IP nodes reside on two LAN subnets: ELAN and TLAN. The administrator can add several Signaling Servers to the node but must have a minimum of one Signaling Server as a node element. All the node elements also contain the same set of enabled application services; however, only one physical server can be active at a time. This active server can run all the configured services on that physical server; for example, UNIStim LTPS, SIPGw, and H323Gw can all be configured and enabled on the same server. The LTPS application is one exception where several servers can run active instances of LTPS service. The LTPS application does support load sharing.

The Centralized Deployment Manager (CDM) deploys software applications from Unified Communication Management (UCM). The node management interface in Element Manger is used to add servers to a node

from the list of servers that UCM has learned. Before you add the servers to a node, it is required that the CDM feature deploys the necessary software applications to each of the Linux servers.

For more information about configuring IP Telephony nodes using Element Manager, see *Signaling Server IP Line Applications Fundamentals* (NN43001-125)

IP Telephony Node Management

The IP Telephony Node Management includes the overall status of the nodes and other functions such as import and export.

The nodes provide scalability (by deploying multiple nodes) and optionally load sharing (by distributing processing to other node members).

The node must designate a minimum of one server as a node element for that node to operate. The administrator can add as many servers as part of the Node. All the node elements have the same set of application services enabled, however, only one physical server can be active at a time.

The active server can run all configured services on the physical server; for example, an administrator can configure and enable UNIStim LTPS, SIPGw, and H.323Gw on the same server.

Note: The LTPS application supports load sharing. The LTPS application is the exception by where several servers can run active instances of the LTPS service.

ATTENTION
The SIP Line application in Release 6.0 cannot co-reside with LTPS or any other virtual trunk applications like SIPGw or H.323Gw. The node management interface does not allow you to configure SIP Line service with any other application services.

Zone Based Dialing

The primary objective of the Zone Based Dialing (ZBD) is to remove the traditional nodal PBX networks and replace them with a single or a few high-capacity soft switches and branch gateways for PSTN access. New customers, who plan to set up private networks in multiple locations, can deploy the ZBD.

The migration is transparent to the users, that is, the private and public (E.164) dial plans and features are retained.

Switching to a ZBD requires development on dial plans, numbering plans and routing features to make sure that the migration is transparent to the enterprise network users and that the same dial plan and business grade telephony features are used.

Gateway Controller serial ports

Each Gateway Controller installed in a Media Gateway provides the opportunity for three remote Serial Data Interfaces (SDI). The maximum number of TTYs remains unchanged. Therefore, after you configure the maximum, additional support is unavailable for TTYs.

The Gateway Controller has three SDI ports; SDI0, SDI1, and SDI2.

You can use SDI ports for local debugging; or, you can configure the ports in the MG 1000B Call Server as system terminals in LD 17.

During the initial configuration of the Gateway Controller, you must connect to either SDI0 or SDI1 to access the installation menu. Only SDI0 has full modem support, as SDI1 and SDI2 have no hardware flow control (limitation of the three-port cable).

SDI2 is not available during the Gateway Controller bootup; therefore, you cannot use it to access the installation menus.

There are no DIP switches are on the Gateway Controller for configuring the baud rate of SDI0.

Single CPU Implications

Single CPU installations do not require dynamic binding of TTY ports to the active CPU because only one CPU exists. Therefore, single-CPU installations can use the Server TTY ports or the Gateway Controller remote TTY ports.

Gateway Controller serial port default configuration

The default settings for the serial ports are as follows:

- Baud rate = 9600
- Number of data bits = 8
- Number of stop bits = 1
- Parity = none
- Flow control = none

Gateway Controller serial ports configuration change in Overlay 17

If you configure the Gateway Controller serial ports as SL1 terminals on the Call Server, then the baud rate, number of data bits, number of stop bits, parity, and flow control are configured in LD 17.

Values configured in LD 17 are downloaded to the Gateway Controller and override the default values. The downloaded values are stored on the Gateway Controller and persist over restarts and power outages. When the serial port baud rate changes, a system message indicates the change.

CEMux Support

Cabinet and chassis CEMux type cards are supported in a MG 1000B. The list of supported cards is as follows.

Table 6
CEMux Packs and daughter boards supported in MG 1000B

Pack	Daughterboard	IP expansion CEMux Application
1.5 MB DTI/PRI (NTAK09)	DCHI (NTAK93)	Nondownloadable DCH
	DDCH (NTBK51)	Downloadable DCH
	CC (NTAK20)	Clock controller (stratum 3/4)
1.5 MB TMDI (NTRB21)	CC (NTAK20)	Downloadable DCH, clock controller (stratum 3/4)
2.0 MB DTI (NTAK 10)	N/A	Clock controller (stratum 3/4)
2.0 MB PRI (NTAK79)	N/A	Clock controller (stratum 3/4), nondownloadable DCH
2.0 MB PRI (NTBK50)	DDCH (NTBK51)	Downloadable DCH
	CC (NTAK20	Clock controller (stratum 3/4)
MISP (NTBK22)	CC (NTAK20)	MISP BRI processor, clock controller (stratum 3/4)
SDI_DCH (NTAK02)	N/A	Only DCH is supported
SSTD (NTAK03) not supported	N/A	N/A
Card Option Mail not supported	N/A	N/A

Attempts to install unsupported CEMux packs or to configure an unsupported application are blocked.

Support of CEMux requires Communication Server 1000 Release 5.5 or later Softswitch software and a Gateway Controller. It is supported by all MG 1000B systems.

Features supported by Option 11C SIPE related to CEMux are supported in MG 1000B, which includes support for nB+D by having single D-Channel support trunk packs in separate MG1000Bs.

The TMDI D-Channel ISM used on small systems IS NOT included for the MG 1000B. D-Channels configured or removed for TMDI cards increment the existing large system software based DCH ISM. The maximum number of D-Channels, which is 255, supported with MG 1000B in Communication Server 1000 Release 5.5 or later, matches that of the Communication Server 1000M large systems.

For BRI, you must provision the MISP and the SILC/UILC in the same Media Gateway. This is the only supported configuration.

Clock References

With CEMux support, you can configure digital trunks and the clock controller in the Media Gateway. Each Media Gateway that contains a digital trunk card requires a clock controller on that shelf. You cannot use clock references across Media Gateways, and you can configure only one clock controller for every shelf.

Main office hardware description

The Main Office must be one of the following systems:

- CS1000E
- CS1000M

The diagrams throughout this document show a Communication Server 1000E Main Office. All of the systems appearing in the list perform identical Main Office functions as far as the Branch Office feature is concerned.

MG 1000B platform hardware description

The MG 1000B basic hardware consist of a Media Gateway cabinet or chassis, a Gateway Controller, a Call Server, and a Signaling Server.

MG 1000B for Release 7.0 supports the Co-resident Call Server and Signaling Server (Co-res CS & SS), an option in which both the Call Server software and the Signaling Server software run on the same hardware platform. The Call Server and Signaling Server, on separate Intel Pentium processor-based hardware platform remains a supported and available option.

The Gateway Controller can provide Digital Signal Processor (DSP) resources. The CP MG card is available with 32 or 128 non-removable DSP ports. The card provides two expansion slots for installing DSP

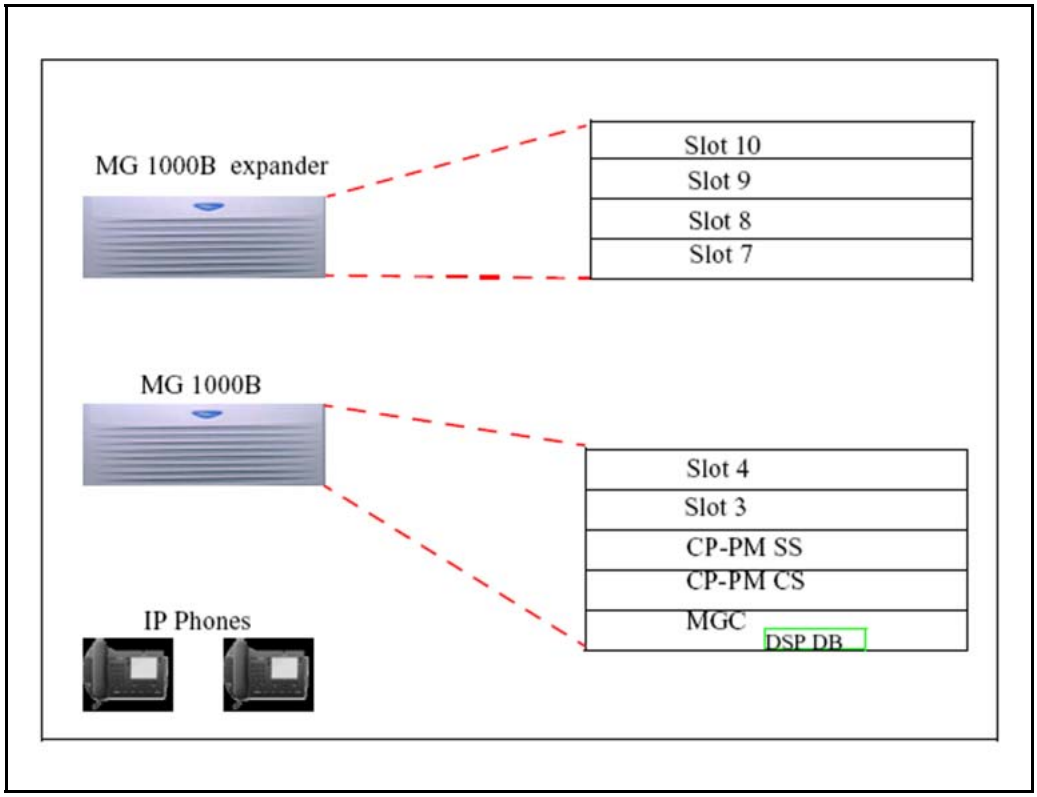
Daughterboards (DSP DB). The DSP DB are available three capacities. A 32-port DSP DB (DB-32), a 96-port DSP DB (DB-96), and a 128-port DSP DB (DB-128). These DSP DB can be installed on the card to provide DSP resources to transcode between IP and TDM devices. DSP ports reduce the need to install Voice Gateway Media Cards within the Branch Office, saving slots, and reducing costs. The addition of the DSP DB into an MG 1000B system does not limit the use of Voice Gateway Media Cards, either for DSP-only functionality or for the full IP Line application within the same system.

Support exists for the following DSP configurations:

- a system with a CP MG 32
- a system with a CP MG 128
- a system with a card without DSP DBs and Voice Gateway Media Cards
- a system with a card with DSP DBs (any combination of DSP DB in the two expansion slots)
- a system with a Gateway Controller and Voice Gateway Media Cards.

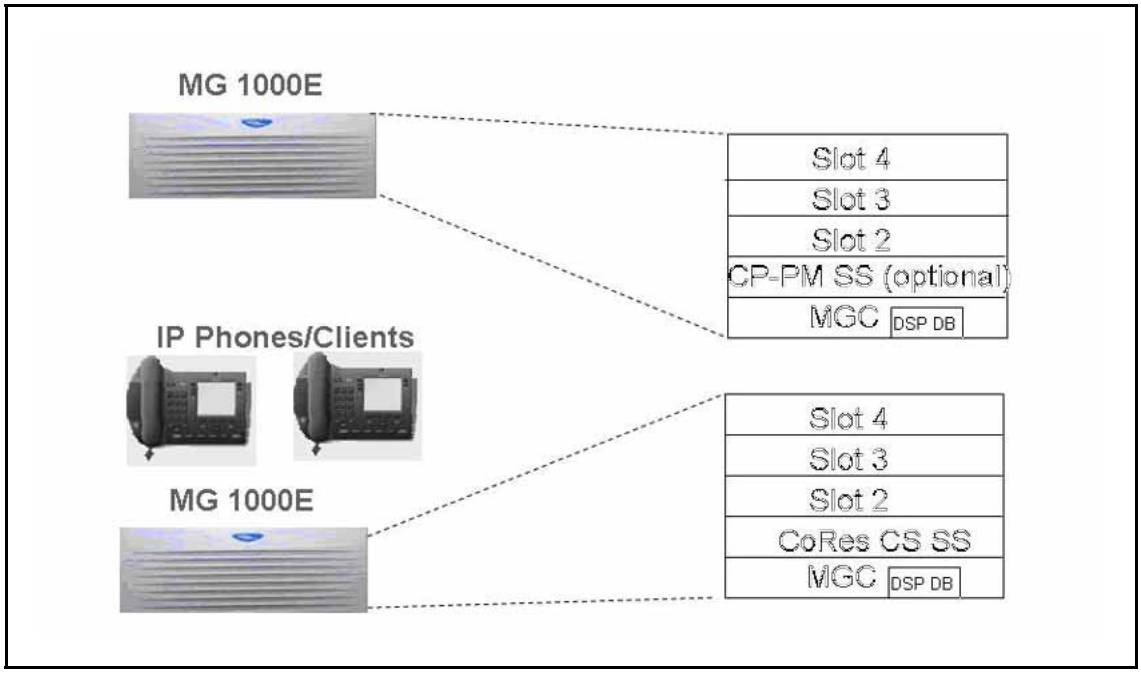
The following figure shows an example of a Branch Office Communication Server 1000E with a CP PM Call Server, CP PM Signaling Server, and a card with DSP DB as the Gateway Controller. The following examples show a Chassis and Chassis Expander, but you can also use an MG 1010 Chassis.

Figure 5
Communication Server 1000 MG 1000B system



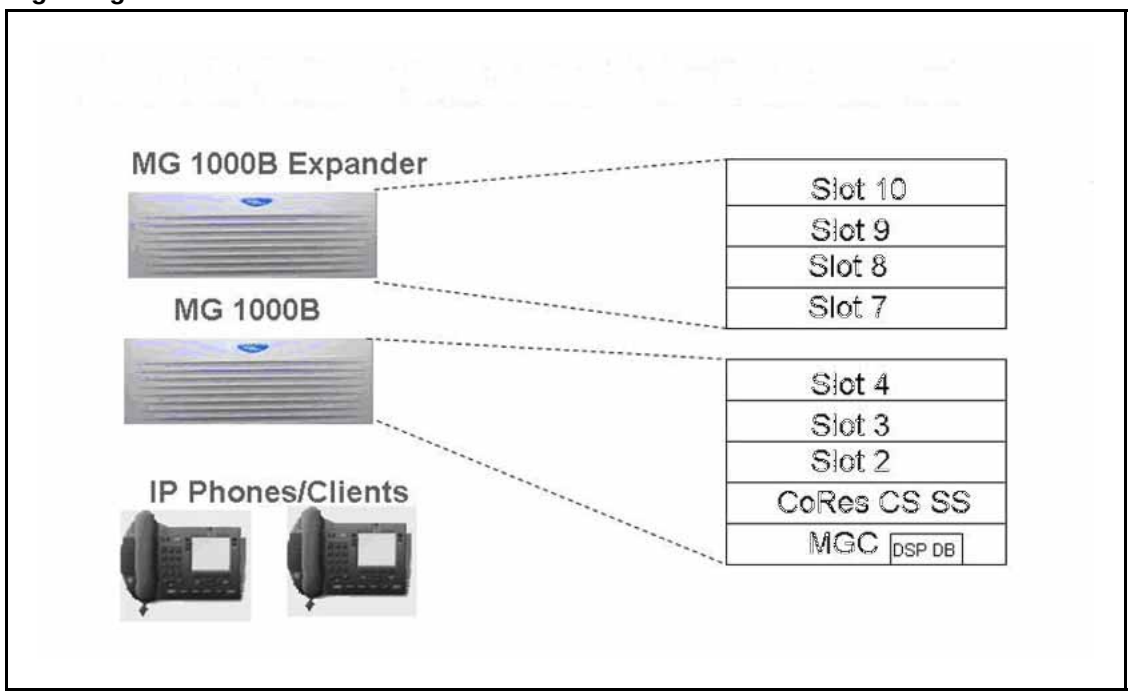
The following figure shows an example of Communication Server 1000E with CP PM based Co-resident Call Server and Signaling Server.

Figure 6
Communication Server 1000E with CP PM Co-resident Call Server and Signaling Server



The following figure shows an example of a Branch Office (MG 1000B) with a CP PM based Co-resident Call Server and Signaling Server.

Figure 7
Communication Server 1000 MG 1000B System with CP PM Co-resident Call Server and Signaling Server



Communication Server 1000 Release 7.0 continues to support the legacy Branch Office configuration that uses the SSC processor and Release 5.0 or 5.5 software. Nortel no longer sells the SSC based-Branch Office.

Various hardware platforms are supported as Signaling Servers. CS 1000 Release 7.0 supports the following hardware as Signaling Servers:

- CP PM card
- CP DC card
- Commercial-off-the-shelf (COTS) servers

Note 1: The HP DL320 G4 and IBM x306m (COTS1) servers are not supported for the CS 1000 Release 7.0 Co-res CS and SS configuration.

Note 2: The ISP1100 hardware platform is not supported in Communication Server 1000 Release 6.0 or later.

An MG 1000B platform can be a new hardware configuration. It can also be a small system platform converted to an MG 1000B platform. In the latter case, the cabinet or chassis performs the same functionality as the MG 1000B Core, and the optional chassis expander performs the same functionality as the MG 1000B Expander. Refer to “Converting a small system to a Branch Office” (page 107) for more information.

After you convert an MG 1000B platform, the small system cabinet or chassis is referred to as an MG 1000B Cabinet or MG 1000B Chassis, as applicable. The optional chassis expander is referred to as the "MG 1000B Chassis Expander.

Throughout this document, the term MG 1000B Core can refer to any Media Gateway, including a converted small system, unless otherwise indicated. Also, the term MG 1000B Expander can refer to an MG 1000B Chassis Expander.

MG 1000B Core

The MG 1000B Core provides access to the local PSTN for users in the Branch Office. It also provides support for digital telephones and analog devices, such as fax machines and analog (500/2500-type) telephones in the Branch Office.

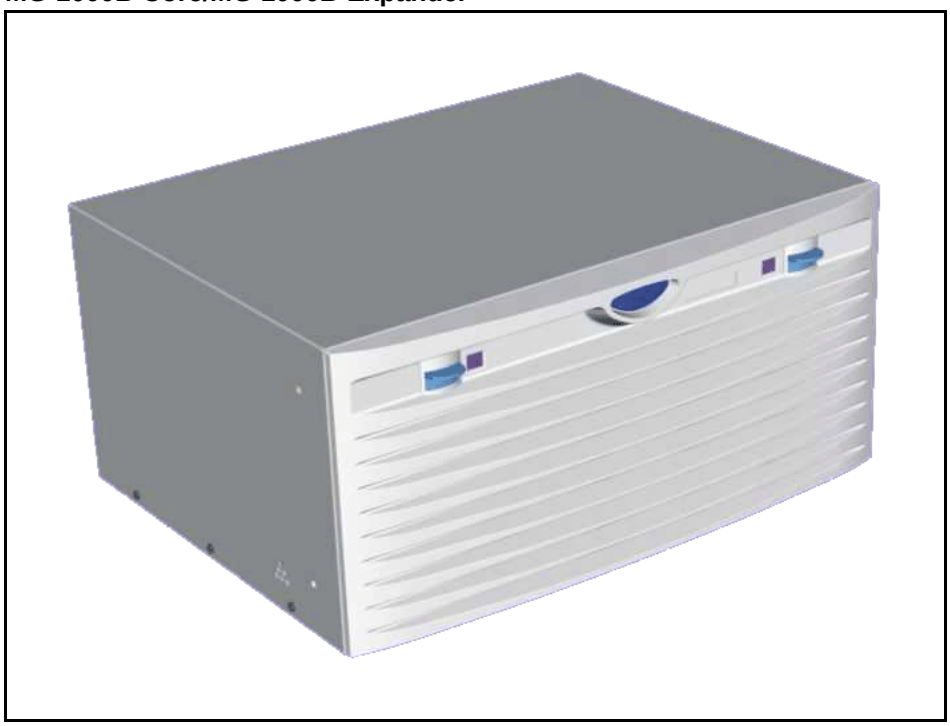
The MG 1000B Core capacity is a maximum 128 TDM sets (a single MG1000B and MB1000B expander). See Figure 8 "MG 1000B Core/MG 1000B Expander" (page 46).

The MG 1000B Core must contain a Server and a Gateway Controller. The Server provides telephony services to elements at the Branch Office, such as digital telephones, analog devices, digital trunks, and analog

trunks. The Server also provides call processing services to IP Phones when the phones are registered to the MG 1000B Core (Local Mode). The MG 1000B Core provides a dedicated slot (slot 0) for the Gateway Controller. The software feature set on the MG 1000B Server can differ from the CS 1000E Server at the main office.

Figure 8 "MG 1000B Core/MG 1000B Expander" (page 46)shows an MG 1000B Core/MG 1000B Expander.

Figure 8
MG 1000B Core/MG 1000B Expander



MG 1000B Chassis

CEMux packs are supported in card positions 1 to 4 of an MG 1000B chassis. They are not supported in the MG 1000B chassis expander.

Card slots

The Table 7 "Card slots for MG 1000B" (page 47) shows the card slot assignments for all configurations of the MG 1000B Core and MG 1000B Expander (discussed in “MG 1000B Expander” (page 49)).

Table 7
Card slots for MG 1000B

MG 1000B Configuration	Main Cabinet/Chassis				Expander Chassis		
	Cabinet Chassis PEC	Total slots	Gateway Controller slot #	Usable slot #s	Cabinet Chassis PEC	Total slots	Usable slot #s

Table 7
Card slots for MG 1000B (cont'd.)

MG 1000 Cabinet MG 1000 Chassis	NTAK11 NTDU14	11 5	0 0	1-10 1-4	N/A NTDU15	N/A 4	N/A 7-10
Mini Chassis	NTDK91	4	0	1-3 (see note 1)	NTDK92	4	7-10
MG1010 Chassis	NTC310	13	0	1-10, 22,23 (see note 2)	N/A	N/A	N/A
Note 1: **On a converted CS 1000 Mini Systems, slot 4 is dedicated to the 48-Port Digital Line Card (DLC). If you do not require the 48-Port DLC, you can cover it with a double-slot card inserted in slot 3.** **Note 2: The MG1010 chassis slots 22 and 23 are dedicated slots for CP PM and CP DC cards.**							

For more information on media gateway card slots, see *Communication Server 1000E Planning and Engineering* (NN43041-220).

In Table 7 "Card slots for MG 1000B" (page 47), the term "usable" denotes those card slots which are not reserved for, or dedicated to, a specific card type. The following circuit cards can be installed in any usable slot:

- Voice Gateway Media Cards
- Digital Trunk cards
- Analog Trunk cards
- Analog Line cards
- Digital Line cards
- Nortel Integrated Recorded Announcer card
- Nortel Integrated Conference Bridge card
- cards to support CallPilot Mini or CallPilot 201i
- Server cards

The Voice Gateway Media Cards act exclusively as Voice Gateway Media Cards on the MG 1000B platform.

Note: Voice Gateway Media Cards have no LTPS application on board in Communication Server 1000 Release 6.0 and later.

MG 1000B Expander

The chassis expander can be connected to the chassis through two copper cables to provide 4 additional card slots with the following limitations:

- Digital trunk cards are not supported in the MG 1000B Expander.
- The MG 1000B Expander is connected to the MG 1000B Core with copper wire. Therefore, the back of the MG 1000B Expander does not have an Ethernet port.

Figure 8 "MG 1000B Core/MG 1000B Expander" (page 46) shows the MG 1000B Expander. Table 7 "Card slots for MG 1000B" (page 47) shows the card slots for the MG 1000B Expander.

The MG 1010 provides 13 slots and does not require or support an Expander.

Signaling Server

The Signaling Server is required for the Branch Office feature. It provides the following functions:

- IP Peer Networking, incorporating:
  - SIP and H.323 Gateways
  - Network Routing Service (NRS), consisting of:
    - SIP Redirect Server
    - H.323 Gatekeeper
    - Network Connection Service (NCS)
- IP Phone registration to the IP Phone Terminal Proxy Server (TPS) during Local Mode for survivability
- Web server for Element Manager and NRS Manager

A second Signaling Server can be used to provide redundancy in the case of a failure in the other Signaling Server at the Branch Office. The NRS must reside on the Leader Signaling Server. Only failsafe is allowed on Branch Office.

A network requires one NRS. However, Nortel recommends that an Alternate NRS, and in some cases at least one Failsafe NRS, be configured in the network. In a Branch Office network, configuring a Primary or Alternate NRS at a Branch Office location is not appropriate due to possible network outages. For maximum coverage, Nortel recommends that a Failsafe NRS be configured at each Branch Office location that is not otherwise configured with a Primary or Alternate NRS.

In a SIP-enabled system, the Signaling Server supports only en bloc signaling.

In an H.323-enabled system, the Signaling Server supports both en bloc and overlap signaling. En bloc signaling is standard. If overlap signaling is to be used, Nortel highly recommends that it be installed and enabled on all Signaling Servers in the network. Failure to do so results in delays in call completion due to overlap to en-bloc conversion.

For more information on the Signaling Server, refer to *Signaling Server IP Line Applications Fundamentals* (NN43001-125). For more information on SIP, H.323, and overlap signaling, refer to *IP Peer Networking Installation and Commissioning* (NN43001-313).

The NCS is required to provide the Main Office Node IP's actual status. The redirection procedure cannot be performed without the NCS. Interaction with the NCS Branch Office requires the same H.323 ID to be configured for each Branch Office node element (CP PM). This H.323 ID exists in the NCS (NRS H.323 Gatekeeper) Database. If there is no H.323 ID in the NCS database, the NCS ignores the request for translation from the Branch user ID (BUID) into associated Main office node IP. For more information on the NCS, refer to "MG 1000B Core interoperability" (page 83) and "Adding the Branch Office endpoints to the NRS database" (page 175).

Network Routing Service (NRS)

The NRS application provides network-based routing, combining the following into a single application:

- **H.323 Gatekeeper** — provides central dialing plan management and routing for H.323-based endpoints and gateways.
- **SIP Redirect Server** — provides central dialing plan management and routing for SIP-based endpoints and gateways.
- **NRS Database** — stores the central dialing plan in XML format for both the SIP Redirect Server and the H.323 Gatekeeper. The SIP Redirect Server and the H.323 Gatekeeper accesses this common endpoint and gateway database.
- **Network Connect Server (NCS)** — used only for Media Gateway 1000B (MG 1000B), SRG, Geographic Redundancy and Virtual Office solutions. The NCS allows the Line TPS (LTPS) to query the NRS using the UNIStim protocol.
- **NRS Manager web interface** — the NRS provides its own web interface to configure the SIP Redirect Server, the H.323 Gatekeeper, and the NCS.

The NRS application provides routing services to both H.323 and SIP-compliant devices. The H.323 Gatekeeper can be configured to support H.323 routing services, while the SIP Redirect Server can be configured to support SIP routing services. The H.323 Gatekeeper and the SIP Redirect Server can reside on the same Signaling Server.

Each system in an IP Peer network must register to the NRS. The NRS software identifies the IP addresses of systems based on the network-wide numbering plan. NRS registration eliminates the need for manual configuration of IP addresses and numbering plan information at every site.

When configuring the NRS it is necessary to enable the NCS. Ensure the check box "Network Connection Server enabled" is checked in the NRS configuration window of Communication Server 1000 Element Manager.

For information on configuring the NRS, refer to *Network Routing Service Installation and Commissioning* (NN43001-564).

Telephones

The Branch Office supports IP Phones as detailed in *IP Phone Fundamentals* (NN43001-368), and analog and digital telephones as detailed in *Telephones and Consoles Fundamentals* (NN43001-567).

Throughout this document, the telephones are referred to collectively as IP Phones. IP Phones in the Branch Office are referred to as Branch Users.

In an H.323-enabled system, the IP Phones are provisioned in the Branch Office using Set-Based Installation, Command Line Interface (CLI) overlays, Element Manager (EM), or Subscriber Manager (SM).

Firmware download

The Enhanced UniStim Firmware Download for IP Phones feature provides an improved method of delivering new firmware to Nortel IP Phones.

For further information on the Enhanced UniStim Firmware Download for IP Phones feature, refer to *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

Voice Gateway Media Card

The MG 1000B uses the large system TN format (loop shelf side card) and the phones are configured with this format.

> ***Note:*** In Communication Server 1000 Release 6.0 and later, the MC32S and the Voice Gateway Media Card 32 (MC32) cards are supported. The Internet Telephony Gateway-P (ITP-P) card is not supported.

For more information, about Voice Gateway Media Card and IP Phone configuration, see*Signaling Server IP Line Applications Fundamentals* (NN43001-125) or *Circuit Card Reference* (NN43001-311).

The Voice Gateway Media Card provides a pool of Digital Signal Processor (DSP) ports for media transcoding between IP voice packets and circuit-switched resources. The card comes equipped with DSP modules. Each call between an IP Phone and an analog (500/2500-type) or digital telephone or the PSTN uses one DSP port. Calls between two IP Phones do not require any DSP ports, as there is no need for IP-to-circuit-switched transcoding.

Voice Gateway Media Cards provide echo cancellation, compression, and decompression of voice streams.

A Gateway Controller with DSP resources also acts as a Voice Gateway Media Card and provides the same features described previously. Therefore, a MC32S or MC32 card is not required in a Branch Office system that already has a Gateway Controller with DSP resources.

Both Gateway Controllers and MC32S both support SRTP.

For more information about DSP resources residing on the card that are configured with DSP Daughterboards, see *Communication Server 1000E Installation and Commissioning* (NN43041-310).

Analog or digital trunk cards

All analog and digital trunk interfaces supported on Communication Server 1000 systems are also supported by the Branch Office feature. Analog and digital trunk cards interface with the PSTN. For information on trunk cards, refer to *Circuit Card Reference* (NN43001-311).

Analog or digital line cards

Analog (500/2500-type) or digital telephones and devices are supported by the Branch Office feature. For information about line cards, refer to *Circuit Card Reference* (NN43001-311).

When additional digital and analog (500/2500-type) telephones are located in the Branch Office, additional DSP resources are required. Refer to "Voice Gateway Media Card DSP capacity" (page 61).

Lineside cards

MG 1000B supports the following lineside cards:

- NTD514 line side T1
- NTD534 line side E1

For further information about Lineside T1/E1 cards, refer to *Circuit Card Reference* (NN43001-311).

MG 1000B Data Networking

MG 1000B with a Gateway Controller communicates with the Main Office Call Server using the built-in Ethernet ports on the Gateway Controller. The Ethernet ports on the Gateway Controller are

- CE: Connection to Server ELAN port (card only)
- CT: Connection to Server TLAN port (card only)
- 1E: ELAN connection to the data network (layer 2)
- 2T: TLAN connection to the data network (layer 2)
- E: ELAN connection for dual-homed
- T: TLAN connection for dual-homed

Note: The CP MG card functions as a Server and Gateway Controller. The CP MG card CE and CT Ethernet connections are embedded internal on the card. You do not require external cables to network the Server to the Gateway Controller on a CP MG card.

You must connect the Gateway Controller to a Layer 2 switch to handle signaling between the Main Office Call Server and the MG 1000B. If the 1E/2T and the E/T Ethernet ports are connected to a separate Layer 2 switch, the MG 1000B can remain operational if one of the Layer 2 switches fails.

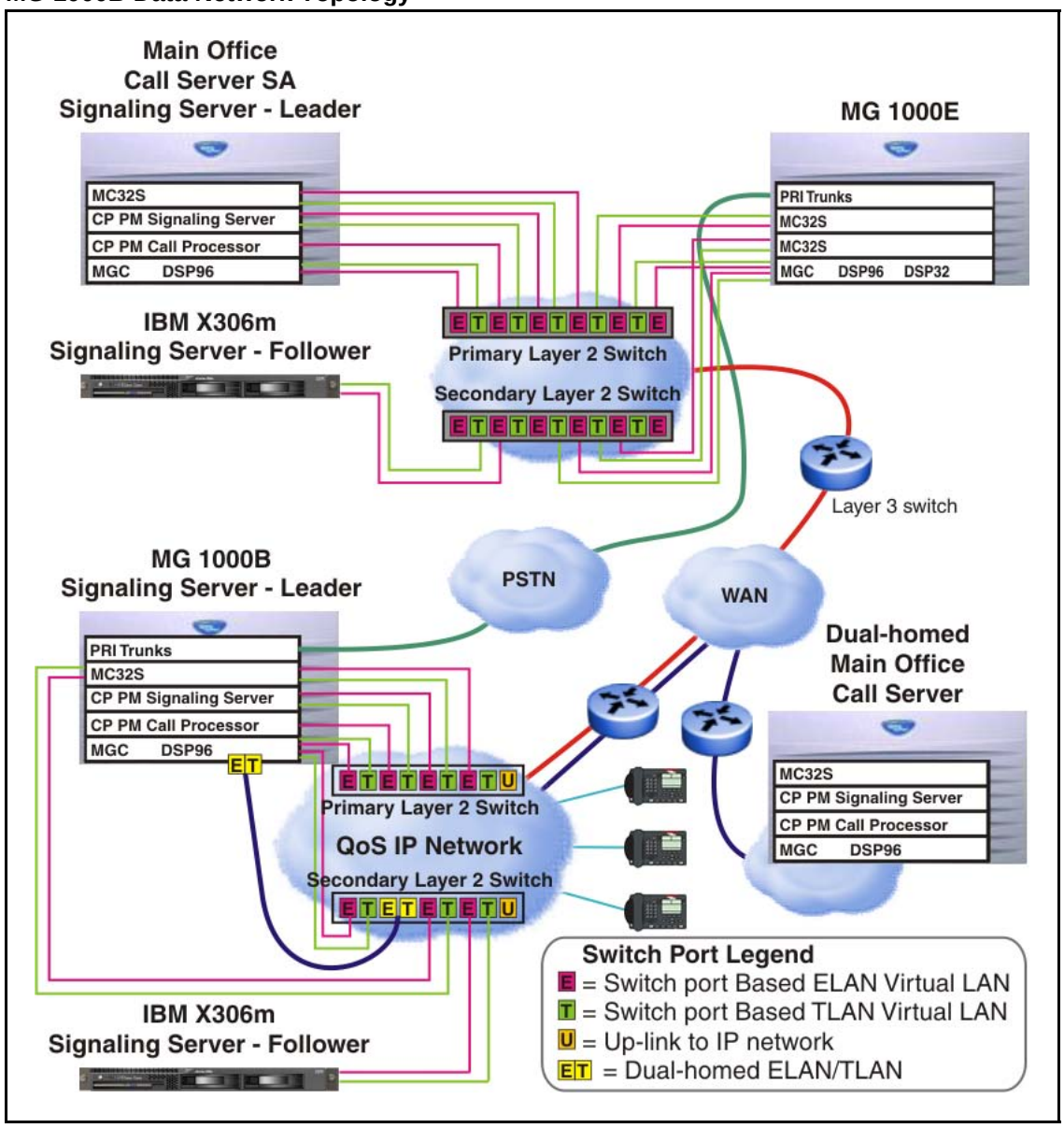
The MG 1000B must have a data network connectivity to the ELAN port of the Main Office Call Server. The design of the data networking configuration is outside the scope of this document. The engineering of the data network is documented in the *Converging the Data Network with VoIP Fundamentals* (NN43001-260).

The MG 1000B with Gateway Controller by default supports *Auto Negotiate* mode on the embedded Ethernet interfaces; you must configure the networking equipment to which they connect as *Auto Negotiate*. If

the Gateway Controller Ethernet ports do not auto-negotiate to 100 Mb Full Duplex, an alarm occurs. A CLI command is also available on the Gateway Controller to turn off auto-negotiation for the embedded Ethernet interfaces, which configures the interfaces to 100 MB Full Duplex. No other speed or duplex options are available on the Gateway Controller.

MG 1000B Data Network Topology illustrates an example of a robust network topology.

Figure 9
MG 1000B Data Network Topology



Gateway Controller network connections

In the following diagrams, two connections are shown to the external data equipment for the dual-homing feature, distributed and nondistributed. Nondistributed means that both Ethernet ports (TLAN or ELAN) of the dual-homing feature connect to a single Layer 2 switch, thus providing a single point of failure if that switch goes out of service.

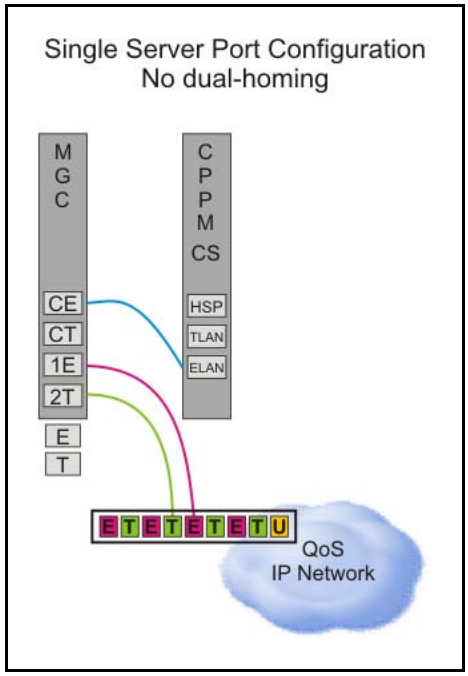
Distributed means that the two Ethernet ports (TLAN or ELAN) of the dual-homing feature connect to separate Layer 2 switches, to provide another level of redundancy and no single point of failure with a Layer 2 switch. Nortel recommends distributed connections; support is available for nondistributed connections if the cost of the additional data networking equipment is an issue.

The CE and CT ports on the are the only embedded Ethernet ports that allow a direct connection to another device, and the only hardware supported for this direct connection are CP PM or CP DC card Ethernet ports.

The following Gateway Controller network configuration examples are shown with an MGC card and a CP PM Server. You can also use a CP DC or COTS Server with a MGC card. The CP MG card functions as the Gateway Controller and the Server.

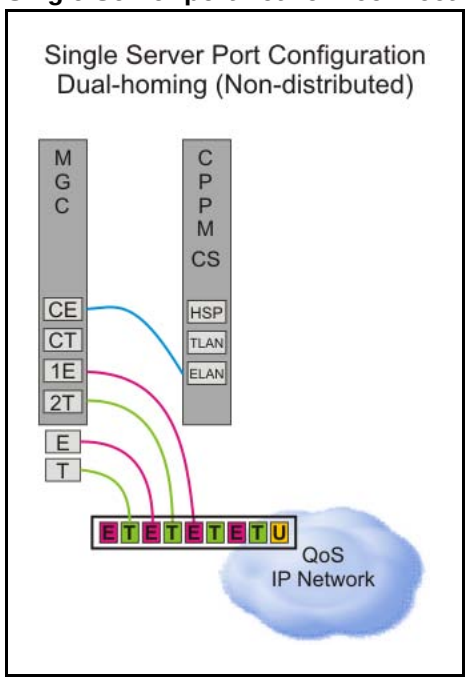
The figure below shows the supported configuration for a single Server configuration without redundant network configurations. This is the standard configuration of a cost effective single Server configuration.

Figure 10
Single Server port network connections (no dual-homing)



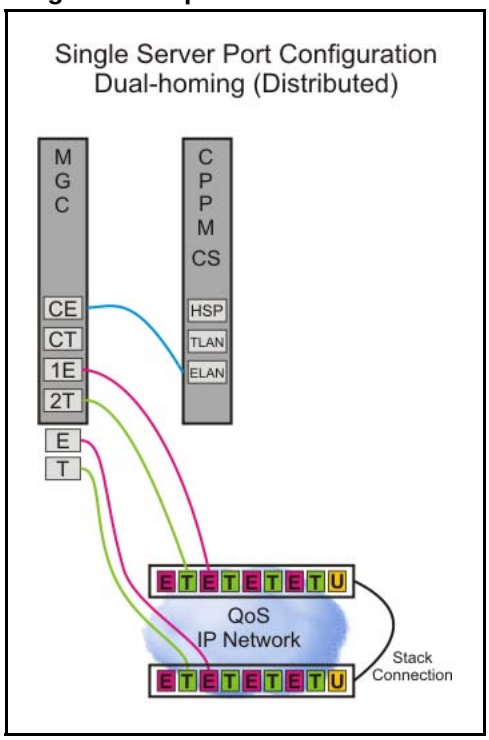
The following figure illustrates a typical network configuration that supports the dual-homed feature. With this configuration, however, a single Layer 2 switch remains a single point of failure.

Figure 11
Single Server port network connections (dual-homing - non distributed)



The following figure illustrates a typical network configuration that supports dual homing of both the ELAN and TLAN. Multiple Layer 2 switches ensure there isn't a single point of failure. Nortel recommends this configuration for the highest reliability in a single CPU Call Server configuration. You must partition the layer 2 switch into separate VLANs to keep the ELAN and TLAN traffic on separate subnets

Figure 12
Single Server port network connections (dual-homing - distributed)



MG 1000B platform configuration overview

The MG 1000B can be configured on three hardware platforms:

- chassis and expander
- cabinet
- MG 1010

Each configuration requires a Gateway Controller and a Server. The Gateway Controller must be in slot 0. The remaining slots can contain Server cards, analog line cards, analog trunk cards, digital line cards, or digital trunk cards. For a summary of the allowable card slots, see Table 7 "Card slots for MG 1000B" (page 47).

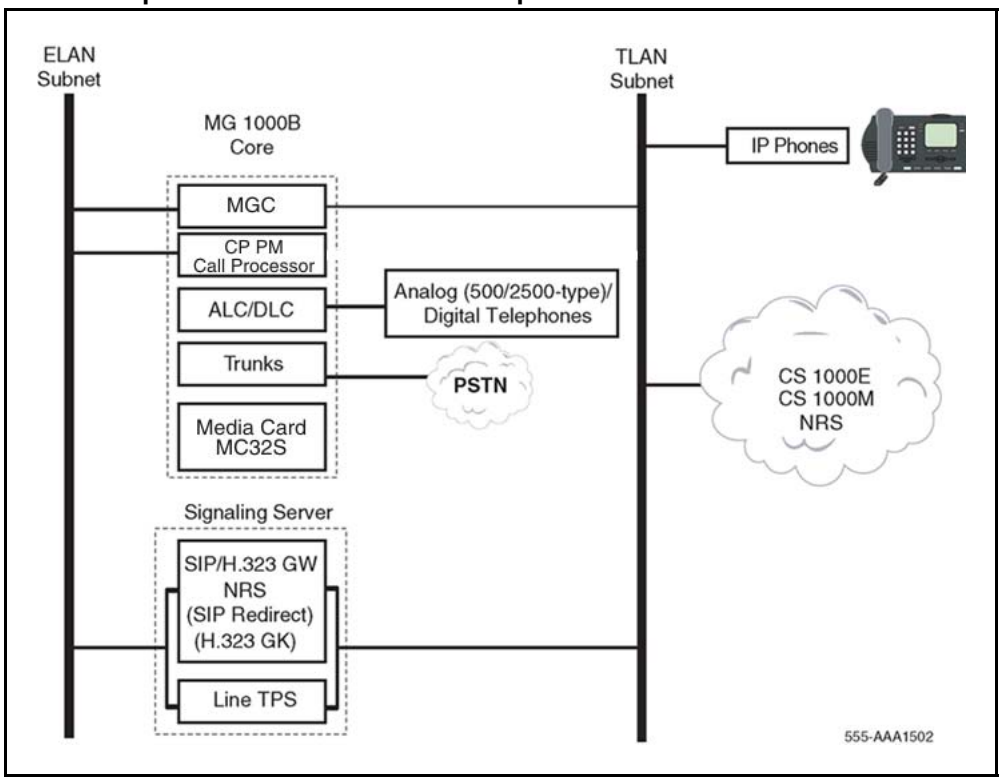
Each MG 1000B Core with a digital trunk card must have a clock controller.

For more information on line side T1 and line side E1 cards, see *Circuit Card Reference* (NN43001-311).

MG 1000B platform without a chassis expander

Figure 13 "MG 1000B platform without a chassis expander" (page 58) shows an MG 1000B platform configured without a chassis expander. This configuration has a single MG 1000B Core.

Figure 13
MG 1000B platform without a chassis expander



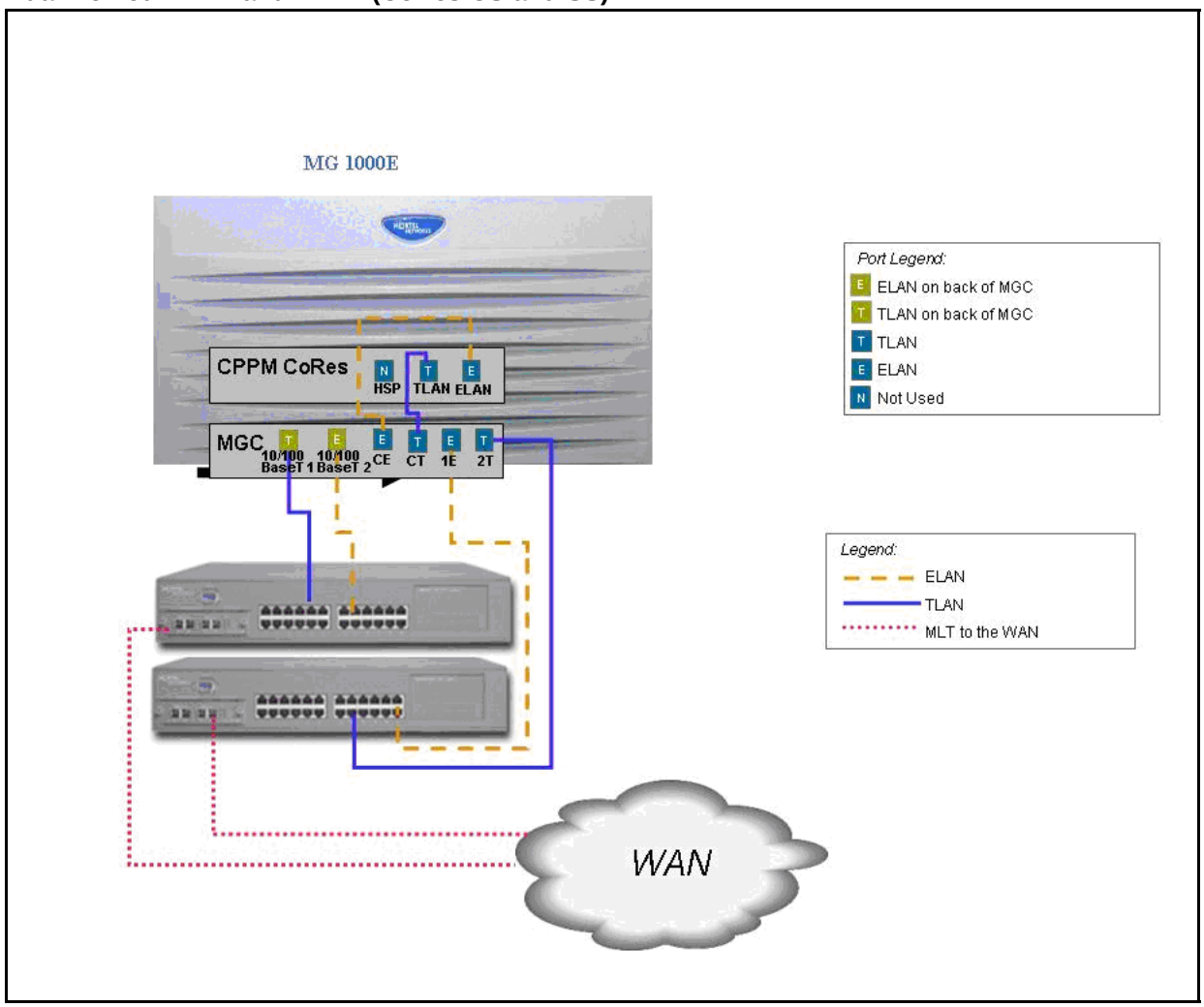
This MG 1000B platform configuration requires at least one Voice Gateway Media Card or a Gateway Controller with DSP resources. The additional slots can be used for any combination of the following:

- Server card
- trunk card
- analog or digital line card
- second Voice Gateway Media Card
- Nortel Integrated Conference Bridge card

- Nortel Integrated Recorded Announcer card
- cards to support CallPilot Mini or CallPilot 201i

For more information on the Voice Gateway Media Card configuration, refer to *Signaling Server IP Line Applications Fundamentals* (NN43001-125). For more information on Integrated Conference Bridge, refer to *Integrated Conference Bridge Service Implementation Guide* (NN43001-558).

Figure 14
Dual Homed ELAN and TLAN (Co-res CS and SS)



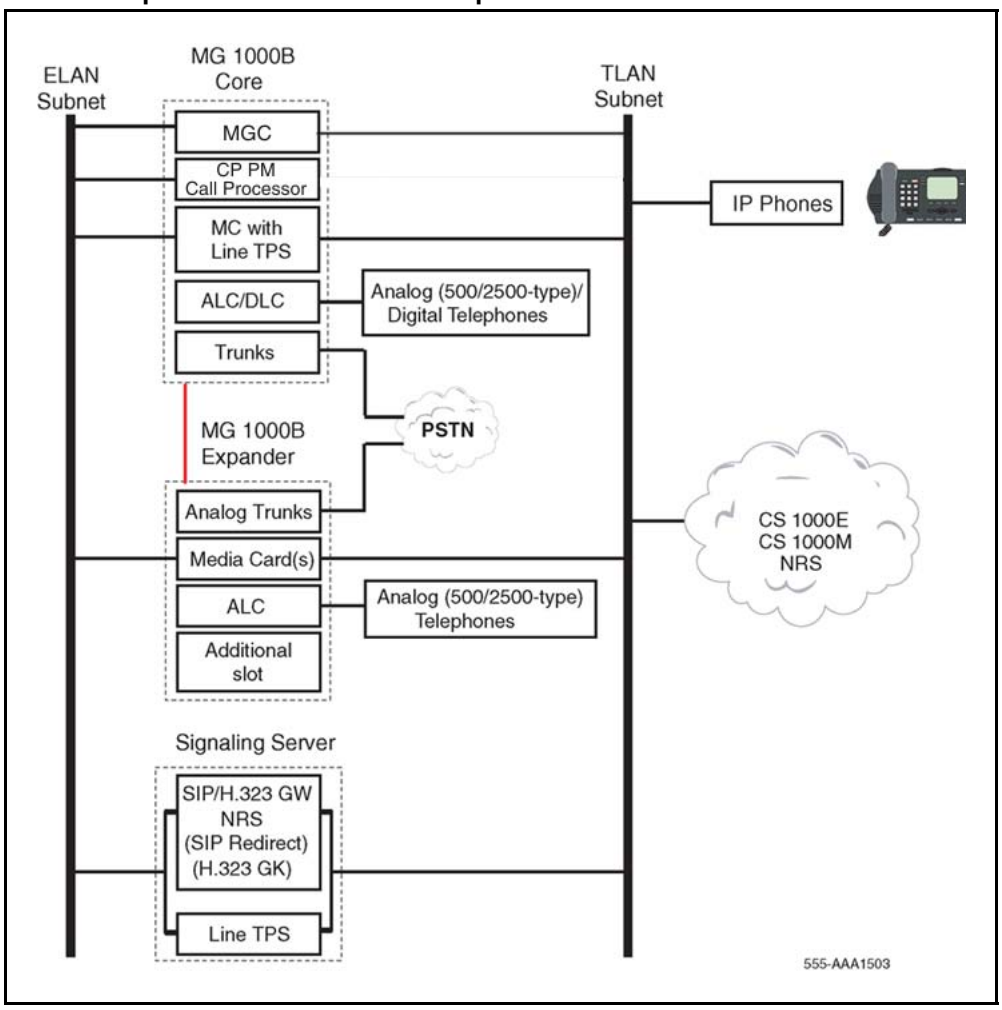
In a Co-resident Call Server and Signaling Server (Co-res CS and SS) configuration with an card as the Gateway Controller, if the ELAN or TLAN ports (or both) are connected directly to a Layer 2 switch instead of the CE or CT ports, autonegotiate must be set on the port settings on the Layer 2 switch to prevent Ethernet port duplex mismatching. Autonegotiation is enabled by default on the CE and CT ports.

MG 1000B platform with a chassis expander

Figure 15 "MG 1000B platform with a chassis expander" (page 60) shows an MG 1000B platform configured with a chassis expander. There must be at least one Voice Gateway Media Card (32-port cards) or a Gateway Controller with DSP resources for the MG 1000B core. If more than one Voice Gateway Media Card is used, the cards may be located in the chassis or expander.

The MG 1000B Expander does not support digital trunks. An MG 1000B Expander is not required or supported with a MG 1010 chassis.

Figure 15
MG 1000B platform with a chassis expander



Capacity

Each Communication Server 1000 Main Office (SA or HA) can support up to 1000 branch offices, consisting of combinations of SRGs, MG 1000Bs, SIP Media Gateways, and Geographically Redundant Survivable Media

Gateways (GR-SMG). The SRGs, MG 1000Bs, SIP Media Gateways, and GR-SMGs can be deployed in various combinations but the total cannot exceed 1000. The following limitations apply to the deployed combinations:

- There can be a maximum of 255 SRGs
- There can be a maximum of 1000 MG 1000Bs
- There can be a maximum of 1000 SIP Media Gateways, of which 511 can be survivable with N-Way database replication
- There can be a maximum of 50 GR-SMGs

Note: If there are 50 GR-SMGs there can only be 461 Survivable SIP Media Gateways (this allows for 511 end points with N-Way database replication).

Each Branch Office supports up to 400 IP Phone and SIP Line users. Branch Office also supports up to 128 Time Division Multiplexing (TDM) telephone users. However, since all IP Phones register with the Main Office, the governing factor is the maximum number of IP Phones that can be supported at the main office. This means the total number of IP Phones in all offices can be no greater than the capacity of the main office, as determined using*Communication Server 1000E Planning and Engineering* (NN43041-220).

You can use a Co-res CS and SS system as a Main Office, but in a limited capacity (Nortel recommends no more than 5 branches). The Co-res CS and SS system is limited to 1000 IP phones (UNIStim and SIP Line) and only 400 Virtual Trunks. The Co-resident Call Server is also limited to processing 10 000 calls per hour. These numbers directly affect the number of branches supported.

The configuration of an MG 1000B platform depends on:

- the number of line and trunk cards being provisioned
- the number of Voice Gateway Media Cards required to provide a sufficient number of DSP channels

Voice Gateway Media Card DSP capacity

The Media Gateway Controller (MGC) card can provide up to 256 DSP ports. The Common Processor Media Gateway (CP MG) card can provide 32 or 128 DSP ports. You can also add MC32 or MC 32S Voice Gateway Media Cards to increase the total number of DSP ports available.

For more information about DSP port provisioning for MG 1000B, see *Communication Server 1000E Planning and Engineering* (NN43041-220). When the MG 1000B is running in local mode (connection to Main Office

is down), you need to have enough DSPs to support all IP to TDM connections (IP set to TDM trunk, IP set to TDM sets). For example, use one DSP for each trunk port and a cumulus of 32 DSPs to support local conference and connections to local TDM sets.

If you equip digital telephones and analog telephones (500 and 2500-type) at the Branch Office, you need to add more DSP ports for digital-to-IP Phone and analog-to-IP Phone connections. The number of additional DSP ports must be equal to or greater than the expected number of simultaneous connections of these types. You can engineer fewer DSP ports depending on their blocking ratio.

Software requirements

This section describes the relative software versions required in the main office and Branch Office locations. The actual software packaging requirements are given in “Main office requirements” (page 98) and “Branch Office requirements” (page 99).

Main and Branch Office running the same release

Normally, the main office and associated Branch Office run the same software release.

However, a Branch Office location can be running an earlier software release than the software release running at the main office. This situation is discussed in the next section.

Main and Branch Office running different releases

It is recommended that the software release on the Branch Office match the software release on the Main Office. However, the Main Office Call Server and the Branch Office can have different software releases, as long as the Main Office runs at the highest release. The Main Office runs Communication Server Release 7.0 and supports a Branch Office running Communication Server 1000 Release 7.0, Release 6.0, Release 5.5, or Release 5.0.

Indefinite operation with a mixed-software configuration of Communication Server 1000 Release 5.0, Release 5.5, Release 6.0, and Release 7.0 Branch Offices, and a Communication Server 1000 Release 7.0 Main Office is supported.

Consider this mixed software policy when planning your system upgrade. Branch Offices must be at Communication Server 1000 Release 5.0 or later prior to upgrading the Main Office to Communication Server 1000 Release 7.0 to ensure a supported configuration during the upgrade period.

Note 1: Both the Call Server and Signaling Server in the Main Office must run the same release of software. Upgrade the Branch Office Communication Server 1000 within thirty days, to the same Communication Server 1000 release installed on the Main Office.

Note 2: If the NRS at the Branch Office is also the Alternate NRS in the network, then both it and the Primary NRS must be running the same software release.

Features in mixed-software configurations

Feature operation of IP Phone users in Normal Mode is the feature set on the main office. IP Phone users in Local Mode use the feature set on the Branch Office. Users of analog and digital devices always use the feature set on the Branch Office.

However, be advised that if the Branch Office is running a lower release of software than the main office, features involving interaction between the main office and the Branch Office will not function for the Branch Office IP Phone users. For example, if the main office is on Communication Server 1000 Release 7.0 and the Branch Office is on Communication Server 1000 Release 5.5, features introduced in Release 7.0 will not operate for the Branch Office IP Phone users since these features are not supported on earlier releases. In this case, the Branch Office would need to be upgraded to Communication Server 1000 Release 7.0 to support these features.

Adding a Branch Office to an existing network

For customers wanting to add a Branch Office to their existing network, customers are permitted to order a Branch Office running Communication Server 1000 Release 6.0, 5.5 or 5.0 if their Main Office is running Communication Server 1000 Release 7.0.

IP Phone firmware

When you add a new Communication Server 1000 Branch Office release to a network that has a previous release of Communication Server 1000 Branch Office, you must choose whether to upgrade IP Phone firmware for existing Branch Offices. You can choose not to upgrade the IP Phone firmware at the existing Branch Offices only if the IP Phones in those Branch Offices are running at least the minimum version of firmware. For information on minimum firmware versions see *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

If you choose to upgrade only the IP Phone firmware, you must upgrade the IP Phone firmware at the existing Branch Offices first. The main office may not require an IP Phone firmware upgrade, depending on its current version

With the Enhanced UNIStim Firmware Download feature, IP Phone firmware at the Branch Office is automatically downloaded from the main office.

Package Combinations

The MG 1000B with Gateway Controller requires existing packages 402 SOFTSWITCH, 403 Media Gateway, and Branch Office Package 390.

Package combinations supported using the CS 1000 Release 4.5 MG 1000B are supported by the MG 1000B with Gateway Controller.

GRPRIM (Geographic Redundancy Primary CS Package) and GRSEC (Geographic Redundancy Secondary CS Package) are restricted on Branch Office environment.

Supported applications

The Branch Office feature supports Nortel Integrated Conference Bridge, Nortel Integrated Recorded Announcer, CallPilot Mini, and CallPilot 201i at the Branch Office location.

Survivability

The Branch Office provides survivability against WAN failure, Main Office Call Server failure, or Signaling Server failure. Survivability is also provided during the Main Office upgrade, including Signaling Server and Call Server upgrade. A Call Server and Signaling Server are required in the Branch Office with Communication Server 1000 Release 5.5 or later. For Communication Server 1000 Release 6.0 or later the Co-resident Call Server and Signaling Server is optional, however the Signaling Server is required for an IP-enabled Communication Server 1000 system. For more information on the Co-Resident Call Server and Signaling Server, see*Co-resident Call Server and Signaling Server Fundamentals* (NN43001-315)

The Branch Office supports Geographic Redundancy as a Main Office feature. For further information on Geographic Redundancy, see *System Redundancy Fundamentals* (NN43001-507).

Branch Office supports the Network Wide Redundancy Phase II feature, which is supported by the MG 1000B to provide survivability to IP telephones normally registered with a CS 2100 and Communication Server 1000. For additional information see *System Redundancy Fundamentals* (NN43001-507).

If a LAN/WAN fails, the MG 1000B IP Phones lose communication with the main office TPS. This causes the IP Phones to reset and register with the MG 1000B TPS and the MG 1000B Call Server. The IP Phones operate in

Local Mode, and receive call processing services from the call server. In Local Mode, the MG 1000B TPS tries to communicate with the main office TPS at regular intervals. Once communication is established with the main office TPS, the MG 1000B IP Phones are redirected to the main office.

If the main office Call Server fails and call processing services are provided by an alternate Call Server, the MG 1000B IP Phones register with the alternate Call Server and receive call processing services from it. If no alternate Call Server is available, the MG 1000B IP Phones stay registered with the main office TPS for ten minutes. At the end of the ten minutes, the IP Phones reset and register with the call server. If a key on a particular IP Phone is pressed before the end of the ten minutes, that telephone resets and registers with the call server immediately after the key is pressed.

When the main office Signaling Server fails and an Alternate Signaling Server is available, the MG 1000B IP Phones reset and reregisters with the main office Call Server through the Alternate Signaling Server, and continue to receive call processing services from the main office Call Server. If no Alternate Signaling Server is available, the MG 1000B IP Phones reset and register with the call server. IP Phones that were registered with the call server before the main office Signaling Server failure was detected are then redirected back to the main office and register with the Voice Gateway Media Card. These telephones stay in Normal Mode. IP Phones that registered with the call server after the main office Signaling Server failure was detected stay registered at the Branch Office.

If the Main Office has VTRK applications on the failed Signaling Server, the NCS de-registers the Main Office from its database. Therefore, redirection from local mode cannot be completed. If the alternative Signaling Server has no TPS services configured (for example, it is purely an NRS, Personal Directory (PD) Server, or pure VTRK), once again, redirection cannot be completed. The correct scenario occurs when the NCS has a static endpoint for the Main Office Node IP so there is no VTRK dependency. All TPSs configured at the Main Office have the same H.323 ID. The Branch Office maintains a connection to the NCS, or alternative NCS. In this particular case, IP Phones are redirected to the Main Office even when a primary Signaling Server fails.

When an MG 1000B IP Phone powers up, it registers first with the MG 1000B TPS, and second with the MG 1000B Call Server. It is then redirected to the main office by the call server. The MG 1000B TPS queries the Primary NCS for the main office node IP address to redirect the IP Phone. The NCS provides the IP based on BUID value. If there are several routes for a particular BUID route, the smaller route cost factor is chosen. If the Primary NCS is down or unreachable, the MG 1000B

TPS queries the Alternate NCS. If the MG 1000B TPS receives a positive response, the MG 1000B IP Phone is redirected to the main office. If the Alternate NCS is also down or unreachable,the MG 1000B TPS queries the Failsafe NRS. If a successful response is received from the Failsafe NRS, the IP Phone registers with the main office. Otherwise, if neither an Alternate NRS nor a Failsafe NRS is available, the MG 1000B IP Phone remains in Local Mode at the Branch Office, the MG 1000B telephones remain in Local Mode, displaying a **Server Unreachable (1)** message and receives all call processing services from the CP PM in the MG 1000B Core.

MG 1000B IP Phones in Normal Mode remain registered with the main office when the Primary NRS fails and no Alternate or Failsafe NRS is available. They can call any main office telephone or IP Phones in Normal Mode in other branch offices. However, they cannot call any MG 1000B digital telephones, analog (500/2500-type) telephones, or any external number through the MG 1000B trunks in the normal way, because the Virtual Trunks are not available. (MG 1000B digital or analog (500/2500-type) telephones are accessible if alternate routing is available through the PSTN.) The user has the option of staying in Normal Mode, or going to Local Mode manually by resetting the telephone or using Test Local Mode. In Local Mode, the IP Phones can make local calls to other IP Phones, digital telephones, and analog (500/2500-type) telephones at the Branch Office. They can also be used to make outgoing PSTN calls as usual.

You must plan for, and obtain, the Primary and optional Alternate NRS addresses for installing the Branch Office feature software. Determine the NRS role, that is, the Alternate or Failsafe configuration, for the MG 1000B Signaling Server.

Nortel recommends that the NRS in the MG 1000B be configured as a Failsafe NRS. If the MG 1000B IP Phones go into Local Mode, they can use the MG 1000B NRS services.

For CallPilot Mini and CallPilot 201i applications, a Message Waiting Indication (MWI) does not survive a Mode change (Normal to Local or Local to Normal). The message itself is preserved, but the lamp indicator may not be lit after the Mode change.

Active Call Failover

The Active Call Failover (ACF) feature for IP Phones allows active IP calls to survive the following failures:

- IP/IP calls and IP/TDM calls survive signaling path TLAN subnet failures.
- IP and IP/TDM calls survive Signaling Server restarts.

- IP and IP/TDM calls survive LTPS ELAN subnet failures.
- IP calls survive a Call Server cold start and Call Server failures in system configuration with a redundant Call Server.

ATTENTION
Only 2050v3 phones support Active Call Failover.

ACF mode

The ACF feature for IP Phones enables an IP Phone to reregister in the ACF mode during a supported system failure.

The ACF mode preserves the following:

- active media session
- LED states of the Mute, Handsfree, and Headset keys
- DRAM content

All other elements (the feature keys, soft keys and text areas) are retained until the user presses a key or the connection with the Call Server is resumed. If the user presses a key during the failover, the display area is cleared and a localized "Server Unreachable" message is displayed.

The IP Phone uses this new mode of reregistration only when the Call Server explicitly tells the IP Phone to do so. IP Phones clear all call information when registering to a Call Server or LTPS that does not support the feature.

For further information on Active Call Failure, refer to *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

Configuring S2 IP Address to point to the main office TPS

This configuration programs the S1 IP address parameter on the MG 1000B IP Phone as the Node IP of the Branch Office, and S2 as the Node IP of the main office (normally, S2 would be set to NULL).

This configuration provides better resiliency when an MG 1000B IP Phone cannot access the Branch Office over the local LAN or WAN (due to network problems, for example), but can access the main office. In this case, the IP Phone tries to register directly with the main office.

This configuration is supported only under the following conditions:

- Enhanced Redundancy for IP Line nodes checking is in operation between the Branch Office and the main office. Four digits are configured on the TPS for the Node ID, and the first three digits of that

Node ID make up the Node ID on the IP Phone. For example, 5701 is configured on the main office TPS and 5702 on the MG 1000B TPS, where 570 is the Node ID on the IP Phone.

- The same TN is programmed on the main office and Branch Office for the IP Phone.
- The main office is a Communication Server 1000E system.

The IP Softphone 2050 does not support S2 Addresses. However, the IP Softphone 2050v2 does have the ability to configure S2.

For information on configuring the S2 IP address to point to the Main Office TPS and its limitations, see *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

Patch Management Enhancements

The changes completed under this feature are applicable to Call Server, Gateway Controller, and Voice Gateway Media Cards.

This feature supports proactive patching tool as it handles patches individually.

When a patch conflict was encountered, the patch activation was aborted. In this feature, there is a mechanism provided to handle this functionality in more efficient manner.

Note: Installation of the Deplist menu is removed when there are no DepLists to be added to the Software image. This is a requirement for new installs or upgrades. The prompt to install a DepList applies only if there is one being delivered during the software installation.

How the Branch Office feature works

Contents

This chapter contains the following topics:

"Introduction" (page 69)
"Normal Mode and Local Mode operation" (page 69)
"Local Mode operation" (page 77)
"Configuring non-zero S2 IP Addresses for UNIStim phones" (page 78)
"Multiple Appearance DN (MADN)" (page 80)
"Emergency services" (page 81)
"MG 1000B Core interoperability" (page 83)
"Network Wide Redundancy Phase II and Network Music" (page 83)

Introduction

The Branch Office connects to the main office using Virtual Trunks over the LAN or WAN. Virtual Trunks are software components that provide the trunking features of the Meridian Customer-Defined Networking (MCDN) feature set. The main office and the Branch Office are configured as Electronic Switched Network (ESN) nodes, connected by Virtual Trunks. The MG 1000B Core provides a trunk gateway to the PSTN. Access to PSTN digital or analog trunks at the Branch Office occurs through the MCDN Virtual Trunk.

For more information on Virtual Trunks, refer to *IP Peer Networking Installation and Commissioning* (NN43001-313). For more information about Electronic Switched Networking (ESN), refer to *Electronic Switched Network: Signaling and Transmission Guidelines* (NN43001-280).

Normal Mode and Local Mode operation

Normal Mode

The Main Office provides central call processing for the Branch Office Internet Telephones in Normal Mode. The Branch Office Internet Telephones are configured at the Main Office Call Server. These

telephones are registered to the Main Office Line Terminal Proxy Server (LTPS) and are controlled by the Call Server at the Main Office in Normal Mode.

Users of the MG 1000B IP Phones receive the features, key layout, and tones of the main office Call Server. This provides feature and application transparency between the Branch Office and the main office.

Local Mode

Devices that are physically located with the Branch Office and are controlled by the Branch Office call server are in local mode. These devices consist of analog (500/2500-type) or digital telephones, analog or digital devices, and may include IP Phones. Normally, IP Phones are registered to the main office in Normal Mode, however, when the IP Phone cannot reach the main office, it reverts to Local Mode.

If the Branch Office Internet Telephone loses communication with the Main Office, the Call server in the Branch Office provides the call processing for the telephone. When the Branch Office Internet Telephones receive service at the Branch Office, the telephone display shows Local Mode.

In Local Mode, IP Phones receive only those features and tones that are provisioned on the Branch Office.

An IP Phone at the Branch Office may be in Local Mode for two different reasons:

- IP Phone may have just booted up
- IP Phone cannot communicate to the main office because of a WAN failure or a failure of the main office components.

In the event of a WAN failure, the Branch Office IP Phones lose communication with the main office. This causes the Branch Office IP Phones to reset and reregister with the Branch Office. The IP Phones then operate in Local Mode.

If the main office Call Server fails and call processing services are provided by an Alternate Call Server, the Branch Office IP Phone reset and reregister with the Alternate Call Server and receive call processing services from it. If no Alternate Call Server is available, the Branch Office IP Phones go to Local Mode while the MG 1000B attempts to find an Alternate Call Server by way of the Network Connect Server (NCS).

When the main office Signaling Server fails and an Alternate Signaling Server is available, the Branch Office IP Phones reset and reregister with the Branch Office. The MG 1000B will query the NCS for the Alternate Signaling Server's IP address. The MG 1000B will redirect the IP Phone

to the Alternate Signaling Server and continue to receive call processing services from the main office Call Server. If no Alternate Call Server is available, the Branch Office IP Phones reset and reregister with the MG 1000B in Local Mode.

The user has the option of going to Local Mode manually by resetting the telephone or using Test Local Mode. In Local Mode, the IP Phones can make local calls to other IP Phone and analog (500/2500) or digital phones at the Branch Office. They can also be used to make outgoing PSTN calls and receive incoming calls as usual.

ATTENTION
When a telephone or trunk in the Main Office calls an MG 1000B IP Phone in Local Mode, the call is treated according to the Main Office call redirection configuration (such as forwarding to voicemail or continuous ringback).

When an IP Phone at the Branch Office first boots up it attempts to communicate with the MG 1000B. Once it has established communications with the MG 1000B, the MG 1000B will redirect the IP Phone to the main office.

Before the Branch Office IP Phone attempts to register with the main office, the MG 1000B first queries the Primary NRS (NCS) fro the main office for the Virtual Trunk node IP address to redirect the IP Phone. If the Primary NRS (NCS) is down or unreachable, the MG 1000B queries the Alternate NRS, if one is specified. If it receives a positive response, the MG 1000B is redirected to the specified main office. Otherwise, it neither a Primary or an Alternate NRS is available, the Branch Office IP Phone remains in Local Mode, and receives call processing services from the MG 1000B until communication is reestablished.

If an IP Phone is in Local Mode due to WAN failure, the MG 1000B tries to communicate with the main office TPS at regular intervals. Once communication is established with the main office Call Server, the idle Branch Office IP Phones are automatically redirected and reregistered to the main office. IP Phones that were busy at the time communication was reestablished, complete the call in Local Mode, and then reregister with the main office once the call is complete.

MG 1000 IP Phones in Normal Mode remain registered with the main office if the Primary NRS fails and no Alternate NRS is available. They can call any main office telephone or IP Phones in Normal Mode in other branch offices. However, they cannot call an Branch Office analog (500/2500-type) telephones, digital telephones, or any external numbers

through the MG 1000B trunks because the Virtual Trunks are not available. (MG 1000B analog [500/2500-type] or digital telephones, are accessible if alternate routing is available through the PSTN.)

Features supported in Local Mode

In Local Mode, IP Phones receive only those features and tones that are provisioned on the call server. The features are not necessarily the same in Normal Mode due to local configuration, or if the Branch Office and main office are running different software releases or different service levels.

When the Branch Office is running a previous software release, the Local Mode features are limited to those available in that release. Depending on what is provisioned, this means that Normal Mode may have more features than Local Mode.

A user can attempt a Virtual Office Login to an MG 1000B IP Phone from an MG 1000B IP Phone in Local Mode. If the Virtual Office Login is successful, the Virtual Office user is registered with either the Branch Office or main office. A Branch Office in local mode only accepts Coordinated Dialing Plan (CDP) numbers as Virtual Office user ID's.

After Virtual Office login, the Branch Office does not start the redirection procedure to the Main Office for a logged in set immediately. A phone configured on the Main Office TN (MOTN) must match the phone type on Branch Office. For example, the IP Phone 2004 cannot register in normal mode if the Main Office is configured for IP Phone 2002 and the IP Phone 2002 cannot register in normal mode if the Main Office is configured for IP Phone 2001.

If the network is using CDP, the Network Ring Again (NRGN) feature does not work for a Branch User in Local Mode. In the CDP environment, the NRS database configures the main office as the endpoint for the Branch User DN. The Virtual Trunk obtains the endpoint of NRGN response messages from the NRS. It sends admission requests to the NRS with the Branch User DN. The NRS returns the address associated with the destination DN. In this case, the returned address is that of the main office.

Users in a Branch Office cannot access their Personal Directory, Callers List, or Recall List when in Local Mode, because the lists are stored on a Signaling Server in the main office.

ATTENTION
As per PD/CL/Rl these features are not supported in Local Mode (on MG1000B) to avoid confusion. These features are available only in Normal mode.

Licensing

A licensing feature for the Internet Telephones in the Branch Office notifies Branch Office administrators of a license violation; the extended use of Branch Office Internet Telephones in Local Mode.

Operation of IP Phones in Local Mode is meant to provide survivability during conditions of network failure only. It is not intended for prolonged operations. Therefore, a Licensing Period of 90 days is allowed for MG 1000B IP Phones to stay in Local Mode. When the Licensing Period expires, a BUG0103 system message is written to the MG 1000B Call Server log file. The message is also printed on the teletype terminal (TTY). The IP Phones are reset at the end of every call, and try to register with the main office.

When nine or fewer days remain on the licensing feature, IP Phones display a "Licensed days left: *n*" message to indicate how many days you can use the MG 1000B IP Phone in Local Mode. This message also appears as a banner when the technician logs into a maintenance terminal. After the Licensing Period has expired, IP Phones in Local Mode display "Beyond Licensed Period".

Licensing is based on a debit-and-credit system for the amount of time the IP Phones have been registered to the main office or Branch Office. Credits are in two-hour units. After a software upgrade, 1080 initial credits, equivalent to a 90-day period, are provided. The total credits are decreased by one every time five or less IP Phones stay in Local Mode for two hours. The total credits are increased by one for every two hours that five or less IP Phones are registered with the main office. Total credits cannot exceed 1080 credits, or 90 days.

The licensing feature applies only if more than four IP Phones are in Local Mode at the same time. If four or fewer phones are in Local Mode simultaneously, the licensing feature is not activated.

Testing the telephone in Local Mode

From Normal Mode, a Branch Office user can use Test Local Mode to test telephone functionality in Local Mode. The user can perform the test at any time and does not require a password. This test is invoked from the Internet Telephone.

Nortel recommends testing Local Mode operation after changing the provisioning for a telephone on the MG 1000B.

To ensure that users do not forget to resume Normal Mode operation, the MG 1000B TPS redirects the telephone to the main office to return the telephone to Normal mode. This occurs if the telephone remains

registered to the MG 1000B Call Server in Test Local Mode for ten minutes. Alternatively, the user can select Resume Normal Mode from the **Options** menu.

If a Branch Office phone in Test Local Mode logs into another Branch Office TN through Virtual Office, makes an ESA call and is redirected (for example, their location isn't known), the phone is correctly redirected to its original TN to complete the call. When the ESA call is complete, the phone immediately reregisters with the Main Office rather than remaining registered to the Branch Office for 10 minutes.

For more information see the *Emergency Services Access: Description and Administration (NN43001-613)*NTP.

Virtual Trunks

In order for endpoints in the Communication Server 1000 network to access endpoints in local mode at the Branch Office or to access the PSTN at the Branch Office, Virtual Trunks are used over the LAN/WAN.

Virtual Trunks are software components that provide the trunking features of the Meridian Customer-Defined Network (MCDN) feature set. Access to PSTN digital or analog trunks at the Branch Office occurs through the MCDN Virtual Trunk.

For more information on Virtual Trunks, refer to *IP Peer Networking Installation and Commissioning* (NN43001-313).

IP Phone calls

When an IP Phone calls another IP Phone, each telephone receives the address of the other to exchange media directly between the telephones. Also note that when in Normal Mode, an MG 1000B IP Phone calling a main office IP Phone does not require any trunking to setup the call. However, LAN/WAN bandwidth is used to provide a media path for the call. For more information on Direct IP media path functionality, see *IP Peer Networking Installation and Commissioning* (NN43001-313).

MCDN ALTernate Routing and Vacant Number Routing

Vacant Number Routing (VNR) is a default route used for routing untranslatable, invalid, and unassigned dialed numbers (DNs). When the call is routed by VNR to the IP network, the user has the flexibility to perform MCDN ALTernate Routing (MALT) on the Call Server for an additional 10 causes other than the existing six. Configure these additional MALT causes within Element Manager (EM). If the call is determined to be a VNR call, which is tried at least once to route over an IP route, then vacant number treatment is provided to the call. Thus, this feature

development combines both the VNR and MALT functionality for calls routed over IP, to give more benefit to the customer, by routing a call to the proper destination and providing appropriate vacant number treatment.

Calls to the IP network need the ability to reroute to another alternate, while maintaining the ability to receive vacant number treatment when the called destination is an unassigned number. There are two parts of this feature:

1. **MALT on calls routed to the IP domain**

   This feature deals with VNR calls at the CS1K, routed over H.323/SIP. If the call fails to route to the destination the call gets disconnected with a cause which matches one of the original MALT cause codes, or disconnects with an indication to use MCDN Alternate Routing. If MALT exhausts all routes in the VNR route list block hen the treatment corresponding to the disconnect cause is provided.

   With the default MALT handling, there are six causes, which perform MALT at the CS1000:

   — 3 - No route to destination

   — 27 - Destination is out of service

   — 34 - No circuit or channel available

   — 38 - Network out of service

   — 41 - Temporary failure

   — 42 - Switching equipment congestion

2. **Configurable MALT causes for different vendors**

   A configurable option is provided in EM for the different vendors in order to configure causes to accomplish MALT at the CS1000. Element Manager provides the following causes to be configured to perform MALT:

   — 01 – unassigned number

   — 20 – subscriber absent

   — 47 – Resources unavailable

   — 51 - Call rejected; blocked by MBG

   — 52 - Outgoing call barred

   — 53 - Outgoing call barred in closed user group

   — 54 - Incoming call barred

   — 55 - Incoming call barred in closed user group

   — 63 – service or option not available

   — 127 – Interworking unspecified

If a call is disconnected prior to establishing with the clearing message using one of the causes listed previously and the causes are configured on the Signaling Server to perform MALT, then a new IP IE is built with an indication `use MALT` with the cause. This IE is sent to CS with the `in the received clearing` message. The CS would trigger MALT for the cause.

IP Phone to analog (500/2500-type) or digital telephone calls

When an MG 1000B IP Phone in Normal Mode calls an analog (500/2500-type) or digital telephone in the Branch Office, the call is processed at the main office Call Server. A Virtual Trunk route is selected according to the digits dialed. The call is routed over a Virtual Trunk to the Branch Office. The MG 1000B Call Server processes the incoming Virtual Trunk call and terminates it to the local analog (500/2500-type) or digital telephone. Since this is a call between IP and circuit-switched devices, a DSP resource on a Voice Gateway Media Card is allocated and connected to the analog (500/2500-type) or digital telephone. The IP address of the DSP resource is returned to the main office Call Server so a direct media path between the IP Phone and the DSP resource can be set up when the call is established. Refer to *IP Phone to analog (500/2500-type) or digital telephone calls* (NN43001-313) for details.

Incoming calls from the local PSTN

The Vacant Number Routing (VNR) feature must be configured on the MG 1000B Call Server to route all vacant numbers to the main office. An incoming Central Office trunk call can be configured to terminate at the local attendant console, an analog (500/2500-type) telephone, or a digital telephone. It can also be routed to a remote attendant console, an MG 1000B IP Phone, or an analog (500/2500-type) or digital telephone in the main office. Direct-Inward-Dial (DID) calls from local PSTN trunks are routed according to the destination DNs. Incoming calls to MG 1000B IP Phones in Normal Mode are routed to the main office Call Server over the Virtual Trunks. Calls to local analog or digital devices are terminated locally. For more information about Vacant Number routing, see *Converging the Data Network with VoIP Fundamentals* (NN43001-260).

Conference calls

When a branch user initiates a conference call while registered in normal mode, the conference facilities of the main office are used. This means that in a conference among three Branch Users, the LAN/WAN bandwidth of three media paths is used. The main office controls the calls except in Local Mode, where local resources are used.

In sites with limited LAN/WAN bandwidth between the main office and the Branch Office and with heavy conference traffic among Branch Users, you can install the Nortel Integrated Conference Bridge card in the MG 1000B Core or the MG 1000B Expander. This configuration provides a *meet-me* conference facility and reduces LAN/WAN bandwidth usage requirements.

The conferencing feature for MG 1000B with a Gateway Controller supports up to 30 parties.

- If you configure a conference loop in LD 17, the maximum number of parties for *any* conference on the system is six.

- If you have no conference loops configured in LD 17 , the maximum number of parties for all conferences on the system is 30.

Group Call

With the conference capabilities on the Gateway Controller, the Group Call feature supports 20 group members.

If the MG 1000B system has a Gateway Controller for the MG 1000Bs, the maximum number of group members (and member DNs in a call) is 6.

Local Mode operation

Also see “Survivability” (page 64).

Survivability of IP Phones

ATTENTION
When a telephone or trunk in the main office calls an MG 1000B IP Phone in Local Mode, the call is treated according to the main office call redirection configuration (such as forwarding to voicemail or continuous ringback).

When the telephone detects that it has lost communication with the main office, it reboots and registers to the MG 1000B TPS. This means that, depending on the network configuration (or the point of failure in the network), not all MG 1000B IP Phones go into Local Mode at the same time. Calls are not maintained during switchover from Normal Mode to Local Mode.

IP Phones that are in Local Mode due to a network or main office failure are automatically redirected to the main office when connectivity is restored. Established calls are completed before the switchback from Local Mode to Normal Mode.

To provide survivability for the IP Phones, the MG 1000B IP Phones must be provisioned on both the Call Server at the main office and the MG 1000B Call Server. “Installing and configuring IP Phones” (page 177)

Configuring non-zero S2 IP Addresses for UNIStim phones

This section describes how to configure the S2 IP Address parameter on an IP Phone at a Branch Office to provide additional survivability when:

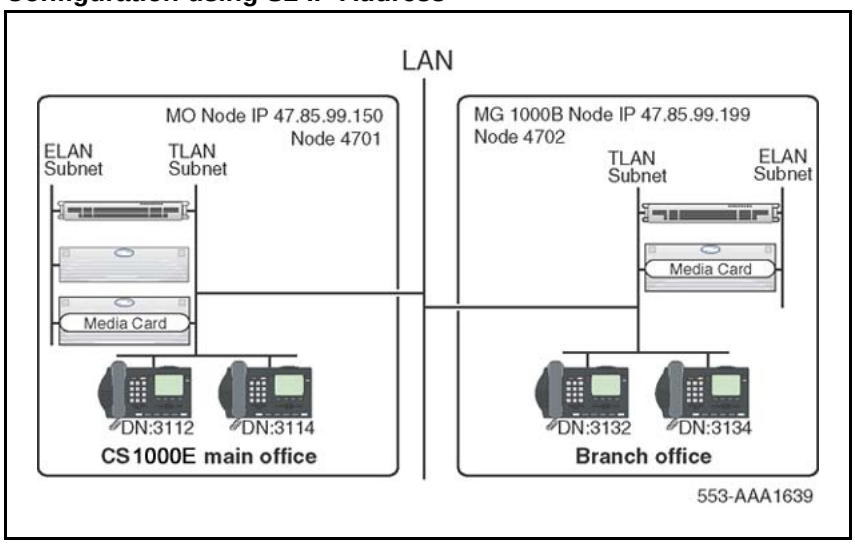
- The MG 1000B TPS on the MG 1000B Signaling Server is not available. Therefore, MG 1000B IP Phones cannot be redirected to the main office TPS because the S2 parameter is set to NULL.
- The MG 1000B Call Server is not available. Therefore, MG 1000B IP Phones cannot be redirected to the main office TPS because the S2 parameter is set to NULL.

MG 1000B IP Phones register with the MG 1000B Call Server before being redirected to the main office. If the sets cannot register with the MG 1000B Call Server as described in the previous paragraph, they are not redirected to the main office, even though the main office is fully functional and no network problems exist between the Branch Office and main office.

Normally, an MG 1000B IP Phone registers with the main office TPS using its S1 IP Address parameter. This section describes how an MG 1000B IP Phone can register with the main office TPS using its S2 IP Address parameter if one or more of the above events occur at the Branch Office.

Figure 16 "Configuration using S2 IP Address" (page 78) shows a typical configuration using the S2 IP Address.

Figure 16
Configuration using S2 IP Address



Points to remember

When an IP set registers to the main office using S2, remember the following important points:

- An IP Phone registered to the main office using S2 appears in the main office TPS as a "regular online" user. Normally, an MG 1000B IP Phone registered to the main office Call Server appears as a "branch online" user. Commands can be executed on the main office Signaling Server to verify this operation.
- The display on an IP Phone registered to the main office using S2 does not show the "Branch USER: XXXX" prompt.
- For an MG 1000B IP Phone to register successfully with the main office TPS using S2, Enhanced Redundancy for IP Line nodes checking must be used. Four digits must be configured for the Node ID on both the Main Office TPS and MG 1000B TPS. The first three digits must be the same, and are configured as the Node ID during the IP Phone configuration.
- When an MG 1000B IP Phone is registered to the main office using S2, an administrator must manually redirect the IP Phone back to the MG 1000B TPS once the IP Phone becomes available again. This action enables the MG 1000B IP Phone to go back to Normal Mode by using S1 to register to the main office.
- If the MG 1000B LTSP becomes unavailable, MG 1000B IP Phones registered to the main office LTPS (in Normal Mode) are unaffected. MG 1000B IP Phones that are rebooted try to register using S1, or S2 if programmed.
- If the MG 1000B TPS is unavailable, IP Phones at the main office or Branch Office have no access to TDM resources (digital and analog telephones or PSTN trunks) at the Branch Office, whether the IP Phones are registered using S1 or S2.
- Bandwidth management zones, emergency access, and time of day continue to work normally, regardless of whether an IP Phone is registered using S1 or S2.
- If the CP PM at the Branch Office is initialized or rebooted, MG 1000B IP Phones can register using S1 or S2. In this case, an administrator must manually redirect the S2-registered IP Phones to register using S1 again.
- MG 1000B IP Phones registered to the main office using S2 are not redirected to the MG 1000B TPS during IP Phone firmware upgrade at the main office. MG 1000B IP Phones registered using S2 receive firmware upgrades in the same manner as main office IP Phones. The first time the MG 1000B IP Phone reboots after the firmware upgrade,

it is directed to the MG 1000B TPS using S1. Any different firmware is applied at that time, before the IP Phone is redirected back to the main office TPS.

- MG 1000B IP Phones registered using S1 are redirected back to the MG 1000B Signaling Server for any firmware upgrades, as described in "Firmware downloads" (page 215).
- MG 1000B IP Phones registered using S2 do not display "Test Local Mode."

Configuring the S2 IP Address parameter

For detailed information on configuring IP Phones, refer to *IP Phones Fundamentals* (NN43001-368). This section contains a brief summary.

To configure the S2 parameter, do the following:

Step	Action
1	Reboot the MG 1000B IP Phone.
2	When the "Nortel" banner displays, quickly press the four keys under the display in sequence, from left to right.
3	Program the IP address, subnet mask, and gateway addresses for the MG 1000B IP Phone.
4	Program the S1 IP Address, action, and retry parameters. The S1 IP Address is the MG 1000B Node IP Address.
5	Program the S2 IP Address, action, and retry parameters. The S2 IP Address is the main office Node IP Address.
6	Program the remaining parameters. The IP Phone reboots again.

--End--

If the MG 1000B IP Phone can register with the main office using S1, it is redirected to the main office TPS and operates as a normal Branch User.

If the MG 1000B IP Phone cannot register with the main office using S1 after the number of programmed S1 retries, it uses S2 to register with the main office as a regular online main office user.

Multiple Appearance DN (MADN)

IP Phones with the same DN at the Branch Office

When the MG 1000B Server processes incoming calls from a local trunk or from an analog (500/2500-type) or digital telephone, the Server determines if the dialed DN is a Multiple Appearance DN (MADN). If any telephone in

an MADN arrangement is analog or digital, or if one or more IP Phones are registered in Local Mode at the Branch Office, the call terminates at the Branch Office. In this case, the analog (500/2500-type) or digital telephones, and the IP Phones registered to the MG 1000B Core, ring. IP Phones registered to the main office do not ring.

In other words, if the MG 1000B Server can terminate the call to any telephone in the Branch Office that belongs to the MADN arrangement, the call does not reroute to the main office.

IP Phones with the same DN at the main office

If a call is made to an MADN at the main office, all MADN appearances, including those on MG 1000B IP Phones in Normal Mode, ring. Any appearance can answer the call. MADN appearances on MG 1000B IP Phones in Local Mode do not ring.

Emergency services

Support for access to emergency services by Branch Users in Normal Mode is configured at the main office. For more information on Emergency services, see *Emergency Services Access Fundamentals* (NN43001-613)

The key difference between the main office user and the Branch User is the route selected for the emergency call. An emergency call must be handed off to the PSTN over a trunk at the central office that is geographically closest to the caller — this means that there is normally an emergency trunk in the main office, and one in each of the branch offices. An emergency call originating from an MG 1000B IP Phone must route from the main office Call Server to the MG 1000B Server so that the call can be sent on the MG 1000B PSTN.

ATTENTION
In Normal Mode, an IP Phone must have a Virtual Trunk available and configured between the main office and Branch Office to complete an emergency services call.

ATTENTION
Do not route ESA calls to a node that has no direct ESA trunks.

Refer to “Routing ESA calls” (page 199) for more information on routing ESN calls.

There are two general methods to specify which digit string results in a call to emergency services:

- Use the Emergency Services Access (ESA) feature. This is the preferred method in North America, the Caribbean and Latin America (CALA), and in those countries that are members of the European

Union. ESA provides specific features and capabilities required by legislation in these jurisdictions.

- Use a special dialing sequence, such as a Special Number (SPN) in the Network Alternate Route Selection (NARS) data block.

Refer to "Emergency Services configuration" (page 199) for more information on ESA and SPN configuration.

Configuring ESA for emergency services

Beginning with Communication Server 1000 Release 5.0 and later ESA, it is possible to configure up to 16 distinct ESDNs to better suit the needs of a multinational enterprise. With support for Multiple ESDN you are no longer restricted to a single ESDN for use in placing emergency calls.

If all sites were using the same ESDN, a conflict would occur in the NRS. The conflict is resolved by using a unique prefix for each site, which the main office adds as it routes the call. The suggested prefix is the ESN home location code of the MG 1000B Server, or alternately, the Number Plan Area (NPA) code of the MG 1000B Server if there is not more than one Call Server in the NPA. Virtually any unique string can be used as a prefix because the call is sent to the NRS as an SPN. In the NRS, SPNs have their own separate numbering plan.

The Automatic Number Identification (ANI) data sent to the Public Safety Answering Point (PSAP) identifies the location of the caller. In some constituencies, legislation requires one DID per fixed number of square feet, so the physical location of the emergency can be approximated based on the telephone number delivered to the PSAP. The ESA feature has a comprehensive scheme that can be used to convert an extension into an appropriate DID.

If the Branch Office is relatively small, it can be easier to use a single, fixed DID number for the Branch Office. This can be configured using the CHG ZESA command in LD 117, where the <ESALocator> parameter is the DID telephone number to be sent for use by the PSAP to locate the source of the emergency call. For more information on this command, refer to *Emergency Services Access Fundamentals* (NN43001-613).

Configuring SPN for emergency services

Using an SPN for access to emergency services uses the digit manipulation capabilities configured for the MG 1000B zone as follows:

- If the Branch User is in Normal Mode, the user dials the Access Code for the local PSTN and the normal DN for emergency services.

  If the main office and Branch Office use the same DN for accessing emergency services, a conflict occurs in the NRS. The conflict is resolved by using the Zone Dialing Plan (ZDP) configured in the

Branch Office. The digits specified by the ZDP are prefixed to the dialed digits, and the call is then sent to the NRS as an SPN. In the NRS, the SPNs have their own separate numbering plan. The call is routed to the MG 1000B Call Server so that it can be sent out to the MG 1000B PSTN.

- If the Branch User is in Local Mode (or an analog [500/2500-type] or digital telephone at the MG 1000B), the user dials the Access Code for the local PSTN and the normal DN for emergency services access. This selects the appropriate trunk for local PSTN access.

MG 1000B Core interoperability

MG 1000B Core to MG 1000B Core interoperability is fully supported between Communication Server 1000 and Multimedia Communication Server 5100 (MCS 5100). A Network Connection Server (NCS) is required for Branch Office, Virtual Office, and Geographic Redundancy features to work.

Alternatively, Virtual Trunks can utilize the MCS 5100 H.323 Gatekeeper. In this case, at least one dedicated Signaling Server is required to run as the primary Communication Server 1000 NCS, where the H.323 endpoints are configured as non-RAS endpoints because Virtual Trunks will establish a connection with MCS, not NCS. During endpoint configuration on that NCS, set the NCS option to On; otherwise, all incoming requests from this endpoint are rejected. Set the Route cost to 1. Only those routes with the cost factor 1 are used for set redirections. However, the private numbering plan must be configured on both the MCS 5100 H.323 Gatekeeper and the NCS (Communication Server 1000 H.323 Gatekeeper). Without proper NCS server configuration, redirection to the main office does not work. For further information on configuring the Branch Office in the MCS database, refer to MCS documentation.

Network Wide Redundancy Phase II and Network Music

The Network Wide Redundancy Phase II feature interacts with the Branch Office feature. If you configure a Branch Office as an endpoint in the NRS, and an IP set in a node in an IP Network has NUID and NHTN configured to point to a Branch Office, the set is redirected to the Branch Office and registered as a Branch Office set.

The Network Wide Redundancy Phase II feature extends the Network Wide Redundancy sub feature of the Geographic Redundancy feature to small systems to provide survivability of IP telephones normally registered with a Communication Server 1000/2100. With this solution, you can register a number of IP sets with the Communication Server 1000 and to receive telephony services from it. Other IP sets are normally registered with a remote Communication Server 1000/2100 to receive telephony

services from the 2100/Communication Server 1000. In the case the link to the remote Communication Server 1000/2100 or to the remote 2100/Communication Server 1000 itself goes down, the IP telephones survive by registering with the local Communication Server 1000, which provides telephony services while the link to the Communication Server 1000/2100 or the Communication Server 1000/2100 itself is down. When the link to the remote 2100/Communication Server 1000 or to the remote Communication Server 1000/2100 itself is restored, the IP telephones are automatically redirected back to the remote Communication Server 1000/2100 to receive telephony services. Support for this feature is available in the MG 1000B to provide survivability to IP telephones normally registered with a CS 2100/Communication Server 1000.

The Network Music feature connects a Central Audio Server attached to a Communication Server 1000/2100 as the music source on demand to provide music to parties (be it through a CO trunk, TIE trunk, FX trunk, WATS trunk, virtual trunk, or extension) on hold in a Communication Server 1000. The Central Audio Server is accessed through a call to an external DN over an H.323/SIP virtual trunk or a TDM trunk. The virtual trunk or TDM trunk connects to a network music trunk through an analog TIE trunk, the Network Music TIE trunk. The virtual trunk implemented with an XUT pack (NT8D14) and a network music agent. Two trunk units in the XUT are used, one is configured as a Network Music trunk, the other is configured as an incoming-only Network Music TIE trunk. The two trunk units connect back to back, (for example,TIP lead to TIP lead and Ring lead to Ring lead). The TIE trunk is auto terminated to the network music agent, which is a PCA with a target PCA DN to ring the external DN to reach the Central Audio Server. When a party is put on hold, the party connects to the Network Music trunk, the capture of which initiates an incoming call to the Network Music TIE trunk. The incoming TIE trunk call is redirected to the Central Audio Server through the network music agent.

If an MG 1000B is to provide survivability, you require the SBO package (390).

The Network Music Service feature requires the packages shown in Table 27: Network Music Service Feature Packaging Requirements.

Figure 17
Network Music Service Feature Packaging Requirements

Package Mnemonic	Package Number	Package Description	Package Type (New or Existing or Dependency)	Applicable Market
MUS	44	Music	Existing	All
EMUS	119	Enhanced Music	Existing	All
PCA	398	Personal Call Assistant	Existing	All

For additional information see the*System Redundancy (NN43001-507)* ()NTP.

Planning and management

Contents

This chapter contains the following topics:

"Branch Office dialing plan" (page 87)

"Management" (page 92)

Branch Office dialing plan

Since IP Phone users can be located at a Branch Office equipped with an MG 1000B Core, the routing of calls to the local gateway is important (especially when toll charges apply to calls made from the central Call Server that controls the telephone). The administrator can configure digit manipulation through zone attributes for IP Phones to select a main office or Branch Office that provides PSTN access local to the destination of the call.

The Branch Office feature supports the various PSTN interfaces. Refer to *Electronic Switched Network: Signaling and Transmission Guidelines* (NN43001-280) for further information.

Calls from the PSTN to users within the network can be routed with the various ESN numbering plan configurations or the Vacant Number Routing (VNR) feature. This enables small sites, such as a Branch Office, to require minimal configuration to route calls through other Call Servers or through the NRS.

Outgoing calls can include local and, optionally, long-distance calls.

To access local PSTN resources, outgoing calls can be routed using ESN as well as zone parameters that enable digit insertion. The zone parameters force calls made by a Branch User to be routed to the desired local PSTN facilities.

For more information about PSTN configuration, see "Configuration example for PSTN resources at the Branch Office" (page 90).

Nortel recommends that the Branch User ID (BUID) be the same at the Branch Office as the DN at the main office. A BUID has a maximum of 15 digits. Under the recommended Coordinated Dialing Plan (CDP), it can be an extension (for example, 4567). Under the Uniform Dialing Plan (UDP), it is the user's main office DN, the Location Code (LOC), plus the Access Code (for example, 6 343-5555).

The main office DN must be an ESN-compliant DN. See "ESN Access Codes" (page 89).

For more information about CDP, refer to *Dialing Plans Reference* (NN43001-283). For details on other Numbering Plan options, refer to *Communication Server 1000S: Overview ,* (NN43031-110). For more information on ESN, refer to "ESN Access Codes" (page 89).

Emergency Services

To understand Emergency Service Access (ESA), see "Emergency services" (page 81). The main office Call Server supports only one Emergency Service DN (ESDN). If the ESDN is different at the Branch Office and at the main office, or if there is more than one emergency number, then a Special Number (SPN) must be configured to route ESA calls from the MG 1000B telephone to the MG 1000B PSTN. Refer to "Emergency Services configuration" (page 199).

Zone Based Dialing

The following components interact with this feature:

- CLID
- Features which depend on CLID
- DAPC
- Keymap download
- LNR
- ISDN (new ZBD IE)
- OCS
- Tone Table
- Call Pilot
- Call Park
- Remote Call Forward
- BSF
- GR
- Pre-translation

- EM
- VNR
- Call Forward
- Call Transfer
- Conference
- PD/Corp directory
- ESA

To provide Zone Based Dialing (ZBD) functionality, the numbering zone and zone-based flexible dial plan are introduced. Numbering zones are assigned to all sets and attendant, they contain zone specific information such as site prefix, country code, access prefixes (for international, national, subscriber calls). For every call, information is taken from the numbering zone to process a CLID.

Zones

The Branch Office feature enables IP Phones in more than one geographic location to have dialing plan behaviors that are localized to the location of the telephone rather than the location of the main office Call Server. Use different zone numbers for different branch offices. For additional information, see the *Communication Server 1000E: Planning and Engineering* (NN43041-220).

.

Music on Hold

For Branch Users in Normal Mode, the main office provides music to the user if Music on Hold is provisioned. The use of the G.729A, G.729 +VAD option, and G.723 codecs between the main office and the MG 1000B impacts the music quality.

ESN Access Codes

ESN data is configured with two Access Codes called AC1 and AC2. AC1 normally applies to long-distance calls, whether placed on or off the customer's private network (for example, dialing "6"). AC2 normally applies to local calls (for example, dialing "9"). For more information, refer to *Electronic Switched Network: Signaling and Transmission Guidelines* (NN43001-280).

Provisioning the IP Phones

Users must provision the IP Phone on any Call Server that provides service to that telephone. There is no automatic data synchronization between the main office Call Server and the MG 1000B Call Server.

Configuration example for PSTN resources at the Branch Office

IP Phones registered to the main office Call Server can be grouped into one of two categories:

- those configured with a main office dialing plan, similar to any other non-IP Phone at the main office
- those configured with a Branch Office dialing plan because the telephone is physically located in a Branch Office

Customer data must first be configured to recognize numbers that are local to each location (a standard NARS configuration issue). This example specifically focuses on the additional changes necessary to physically enable an MG 1000B telephone, registered with the main office Call Server, to reach PSTN resources in the Branch Office.

Assume that the main office and Branch Office have been configured with local numbers, such as 555-1212 or 967-1111.

Table 8 "Example dialing string, area codes, and Access Codes" (page 90) uses the following configuration at the main office for MG 1000B telephones to reach the PSTN.

Table 8
Example dialing string, area codes, and Access Codes

	At the main office node	At the Branch Office node
Local dialing string	Local calls use 7-digit dialing	Local calls use 7-digit dialing
Area code (NPA)	The NPA is 613	The NPA is 506
Country code	The main office Node Country Code is 1	The Branch Office Node Country Code is 1
NARS configuration	Local calls use AC2, which is "9" Long-distance calls use AC1, which is "6"	Local calls use AC2, which is "9" Long-distance calls use AC1, which is "6"
The Public National (E.164) entry points to...	"506" points to Branch Office node	"613" points to main office node

At the main office, the following items must be configured:

- Long-distance numbers in the same area code, such as 1-613-531-1234 or 1-613-320-1234.
- Long-distance numbers at the MG 1000B are configured to go over the Virtual Trunk and use PSTN trunks at the Branch Office, such as 1-506-555-1212 or 1-506-472-1234.
- All other long-distance numbers have other routing as appropriate (1-NPA-NXX-XXXX).

At the Branch Office, the following items must be configured:

- Long-distance numbers in the same area code, such as 1-506-234-1234 or 1-506-675-1234.
- Long-distance numbers at the main office are configured to go over the Virtual Trunk and use PSTN trunks at the main office, such as 1-613-967-1111 or 1-613-555-1212.
- All other long-distance numbers have other routing as appropriate (1-NPA-NXX-XXXX), but most are routed through the main office.

If a main office telephone goes off-hook and dials "9 555-1212," the Call Server assumes the user intends to reach the number 555-1212 in the local NPA. The fully-qualified number (E.164) is 1-613-555-1212.

If an MG 1000B IP Phone goes off hook and dials "9 555-1212," the MG 1000B Call Server assumes that the user intends to reach the number 555-1212 in the NPA that is local to the Branch Office, and thus the fully qualified number (E.164) is 1-506-555-1212.

Since the main office must reach the MG 1000B PSTN resources (through the MG 1000B Core), the call is treated like a PSTN toll-avoidance call. (This is a private-network-routed call with public network termination.)

Zone configuration description

Configure Branch Office features on the IP Phones using the Branch Office zone characteristics in LD 117 at the main office. For example, assuming that telephones in the Branch Office are in zone 10, use the commands given in Table 9 "LD 117 Zone configuration example." (page 91)

Table 9
LD 117 Zone configuration example.

Command	Description
CHG ZBRN 10 YES	Sets the flag that shows (literally, in the PRT ZONE output) whether the zone is a main office or Branch Office zone.

Table 9
LD 117 Zone configuration example. (cont'd.)

Command	Description
CHG ZACB 10 AC2 AC1	Tells the system the NARS Access Codes for local dialing and the NARS Access Code to convert the call into a long-distance call, to route the call to the Branch Office. In this case we are converting a call, such as "9 555-1212" into the call "6 1 506 555-1212", a conversion from AC2 to AC1.
CHG ZDP 10 1 506	Specifies the additional digits needed to convert a local call to a long-distance call. In this case, insert the PSTN Access Code for long-distance (which also happens to be the country code in North America) and the NPA into the digit string. The system can recognize when these values are already present, so if the user were to dial "9 506 555-1212" only the "1" would be added when the conversion to "6 1 506 555-1212" is performed.
ENL ZBR 10 LOC	Enables the Branch Office zone behaviors. Other options can be enabled or disabled separately. For instance, the LOC command turns on the local dialing option, also called "dial 9 for outside line". This can also be applied to long-distance calls originating in the MG 1000B.

The dialed digits can now be converted to a long-distance format. It is up to NARS to partially route the number over the private network to take advantage of any long-distance benefits.

Management

The following sections pertain to MG 1000B management. Refer to *System Management Reference* (NN43001-600).

Remote Access

Remote Access to the MG 1000B Server is available through Ethernet connection or remote login through a dial-up modem.

Element Manager

The Element Manager application:

- configures the Voice Gateway Media Card for IP Line
- configures the IP Phone Terminal Proxy Server (TPS)
- configures the Virtual Trunks
- upgrades the Voice Gateway Media Card
- upgrades the IP Phone firmware
- manages CS1000E and CS1000M information, such as:
  - customer data
  - routes
  - trunks

— the IP telephony node
— Electronic Switched Network (ESN) data
— Digital Signal Processing (DSP) channels
— Branch Office zone features
— Emergency Services Access at the Branch Office
— Daylight Savings Time at the Branch Office

Traffic measurement

Traffic measurement at the Branch Office includes calls involving local trunks, Virtual Trunks, and analog and digital devices. It does not include calls of MG 1000B IP Phones in Normal Mode with any terminal at the main office, or any other Branch Office in the network. However, IP Phone calls to devices or local trunks at the Branch Office are counted as incoming Virtual Trunk calls to the analog or digital devices or local trunks.

When an IP Phone is in Local Mode, any calls to or from the IP Phone are included in the traffic measurement at the Branch Office.

Call Detail Recording (CDR)

The format of CDR output for the Branch Office feature is no different from the existing CDR format.

CDR at the Branch Office reports calls processed at the MG 1000B Call Server. CDR includes:

- incoming Virtual Trunk calls to local devices
- incoming Virtual Trunk calls to outgoing local analog and digital trunks
- incoming local trunks (analog and digital) to outgoing Virtual Trunks
- incoming local trunk calls to local devices
- local device calls (IP Phones in Local Mode, analog (500/2500-type) telephones and digital telephones) to outgoing local trunks
- local device calls to outgoing Virtual Trunks

Calls from MG 1000B IP Phones in Normal Mode generate CDR records at the main office for the following call types involving MG 1000B IP Phones:

In the case of VO Logged out phones, CDR records will not be generated since the emergency TNs are fully restricted.

- Incoming Virtual Trunks – CDR records are generated when a call from another Call Server in the network over a Virtual Trunk terminates at an MG 1000B IP Phone.
- Incoming local (analog and digital) trunks – CDR records are generated when a call from the local PSTN terminates at an MG 1000B IP Phone.
- Outgoing Virtual Trunks – CDR records are generated when an MG 1000B IP Phone makes a call to another Call Server in the network over a Virtual Trunk, to a device at the Branch Office, or to a destination over the local trunks at the Branch Office. An associated CDR record is also generated at the Branch Office when the call involves MG 1000B facilities. When the call goes out on the local trunks at the Branch Office, the CDR record shows the user as having made a long-distance call to the PSTN at the Branch Office.
- Outgoing local trunks (analog and digital).

The identifying digits in the main office Call Server's CDR log are the manipulated string as specified by the Branch Office zone. For example, the Branch Office user dialed "9, 555-1212", but the main office Call Server changes it to "6, 1-613-555-1212". CDR records the dial string as "1-613-555-1212". In other words, the main office Call Server produces a CDR record indicating that the user dialed a "long-distance" digit string because the feature converts the call from a local dialing pattern to a long-distance dialing pattern.

System security

CS1000E and CS1000M (Large System) system security is explained in detail in *Security Management Fundamentals* (NN43001-604). This is required reading for any Branch Office administrator. Refer to *System Management Reference* (NN43001-600) for additional information.

Nortel recommends that the Station Control Password (SCPW) be longer than four characters. This recommendation is not enforced by the software. The SCPW does not have to be the same in the main office and the Branch Office, but the user can set them to be the same for convenience.

Unauthorized access

When using Branch User Config during the installation phase, a branch password and a main office password are required. The branch password is the IP Phone Installer's Password or the Temporary IP Phone Installer's Password. If the required password is not configured, an error message (or otherwise failure to login) results. Three failed attempts lock that particular user ID from logging in for one hour. The lock is recorded in the TPS system log, and is printed to the Teletype Terminal (TTY). The

system administrator can clear the lockout. Also, rebooting or reregistering the telephone to the TPS node can also clear the lock. “Signaling Server CLI commands” (page 223)

Three failed attempts to enter the main office password also locks the user out (this time at the main office Call Server). The main office Call Server lock can be removed only by an administrator using a LD 32 command to disable and re-enable that Terminal Number (TN) at the main office. For additional information, see the *Communication Server 1000E: Planning and Engineering (NN43041-220)* NTP.

IP Security

IP security (IPsec) for Communication Server 1000 networks is centrally managed from the IPsec for Intra System Signaling Security (ISSS) management interface of the Primary UCM server. ISSS employs IPsec to provide security services, including confidentiality, authentication, and antireplay, to application layer protocols. Communication Server 1000 provides simple, automated IPsec policy configuration and avoids the complex configuration requirements inherent in many implementations of IPsec.

ISSS network elements, or targets, are classified into two categories:

- UCM targets: these elements automatically belong to the UCM security domain; you need not add them using the UCM ISSS management interface. An example of a UCM target is a Call Server.
- Manual targets: you must manually configure these elements using the UCM ISSS management interface before you can enable ISSS. An example of a manual target is Call Pilot.

ISSS can manage up to a maximum of 1500 combined UCM and manual targets.

For more information on IP Security, see *Security Management Fundamentals* (NN43001-604).

Patch Management

This feature has the following dependencies and restrictions:

- Linux dependency: This feature does not support Linux SS.
- The Server and Gateway Controller must support CS 1000 Release 7.0. The CP PII and SSC are not supported.
- This feature is not backward compatible.
- This feature is not applicable for Loadware PEP’s.
- Special Instructions appear by using PLIS command but not the overlay commands.

Adding a Branch Office

Contents

This chapter contains the following topics:

"Introduction" (page 97)

"Main office requirements" (page 98)

"Implementation summary" (page 100)

"Adding a Communication Server 1000 Release 7.0 Branch Office to a Main Office with a previous software release" (page 102)

Introduction

To install a Branch Office:

Step	Action
1	Upgrade the main office to Communication Server 1000 Release 7.0 software. For more information, refer to *Communication Server 1000E - Software Upgrades* (NN43041-458) or *Communication Server 1000M and Meridian 1 Large System Upgrades Overview* (NN43021-458), or *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).
2	Configure the Branch Office implementation parameters at the main office before installing the Branch Office. These parameters are the dialing plan, zone parameters, IP Phone parameters, and passwords.
	--End--

A Communication Server 1000 Release 7.0 Branch Office can only be added to a Communication Server 1000E or 1000M main office running Communication Server 1000 Release 5.5 or later software. However, branch offices that already exist in the network can run a previous release of the software. In this case, you must choose whether or not to upgrade the set firmware for the existing branch offices. You can choose not to

upgrade the firmware at the existing branch offices only if the IP Phones in those branch offices are running at least the minimum version of firmware as specified in *IP Phone Fundamentals* (NN43001-368).

If you choose to upgrade the firmware, you must upgrade the firmware at the existing branch offices first. The main office may not require a firmware upgrade, depending on its current version.

Refer to "Firmware downloads" (page 215) for more information on upgrading firmware for IP Phones.

Main office requirements

The Branch Office feature requires IP Peer H.323 Trunk (H323_VTRK) package 399. This package is required to support H.323 functionality. Overlap Signaling (OVLP) package 184 is included with package 399.

The main office requires the following software packages to support the specified Basic Network features. Refer to *Basic Network Feature Fundamentals* (NN43001-579) for more information on these features.

- Network Call Back Queuing (MCBQ) package 38. This package is required for IP Phones to invoke any queuing feature or Ringback When Free feature.
- Network Speed Call (NSC) package 39. This package is required for IP Phones to invoke the Network Speed Call feature.

The main office requires the following software packages to support the specified ISDN Primary Rate Interface features. Refer to *ISDN Primary Rate Interface Fundamentals* (NN43001-569) for more information on these features.

- Network Attendant Service (NAS) package 159. This package is required for analog (500/2500-type) telephones in the Branch Office to access attendant services when the attendant is configured on the main office.
- Network Message Services (NMS) package 175. This package is required for analog (500/2500-type) telephones in the Branch Office to share the voicemail system in the main office. For any configurations using centralized Call Pilot on the main office with one or more branch offices in separate time zones, the NMS package is required at the main office for the branch IP Phones.

Optional features

- Network Alternate Route Selection (NARS) package 58. Refer to *Basic Network Feature Fundamentals* (NN43001-579).
- Overlap Signaling (OVLP) package 184. This package is optional; it is required for overlap signaling. It is packaged with H.323 Virtual Trunk (H323_VTRK) package 399.
- Emergency Services Access (ESA) package 329. This package is optional; it is required only to receive 911/ESA features in North American and some Caribbean and Latin American (CALA) markets. Refer to *Emergency Services Access Fundamentals* (NN43001-613).
- Virtual Office (VIRTUAL_OFFICE) package 382 and M3900 Phase III Virtual Office Enhancement (VIR_OFF_ENH) package 387. These packages are optional; they are required only for Virtual Office functionality.
- Network Signaling (NSIG) package 37. This package is optional for IP Phones to access set-based Network Class of Service (NCOS) features.
- Adaptive Network Bandwidth Management package 407.
- Alternate Routing for Network Bandwidth Management
- SIP Gateway and Converged Desktop (SIP) package 406. This package is optional; it is required to support SIP functionality.

Branch Office requirements

The Branch Office feature requires the hardware described in "MG 1000B platform hardware description" (page 41). The MG 1000B Call Server also requires the following software packages:

- Command Status Link (CSL) package 77
- Integrated Services Digital Network (ISDN) package 145
- Flexible Numbering Plan (FNP) software package 160. Refer to *Dialing Plans Reference* (NN43001-283)
- Overlap Signaling (OVLP) package 184. This package is required only if overlap signaling is to be implemented in the Branch Office. Refer to *IP Peer Networking Installation and Commissioning* (NN43001-313).
- Enhanced ACD Routing (EAR) package 214
- Enhanced Call Trace (ECT) package 215
- Emergency Services Access (ESA) package 329
- Virtual Office (VIRTUAL_OFFICE) package 382 and M3900 Phase III Virtual Office Enhancement (VIR_OFF_ENH) package 387. These

packages are optional; they are required only for Virtual Office functionality.

- SBO package 390
- IP Peer H.323 Trunk (H323_VTRK) package 399. This package is optional; it is required for H.323 functionality. The packaging for package 399 also includes package 184.

ATTENTION
These packages are automatically enabled in the Branch Office software.

The Branch Office feature also requires the SIP Gateway and Converged Desktop (SIP) package 406 for SIP. This package may or may not be automatically enabled in the Branch Office software, depending on the region in which the software is used.

The feature packages listed above are automatically enabled in the Branch Office software.

If the main office is equipped with Location Code Expansion (LOCX) package 400, the Branch Office must also have this package. Refer to *ISDN Primary Rate Interface Fundamentals* (NN43001-569).

The keycodes used to install software at the Branch Office differ from those used to install software at the main office.

Implementation summary

To prepare for a Branch Office, refer to the *Communication Server 1000E: Planning and Engineering (NN43041-220)* NTP. This contains important electrical information and safety guidelines.

Follow these steps to implement the Communication Server 1000 Branch Office:

Step	Action
1	At the main office: **a** Upgrade the main office software to Communication Server 1000 Release 7.0. Refer to , *Communication Server 1000E - Software Upgrades* (NN43041-458) or *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315) **b** If not already implemented, implement IP Peer Networking as part of a system installation or upgrade. Refer to *IP Peer Networking Installation and Commissioning* (NN43001-313).

c Configure the Branch Office zones. .

d Configure the Branch Office dialing plan.

e Configure the IP Phone passwords. See Procedure 8 “Setting and changing the Station Control Password Configuration” (page 127).

f Use NRS Manager to add the System Host Name of the MG 1000B Signaling Server to the H.323 endpoint list. This action enables the Signaling Server at the Branch Office to register with the Gatekeeper (H.323). Refer to *Network Routing Service Installation and Commissioning* (NN43001-564).

2 For each Branch Office:

a Install the MG 1000B Core. See “Installing an MG 1000B Core” (page 131).

b Install the MG 1000B Signaling Server. For more information on installing the Signaling Server, see*Signaling Server IP Line Applications Fundamentals* (NN43001-125) .

c Install the Branch Office software, starting with Server and Gateway Controller.

Software for the MG 1000B Server and Gateway Controller comes with preprogrammed data that can be selected during the installation procedure. For Co-resident Call Server and Signaling Server, use the UCM Deployment Manager to install the software. For more information about installing the Co-resident Call Server and Signaling Server, see *Co-resident Call Server and Signaling Server Fundamentals* (NN43001-509).

d Configure the Branch Office (Customer Data Block and ELAN subnet). For more information about configuring a new or existing Bandwidth Management zone, see*IP Peer Networking Installation and Commissioning* (NN43001-313)

e Configure the Branch Office dialing plan.

f Configure the Voice Gateway Media Cards. Refer to *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

Use the same zone for DSP physical TNs and IP Phone TNs. The zone number must match that at the main office. Refer to *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

g Install and provision the local trunks (the XUT, PRI, and DTI cards).

h If applicable, configure Abbreviated Dialing.

i Provision the Virtual Trunks. Refer to *IP Peer Networking Installation and Commissioning* (NN43001-313).

When configuring NRS, enable the Network Connection Service (NCS). Ensure that each Branch User ID (BUID) is entered in the Branch Office numbering plan so it points to the main office. For survivability reasons, ensure that the Signaling Server uses the same H.323 ID. This ensures that the Branch User will be properly redirected to the Main Office. In a pure SIP environment, ensure that the Signaling Server H.323 ID matches the SIP endpoint name on NCS. For more information, see"Adding the Branch Office endpoints to the NRS database" (page 175).

j Install MG 1000B telephones, starting with "Installing and configuring IP Phones" (page 177).

--End--

Adding a Communication Server 1000 Release 7.0 Branch Office to a Main Office with a previous software release

The Communication Server 1000 Release 7.0 Branch Office feature requires a Main Office running CS 1000 Release 7.0. Therefore, you must upgrade the Main Office to CS 1000 Release 7.0 before you upgrade the Branch Office to CS 1000 Release 7.0.

Two options are available when an existing Main Office running a prior release requires the addition of a new Branch Office. These options are:

1. Upgrade the entire network to Communication Server 1000 Release 7.0, and then add the new Branch Office (see "Upgrade the entire network to Communication Server 1000 Release 7.0" (page 102)).
2. Upgrade only the Main Office to Communication Server 1000 Release 7.0, and then add the new Branch Office (see "Upgrade only the Main Office to Communication Server 1000 Release 7.0" (page 103)).

If, in a given network, there is one or more Succession 3.0 Branch Offices, all Branch Offices must be upgraded to Communication Server 1000 Release 4.5 before you can upgrade the Main Office to Communication Server 1000 Release 7.0

For information about upgrading the IP Phone firmware, see *IP Phone Fundamentals* (NN43001-368). For information about upgrading and reconfiguring the Signaling Server software, see *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

Upgrade the entire network to Communication Server 1000 Release 7.0

To upgrade the entire network to Communication Server 1000 Release 7.0:

Step	Action
1	At the Main Office: **a** Upgrade the Call Server software to Communication Server 1000 Release 7.0. **b** Upgrade the main office Signaling Servers software to Communication Server 1000 Release 7.0 with the Automatic Firmware Upgrade set. **c** Reconfigure the main office Signaling Server to configure the NRS. **d** Upgrade the main office Voice Gateway Media Cards to Communication Server 1000 Release 7.0.
2	At each existing prior release Branch Office: **a** Replace any SSC cards with a supported Gateway Controller. Replace any CP PII to a supported Server platform. (Communication Server 1000 Release 7.0). **b** Upgrade the MG 1000B Signaling Servers software to Communication Server 1000 Release 7.0 with the Automatic Firmware Upgrade set. **c** Reconfigure the MG 1000B Signaling Servers to configure the NRS. **d** Upgrade the MG 1000B Voice Gateway Media Cards to Communication Server 1000 Release 7.0.
3	Execute the **`umsUpgradeAll`** command on the Main Office Signaling Servers if necessary.
4	Install the new Communication Server 1000 Release 7.0 Branch Office as described in “Implementation summary” (page 100).
	--End--

Upgrade only the Main Office to Communication Server 1000 Release 7.0

ATTENTION
A mixed software configuration between the CS 1000 Release 7.0 Main Office and Branch Offices running CS 1000 Release 4.5, 5.0, 5.5, or 6.0, is permitted. In this case, indefinite operation with a mixed software configuration is supported.

If you choose to upgrade only the Main Office to Communication Server 1000 Release 7.0, you have the option of upgrading the IP Phone firmware. Specifically, the options are:

1. Upgrade the IP Phone firmware in the existing CS 1000 Release 4.5, 5.0, 5.5, or 6.0 Branch Offices (see “Upgrade Main Office with IP Phone firmware upgrade” (page 104)).
2. Do not upgrade the IP Phone firmware in the existing CS 1000 Release 4.5, 5.0, 5.5, or 6.0 Branch Offices (see “Upgrade Main Office without IP Phone firmware upgrade” (page 105)).

Upgrade Main Office with IP Phone firmware upgrade

To upgrade the Main Office to Communication Server 1000 Release 7.0 and upgrade the IP Phone firmware in Communication Server 1000 Release 4.5, 5.0, 5.5, or 6.0 Branch Offices to Communication Server 1000 Release 7.0:

Step	Action
1	At the Main Office: **a** Upgrade the Call Server software to Communication Server 1000 Release 7.0. **b** Upgrade the Main Office Signaling Server(s) software to Communication Server 1000 Release 7.0 with the Automatic Firmware Upgrade set. **c** Reconfigure the Main Office Signaling Server to configure the NRS. **d** Upgrade the Main Office Voice Gateway Media Cards to Communication Server 1000 Release 7.0. **e** If necessary, execute the **`umsUpgradeAll`** command on the Main Office Signaling Server(s).
2	At each existing Communication Server 1000 Release 4.5, 5.0,. 5.5, or 6.0 Branch Office: **a** Upgrade the IP Phone firmware to Communication Server 1000 Release 7.0 IP Phone firmware.
3	Execute the **`umsUpgradeAll`** command on the Main Office Signaling Server(s), if necessary.
4	Install the new Communication Server 1000 Release 7.0 Branch Office as described in “Implementation summary” (page 100).

--End--

Upgrade Main Office without IP Phone firmware upgrade

To upgrade the Main Office to Communication Server 1000 Release 7.0 without upgrading the IP Phone firmware in the existing Communication Server 1000 Release 4.5, 5.0, 5.5, or 6.0 Branch Offices:

Step	Action
1	At the Main Office: **a** Upgrade the Call Server software to Communication Server 1000 Release 7.0. **b** Upgrade the Main Office Signaling Server software to Communication Server 1000 Release 7.0 with the Automatic Firmware Upgrade set. **c** Reconfigure the main office Signaling Server to configure the NRS. **d** Upgrade the Main Office Voice Gateway Media Cards to Communication Server 1000 Release 7.0.
2	At each existing Communication Server 1000 Branch Office: **a** If necessary, execute the **`isetResetAll`** command on the MG 1000B Signaling Server(s).
3	Install the new Communication Server 1000 Release 7.0 Branch Office, as described in “Implementation summary” (page 100).

--End--

Converting a small system to a Branch Office

Contents

This chapter contains the following topics:

"Introduction" (page 107)

"Requirements" (page 107)

"Conversion" (page 108)

Introduction

Customers with a Communication Server 1000M installed base can re-configure existing satellite small system to function as Branch Offices. This configuration allows customers to incorporate systems that were previously stand-alone into a Branch Office network.

ATTENTION
This document demonstrates, to the customer, how to upgrade Communication Server 1000M small system into Survivable MG1000E.

Where no main office exists, one office can be configured as the main office, and the others converted to branch offices. Alternatively, if a main office already exists, each of the other offices can be converted to a Branch Office and associated with that main office. Therefore, customers with a number of small systems can obtain the advantages of the Branch Office feature without replacing their existing hardware.

Once a small system has been converted to a Branch Office, it cannot revert directly back to a stand-alone system.

Requirements

Any system can be configured as a Main Office, as listed in "Main office hardware description" (page 41).

You can convert the following small systems to a Branch Office:

- single-cabinet Meridian 1 Opt 11C Cabinet
- single-chassis Meridian 1 Opt 11C Chassis with or without a chassis expander
- single-cabinet CS1000M Cabinet
- single-chassis CS1000M Chassis, with or without a chassis expander

You can convert only single-cabinet and single-chassis systems (with or without a chassis expander). You must first reduce multiple-cabinet and multiple-chassis Small Systems to single cabinets or chassis.

To function as a Branch Office, the small system must be equipped with the following components:

- a Gateway Controller that meets the requirements for Communication Server 1000 Release 7.0 software.
- DSP resources provided by the Gateway Controller or Voice Gateway Media Cards.
- a Signaling Server: if you add a Signaling Server to a previously CISPR Class B system (previously used in some specific countries), the system complies to Class A, as noted in the front and back pages of this document.

For more information about preparing a small system for conversion, see*Communication Server 1000E - Software Upgrades* (NN43041-458).

Conversion

A Main Office must exist before you can convert a small system to a Branch Office. The Main Office must be a Communication Server 1000M or Communication Server 1000E system.

For more information about instructions on upgrading an existing system to the latest Communication Server 1000 software release, see *Communication Server 1000M and Meridian 1 Large System Upgrades Overview* (NN43021-458) or *Communication Server 1000E - Software Upgrades* (NN43041-458). For more information about instructions on installing a Signaling Server, see *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

If you add a Signaling Server to a previously CISPR Class B system (previously used in some specific countries), the system complies with Class A, as noted in the front and back pages of this document.

If a main office does not exist, you can designate an existing office as a main office. Refer to “Main office configuration” (page 115) for instructions on setting up a main office.

Implementation summary

CAUTION
Service Interruption
Converting an existing small system is equivalent to installing a new Branch Office, and service is interrupted during the conversion process.

The duration of the service outage depends on the extent of reconfiguration required at the existing small system and main office sites.

While it may theoretically be possible to convert a fully pre-equipped small system without shutting down service, Nortel recommends a cold start for the Branch Office installation.

ATTENTION
Nortel recommends that you back up your database before beginning the conversion. Use the EDD command in LD 43 or use Element Manager to perform the datadump.

Use the following steps to convert a small system to a Branch Office and incorporate it into a Branch Office network:

Step	Action
1	Configure the main office: **a** Follow the procedures in ""“Implementation summary” (page 100)," step 1 to set up and configure the main office. **b** Use the new keycode to change the Licenses to allow for the additional requirements of the associated branch offices. In particular, ensure that the IP USERS and BASIC IP USERS licenses are increased to include the total number of IP Phones in the main offices and the new branch offices.
2	For each small system that is to be converted to a Branch Office: **a** Power down the system, including reserve power if so equipped. **b** Remove the SSC card. **c** Add a Gateway Controller with DSP resources **d** For a VxWorks Call Server, add a CP PM Call Server card with security dongle. For a Co-resident Call Server and Signaling Server, add a supported Server. For CP PM cards,

ensure the CP PM has at least 2 GB of RAM and a 40 GB drive.

e Install a Voice Gateway Media Card if required. Refer to *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

If the small system already has a Voice Gateway Media Card, upgrade it to IP Line 5.0. Refer to *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

f Install a Signaling Server if required. Follow the procedures in “Installing a Signaling Server” (page 149).

A Signaling Server must be installed on an single-cabinet Meridian 1 Opt 11C Cabinet or a single-chassis Meridian 1 Opt 11C Chassis with or without a chassis expander. A Communication Server 1000M Signaling Server already has a Signaling Server installed.

g Configure the Signaling Server.

1. Run the Signaling Server Install Tool, as described.
2. Transfer the node information using Element Manager.

h Install the Branch Office software, using the Branch Office keycodes. Configure the Gateway Controller.

The software for a Branch Office is significantly different from the software for a small system. Media Gateway 1000B licenses are orderable for expanding capability. The Media Gateway 1000B uses the standard license increment codes. Unique codes are available for Branch office. The balance of the Branch licenses are set at a default limit and cannot be incremented or decremented.

Media Gateway 1000B licenses are orderable for expanding capability and are highlighted in the table below. The Media Gateway 1000B uses the standard license increment codes. Branch office unique codes are listed in the following table, see Figure 18 "Media Gateway 1000B Parameters" (page 111).

Figure 18
Media Gateway 1000B Parameters

Media Gateway 1000B Parameters	APAC Defaults	CALA Defaults	EMEA Defaults	NA Defaults	DSN Defaults	Order Increments
TNS	5000	5000	5000	5000	5000	n/a
ACDN	300	300	300	300	300	n/a
AST (association of set with CTI server)	400	400	400	400	400	n/a
LTID	0	0	0	0	0	n/a
RAN_CON	120	120	120	120	120	n/a
RAN_RTE	120	120	120	120	120	n/a
MUS_CON	120	120	120	120	120	n/a
BRAND	2	2	2	2	2	n/a
ACD_AGENTS	400	400	400	400	400	n/a
Analog User - NTM487CB	**0**	**0**	**0**	**0**	**0**	**8**
ATTENDANT_CONSOLES	16	16	16	16	16	n/a
BRI_DSL	150	150	150	150	150	n/a
CLASS User - NTM487DB	**0**	**0**	**0**	**0**	**0**	**8**
DATA_PORTS	2500	2500	2500	2500	2500	n/a
Digital User - NTM487AB	**0**	**0**	**0**	**0**	**0**	**8,**
IP User	400	400	400	400	400	n/a
Basic IP User	0	0	0	0	0	n/a
PHANTOM_PORTS	400	400	400	400	400	n/a
DECT User - standard code	**0**	**0**	**0**	**0**	**0**	**NA/CALA=0 AP/EMEA=8**
DECT Visitor (AP/EMEA only)	**0**	**0**	**0**	**0**	**0**	**NA/CALA=0 AP/EMEA=8**
SIP CONVERGED DESKTOPS	0	0	0	0	0	Set to 400 if NTE95049 is provisioned
SIP CTI TR87	0	0	0	0	0	Set to 400 if NTE95049 is provisioned
ITG_ISDN_TRUNKS	0	0	0	0	0	n/a
H.323 Access Port - standard code	**30**	**30**	**30**	**30**	**30**	**1**
SIP Access Port - standard code	**30**	**30**	**30**	**30**	**30**	**1**
TRADITIONAL_TRUNKS	120	120	120	120	120	n/a
TMDI_D-CHANNELS	0	0	0	0	0	n/a
DCH	64	64	64	64	64	n/a
SURVIVABILITY	0	0	0	0	0	n/a
Temporary IP User	0	0	0	0	0	n/a

Note: CPPM based systems do use TMDI channels. Channels will be counted with DCH license.

i Configure the Branch Office (Customer Data Block and ELAN subnet).

j Configure the Branch Office dialing plan.

k Configure the Voice Gateway Media Cards. Refer to *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

Use the same zone for DSP physical TNs and IP Phone TNs. The zone number must match that at the main office. Refer to *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

l Install and provision the local trunks (the XUT, PRI, and DTI cards). Refer to *Communication Server 1000M and Meridian 1 Small System Installation and Commissioning* (NN43011-310).

m If applicable, configure Abbreviated Dialing.

n Provision the Virtual Trunks. Refer to *IP Peer Networking Installation and Commissioning* (NN43001-313).

When configuring NRS, enable the Network Connection Service (NCS). Ensure that each Branch User ID (BUID) is entered in the Branch Office numbering plan so it points to the Main Office. This ensures that the Branch User will be properly redirected to the main office. Ensure the Signaling Server H.323 ID matches the gateway endpoint name on NRS (in SIP environment as well) Refer to "Adding the Branch Office endpoints to the NRS database" (page 175) for more information.

o Configure the IP Phones as Branch Users. Refer to "Branch User Config" (page 181) for details on Branch User Configuation.

--End--

Upgrading to Communication Server 1000 Release 7.0

Contents

This chapter contains the following topics:

- "Introduction" (page 113)
- "Upgrading to Communication Server 1000 Release 7.0" (page 113)

Introduction

This chapter describes upgrading an existing main office and its associated branch offices from Communication Server 1000 Release 6.0 to Communication Server 1000 Release 7.0.

When you upgrade the Branch Office, the following components remain unaffected:

- telephone services between MG 1000B IP Phones in Normal Mode
- telephone services between MG 1000B IP Phones in Normal Mode and main office telephones or trunks other than those to the Branch Office

Communication Server 1000 Release 6.0 and later software is required to enable and configure SIP Line Service. Configure the SIP client telephony users as Universal Extensions of subtype SIP Line.

As part of the Communication Server 1000 Release 7.0 software upgrade process, you must save, restore, and upgrade the Communication Server 1000 IP Telephony Nodes with Communication Server 1000 Release 7.0 software.

Upgrading to Communication Server 1000 Release 7.0

Upgrade the Main Office and Branch Office systems to Communication Server 1000 Release 7.0.

CAUTION
LOSS OF DATA
VxWorks based Branch Office systems do not require a CP PM card BIOS upgrade.

Procedure 1
Upgrading the Main Office to Communication Server 1000 Release 7.0

Step	Action
1	Upgrade the main office software to Communication Server 1000 Release 7.0 through the deployment manager, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).
	ATTENTION Signaling Server software is available on the Linux platform only.
2	Upgrade the main office Voice Gateway Media Cards to Communication Server 1000 Release 7.0.
3	Upgrade the MG 1000B Voice Gateway Media Cards to Communication Server 1000 Release 7.0.

--End--

Procedure 2
Upgrading the Branch Office to Communication Server 1000 7.0

Step	Action
1	Upgrade the Small System to Communication Server 1000 Release 7.0.
2	Upgrade the branch office software to Communication Server 1000 Release 7.0 through the Deployment Manager, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).
	ATTENTION Signaling Server software is available on the Linux platform only.

--End--

Main office configuration

Contents

This chapter contains the following topics:

"Introduction" (page 115)
"IP Telephony Nodes" (page 115)
"Adding Linux servers to a Node" (page 120)
"SIP Client configuration" (page 120)
"UNIStim LTPS" (page 125)
"Zone Based Dialing" (page 124)
"Gateway application services" (page 125)
"IP Phone passwords and parameters" (page 125)
"MG 1000B IP Phone configuration" (page 128)

Introduction

This section describes the configuration of zones, IP Phone passwords and parameters, and MG 1000B IP Phones at the main office.

Branch Office configuration procedures at the Branch Office are discussed separately in "Branch Office configuration" (page 173)

For more information about Main Office configuration, see *IP Peer Networking Installation and Commissioning* (NN43001-313). Also refer to *Communication Server 1000E Installation and Commissioning* (NN43041-310) or *Communication Server 1000M and Meridian 1 Large System Installation and Commissioning* (NN43021-310) , appropriate for the system.

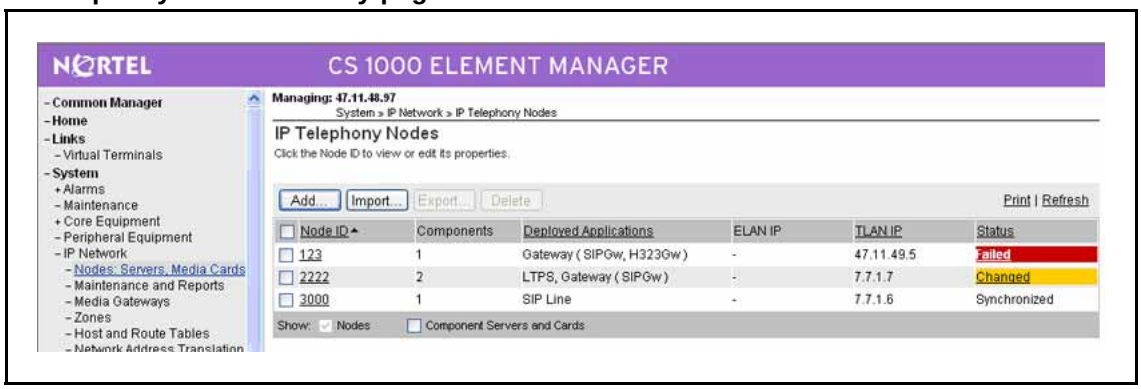
IP Telephony Nodes

The Element Manager application, within the UCM, provides an interface to configure IP Telephony Nodes in a Communication Server 1000 system.

The IP Telephony page displays every Node that is saved on the Call Server where Element Manager starts. Node details, such as server elements, application services configured, IP address information, and overall node status appear in the summary page.

To view the IP Telephony Nodes Web page, select the Nodes: Servers, Voice Gateway Media Cards link in the IP Network branch of the Element Manager navigator. The IP Telephony Node page appears as shown in Figure 19 " IP Telephony Node summary page" (page 116).

Figure 19
IP Telephony Node summary page



The IP Telephony Nodes Web page contains the following functionality which links you to the associated Web pages:

- Add - add a new node
- Import - import a node file
- Export - export a node file
- Delete - delete a node

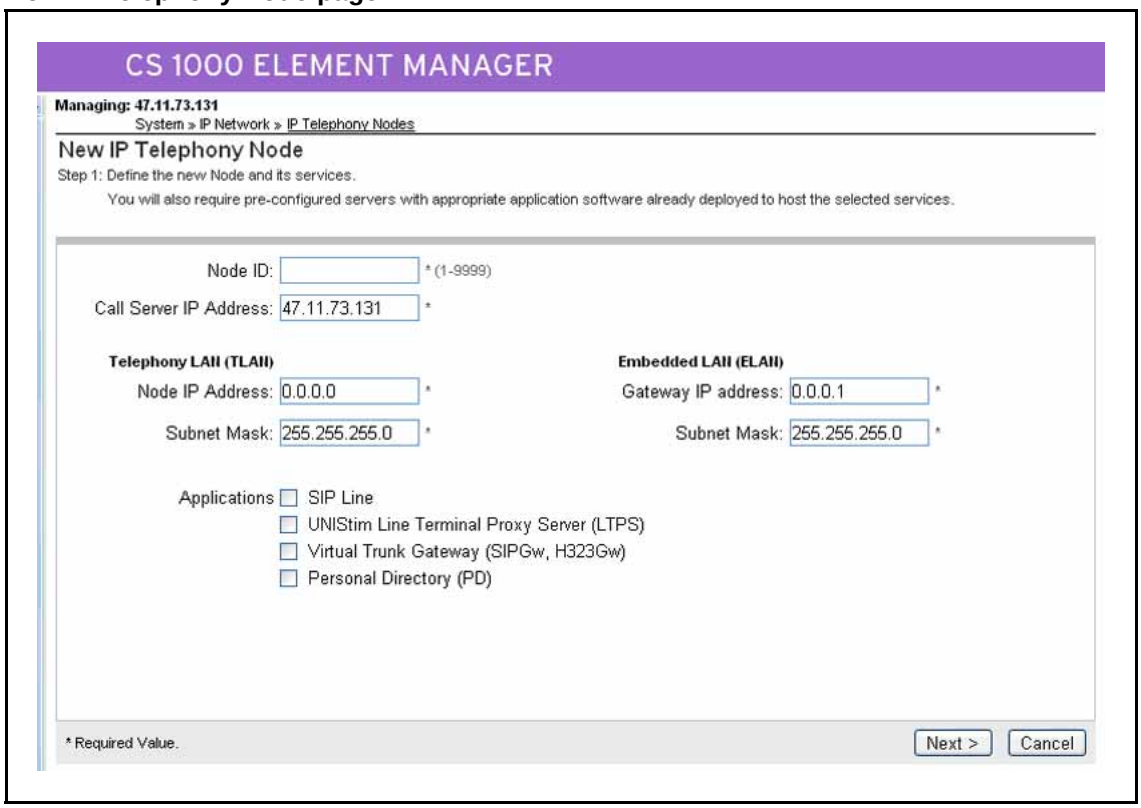
Procedure 3
Adding a Node to the Call Server

Step	Action
1	Log on to Element Manager.
2	From the navigation pane, select **System** , **IP Network** , **Nodes: Servers, Voice Gateway Media Cards** to display the **IP Telephony summary** page.
3	Click **Add** to add a new Node to the Call Server.
4	In the **New IP Telephony Node** page (see Figure 20 "New IP Telephony Node page" (page 117)) enter the Node general

properties, for example, Node ID, Node IP address, ELAN, and TLAN.

--End--

Figure 20
New IP Telephony Node page



For more information about the IP Telephony Management, see *Element Manager System Reference – Administration* (NN43001-632). For more information about adding a new IP Telephony node, see *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

Importing an IP Telephony Node file

Use the import functionality to import a local configuration file from a local work station (XML format) or from a Linux signaling server.

Procedure 4
Importing an IP Telephony Node file

Step	Action
1	Log on to Element Manager.

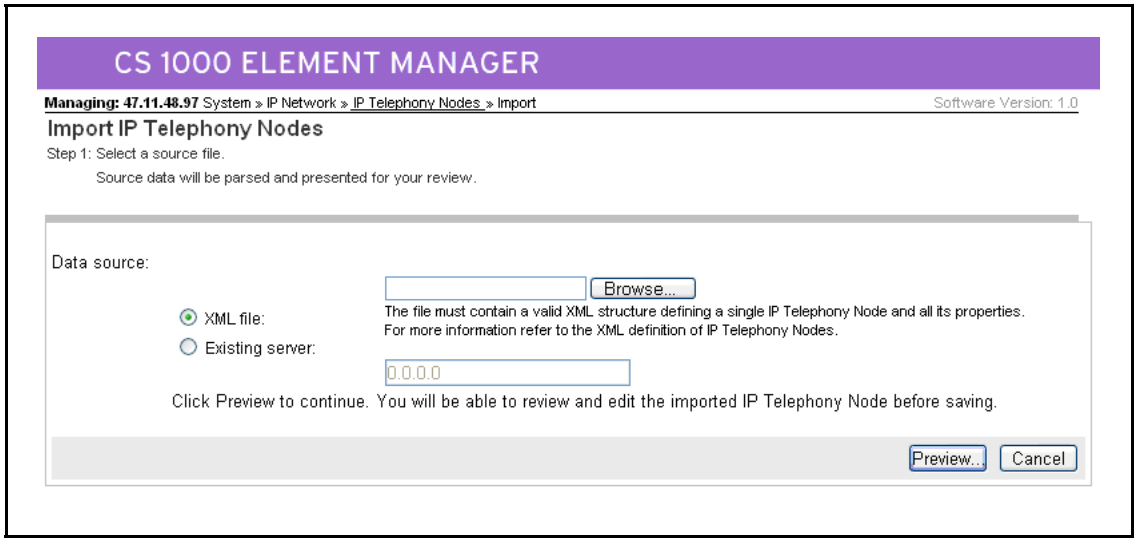
2 From the navigation pane, select **System** , **IP Network** , **Nodes: Servers, Voice Gateway Media Cards** to display the **IP Telephony** page.

3 Click **Import** to import an IP Telephone Nodes file.

4 In the **IP Telephony Import** page (see Figure 21 "IP Telephony Import page" (page 118)) import from an XML file stored on local work station or import from a Leader server that is already part of a Node.

--End--

Figure 21
IP Telephony Import page



For more information about the IP Telephony Management, see *Element Manager System Reference – Administration* (NN43001-632). For more information about importing an IP Telephony Node file, see *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

Exporting an IP Telephony Node file

You can export a previously configured IP Telephony Node to an XML file format and save it to a local desktop. The Export function is limited to one selected Node at a time. If you select more than one node, the Export button remains disabled.

Procedure 5
Exporting an IP Telephony Node file

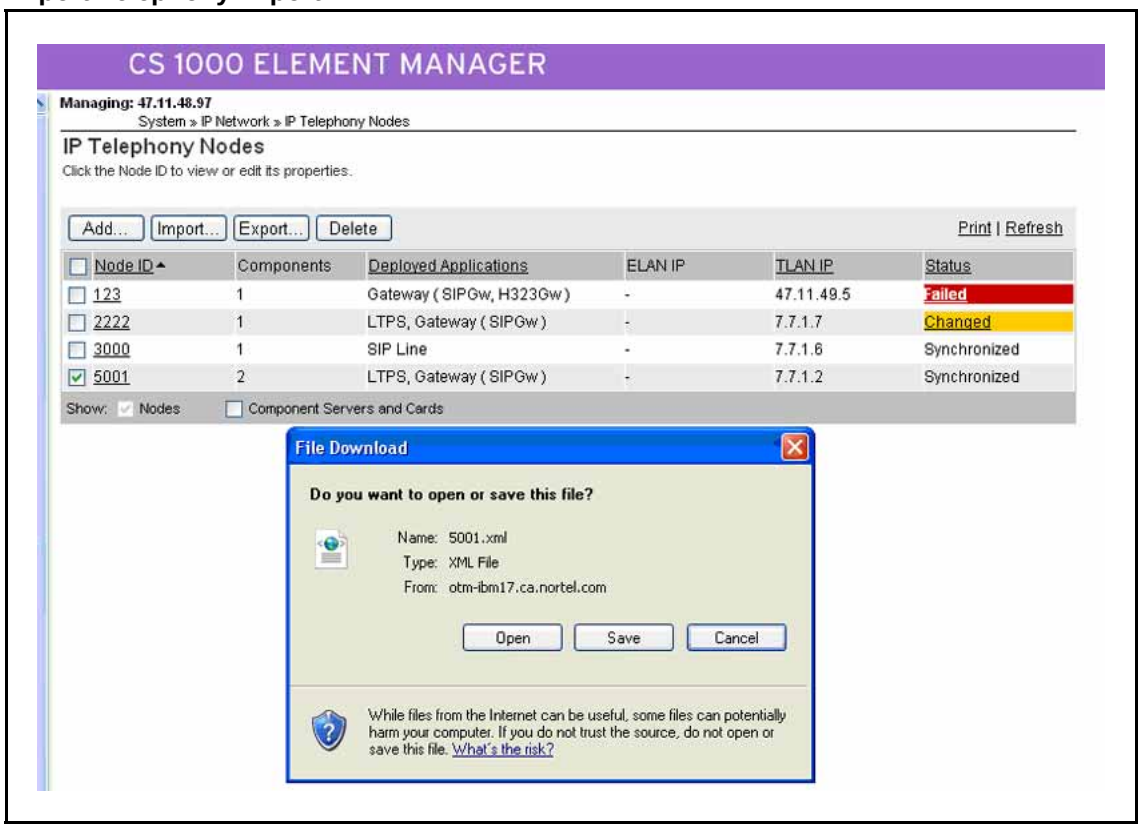
Step	Action
1	Log on to Element Manager.

2 From the navigation pane, select **System** , **IP Network** , **Nodes: Servers, Voice Gateway Media Cards** to display the **IP Telephony** page.

3 Click **Export** to save the configuration files in an XML format file as shown in Figure 22 "Export Telephony Import" (page 119).

--End--

Figure 22
Export Telephony Import



For more information about the IP Telephony Management, see *Element Manager System Reference – Administration* (NN43001-632). For more information about exporting an IP Telephony Node file, see *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

Procedure 6
Deleting an

Step	Action
1	Select, the Node and click **Delete**.

2 To confirm the deletion of the Node, click **OK** in the **Delete Confirmation** window.

--End--

Adding Linux servers to a Node

The UCM framework discovers every Linux server that is installed on the network. The UCM stores this list and the Node Management interface queries this list every time when a new server needs to be added in to the Node. The user can select one or more servers to be part of the defining Node.

For more information about adding a Linux server to a Node, see *Element Manager System Reference - Administration* (NN43001-632).

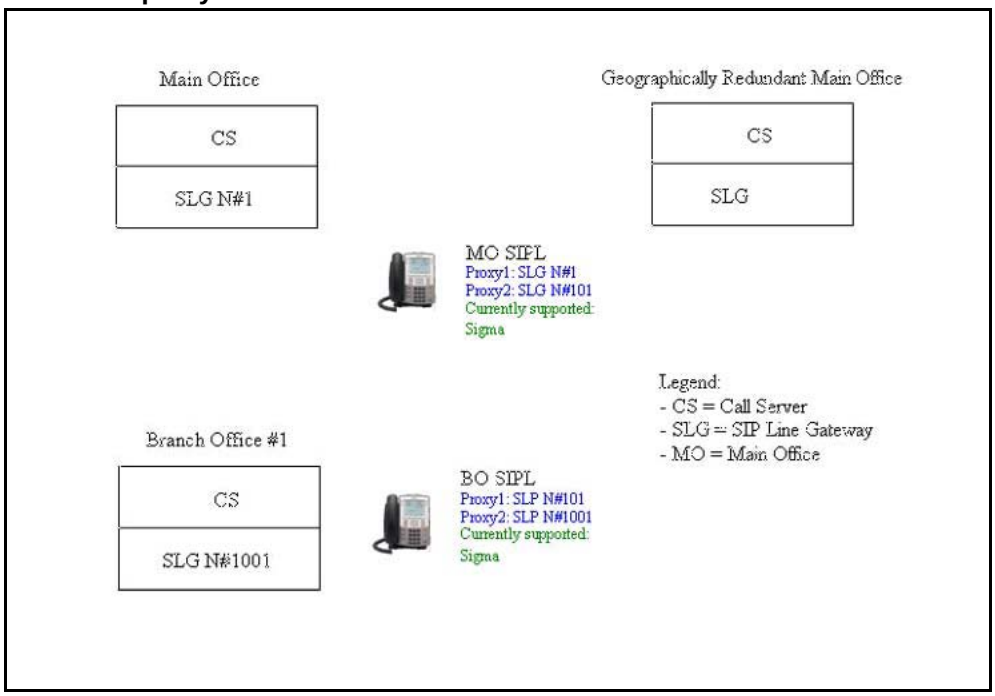
SIP Client configuration

This section describes how to configure the SIP clients in a Main Office (MO), Branch Office (BO), and Geographic Redundancy (GR) configuration using the S1/S2 solution.

Proxy Server 1 and Server 2 solution

The following illustration shows a proxy S1/S2 configuration with a Main Office (MO), Branch Office (BO), and Geographic Redundant Main Office (GR MO).

Figure 23
S1 and S2 proxy solution



SLG configuration

The following sections show examples of the SIP Line Services section of the config.ini file for the Main Office, Geographically Redundant Main Office, and Branch Office.

The following example shows the SIP Line Services section from the config.ini file for the Main Office.

```
[SIP Line Services]
SLP_IP=0.0.0.0
SLP_Port=5060
SLP_Transport=UDP
SLG_LocalSipPort = 5070
SLG_LocalTlsPort = 5071
SLG_Role = 0 --> 0-MO, 1-GR, 2-BO
SLG_Mode = 0 --> 0-Proxy mode
MO_SLG_IP = 0.0.0.0
MO_SLG_Port =
MO_SLG_Transport =
GR_SLG_IP =
GR_SLG_Port =
GR_SLG_Transport =
securityPolicy=0
clientAuthenticationEnabled=0
numByteRenegotiation=
x509CertAuthenticationEnabled=0
```

The following example shows the SIP Line Services section of the config.ini file for the Geographically Redundant Main Office.

```
[SIP Line Services]
SLP_IP=0.0.0.0
SLP_Port=5060
SLP_Transport=tcp
SLG_LocalSipPort = 5070
SLG_LocalTlsPort = 5071
SLG_Role = 1 --> 0-MO, 1-GR, 2-BO
SLG_Mode = 0 --> 0-Proxy mode
MO_SLG_IP =47.11.25.183 --> MO SLG IP
MO_SLG_Port =5070 --> MO SLG Port
MO_SLG_Transport =udp --> MO SLG Transport
GR_SLG_IP =
GR_SLG_Port =5070
GR_SLG_Transport =udp
securityPolicy=0
```

```
clientAuthenticationEnabled=0
numByteRenegotiation=
x509CertAuthenticationEnabled=0
```

The following example shows the SIP Line Services section of the config.ini file for the Branch Office.

```
[SIP Line Services]
SLP_IP=0.0.0.0
SLP_Port=5060
SLP_Transport=UDP
SLG_LocalSipPort = 5070
SLG_LocalTlsPort = 5071
SLG_Role = 2 --> 0-MO, 1-GR, 2-BO
SLG_Mode = 0 --> 0-Proxy mode
MO_SLG_IP =47.11.25.183 --> MO SLG IP
MO_SLG_Port =5070 --> MO SLG Port
MO_SLG_Transport =udp --> MO SLG Transport
GR_SLG_IP = 47.11.25.181 --> GR SLG IP
GR_SLG_Port =5070 --> GR SLG Port
GR_SLG_Transport =udp --> GR SLG Transport
securityPolicy=0
clientAuthenticationEnabled=0
numByteRenegotiation=
x509CertAuthenticationEnabled=0
```

TFTP server configuration (Nortel IP Phone 1120E and 1140E)

The following example shows the of DeviceConfig.dat file for the Trivial File Transfer Protocol (TFTP) server.

```
DNS_DOMAIN opt11c14.com --> SIPL DNS domain
SIP_DOMAIN1 opt11c14.com --> SIPL domain
SIP_DOMAIN2 bell
SIP_DOMAIN3 bell
SIP_DOMAIN4 bell
SIP_DOMAIN5 bell
SERVER_IP1_1 47.11.25.183 --> set to appropriate value
depending on SIPL type
SERVER_IP1_2 47.11.25.181 --> set to appropriate value
depending on SIPL type
...
SERVER_PORT1_1 5070 --> set to appropriate value depending
on SIPL type
SERVER_PORT1_2 5070 --> set to appropriate value depending
on SIPL type
SERVER_RETRIES1 2 --> keep alive retry counter before
```

```
switch over
SERVER_RETRIES2 2
...

#****************Device settings*****************
FORCE_BANNER YES
BANNER SLG
UPDATE_USERS NO
SIP_PING YES --> set to YES for keep alive

AUTOLOGIN_ENABLE YES

# Time configuration
DST_ENABLED YES
TIMEZONE_OFFSET -18000

VMAIL 2300
VMAIL_DELAY 300

AUTO_UPDATE YES
AUTO_UPDATE_TIME 0

DEF_LANG English
MAX_INBOX_ENTRIES 50
MAX_OUTBOX_ENTRIES 50
MAX_REJECTREASONS 5
MAX_PRESENCENOTE 5
MAX_CALLSUBJECT 5
RECOVERY_LEVEL 0

DEF_AUDIO_QUALITY High
DSCP_CONTROL 0
ENABLE_BT YES
#Address book mode - NETWORK, LOCAL, BOTH
ADDR_BOOK_MODE NETWORK
ADMIN_PASSWORD 4321
MAX_IM_ENTRIES 50
ENABLE_3WAY_CALL YES
TRANSFER_TYPE MCS
ENABLE_PRACK NO
REDIRECT_TYPE MCS --> set to MCS for Register redirection
support
DISABLE_PRIVACY_UI No
IM_MODE ENCRYPTED
VQMON_PUBLISH NO
VQMON_PUBLISH_IP 47.11.187.125
LISTENING_R_ENABLE YES
```

```
LISTENING_R_WARN 1
LISTENING_R_EXCE 1
PACKET_LOSS_ENABLE YES
PACKET_LOSS_WARN 1
PACKET_LOSS_EXCE 1
JITTER_ENABLE YES
JITTER_WARN 1
JITTER_EXCE 1
DELAY_ENABLE YES
DELAY_WARN 1
DELAY_EXCE 1
SESSION_RPT_EN YES
SESSION_RPT_INT 30
MADN_DIALOG YES
MADN_TIMER 15
PROXY_CHECKING NO
```

For SIP Line on the Main Office or Geographically Redundant Main Office, you must configure the following parameters:

- SERVER_IP1_1 as the IP address of the MO SLG#1 and SERVER_PORT1_1 as the port of the MO SLG#1.
- SERVER_IP1_2 as the IP address of the GR SLG#101 and SERVER_PORT1_2 as the port of the GR SLG#101.

For SIP Line on the Branch Office, you must configure the following parameters:

- SERVER_IP1_1 as the IP address of the GR SLG#101 and SERVER_PORT1_1 as the port of the GR SLG#101.
- SERVER_IP1_2 as the IP address of the BO SLG#1001 and SERVER_PORT1_2 as port of the BO SLG#1001.

Zone Based Dialing

To configure zone based parameters, the Zone Based Dialing (ZBD) option is activated using LD 15, after it is set to YES, the DIALPLAN prompt is shown and user can select public or private on-net dial plan.

Prompt	Response	Comment
REQ:	CHG	Change existing data block
TYPE:	FTR_DATA	Customer Features and options
VO_CUR_ZONE_TD	NO (YES)	

Prompt	Response	Comment
ZBD	NO (YES)	ZBD option
DIAL_PLAN	PUB/PRV	Type of dialing plan for DN/CLID displaying

The following procedure demonstrates a basic overview of the steps to follow to configure the ZBD. For more information on the ZBD, see *Dialing Plans Reference* (NN43001-283).

Step	Action
1	Enable the **Zone Based Dialing** option in **OVL15**,
2	Set the **dial plan** option to the appropriate dial plan **PUB** or **PRV**.
3	Configure the numbering zones from Overlay 117.
4	Configure numbering zone parameters.
5	Configure CLID entries for a key of a set.
6	Configure sets with numbering zones and appropriate CLIDs.

ATTENTION
The DN of a set should be 7 digits: PREF + shortDN.

--End--

PREF refers the prefix for a Dialed Number (DN), for example, in the following DN, 838-5775, 838 equals PREF.

UNIStim LTPS

Enable the UNIStim LTPS application on each node to enable it on each Server.

Gateway application services

SIP Gateway application service describes the configuration parameters when SIP Gateway is selected as a Gateway service. There are three options to configure on the Gateway configuration page; General, SIP Gateway Settings, and SIP Gateway Services.

For more information on configuring the Gateway, see *Element Manager System Reference - Administration* (NN43001-632)

IP Phone passwords and parameters

Procedure 7 “Setting the IP Phone Installers Password” (page 126) enables any trusted user to install a telephone from its keypad interface. Both main office and branch passwords are required.

Procedure 7
Setting the IP Phone Installers Password

Step	Action

The IP Phone Installer's Password is configured on one Signaling Server in a node. The passwords are then applied to all components in the node.Users must use the Temporary IP Phone Installer's Password if the SCPW is not configured.

1 From a computer terminal connected to the Signaling Server, open a command line shell at the main office TPS node.

2 For a permanent IP Phone Installer's Password, enter the CLI command **`nodePwdSet`**. For a Temporary IP Phone Installer's Password, enter the command **`nodeTempPwdSet`**. The command, related commands, and explanations are given in Table 10 "IP Phone node passwords" (page 126).

Table 10
IP Phone node passwords

Command	Description
nodePwdSet	Sets the node password. If a non-zero length password is configured, all IP Phones that attempt to register after this command is entered display a prompt for node password before the TN can be modified.
nodePwdShow	Shows the node password settings.
nodePwdEnable	Enables node password checking.
nodePwdDisable	Disables node password checking.
nodeTempPwdClear	Deletes the temporary password and resets its uses and time to zero.
nodeTempPwdSet	Sets the node-level TN entry temporary password.

For detailed command-line or Element Manager procedures, refer to *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

--End--

To use the Virtual Office feature, a Station Control Password (SCPW) must be configured at both the Branch Office and the Main Office. This procedure enables you to configure the length of the SCPW and the parameters for telephone modification. The actual SCPW password configuration takes place while configuring the telephone data through the overlays. Telephone data is discussed in "MG 1000B telephones" (page 177).

The SCPW is also used to access the user's Personal Directory, Callers List, and Redial List. The user can configure a second SCPW solely for this purpose if desired. If the user chooses to use the same SCPW for all applications, the SCPW must be the same at both the main office and Branch Office.

Procedure 8
Setting and changing the Station Control Password Configuration

Step	Action

The following steps are used to configure the SCPW.

1 Configure the length of the password, SCPL, to be of non-zero length in LD 15.

Table 11
LD 15 Configure the SCPW length in the Customer Data Block.

Prompt	Response	Description
REQ:	CHG	Change existing data.
TYPE:	FFC	Flexible Feature Code
SCPL	0-8	Length of SCPW, minimum recommended is 4 digits

2 Assign the Automatic Set Relocation security code.

Table 12
LD 15 Assign Automatic Set Relocation security code.

Prompt	Response	Description
REQ:	CHG	Change existing data.
TYPE:	FTR	Customer Features and options
CUST		Customer number
	0-99	Range for CSLS; and CS1000E; system
SRCD	(0000)-9999	Automatic Set Relocation security code X removes security code

3 Configure the Flexible Feature Code in LD 57 to enable Station Control Password Change (SCPC) and Set-Based Removal if desired.

Table 13
LD 57 Enable password change and set removal features.

Prompt	Response	Description
REQ	NEW	Add new data.
TYPE	FFC	Flexible Feature Code
CUST	xx	Customer number as defined in LD 15
FFCT	YES	Flexible Feature Confirmation Tone

Table 13
LD 57 Enable password change and set removal features. (cont'd.)

Prompt	Response	Description
CODE	SCPC	Station Control Password Change
- SCPC	xxxx	Code to invoke password change

4 The SCPW itself is configured during IP Phone configuration using LD 11 (see Procedure 9 "Configuring MG 1000B IP Phones at the main office using LD 11" (page 128)).

--End--

MG 1000B IP Phone configuration

After the Branch Office zones and passwords are provisioned, provision the MG 1000B IP Phones at the main office. These can be provisioned using LD 11 (see Procedure 9 "Configuring MG 1000B IP Phones at the main office using LD 11" (page 128)).

There is no automatic data synchronization between the main office Call Server and MG 1000B Call Server. The technician must provision the telephone on all pertinent Call Servers or Gateway Controllers.

MG 1000B IP Phone configuration using LD 11

Use Procedure 9 "Configuring MG 1000B IP Phones at the main office using LD 11" (page 128) at the main office to configure MG 1000B IP Phones.

Procedure 9
Configuring MG 1000B IP Phones at the main office using LD 11

Step	Action
1	Configure the Branch Office zones and dialing plan. S
2	Configure the following telephone data in LD 11: • Terminal type • Customer Number • TN • Zone • Prime DN to correspond to BUID

Table 14
LD 11 Provision Branch User and SCPW at the main office

Prompt	Response	Description
REQ:	NEW CHG	Add new data, or change existing data.
TYPE:	a...a	Terminal type. Type ? for a list of possible responses.
CUST	xx	Customer number as defined in LD 15.
ZONE	0-8000	Zone Number to which the IP Phone belongs. The zone prompt applies only when the TYPE is 2001P2, 2002P1/2002P2 2004P1/2004P2, or 2050PC/2050MC. Zone number is not checked against LD 117. **ATTENTION** The following phones are supported: 1100, 1210, 1220,1230,1110,1120,1140,1150, 2007, 2033 2210, 2211, 2212, 6110, 6112.
...		
SCPW	xxxx	Station Control Password. Must equal Station Control Password Length (SCPL) as defined in LD 15. Not prompted if SCPL = 0. Precede with X to delete.

--End--

MG 1000B platform hardware installation

Contents

This chapter contains the following topics:

"Installing an MG 1000B Core" (page 131)

"Upgrading the MG 1000B hardware" (page 138)

"Installing a Signaling Server" (page 149)

Installing an MG 1000B Core

For Communication Server 1000, the MG 1000B Core must contain a Server and a Gateway Controller. The Media Gateway can also contain the following interface cards:

- 32-port Voice Gateway Media Card
- Digital Trunk card
- Analog Trunk card
- Analog Line card
- Digital Line card
- Nortel Integrated Recorded Announcer card
- Nortel Integrated Conference Bridge Card
- cards to support CallPilot Mini or CallPilot 201i

To connect to the PSTN, use one of the following interface cards:

- 1.5 Mb T1 Multi-functional Digital Interface
- Extended Universal Trunk (analog)
- 2.0 Mb Digital Trunk Interface (DTI)
- 2.0 Mb Primary Rate Interface (PRI)

Each MG 1000B Core with a digital trunk card must have a clock controller. See *Circuit Card Reference* (NN43001-311).

The MG 1000B platform must have a Signaling Server. The CP PM or CP DC Signaling Server can be installed in the following card slots:

- Chassis NTDU14 slots 1-4
- Chassis NTDK91 slots 1-3
- Cabinet NTAK11 slots 1-10
- MG 1010 NTC310 slots 22-23

Readiness checklist

Before starting the installation, use the checklist in Table 15 "Readiness checklist" (page 132) to make sure you are ready.

Table 15
Readiness checklist

Have you:	ü
Read all safety instructions in *Communication Server 1000E: Installation and Configuration* (NN43041-310)?	
Received all equipment?	
Made sure the area meets all environmental requirements?	
Checked for all power requirements?	
Checked for correct grounding facilities?	
Developed an equipment layout plan for the system? This information is provided by your Planning and Engineering group.	
Completed the card slot assignment plan? This information is provided by your Planning and Engineering group.	
Obtained all the tools required to continue with the installation?	
Prepared the network data as suggested in *Converging the Data Network with VoIP Fundamentals* (NN43001-260) and *Communication Server 1000E Installation and Commissioning* (NN43041-310)?	

Tools checklist

To install the system correctly, make sure that the tools listed in Table 16 "Tools checklist" (page 133) are available before assembling the components.

Table 16
Tools checklist

Tools and components	Check
screwdrivers	
an ECOS 1023 POW-R-MATE or similar type of test meter	
appropriate cable terminating tools	
a drill for making lead holes	
a computer for connecting directly to the MG 1000B Core by a DTE—DTE null modem cable, with: • teletype terminal (ANSI-W emulation, serial port, 9600 bps) for the Call Server, MG 1000B Core, Signaling Server, and Voice Gateway Media Cards • a web browser for Element Manager and NRS Management (configure cache settings to check for new pages every time and to empty the cache when the browser is closed)	

Rack-mounting an MG 1000B

Items required

To install each MG 1000B or MG 1000B Chassis Expander in a 19-inch rack, use the following items:

- Equipment layout plan (for more information see, *Communication Server 1000E Installation and Commissioning* (NN43041-310).
- One pair of left and right guide brackets
- One pair of left and right ear brackets
- Eight #12-24 screws
- Four #8-32 machine screws

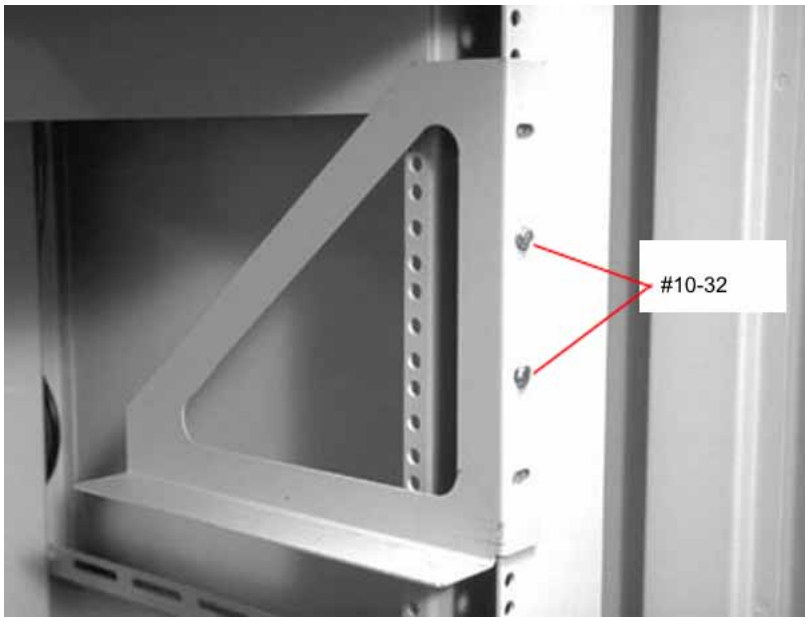
The NTTK09 kit contains all of the above items with the exception of the equipment layout plan and screws.

Procedure 10
Mounting the MG 1000B in a 19-inch rack

Step	Action
1	Fasten the right guide bracket to the right rack support. **a** Insert two #10-32 machine screws into the two middle slots in the guide bracket and into the respective holes in the right rack support. See Figure 24 "Guide bracket installed in a rack" (page 134).

b Fasten the screws.

Figure 24
Guide bracket installed in a rack



The guide brackets guide the MG 1000B into place and enable one person to install the MG 1000B in the rack.

2 Fasten the left guide bracket to the left rack support.

a Insert two #10-32 machine screws into the two middle slots in the bracket and into the respective holes in the left rack support.

b Fasten the screws.

3 Attach the right ear bracket (marked with an “R”) to the holes on the right side of the MG 1000B. See Figure 25 "Right ear bracket on an MG 1000B " (page 135).

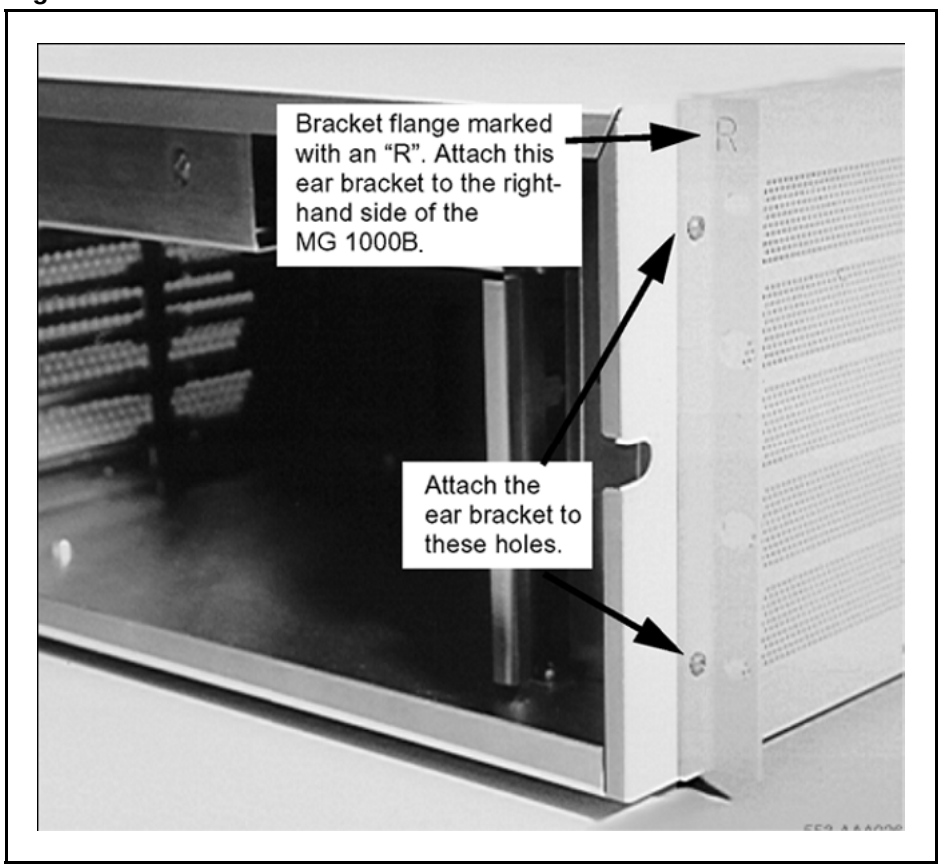
a Use two #8-32 machine screws. Position the ear bracket so that the four holes on the bracket flange are nearer to the rear of the MG 1000B.

> ***Note:*** To determine the front of the bracket, locate the “R” on the bracket. The “R” must be at the top of the bracket and face the front of the MG 1000B (see Figure 25 "Right ear bracket on an MG 1000B " (page 135)).

b Position the ear bracket so that the four holes on the bracket flange are nearer to the back of the MG 1000B. To determine the front of the bracket, locate the "R". This "R" must be at

the top of the bracket and must face to the front of the MG 1000B.

Figure 25
Right ear bracket on an MG 1000B



4 Attach the left ear bracket (marked with an “L”) to the holes on the left side of the MG 1000B (near the front).

a Use two #8-32 machine screws. Position the ear bracket so the four holes on the bracket flange are closer to the rear of the Media Gateway 1000.

Note: To determine the front of the bracket, locate the “L” on the bracket. The “L” must be at the top of the bracket and face the front of the MG 1000B.

WARNING
An MG 1000B or an MG 1000B Chassis Expander weighs approximately 30 lb. (13.5 kg) with circuit cards installed and 26 lb. (12 kg) without circuit cards installed. If necessary, get assistance when lifting the equipment.

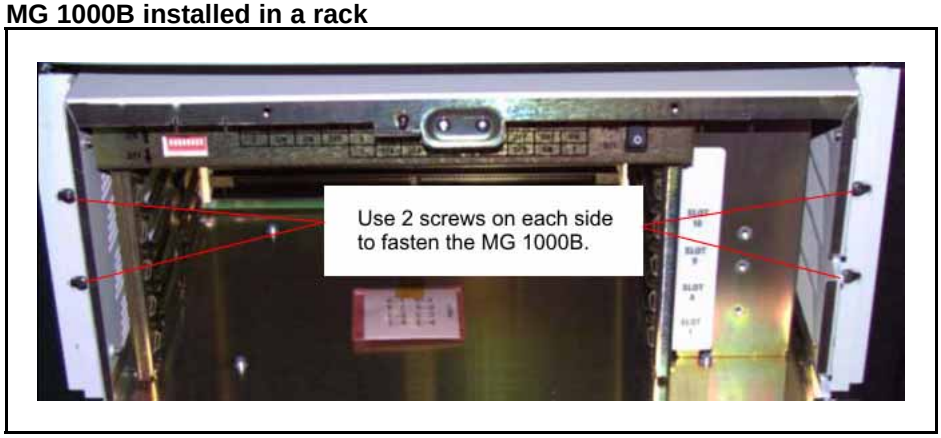
5 Place the MG 1000B on the guide brackets.

a Carefully slide the MG 1000B into the rack until the ear brackets come to rest against the rack support.

Note: Make sure that the rear of the MG 1000B is on the guide brackets.

6 Use the four remaining #10-32 machine screws to fasten the MG 1000B to the rack supports (two screws on each side). See Figure 26 "MG 1000B installed in a rack" (page 136).

Figure 26
MG 1000B installed in a rack



7 Install the equipment ground wires for the MG 1000B and Signaling Server. See *Communication Server 1000E: Installation and Configuration* (NN43041-310).

8 Install a UPS (if required) according to the manufacturer's instructions.

9 In the MG 1000B do the following:

a If using an card as the Gateway Controller, install the DSP software daughterboards on the card.

b Install the Gateway Controller into the chassis.

c Install the security dongle on the Server card.

d For the CP PM card, ensure the S5 dip switch to position 0.

e Install the Server card in the chassis.

f Install the Signaling Server hardware

- If you are using a CP PM Signaling Server, set the S5 switch to position 1 and install card in chassis.
- If you are using a commercial off-the-shelf (COTS) Signaling Server, rack-mount the Signaling Server as per the vendor's directions.

10 Install circuit cards in the MG 1000B. See *Communication Server 1000E: Installation and Configuration* (NN43041-310).

11 Make the Ethernet connections. Configure the Ethernet port to enable Element Manager connectivity as required.

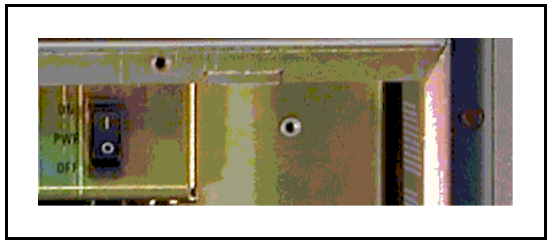
a See Procedure 18 “Connecting the Ethernet ports” (page 160).

Do not connect a serial port to the AUX connector. It can damage the port.

12 Set DIP switches on the power supply for the desired ringing voltage, ringing frequency, and message waiting voltage. These procedures are in *Communication Server 1000E Installation and Commissioning* (NN43041-310).

13 Connect the system to an AC power source. Make sure that the source matches the label on the back of the MG 1000B. Turn the power switch to "ON".

Figure 27
Power switch on the front of the MG 1000B chassis



14 Install any remaining equipment, such as alarms. See *Communication Server 1000E Installation and Configuration* (NN43041-310).

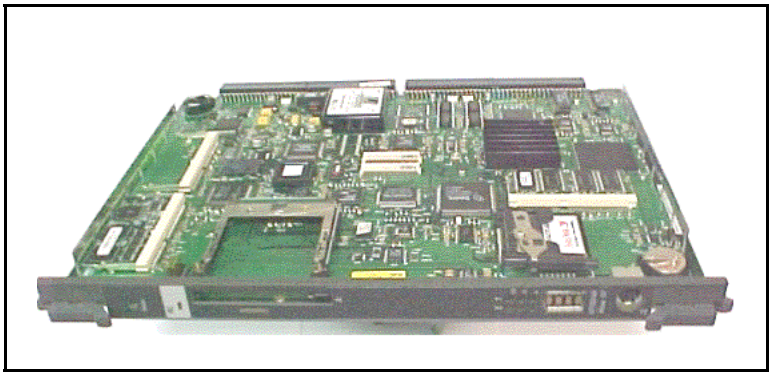
15 Reinstall the front covers on the MG 1000B.

--End--

Installing cards

In the MG 1000B, install Voice Gateway Media Cards. To install and configure the 8- or 32-port Voice Gateway Media Card (see Figure 28 "Voice Gateway Media Card" (page 138)) refer to *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

Figure 28
Voice Gateway Media Card



Install a trunk card to connect with the PSTN and an analog or digital line card to connect with local resources. Consult *Circuit Card Reference* (NN43001-311) for specific details and installation procedures of the various interface cards of the MG 1000B Core.

Upgrading the MG 1000B hardware

To upgrade the hardware for an MG 1000B, perform the following steps:

- Back up the database as shown in "Perform a customer backup data dump (installation release)" (page 139).
- Power down the Media Gateway.
- Remove the SSC card.
- Destroy or return the SSC security device to your local Nortel Repairs/ Returns center.
- If using a card as the Gateway Controller, Install the DSP Daughterboard on the card as described in Procedure 12 "Installing a DSP Daughterboard" (page 141).
- Install the Gateway Controller as described in Procedure 13 "Installing the Gateway Controller card" (page 143).
- Install the Server as described in Procedure 14 "Installing the CP PM or CP DC card" (page 144).
- Cable the cards as shown in "Gateway Controller network connections" (page 55).
- Power up the MG 1000B.
- Enter the 'setup' menu and configure the IP parameters, then reboot the Gateway Controller.

If the Centralized Software Upgrade (CSU) feature is enabled on the Call Server, the firmware for the Gateway Controller is downloaded automatically (or if the internal Compact Flash is blank), otherwise initiate the firmware download using Overlay 143 commands.

Perform a customer backup data dump (installation release)

Step	Action
1	Log in to the system.
2	Insert a Removable Media Device (RMD) into the active Server RMD slot to back up the database.
3	Load the Equipment Data Dump Program (LD 43). At the prompt, enter

Table 17
LD 43 – Load program

`LD 43`	Load program.
`.`	EDD

4 When EDD000 appears on the terminal, enter:

Table 18
Begin the data dump

`EDD`	Begin the data dump.

CAUTION
Service Interruption
Loss of Data

If the data dump is not successful, do not continue; contact your technical support organization. A data dump problem must be corrected before proceeding.

5 When DATADUMP COMPLETE and DATABASE BACKUP COMPLETE appear on the terminal, enter:

Table 19
Exit program

`****`	Exit program

--End--

Installing the cards

The following sections describe the process required to install the Gateway Controller and Server cards.

Procedure 11
Removing the SSC card

Step	Action
1	Unlatch the SSC card.
2	Remove the SSC card from its slot.

ATTENTION
The SSC card should be preserved for a minimum of five days.

It is illegal to continue to run the system software on the existing SSC card. Please DESTROY or RETURN the SSC dongle to your local Nortel Repairs/Returns center. No further orders will be accepted for the serial number since it will be decommissioned and tracked in Nortel's database.

--End--

Installing a DSP Daughterboard

Table 10 lists the configuration options for Position 1 and 2.

Table 20
DSP Daughterboard configurations

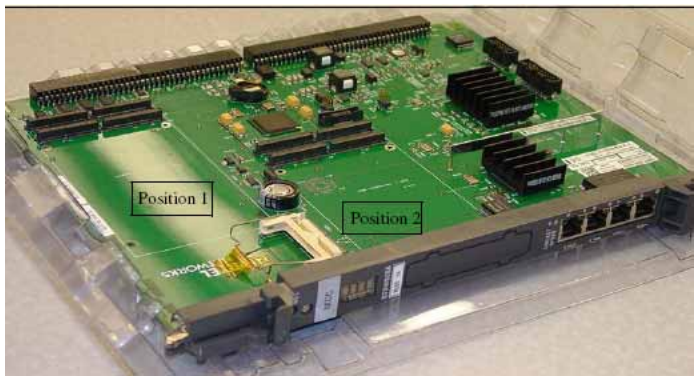
Position 1	Position 2
DB-32 (card slot 11)	None
None	DB-32 (card slot 0)
DB-32 (card slot 11)	DB-32 (card slot 0)
DB-96 (card slot 11, 12, and13)	None
DB-96 (card slot 11, 12, and 13)	DB-32 (card slot 0)
DB-128 (card slot 11, 12, 13 and 14)	DB-128 (card slot 0, 9., 10 and 15)

ATTENTION
Due to historical TN mapping for the Call Server SL1 software, even though the DSP channels will occupy Card 0 in the MG 1000Es, the TN (l s c u) 000 0 00 00, (that is, unit 0 of card 0 in the first Media Gateway) <supl sh> = 000 0) is not available.

A single channel (unit 0) is not available on the first Media Gateway only if there is a 32 port DB installed in daughterboard position #2. If there is a 96 port DB installed in daughterboard position #1, all 96 channels are available. If there is a 32 port DB installed in daughterboard position #1, all 32 channels are available.

The following procedure describes how to install a DSP Daughterboard on an card.

Figure 29
DSP Daughterboard



Procedure 12
Installing a DSP Daughterboard

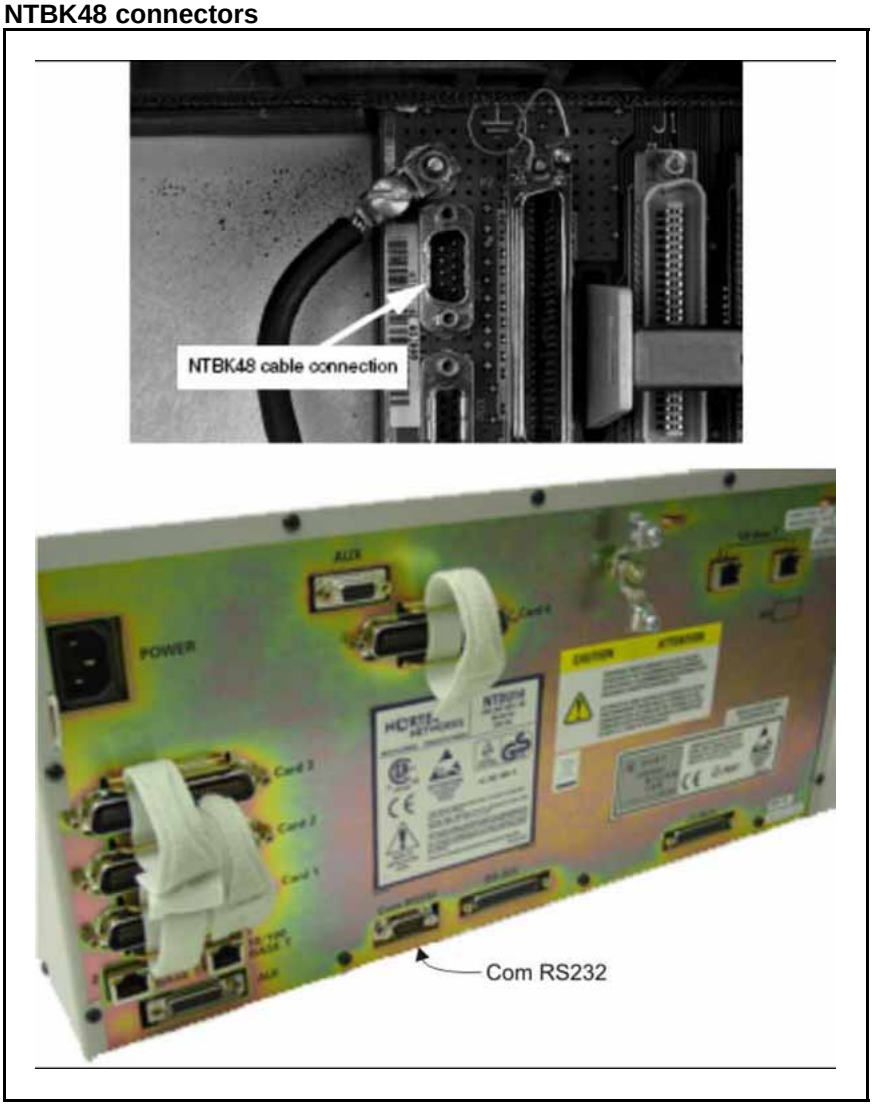
Step	Action
1	Place the on a safe ESD surface.
2	Place the DSP Daughterboard in either Daughterboard position 1, position 2, or both depending on how the Daughterboard will be configured from a TN perspective.
3	Ensure the DSP Daughterboard is securely attached to the (using supplied screws).

--End--

Gateway Controller installation

Reuse the existing 3-port SDI cable (NTBK48) for installation of a Gateway Controller in a MG 1000E cabinet or chassis. Connect it to the SDI port on the cabinet and the COM RS232 port on the chassis. Figure 30 "NTBK48 connectors" (page 142) illustrates the two connectors.

Figure 30
NTBK48 connectors



The 3-port SDI cable is not required for a Gateway Controller installation in a MG 1010 chassis. The MG 1010 MGU card faceplate ports provide the serial connectors. Use the NTC325AAE6 serial port adapter kit with a MG 1010.

Table 21
Gateway Controller serial port capabilities

Port	Modem Support?	Used for initial Configuration?
SD10	Yes (requires null modem to connect to a TTY)	Yes

SD11	No (No hardware flow control)	Yes
SD12	No (No hardware flow control)	No (Only available after FPGA is enabled. Not available during initial configuration menu display)

Procedure 13
Installing the Gateway Controller card

Step	Action
1	Insert the Gateway Controller into Slot 0 of the Media Gateway.

ATTENTION
Please DESTROY or RETURN the SSC dongle to your local Nortel Repairs/Returns center upon confirmation of a successful upgrade. If the SSC system was using remote dongles for any expansion cabinets, please DESTROY or RETURN to your local Nortel Repairs/Returns center upon confirmation of a successful upgrade.

Note: If the upgrade fails, you will not be able to revert back to the old system without the SSC card and dongle.

For the CP PM call server, you must use the dongle provided with the software kit. Chassis Expander dongles may be disposed of, as they are no longer needed.

2 Connect the serial cable.

- For the MG 1000E, connect the 3-port SDI cable (NTBK48AA) to the SDI0 port on the Media Gateway. Connect the opposite end of the cable to a maintenance terminal.
- For the MG 1010, connect a shielded CAT5 Ethernet cable to the NTC325AAE6 serial cable kit. Connect this cable to the MGU faceplate port labelled TTY0 in the Media Gateway. Connect the opposite end of the cable to a maintenance terminal.

3 Power on the Media Gateway.

- The Gateway Controller display shows BOOT.
- The power on self-test runs. The Gateway Controller display shows POST.

- The Gateway Controller display shows PASS if the self-test is successful. Otherwise the Gateway Controller display shows an Exxx error code.
- The Gateway Controller loads the application software. The Gateway Controller display shows LOAD.

--End--

Server card installation

The following procedures describes how to install a Server card in a Media Gateway.

MG 1010 slots 22 and 23 require the metal faceplate NTDW53 CP DC card or NTDW99 CP PM card. If you require more than two Server cards in a MG 1010, you can install the additional Server cards in slots 1-10. MG 1000E and MG 1010 slots 1-10 support NTDW53 CP DC cards, NTDW61, and NTDW99 CP PM cards.

Ensure that the Dip Switch (S5) is set to position 1 if using the CP PM as a Call Server or position 2 if using the card as a CP PM Signaling Server.

Procedure 14
Installing the CP PM or CP DC card

Step	Action
1	Ensure that the security dongle (the one that comes as part of the software kit) is inserted on the Server card. ***Note 1:*** The first step is applicable only when the Server card is used as a Call Server or Co-res CS and SS. ***Note 2:*** Remove the retainer clip from the FMD slot when the CP PM card is used as a Signaling Server. You must remove the clip to prevent it from shorting out adjacent cards.
2	Ensure that the FMD is correctly inserted and locked in place.
3	Insert the Server card. • Slide the Server card into Slot 1 (or higher) of the MG 1000E cabinet or chassis. • Slide the Server card into Slot 22 or 23 of the MG 1010 chassis.
4	Lock the card in place with the faceplate latches.

5 Connect the serial cable.

- For a MG 1000E or MG 1010 with Server cards in slots 1-10, connect the 2-port SDI cable. The 50-pin Amphenol NTAK19EC connects to the back of the Server.
- For a MG 1010, connect a shielded CAT5 Ethernet cable to a NTC325AAE6 serial port adapter. Connect this cable to the MGU faceplate port labelled TTY0 for CP1 or CP2. CP1 is for slot 22, CP2 is for slot 23.
- Connect the opposite end of the serial cable to the serial port on the maintenance terminal.

Note: To connect a terminal to the Server card with a NTAK19EC cable, complete the following steps:

- Connect the NTAK19EC cable to the 50 pin MDF connector on the back of the desired MG 1000E.
- Connect a 25 pin to 9 pin straight through serial cable to the 25 pin DB connector at the end of the NTAK19EC cable (a female to female gender changer may be required). You must povide this adapter.
- Connect the other end of the 25 pin to 9 pin straight through serial cable to the serial port on the maintenance terminal.

Figure 31
SDI cable

--End--

The preceding steps enable users to upgrade the system one MG 1000B at a time. For each additional Media Gateway, repeat Procedure 11 “Removing the SSC card” (page 140) to Procedure 14 “Installing the CP PM or CP DC card” (page 144).

The following procedure describes how to install and connect a CP MG card as a Server. Perform the following procedure to install the CP MG card into a Media Gateway cabinet or chassis.

Note: The CP MG card functions as a Gateway Controller and a Server while occupying one slot in a Media Gateway. You require different cables to connect to each component of a CP MG card.

Procedure 15
Installing the CP MG card

Step	Action
1	Ensure that the security dongle is inserted on the CP MG card.

2 Insert and slide the CP MG card into Slot 0 of a Media Gateway cabinet or chassis.

3 Lock the card in place with the faceplate latches.

4 Connect the serial cable:

Note: The NTC325AAE6 serial port adapter kit is required.

- Connect a Cat5e or Cat6 Ethernet cable to the TTY1 port on the CP MG faceplate.
- Connect a NTC325AAE6 serial port adapter (9 pin or 25 pin) to the other end of the Ethernet cable.
- Connect the Ethernet cable with serial port adapter to the serial port of a maintenance terminal.

Note: If you require a longer cable to reach your maintenance terminal, you can attach a standard serial port cable to the adapter for extended cable length.

5 Configure the maintenance terminal for VT-100 emulation, 9600 bps, 8-N-1.

6 Connect the ELAN cable:

- Connect one end of a shielded Cat5e or Cat6 Ethernet cable to the 1E (ELAN) port on the CP MG faceplate.
- Connect the other end of the cable to the ELAN subnet of the system.

7 Connect the TLAN cable:

- Connect one end of a shielded Cat53 or Cat6 Ethernet cable to the 2T (TLAN) port on the CP MG faceplate.
- Connect the other end of the cable to the TLAN subnet of the system.

8 Power on the CP MG card.

--End--

To connect and configure a CP MG card as a Gateway Controller, the 3-port SDI cable (NTBK48AA) is required. The NTBK48AA cable connects to the SDI port on the Media Gateway cabinet or chassis and provides serial port access to the Gateway Controller portion of the CP MG card.

Upgrading the CP PM software

Note: The CP PM version 1 hardware (NTDW61 and NTDW99BAE6) must run BIOS Release 18 or later to support the Linux base Operating System. The CP PM version 2 (NTDW99CAE6) meets the requirements for Linux base. CP PM version 2 includes an updated hardware design, BIOS, and boot manager.

Step	Action
1	Check that a terminal is connected to COM 1 port in CP 1. The settings for the terminal are: • Terminal type: VT100 • 9600 Baud • Data bits: 8 • Parity: none • Stop bits: 1 • Flow control: none
2	Insert the RMD into the CF card slot on the active core.
3	Press the manual RESET button on the CP PM card faceplate.
4	The CP PM card reboots. Press **F** when prompted to boot from the faceplate Compact Flash card containing the installation software. ***Note:*** For CP PM version 2 cards (NTDW99CAE6), pressing **F** enters the boot menu. Select Faceplate RMD, and press **Enter** to boot from the faceplate CF card.
5	Enter <CR> at the Install Tool Menu.

Table 22
Press enter

```
>Obtaining and checking system configuration ...
>Validate hard disk partitions
Validate number of hard drive partitions and size ...
Number of partitions 0:
Disk check failed: three partitions expected
INST0010 Unable to validate Hard disk partition "/u"
errNo : 0xd0001
Press <CR> when ready ...
INST0010 Unable to validate Hard disk partition "/p"
Press <CR> when ready ...
INST0010 Unable to validate Hard disk partition "/e"
```

```
Press <CR> when ready ...
```

--End--

Installing a Signaling Server

Hardware installation

Installation checklist

Before you start to install a Signaling Server in a Communication Server 1000 system, complete the following checklist.

Table 23
Installation checklist

Have you:
Received all server equipment and peripherals? • For a COTS Signaling Server: — installation accessories for rack-mounting the server — AC-power cord **WARNING** Do not modify or use a supplied AC-power cord if it is not the exact type required in the region where the Signaling Server is installed and used. Be sure to replace the cord with the correct type. — a DTE-DTE null modem serial cable (supplied) • for a Communication Server 1000E CP PM Signaling Server (NTDW61 or NTDW99) or CP DC Signaling Server (NTDW53): — NTDW6102E5 - CP PM Signaling Server Hard Drive kit (CP PM only) — N0118766 - CP PM Signaling Server Hard Drive Installation instructions (CP PM only) — NTAK19ECE6 - 2 port SDI Cable assembly kit (for cabinet or MG 1000 chassis) — NTDU0606E6 - 25cm RJ45 Ethernet Cable kit (for MG 1000 chassis) — a 25-pin to 9-pin straight-through serial cable (not supplied) — NTC325AAE6 serial adapter kit (if branch office is based on MG 1010 chassis) — STP ethernet cables for ELAN and TLAN connections (if branch office is based on MG 1010 chassis). — UTP ethernet cables for serial connections (if branch office is based on MG 1010 chassis) ***Note 1:*** Save the packaging and packing materials in case you must reship the equipment or peripherals. ***Note 2:*** CP PM card Signaling Servers require a 40 GB hard drive and 2 GB of memory. The CP PM version 1 hardware (NTDW61 and NTDW99BAE6) must run BIOS Release 18 or later to support the Linux base Operating System. The CP PM version 2 (NTDW99CAE6) meets the requirements for Linux. CP PM version 2 includes an updated hardware design, BIOS, and boot manager.

Have you:
Made sure the area meets all environmental requirements?
Checked for all power requirements?
Checked for correct grounding facilities?
Obtained the following? • screwdrivers • an ECOS 1023 POW-R-MATE or similar type of multimeter • appropriate cable terminating tools • a computer (maintenance terminal) to connect directly to the Signaling Server, with: — teletype terminal (ANSI-W emulation, serial port, 9600 bps) — a web browser for Element Manager (configure cache settings to check for new web pages every time the browser is invoked, and to empty the cache when the browser is closed)
Prepared the network data as suggested in *Converging the Data Network with VoIP Fundamentals* (NN43001-260) and *Communication Server 1000E Planning and Engineering* (NN43041-220) ?
Read all safety instructions in *Communication Server 1000E Installation and Commissioning* (NN43041-310) ?

Installing a Server card Signaling Server

The CP PM and CP DC Signaling Server is a circuit card, and thus is not mounted in a rack. This section contains instructions for installing a Server card Signaling Server in a MG 1000B system.

Installation in a MG 1000B system The NTDW61 and NTDW99 models of the CP PM card are designed for use in a CS1000E system. The first task that must be performed is to install the CP PM hard drive shipped with the server. For instructions, see Procedure 16 “Replacing the hard drive on a CP PM Signaling Server” (page 151).

The MG 1000B platform must have a Signaling Server . The CP PM or CP DC Signaling Server can be installed in the following card slots:

- Chassis NTDU14 slots 1-4
- Chassis NTDK91 slots 1-3
- Cabinet NTAK11 slots 1-10
- MG 1010 NTC310 slots 22-23

Procedure 16 “Replacing the hard drive on a CP PM Signaling Server” (page 151)provides details on how to install a hard drive on the CP PM Signaling Server (NTDW61BAE5). A CP PM Signaling Server Hard Drive kit (NTDW6102E5) ships with the server, and if required, can also be ordered from Nortel.

The hard drive kit contains a hard drive with a jumper, 4 screws, and installation instructions (document N0120776). You need only a small Phillips screw driver to install the hard drive.

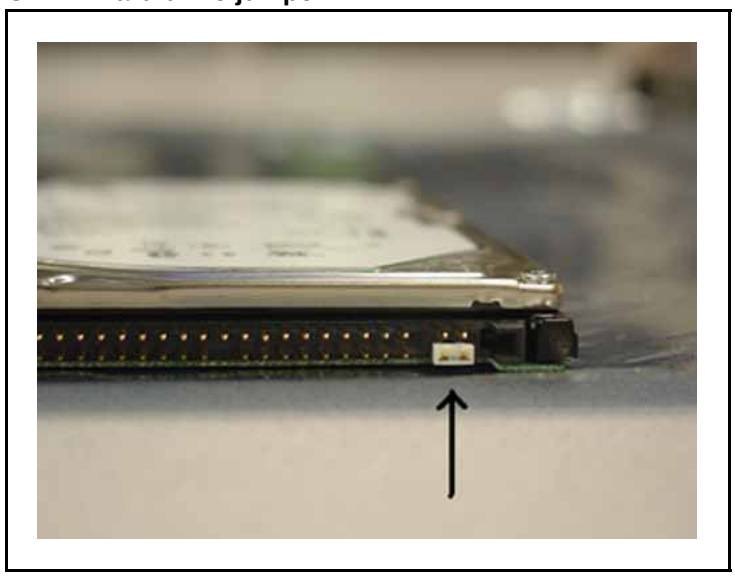
ATTENTION
Observe proper ESD precautions while handling the hard drive and CP PM Signaling Server.

Use the following procedure to replace the hard drive on a CP PM Signaling Server.

Procedure 16
Replacing the hard drive on a CP PM Signaling Server

Step	Action
1	Ensure jumper is located in the cable select (CS) position according to the labeling on the hard drive.

Figure 32
CP PM hard drive jumper

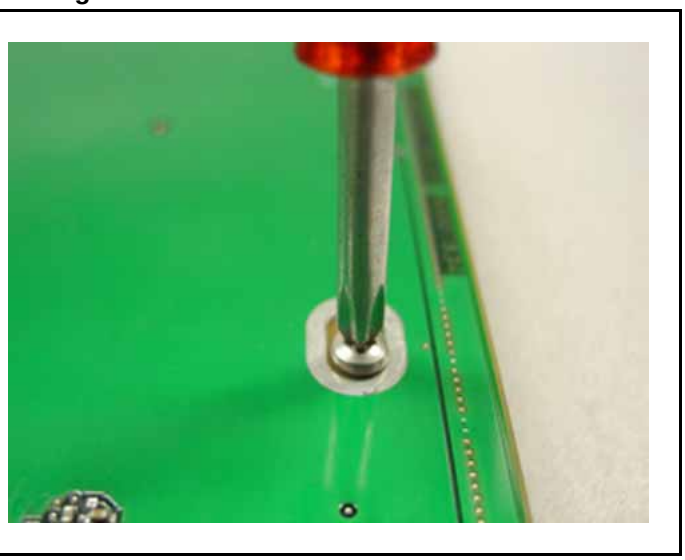


Step	Action
2	Place hard drive on printed circuit board and slide to mate with connector J32.

Figure 33
CP PM hard drive and connector J32

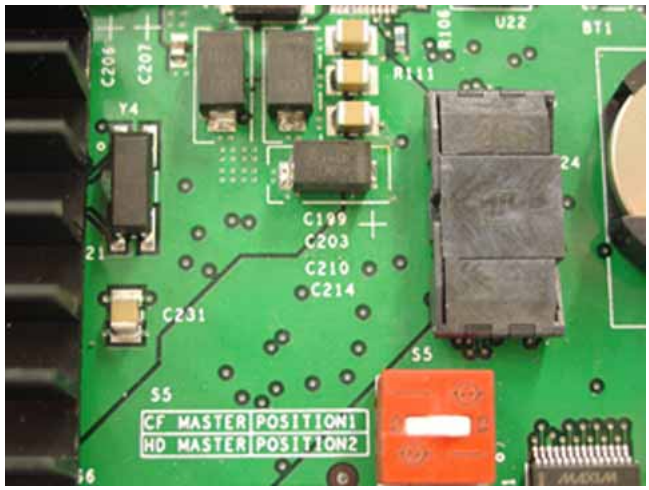
3 Secure hard drive from the bottom side with the included screws.

Figure 34
Securing CP PM hard drive to circuit board



4 Place Dip Switch S5 in position 2 to select HD Master option.

Figure 35
CP PM Signaling Server FMD dip switch



ATTENTION
A CP PM circuit card has an on-board switch (S5) for designating the internal hard drive (HD) or internal Compact Flash (CF) drive as the Fixed Media Device (FMD) for the Signaling Server. You must configure the on-board FMD switch (S5) to position 2 to designate the HD as the FMD for the Signaling Server.

5 Remove on-board compact flash retainer clip if populated.

Figure 36
CP PM Signaling Server internal CF card retainer clip

--End--

MG 1000B software installation

Contents

This chapter contains the following topics:

"Installing MG 1000B software" (page 156)

"Connecting the MG 1000B Core to the network" (page 157)

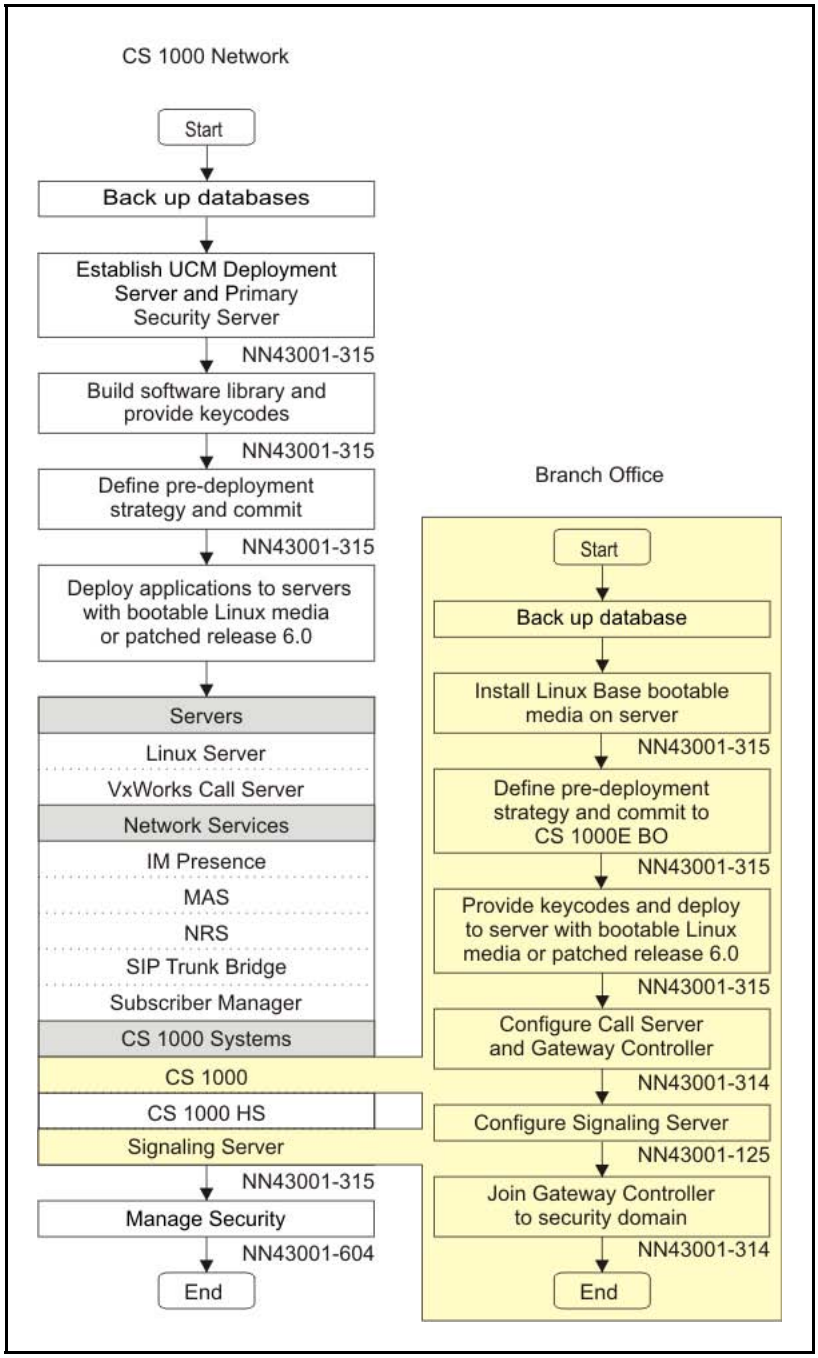
"Signaling Server software installation" (page 164)

"Co-resident Call Server and Signaling Server software installation" (page 165)

"Call Server and Signaling Server software installation" (page 171)

Installing MG 1000B software

Figure 37
Branch Office installation task flow



This section provides a high-level task flow for the installation of Communication Server 1000. The task flow indicates the recommended sequence of events to follow when configuring a system and provides the NTP number that contains the detailed procedures required for the task.

For more information refer to the following NTPs, which are referenced in the task flow diagram:

- *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315)
- *Enterprise Common Manager Fundamentals* (NN43001-116)
- *Network Routing Service Fundamentals* (NN43001-130)
- *Communication Server 1000E Installation and Commissioning* (NN43041-310)
- *Communication Server 1000E - Software Upgrades* (NN43041-458)
- *Signaling Server IP Line Applications Fundamentals* (NN43001-125)
- *SIP Line Fundamentals* (NN43001-508)
- *Security Management Fundamentals* (NN43001-604)

Installing Gateway Controller software

For details on installing software on an Gateway Controller card refer to *Communication Server 1000E Installation and Commissioning* (NN43041-310).

Installing Server software

For details on installing software on a Server card refer to *Communication Server 1000E Installation and Commissioning* (NN43041-310).

Upgrading Gateway Controller software

For details on upgrading software on an Gateway Controller card refer to *Communication Server 1000E - Software Upgrades* (NN43041-458).

Upgrading Server card software

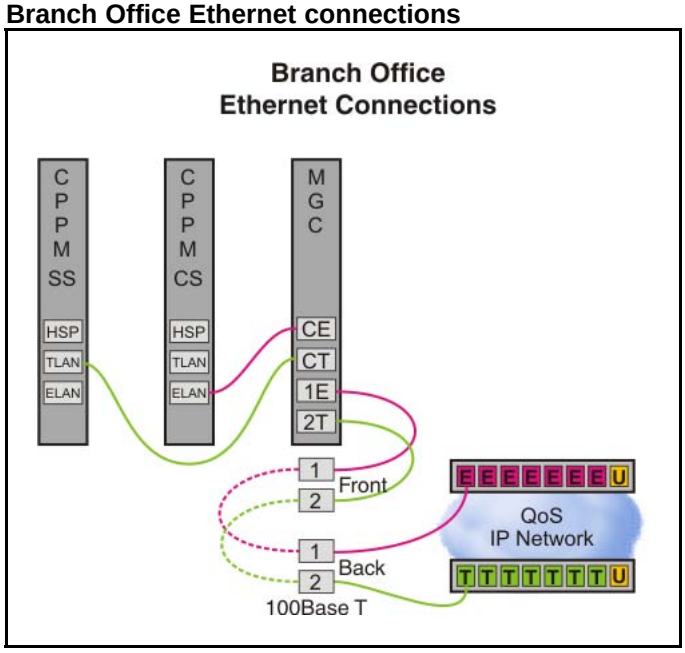
For details on upgrading software on a Server card refer to *Communication Server 1000E - Software Upgrades* (NN43041-458).

Connecting the MG 1000B Core to the network

Connecting the MG 1000B Core to the network

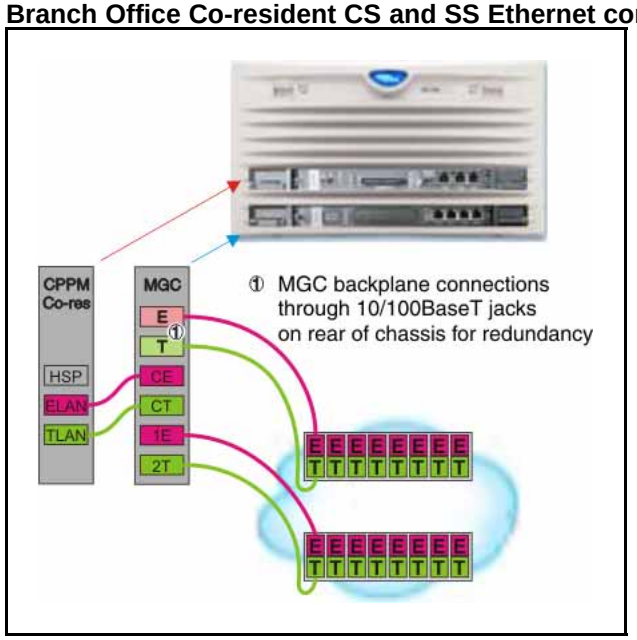
The MG 1000B Core has two 100BaseT ports (1 and 2) for Ethernet connection to the network. See Figure 38 "Branch Office Ethernet connections" (page 158).

Figure 38
Branch Office Ethernet connections



From the Gateway Controller, connect the two short Ethernet cables between the Media Gateway bulkhead and the two 100BaseT ports at the top right corner of the MG 1000B Core. The TLAN network interfaces exist only on the MG 1000B Voice Gateway Media Cards, IP Phones, and the Signaling Server, as shown in Figure 13 "MG 1000B platform without a chassis expander" (page 58) and Figure 15 "MG 1000B platform with a chassis expander" (page 60).

Figure 39
Branch Office Co-resident CS and SS Ethernet connections



In the case of Co-resident Call Server and Signaling Server, connect the two short Ethernet cables between the Server card and the two 100BaseT ports at the top right corner of the MG 1000B Core.

Procedure 17
Configuring primary and secondary call server IP addresses

Step	Action

Given: Primary IP address: 47.1.1.10 ; Secondary IP address: Subnet mask: 255.255.255.0; Default Gateway IP: 47.1.1.1

1 Load Overlay 117.

2 Create host entries. Enter one of the following commands:

NEW HOST PRIMARY_IP 47.1.1.10
NEW HOST GATEWAY_IP 47.1.1.1 (if connected to customer LAN)
NEW HOST GATEWAY_IP 47.1.1.1

3 Assign host to primary and/or secondary IP address(es). Enter one of the following commands:

CHG ELNK ACTIVE PRIMARY_IP
CHG ELNK INACTIVE SECONDARY_IP (for Dual CPU only)

Verify your IP address for Ethernet by entering the PRT ENLK command.

> ***Note:*** To reuse the active host entry and/or associated IP address, the existing entry must be removed. Prior to removing the existing enty, you must first create a temporary host entry and make it active. Out the original host entry, then proceed to Step 2.

4 Set up Ethernet subnet mask. Enter the command:

CHG MASK 255.255.255.0

Verify subnet mask setting by entering the command:

PRT MASK

5 Set up routing entry. Enter the command:

NEW ROUTE <destination IP> 47.1.1.1: (if connected to customer LAN)

Where: <destination IP> = destination network IP and <gateway IP> = default gateway IP

> ***Note:*** When more than one gateway exists, replace 0.0.0.0 with the destination network address for each entry of the routing table.

6 Verify default routing by entering the command:

```
PRT ROUTE
```

Note 1: For a single CPU machine, the secondary IP is not used.

Note 2: The secondary IP is accessible only when a system is in split mode.

Note 3: The subnet mask must be the same value used for the system Ethernet network.

Note 4: The system private Ethernet (ELAN subnet) is used for system access and control. Use an internet gateway to isolate the system private Ethernet from the Customer Enterprise Network.

Note 5: Routing information is required if an internet gateway or router connects a system private network (ELAN subnet) to the Customer Enterprise | | Network. New routes use network IPV4 classification to determine the whether | | the route is network or host based.

Note 6: INI is required for the activation of subnet Mask.

--End--

Perform the following procedure to configure the active ELNK Ethernet interface for the Branch Office.

Perform the following procedure to configure the TLAN and ELAN network interfaces at the MG 1000B core and enable traffic over the LAN WAN.

Procedure 18
Connecting the Ethernet ports

Step	Action
1	Insert the CAT5 cable into the RJ-45 10BaseT Port labelled ELAN on the front of the CP PM Call Processor card. Connect the other end of the CAT5 cable to the Ethernet switch. An alternative method is to connect the CP PM ELAN port directly to the card on the CE port and then make the ELAN connection from the 1E port of the card to the Ethernet switch. For more information about the switch, see *Converging the Data Network with VoIP Fundamentals* (NN43001-260). This connects the MG 1000B Core to the ELAN network interface. The switch connects to the LAN/WAN router.
2	Install and put the Signaling Server into operation, and connect the Signaling Server ELAN and TLAN network interfaces to the

switch. See “MG 1000B platform hardware installation” (page 131).

--End--

For more detailed information on the switch and router connections, see *Converging the Data Network with VoIP Fundamentals* (NN43001-260)

Using Element Manager to configure the node

In Element Manager, configure the following IP telephony node values that are specific to the MG 1000B:

- under H323 GW Settings (see Figure 40 "Confirm IP telephony node values for H.323 Gatekeeper" (page 162)):
  - Primary gatekeeper IP address
  - Alternate gatekeeper IP address (if equipped)
  - Primary Network Connect Server IP address
  - Primary Network Connect Server Port number
  - Alternate Network Connect Server IP address
  - Alternate Network Connect Server Port number
  - Primary Network Connect Server time-out

  If NRS and NCS have different IP addresses, then the Branch Office must be configured as non-RAS H.323 endpoint with NCS support in the NCS database.

  The name of static H.323 endpoint should match H.323 ID field.

  H.323 plays and important part in redirection. If there are no H.323 trunks, configure H.323 anyway.

  ATTENTION
  H.323 ID is now Node wide, not element wide.

  See forFigure 41 "Confirm IP telephony node values for Primary and Secondary NCS" (page 163) Primary or Secondary NCS sample configuration located within the H.323 Gateway settings in EM.l
- under SIP GW Settings (see Figure 42 "Confirm IP telephony node values SIP Redirect Server" (page 163)):
  - Primary Proxy/Redirect IP address
  - Primary Proxy/Redirect IP port
  - select Primary Proxy Supports Registration
  - Primary Proxy or Redirect server flag
  - Secondary Proxy/Redirect IP address (if equipped)
  - Secondary Proxy/Redirect IP port

— select Secondary Proxy Supports Registration

— Secondary CDS Proxy or Redirect server flag

To configure a Follower Signaling Server, refer to *Signaling Server Installation and Commissioning* ().

To configure an Alternate and Failsafe (if required) NRS, refer to the corresponding procedures in *IP Peer Networking Installation and Commissioning* (NN43001-313).

Figure 40
Confirm IP telephony node values for H.323 Gatekeeper

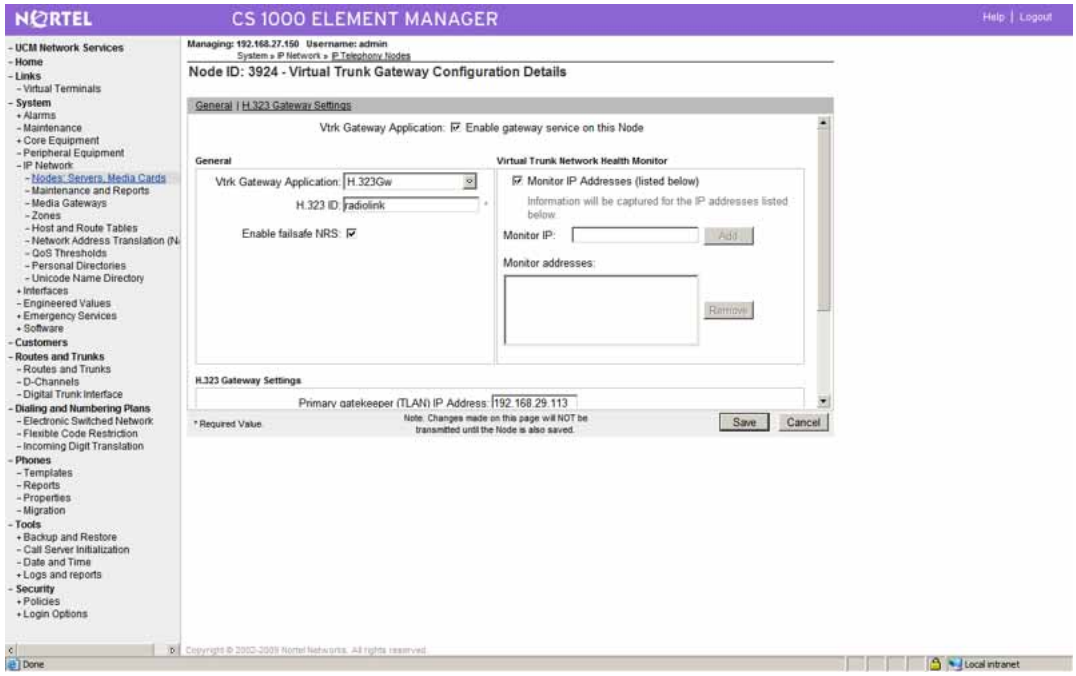


Figure 41
Confirm IP telephony node values for Primary and Secondary NCS

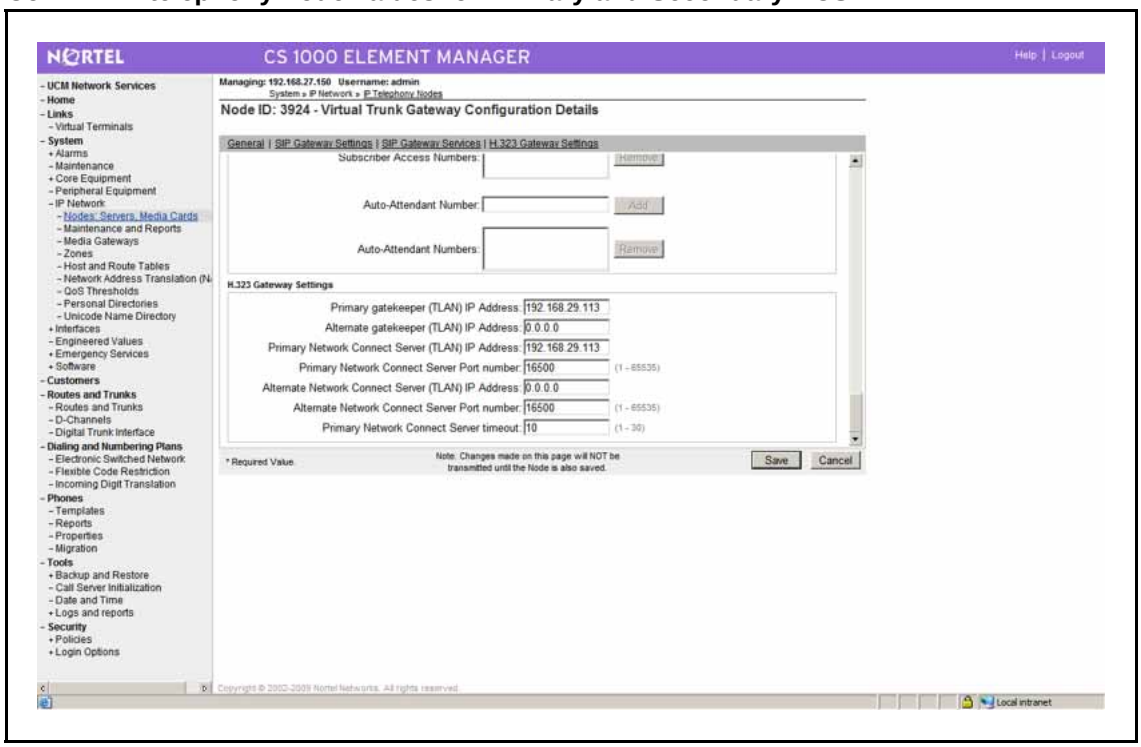


Figure 42
Confirm IP telephony node values SIP Redirect Server

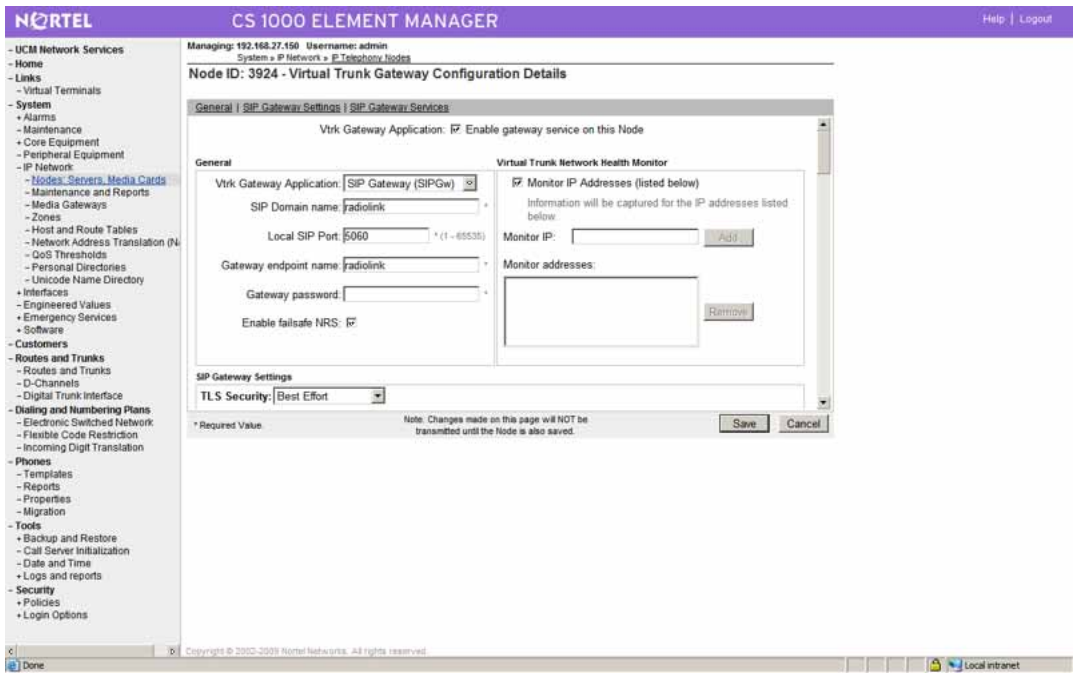
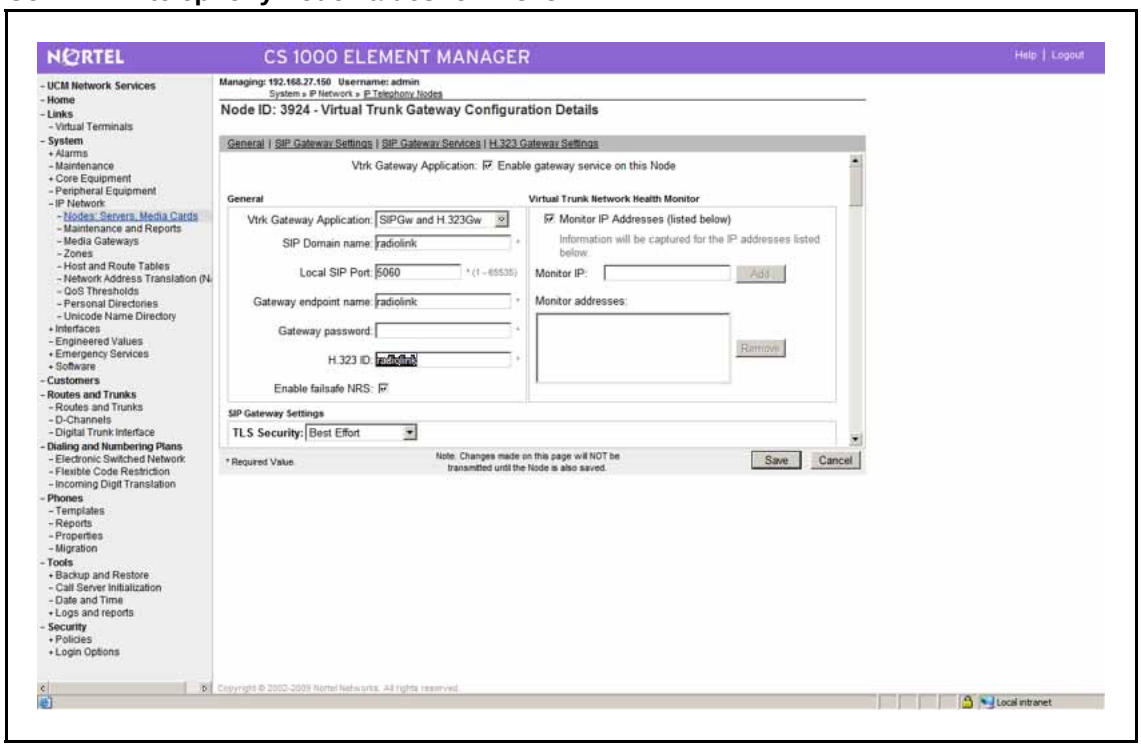


Figure 43
Confirm IP telephony node values for H.323 ID



Signaling Server software installation

The Signaling Server is installed on a Linux base platform. Existing systems with Signaling Server installed on VxWorks platform must back up data before upgrading and moving to Linux based Signaling Server. For more information on installing Signaling Server, and backing up and importing your database, see *Signaling Server IP Line Applications Fundamentals* (NN43001-125)

During the install of Linux base, the Signaling Server software is deployed and can be accessed through the Unified Communications Management (UCM) console. For more information about the Linux platform base install, see*Linux Platform Base and Applications Installation and Commissioning* (NN43001-315) .

The Signaling Server software is available and can be deployed from one of the following predefined deployment packages:

- Signaling Server (SS)
- Signaling Server and Network Routing Service
- Call Server (CS) and Signaling Server (basic stand-alone Co-resident system. For more information about the Co-resident Call Server and

Signaling Server, refer to *Co-resident Call Server and Signaling Server Fundamentals* (NN43001-509).

Co-resident Call Server and Signaling Server software installation

The Co-resident Call Server and Signaling Server (Co-res CS and SS) is supported on various hardware. For more information, see *Co-resident Call Server and Signaling Server Fundamentals* (NN43001-509).

The CP PM hardware platform must be equipped with a 40 GB hard disk and 2 GB memory to support the Co-res CS and SS configuration. The CP PM version 1 hardware (NTDW61 and NTDW99BAE6) must run BIOS Release 18 or later to support Co-res CS and SS. The CP PM version 2 (NTDW99CAE6) meets the requirements for Co-res CS and SS. CP PM version 2 includes an updated hardware design, BIOS, and boot manager. For more information about the methods for ensuring the CP PM hardware meets the above requirements, see *Co-resident Call Server and Signaling Server Fundamentals* (NN43001-509).

The installation of a Co-res CS and SS consists of two parts:

- Linux Base installation
- Linux application installation

Two separate installation media are provided: one contains the Linux Base image and the second contains all the Co-resident Call Server, Signaling Server, and system management application software.

For more information about Nortel Linux Base installation, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

CAUTION
LOSS OF DATA
Branch Office CP PM based VXWorks systems do not require a BIOS upgrade for CS 1000 Release 7.0.

Preinstallation checklist

The CP PM Co-res CS and SS requires a CP PM hardware platform with a 40 GB hard drive and 2 GB of memory. The CP PM version 1 hardware (NTDW61 and NTDW99BAE6) must run BIOS Release 18 or later to support Co-res CS and SS. The CP PM version 2 (NTDW99CAE6) meets the requirements for Co-res CS and SS.

You must perform the following procedures before any installation to ensure CP PM hardware meet the preceding requirements.

Note: The Call Server Overlay 135 **`stat mem`** command on a CP PM Co-res CS and SS does not show the actual physical memory size on the CP PM hardware. It displays the amount of memory that the Call Server application uses.

Procedure 19
Determining CP PM BIOS Method 1

Step	Action
1	Power up the CP PM hardware.
2	Observe the CP PM version 1 BIOS output from bootup screen.

```
+-------------------------------------------------------------+
| System BIOS Configuration, (C) 2005 General Software, Inc.
+---------------------------+---------------------------------+
| System CPU : Pentium M    | Low Memory      : 632KB         |
| Coprocessor: Enabled      | Extended Memory : 1011MB        |
| Ide 0 Type : 3            | Serial Ports 1-2 : 03F8 02F8    |
| Ide 1 Type : 3            | ROM Shadowing   : Enabled       |
| Ide 2 Type : 3            | BIOS Version    : NTDU74AA18 |
|+--------------------------+---------------------------------+
Press F to force board to boot from faceplate drive.
```

3	If the CP PM version 1 BIOS is less than 18, the Linux base installer can update the BIOS, see Procedure 20 “Automatically upgrading the CP PM BIOS with the Linux Base installer” (page 166).

--End--

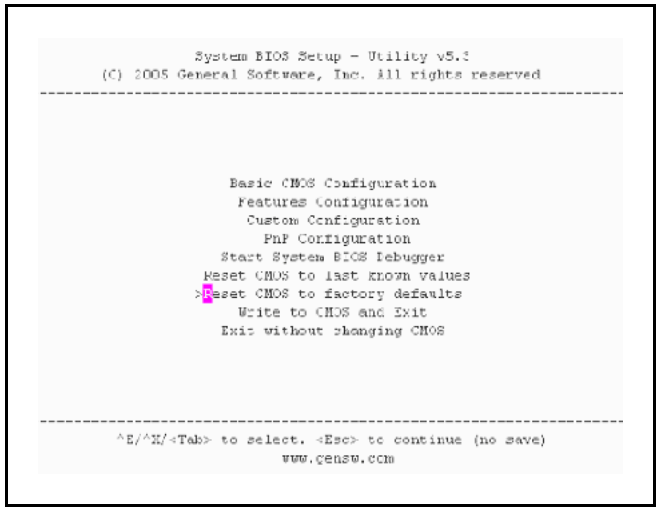
Procedure 20
Automatically upgrading the CP PM BIOS with the Linux Base installer

Step	Action
1	Connect to serial port 1 on the CP PM.
2	Insert the Linux Base installation CF card into the faceplate CF slot.
3	Power on the system.

4 During the reboot memory check, quickly press **CTRL C** to enter the CP PM BIOS.

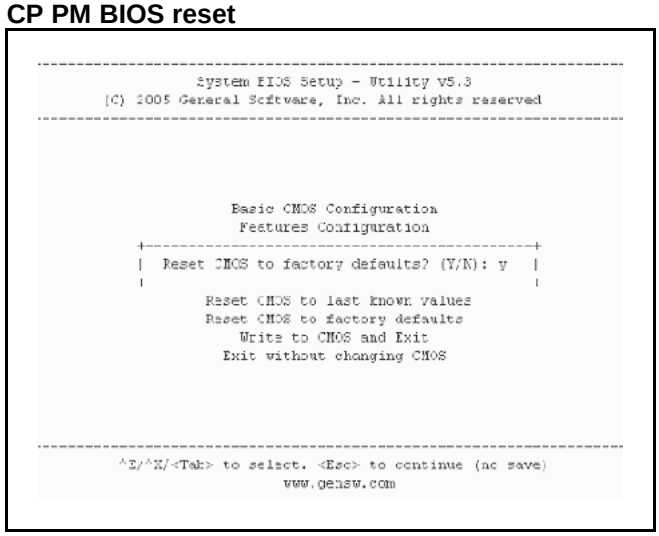
5 Figure 44 "CP PM BIOS setup" (page 167) appears. Select **`Reset CMOS to factory defaults`** from the menu.

Figure 44
CP PM BIOS setup



6 Figure 45 "CP PM BIOS reset" (page 167) appears. Press **`y`** to reset CMOS to factory defaults.

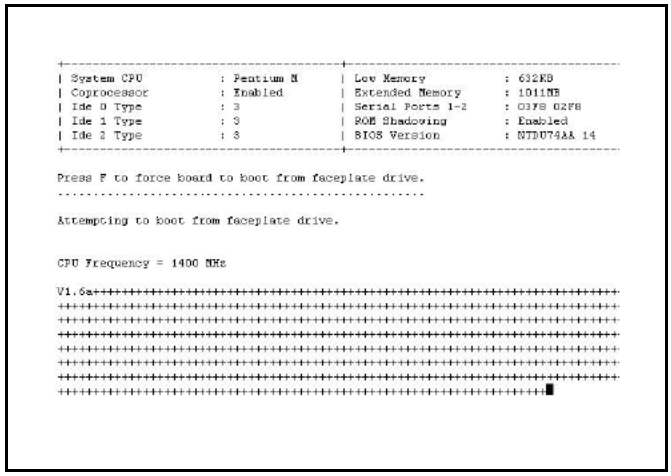
Figure 45
CP PM BIOS reset



7 Once the reboot and memory check completes, Figure 46 "CP PM faceplate drive boot" (page 168)appears. Press the **`F`** key to boot from the Linux Base installation faceplate CF card.

Note: For CP PM version 2 cards (NTDW99CAE6), pressing **`F`** enters the boot menu. Select Faceplate RMD, and press **`Enter`** to boot from the Linux Base installation faceplate CF card.

Figure 46
CP PM faceplate drive boot



8 The welcome screen appears. Press **ENTER** to direct the input and output to COM1.

9 Figure 47 "CP PM BIOS automatic upgrade" (page 169) appears if the CP PM version 1 card has a BIOS version less than 18. Press **y** to proceed with the automatic upgrade.

CAUTION
Do not interrupt the BIOS upgrade process. Damage to equipment may occur.

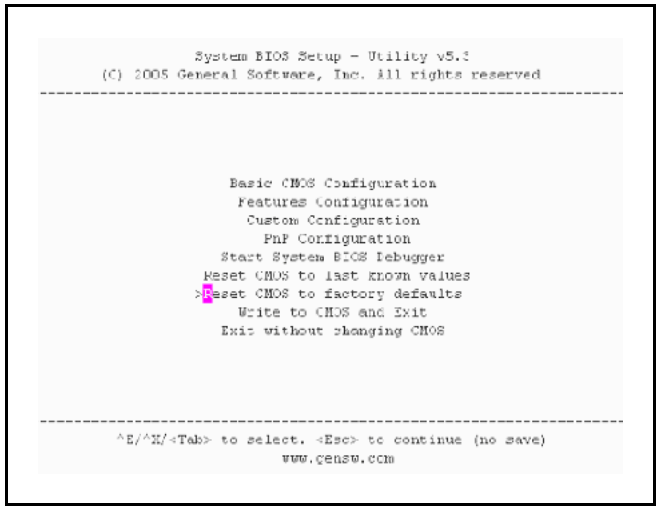
Figure 47
CP PM BIOS automatic upgrade

10 Verify that the BIOS upgrade is finished. Press **Enter** to reboot.

11 During the reboot memory check, quickly press **CTRL C** to enter the CP PM BIOS.

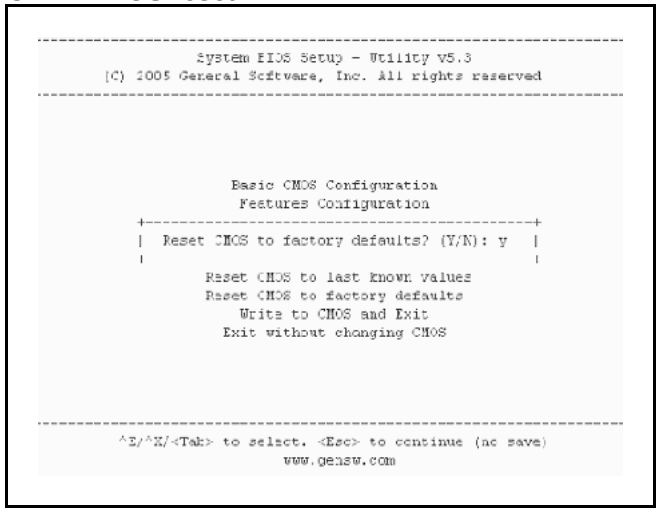
12 Figure 48 "CP PM BIOS setup" (page 170) appears. Select **`Reset CMOS to factory defaults`** from the menu.

Figure 48
CP PM BIOS setup



13 Figure 49 "CP PM BIOS reset" (page 170)appears. Press **y** to reset CMOS to factory defaults.

Figure 49
CP PM BIOS reset



14 The system reboots. Once the reboot is complete, the new BIOS version is displayed. Verify that the BIOS version is 18 or higher. You can now proceed with the Linux Base software installation.

--End--

Nortel Linux Base installation

Install the Linux Base installation by using the CLI interface and bootable DVD, USB or Compact Flash media. Install the basic server properties, for example, ELAN, TLAN IP address, gateway, subnet masks, and date

and time settings during the Linux Base installation. For more information about Nortel Linux Base installation, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

ATTENTION
After you install Linux Base, you must configure the server as a primary, secondary, or member server in the UCM security framework. Perform this configuration using the default user ID and password.

Call Server and Signaling Server software installation

Perform the application installation on the Call Server and Signaling Server (and stand-alone Linux-based Communication Server 1000 servers) using the Communication Server 1000 Software Deployment Manager, graphical user interface (GUI).

The Deployment Manager installs the Call Server, Signaling Server, and System Management applications as Linux Red Hat Package Manager (RPM) packages.

Deployment Manager access occurs through the Web-based Communication Server 1000 UCM navigator.

The Deployment Manager can operate in two modes;

- Centralized Deployment Manager (Remote)

  :

  the Deployment Manager runs on the UCM Primary Security Server. You must start the UCM navigator and log on to the UCM Primary Security Server. In this model, the Centralized Deployment Manager deploys application software to the target servers in the UCM security domain.

- Local Deployment Manager:

  the Deployment Manager runs on the target server itself. Accessing the Deployment Manager is similar to the Centralized Deployment option except you must log on to the local target server by using the default user ID and password. This mode is typically used when you want to install software on the target server before it is configured to join the UCM security framework.

In both Centralized and Local modes, the application software Nortel Application Image (NAI) on the software delivery media is uploaded from the client workstation to the server where Deployment Manager runs:

- For the Centralized Deployment Manager, the application software image is transferred to the hard disk of the UCM primary security server.
- For the Local Deployment Manager, the application software image is transferred to the hard disk on the target server.

ATTENTION
For the Centralized Deployment Manager, you only need to upload the application software once. You can then deploy the software image to multiple target servers in the UCM security domain.

The Deployment Manager supports new installation and upgrades. Both processes are similar but contain the following differences:

- For the upgrade, you cannot remove or add any new type of applications, you must use the existing package configuration. The user can upgrade only the existing applications to a newer version.
- For the upgrade, existing data is backed up and restored when the new version of the application software is installed.

ATTENTION
If you change the package configuration, you must manually back up data on the target by using the **`sysbackup`** command before you use the Deployment Manager to install a new package configuration on the CS and SS.

For more information about the Call Server and Signaling Server installation, see*Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

Branch Office configuration

Contents

This chapter contains the following topics:

"Configuring the Branch Office" (page 173)

"Adding the Branch Office endpoints to the NRS database" (page 175)

Configuring the Branch Office

After connecting the MG 1000B Core to the network and configuring the system user names and passwords (see "MG 1000B software installation" (page 155)), complete the configuration.

Summary of steps

Perform the following steps to configure a Branch Office:

Step	Action
1	Configure the ELAN network interface IP address (see Configuring the ELAN network interface IP address).
2	Configure the ZBD (optional) (see "Configuring the Zone Based Dialing" (page 174)).
3	Configure the Voice Gateway Media Cards (see "Configuring the Voice Gateway Media Cards" (page 174)).
4	Configure trunks and lines (see "Configuring the trunks and lines" (page 175)).
5	Configure IP Phones (see "Installing and configuring IP Phones" (page 177)).
6	Configure ZFDP (optional)
7	Configure Dial Plan (private if **DIALPLAN** option is set to **PRV** in CDB, or public if **DIALPLAN** option is set to **PUB**).

--End--

Configuring the Zone Based Dialing

To configure zone based parameters, the Zone Based Dialing (ZBD) option is activated using LD 15, after it is set to YES, the DIALPLAN prompt is shown and user can select public or private on-net dial plan.

Table 24
New prompts for Overlay 15

Prompt	Response	Comment
REQ:	CHG	Change existing data block
TYPE:	FTR_DATA	Customer Features and options
VO_CUR_ZONE_TD	(NO) YES	
ZBD	(NO) YES	ZBD option
DIAL_PLAN	PUB/PRV	Type of dialing plan for DN/CLID displaying

The following procedure demonstrates a basic overview of the steps to follow to configure the ZBD. For more information on the ZBD, see *Dialing Plans Reference* (NN43001-283).

Step	Action
1	Enable the **Zone Based Dialing** option in **OVL15**,
2	Set the **dial plan** option to the appropriate dial plan **PUB** or **PRV**.
3	Configure the numbering zones from Overlay 117.
4	Configure numbering zone parameters.
5	Configure CLID entries for a key of a set.
6	Configure sets with numbering zones and appropriate CLIDs.

ATTENTION
The DN of a set should be 7 digits: PREF + shortDN.

--End--

PREF refers the prefix for a Dialed Number (DN), for example, in the following DN, 838-5775, 838 equals PREF.

Configuring the Voice Gateway Media Cards

The Voice Gateway Media Cards (see Figure 28 "Voice Gateway Media Card" (page 138)) arrive at a customer location with pre-installed software. To install and upgrade these cards, you need the latest workfile. The

workfile is delivered by the PC card or Element Manager and contains all Voice Gateway Media Card operating system and application files. The workfile is a single packed and compressed file.

For more information on configuring the Voice Gateway Media Card, see *Signaling Server IP Line Applications Fundamentals* (NN43001-125)

Configuring the trunks and lines

To install the line and trunk cards, refer to *Communication Server 1000S: Installation and Configuration* (NN43031-310). If the Branch Office is a converted small system, refer to *Communication Server 1000E Installation and Commissioning* (NN43041-310).

To configure lines, refer to *Communication Server 1000E Installation and Commissioning* (NN43041-310). If the Branch Office is a converted small system, refer to *Communication Server 1000E Installation and Commissioning* (NN43041-310).

To install and configure Virtual Trunks on the Branch Office, refer to *IP Peer Networking Installation and Commissioning* (NN43001-313).

Adding the Branch Office endpoints to the NRS database

The Branch Office feature requires the Network Connection Service (NCS) to redirect a Branch User to the main office. The NCS allows the TPS to query the NRS using the UNIStim protocol, and the TPS then redirects the Branch User accordingly. The NCS is a component of NRS, and is enabled using the NRS Manager.

Each Branch User ID (BUID) must be entered in the Branch Office numbering plan to point to the main office. Nortel recommends that each BUID be a public DN (that is, a number in the public directory). Therefore, the BUID points to both the Branch Office and the main office. However, there may be situations where a separate BUID may be required, such as in a Multiple Appearance DN (MADN) configuration. In this case, the separate BUID may not be a public DN and explicit configuration is required. The BUID must be added to the numbering plan to point to the main office.

If VO User ID or BUID is configured for Coordinated Dialing Plan DN (CPD_DN) then it should be in one of the following formats:

- CDP_DN without Local Steering Code/Distant Steering Code
- Access Code + HLOC (Home Location Code) + CDP_DN

Nortel recommends that routing entries should be set up to consider the cost of redirection. In Normal Mode, the least cost route should be used to redirect the Branch User to the main office. For survivability, an alternate route should be used, such as that route with a second-least cost.

Refer to *IP Peer Networking Installation and Commissioning* (NN43001-313) for the appropriate procedures.

MG 1000B telephones

Contents

This chapter contains the following topics:

"Overview" (page 177)

"Installing and configuring IP Phones" (page 177)

"Using the IP Phones" (page 191)

"Set-Based Removal" (page 197)

"Analog and digital devices in the Branch Office" (page 197)

Overview

After the Branch Office zones and passwords are provisioned, the MG 1000B IP Phones must be provisioned. They can be provisioned using LD 11.

The IP Phones or devices that are supported in the MG 1000B include:

- IP Phones – "Installing and configuring IP Phones" (page 177)
- Analog (500/2500-type) telephones and devices – "Analog devices" (page 197)
- Digital telephones and devices – "Digital devices" (page 198)

This chapter provides information on installing and configuring IP Phones, analog devices, and digital devices at the Branch Office.

Installing and configuring IP Phones

All MG 1000B IP Phones must be configured in the main office on the main office Call Server (see "MG 1000B IP Phone configuration" (page 128)). They are also configured on the MG 1000B CP PM for survivability purposes.

Automatic data synchronization is not carried out between the main office Call Server and MG 1000B CP PM.

Configuring IP Phones is done in two stages – IP Phone data configuration, and Branch User-specific data configuration. The configuration can be done in two ways:

- Enter the Branch User-specific data (follow the procedure Procedure 22 “Configuring a Branch User” (page 183)).

Alternatively, use any method to install the IP Phone and then configure the Branch User information.

This section contains instructions for installing IP Phones in all two ways: Set-Based and overlays.

When the telephone line is inserted into the jack, the IP Phone contacts the MG 1000B TPS for registration, and receives the firmware and features of the Branch Office.

WARNING
Do not plug the IP Phone into an ISDN connection. Severe damage can result. Consult the system administrator to ensure that the telephone is plugged into a 10/100BaseT Ethernet jack.

At the Branch Office, under a Branch User registration request (plugging an IP Phone into a jack), the main office Call Server checks the configured terminal type against the IP Phone type and configuration. This check occurs at the Branch Office.

At the main office, under a Branch User registration request, the main office Call Server checks for a match of the configuration to the IP Phone type. If they do not match, registration is blocked.

Password requirements

To configure Branch User-specific data from the IP Phone keypad, a main office password and a branch password are required.

If you configure an IP Phone Installer’s Password or a Temporary IP Phone Installer’s Password, you can delegate these tasks and continue to configure the system based on *Communication Server 1000E Installation and Configuration NTP (NN43041-310)*. If the Branch Office is a converted small system, refer to *Communication Server 1000E Installation and Configuration NTP* (NN43041-310).

To install an IP Phone at the Branch Office, Nortel strongly recommends that an IP Phone Installer’s Password or a Temporary IP Phone Installer’s Password be configured on the MG 1000B Signaling Server. See Procedure 7 “Setting the IP Phone Installers Password” (page 126) for information on configuring the passwords.

To configure the Branch User from an IP Phone in the main office, one of the following is required:

- IP Phone Installer's Password or Temporary IP Phone Installer's Password configured on the main office Signaling Server. The Temporary IP Phone Installer's Password is usually implemented to enable a "trusted" user to install telephones at the MG 1000B.
- Station Control Password (SCPW) for the IP Phone configured on the main office Call Server. This is not the usual option, since usually a trusted user or administrator installs IP Phones. An SCPW is a user password.

Installing an IP Phone using the keypad

Before proceeding to install an IP Phone using the keypad, be sure to obtain the required passwords, as described in "Password requirements" (page 178).

The procedure to install an IP Phone through the telephone interface consists of three steps.

Step	Action
1	Connect the IP Phone to an Ethernet jack and configure the S1 IP address (or use Dynamic Host Control Protocol (DHCP) to retrieve the IP address). The S1 IP address is the IP address of the MG 1000B TPS. If it is entered as the main office TPS, the IP Phones register to the main office, but do not behave as MG 1000B IP Phones.
2	Configure the Branch User ID (BUID) and its Main Office TN (MOTN) through Procedure 22 "Configuring a Branch User" (page 183).

--End--

These three steps are easily performed and enable an administrator to install and provision a telephone.

WARNING

After all IP Phones have been installed, perform a datadump (using LD 43 EDD or NRS Manager) on the MG 1000B Call Server. Refer to *Communication Server 1000E: Installation and Configuration NTP (NN43041-310)*.

If you have already unpacked and connected the IP Phone, complete Procedure 21 “Using Set-Based Installation” (page 180). It simplifies configuration of MG 1000B IP Phones for survivability. Each MG 1000B IP Phone must also be provisioned at the main office.

To use DHCP addressing (using the automatic installation procedure, see the*Communication Server 1000E: Installation and Commissioning (NN43041-310)* for more detail), verify that the network has DHCP enabled. Refer to *Communication Server 1000M and Meridian 1 Small System Installation and Commissioning* (NN43011-310) for more information.

The IP Phone screen display differs according to the telephone model in use. For example, the screen displays shown in the procedures in this section are for an IP Phone 2004. The IP Phone 2001 and IP Phone 2002 have a one-line display. The IP Phone 2004, IP Phone 2007 and IP SoftPhone 2050 have a three-line display. Users can scroll through the display screens using the navigation keys.

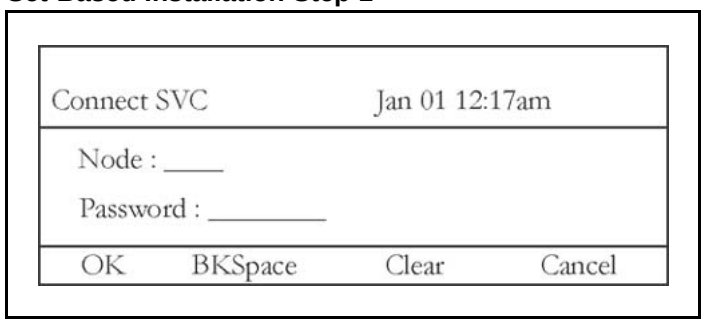
Procedure 21
Using Set-Based Installation

Step	Action

This procedure installs IP Phones at the Branch Office and Main Office. If necessary, the administrator can perform an installation when the Branch User is in Local Mode.

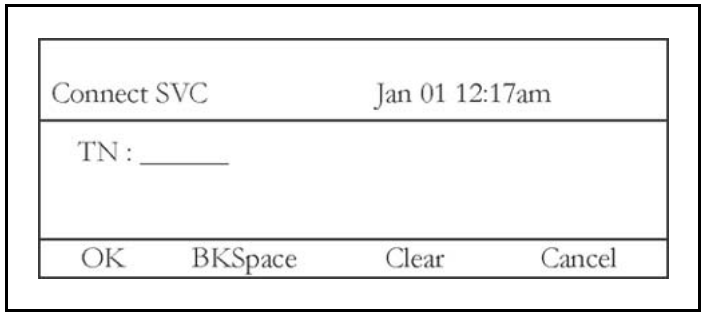
1 To configure the S1 (primary connect server) on the IP Phone, choose DHCP, or manually enter the IP address of the local (MG 1000B) TPS node. Enter the Branch Office node number and password, as shown in Figure 50 "Set-Based Installation Step 1" (page 180).

Figure 50
Set-Based Installation Step 1



2 Enter the TN and press the OK soft key, as shown in Figure 51 "Set-Based Installation Step 2" (page 181).

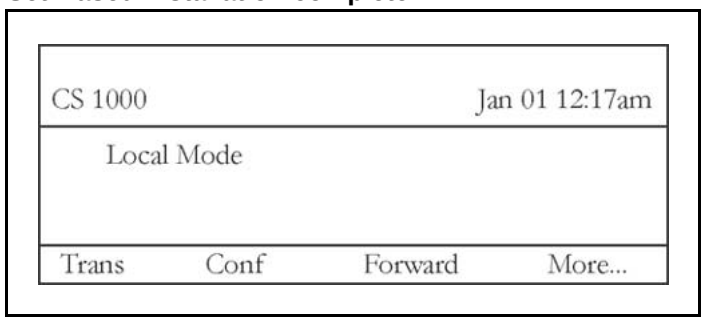
Figure 51
Set-Based Installation Step 2



3 Replace the handset when you hear a relocation tone and see "OK" on the screen display.

4 The IP Phone is now registered with the Call Server. Wait approximately ten seconds for the key map download to complete. The IP Phone is now fully operational in Local Mode. The screen appears as shown in Figure 52 "Set-Based Installation complete" (page 181).

Figure 52
Set-Based Installation complete



5 Test for survival functionality by making and receiving a call on the telephone.

6 The telephone is now configured for basic operation and survivability. To configure the Branch User, see "Branch User Config" (page 181).

--End--

You must also configure the Set-Based Removal feature prompts SRCD (LD 15) and AREM (LD 57) by following Procedure 8 "Setting and changing the Station Control Password Configuration" (page 127).

Branch User Config

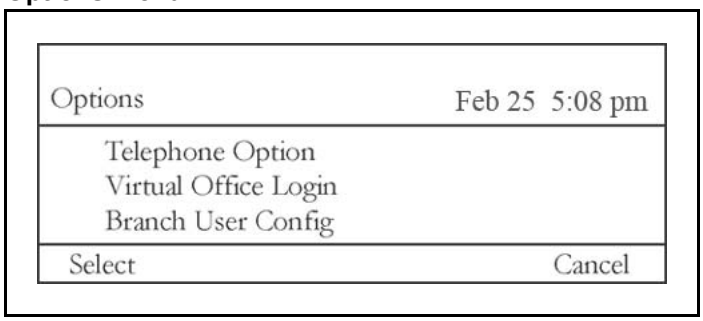
To complete the interface-based configuration of the Branch User, the administrator or a trusted user can configure the IP Phone with the Branch User Config command. Before proceeding, be sure to obtain the required passwords as described in "Password requirements" (page 178).

If the Branch User ID (BUID) is not configured, the IP Phone registers at the MG 1000B CP PM and stays in Local Mode. If the IP Phone is configured with a BUID, it is automatically redirected to the main office TPS and then to the main office Call Server. If there is a BUID, the MOTN is equal to the set TN by default. If there is no BUID MOTN, it has not yet been configured. A BUID is used for redirection, while the MOTN is used on the main office for registration. Redirection may not be successful (refer to Table 33 "Normal Operation troubleshooting" (page 218)).

Branch User Config is the IP Phone-based mechanism to enter the BUID so that the IP Phone can be redirected to the main office to run in Normal Mode. Branch User Config is an option on the **Options** menu display that is available to the Branch User.

The menu option for Branch User Config is shown in Figure 53 "Options menu" (page 182).

Figure 53
Options menu



If an SCPW has been configured, "Password Admin" appears in the list as the second option, forcing the "Branch User Config" option to scroll out of sight. Use the navigation keys to scroll down to "Branch User Config".

To register an IP Phone to the main office, Branch User Config uses the following:

- Branch User ID (BUID)
- Branch password — IP Phone Installer's Password or Temporary IP Phone Installer's Password
- Main Office TN (MOTN), in l s c u. This defaults to the TN at the MG 1000B.
- Main office password — IP Phone Installer's Password, Temporary IP Phone Installer's Password, or SCPW.

For information on setting up passwords, see "IP Phone passwords and parameters" (page 125).

Branch User Config is used for configuration. Once the IP Phone is configured at the Branch Office, its parameters redirect the IP Phone to the main office. This means that configuration is not required a second time unless the Branch User parameters change on that IP Phone.

Attempting to perform a Branch User Config to a TN of a different set type at the main office results in a Permission Denied (4) error message on the display of the IP Phone. See Table 33 "Normal Operation troubleshooting" (page 218) for more information on error messages.

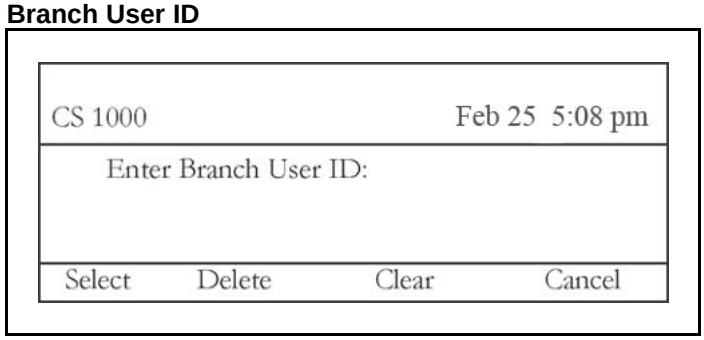
Whenever a valid change is made to BUID/MOTN in LD 11, the IP Phone, if in Local Mode, is automatically redirected to the main office. A service change to BUID/MOTN does not affect IP Phones in Normal Mode. If the BUID of an IP Phone is deleted in a service change, no attempt is made to redirect the telephone to the main office.

WARNING
Do not delete the BUID/MOTN. If they are subsequently deleted, the association between the main office and the Branch Office is lost, and any IP Phones which are in, or go into, Local Mode, remain in Local Mode.

Procedure 22
Configuring a Branch User

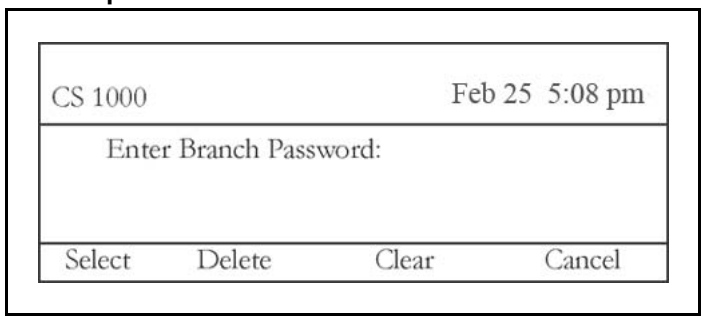
Step	Action
1	To invoke the login and configuration operation for a Branch User, press the Services key (the key with the Globe icon) on an idle IP Phone. If the Branch Office package is equipped, the Branch User Config options are displayed.
2	Select **Branch User Config**, as shown in Figure 53 "Options menu" (page 182).
3	Enter the Branch User ID, that is a dialable DN of the main office. See Figure 54 "Branch User ID" (page 184). For a CDP dialing plan, the Access Code is not required. For example, xxx-xxxx. For a UDP dialing plan, this DN includes the Access Code. For example, 6-xxx-xxxx.

Figure 54
Branch User ID



4 Enter the branch password, that is the IP Phone Installer's Password or Temporary IP Phone Installer's Password for the TPS node at the Branch Office. See Figure 55 "Branch password" (page 184).

Figure 55
Branch password

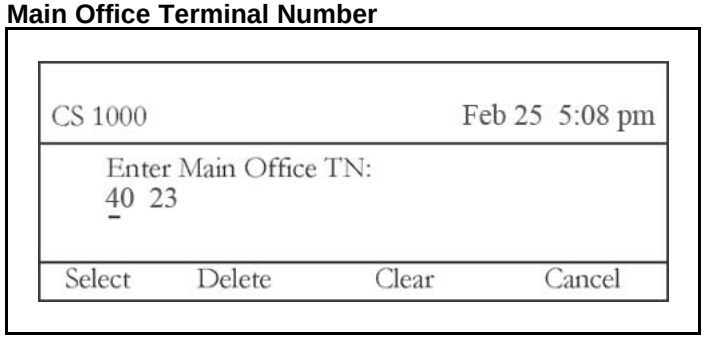


5 To enter the Main Office TN:

- Choose **Select** to accept the default Main Office TN on the display.
- Enter the Main Office TN in a l s c u, and press **Select**.

The default value is the Branch Office TN in l s c u. See Figure 56 "Main Office Terminal Number" (page 184), which shows an example of the display of a TN in small system format.

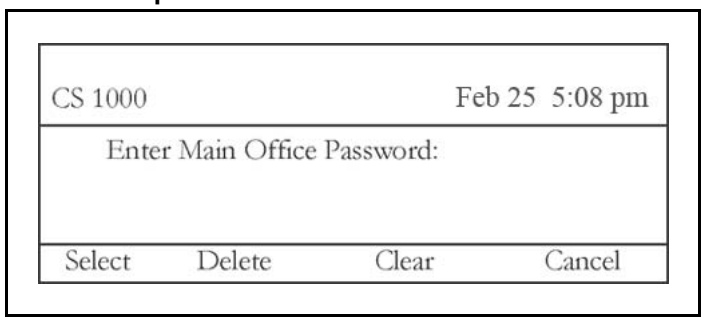
Figure 56
Main Office Terminal Number



6 Enter the IP Phone Installer's Password, Temporary Internet Installer's Password for the main office, or the SCPW for the

Main Office TN. See Figure 57 "Main office password" (page 185).

Figure 57
Main office password



Following entry of this data, the IP Phone is taken offline and the display shows "Locating Remote Server". The IP Phone registers with the main office and becomes operational.

CAUTION
Network Problems During Installation:

Setup: The IP Phone in the Branch Office is on a different subnet to the MG 1000B TPS and has a different route to the main office. The MG 1000B TPS can connect to the main office but the IP Phone cannot.

Symptom: The terminal registers to the MG 1000B TPS and is redirected to the main office (displaying the "Locating Remote Server" message). When it does not successfully register at the main office, it returns to the Branch Office (displaying "Server Unreachable"). The terminal keeps repeating the pattern.

Consequence: The IP Phone does not successfully provide call service.

Diagnosis: When this behavior is observed, check whether a ping succeeds from the IP Phone's subnet to the main office TPS subnet.

CAUTION
After all IP Phones are installed, perform a datadump (using LD 43 EDD or through NRS Manager) on the MG 1000B CP PM. Refer to the *Communication Server 1000E: Installation and Configuration NTP (NN43041-310)*.

7 Execute the EDD command in LD 43.

--End--

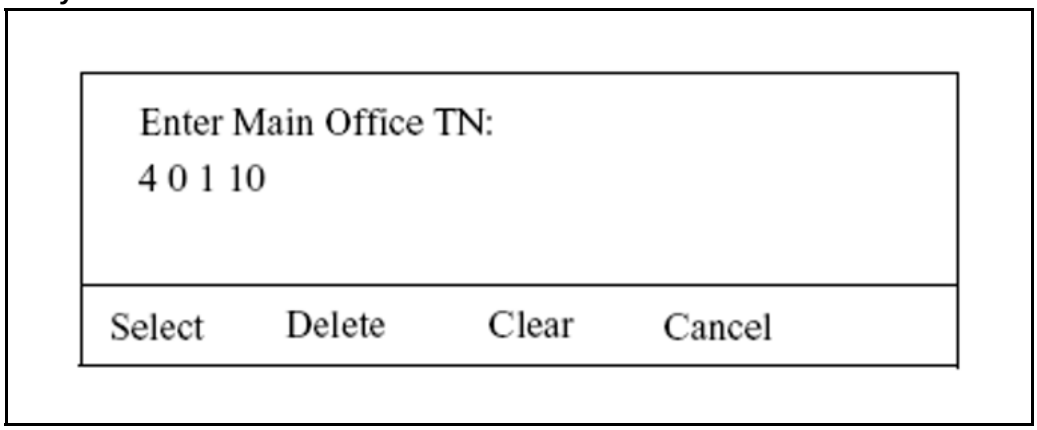
Survivability test

This section pertains to IP Phones installed at a Branch Office. When LAN/WAN connectivity is lost, the IP Phones reboot and are registered at the MG 1000B Call Server. When LAN/WAN connectivity is reestablished, each telephone reregisters at the main office.

After the MG 1000B IP Phones are installed and configured, test the IP Phones for survivability. This is highly recommended when installing the BUID and MOTN through overlays. In these cases, the IP Phones are automatically redirected to the main office without the opportunity to test for Local Mode functionality.

When the Main Office TN is prompted during Branch User config, if the MOTN is not configured through the LD configuration, the default value is displayed as shown in Figure 14. The default is the Branch Office TN in large system format. The user may press the Select softkey to accept the default or enter a new Main Office TN (in 4-fields TN format) and then press the **Select** softkey.

Figure 58
Entry of Main Office TN



Validation of MOTN input from Branch User Config is limited to preliminary range checks. The input string is converted to a packed TN and the MOTN and MOTN type are set as either small or large system.

A Branch User Identification (BUID) and Main Office TN (MOTN) can be provisioned, if the Internet telephone belongs to a MG 1000B. The local TN configured for the Branch Office telephone accepts a four-field format.

This prompt accepts TN's in two or four-field format. If nothing is entered for the BUID, then the set does not get automatically redirected to the Main Office. The value of BUID and MOTN are assigned in the TN block when the crafts person performs the Branch User Config. At this time the User ID entered is saved as the value of BUID and the Main Office TN is saved as the MOTN. Once the value for BUID and MOTN are known at

the Branch Office, a set is automatically redirected to the Main Office when the set re-powers or when WAN connectivity to the Main Office is restored after being temporarily lost.

Table 25
LD 11 Branch Office changes for Internet Telephones

Prompt	Responses	Description	Pkg#
REQ	NEW/CHG		
TYPE	2004P1, 2004P2, 2002P1, 2002P2, 2001P2, 2050PC, 2050MC, 2033, 2210, 2211, 2212, 6120, 6140, 2007, 1110, 1120, 1140,1150 ,1210, 1220,1230,1165	Internet telephones.	
CUST	<num>	Customer number.	
TN	l s c u	With Communication Server 1000 Release 5.0 or later MG 1000B with Gateway Controller, the TN entered for an IP Phone is l s c u.	

Prompt	Responses	Description	Pkg#
BUID	<user id>	dialable DN, Main Office user id Enter X to delete	390
MOTN	l s c u	Main Office TN The default is the Branch Office TN entered above, which for Communication Server 1000 Release 5.0 and later MG 1000B with Gateway Controller is l s c u.	390

LD 20 prints the IP Phone TN Block and MOTN in the l s c u format, shown in the following example:

Figure 59
LD 20 – IP Phone TN Block and MOTN

Command/ Prompt	Command/User Response(s)	Description
REQ	PRT	
TYPE	I2004	

OUTPUT

```
REQ  prt
TYPE I2004
CUST 0
TN 4 0 1 0
BUID 63438888
MOTN 4 0 1 0
....
SCPW 12345678
SFLT No
......
```

Refer to "Test Local Mode" (page 195) for details on testing Local Mode functionality.

Procedure 23
Testing the telephone for survivability

Step	Action

Test the survivability of the connections and functions using the Test Local Mode command on the MG 1000B IP Phone.

1 Press the **Services** key (the key with a Globe icon) to display the **Options menu**.

2 Use the navigation keys to navigate to **Test Local Mode**.

3 Press the **Select** soft key.

This registers the IP Phone to the MG 1000B CP PM.

4 Make and receive a call on the telephone.

5 To redirect the telephone to the main office TPS node:

a Press the **Services** key (the key with a Globe icon).

b Use the navigation keys to navigate to **Resume Normal Mode**.

c Press the **Select** soft key.

This reregisters the telephone at the main office.

If Resume Normal Mode is not selected, the IP Phone automatically returns to Normal Mode after ten minutes.

--End--

Installing IP Phones through LD 11

To use the Virtual Office feature at the Branch Office in Local Mode, a Station Control Password must be configured. Refer to Procedure 8 “Setting and changing the Station Control Password Configuration” (page 127) to provision the Station Control Password at the Branch Office. To prevent user password confusion, Nortel recommends that the same SCPW be used at the main office and the Branch Office.

Procedure 24 “Installing IP Phones through overlays” (page 189) describes the general method of installing a Branch User IP Phone through LD 11.

ATTENTION
If the installation technician uses LD 11 to configure the Branch User ID and Main Office TN for an IP Phone, the IP Phone is automatically redirected to the main office after it is registered to the Branch Office.

Procedure 24
Installing IP Phones through overlays

Step	Action
1	Configure the Branch Office zones and dialing plan. Perform this procedure on the MG 1000B Call Server.
2	Configure the following telephone data in LD 11: • Terminal type • Customer Number • TN • Zone To automatically redirect the IP Phone to the main office, configure a BUID and its MOTN. The BUID and MOTN prompts are unique to the Branch Office feature. Leave the MOTN field blank if it has the same value as the Branch Office TN. If a BUID is not entered, MOTN is not prompted. In this case, Branch User configuration is still required. The BUID, or primary DN, of an MG 1000B IP Phone should match its primary DN at the main office, though this is not a requirement. If different DNs are configured, the dial-in numbers change when the Branch Office is in Local Mode.

WARNING
Do not delete the BUID/MOTN. If they are subsequently deleted, the association between the main office and the Branch Office will be lost, and any IP Phones which are in, or go into, Local Mode, will remain in Local Mode.

Table 26
LD 11 Provision Branch User and SCPW at the Branch Office.

Prompt	Response	Description
REQ:	NEW CHG	Add new data, or change existing data.
TYPE:	a...a	Terminal type. Type.? for a list of possible responses.
CUST	xx	Customer number as defined in LD 15.
BUID	x...x	Branch User ID. A dialable DN to call the telephone in Normal Mode from the Branch Office. Enter X to delete.
MOTN		Main Office Terminal Number.
	l s c u	Format for CSLS; and CS1000E; system, where l = loop; s = shelf, c = card, and u = unit.
ZONE	0-8000	Zone Number to which the IP Phone belongs. The zone prompt applies only when the TYPE is 2001P2, 2002P1, 2002P2, 2004P1, 2004P2, 2007, or 2050PC, 2050MC. Zone number is not checked against LD 117.
...		
SCPW	xxxx	Station Control Password Must equal Station Control Password Length (SCPL) as defined in LD 15. Not prompted if SCPL = 0. Precede with X to delete.

3 (Optional) Disallow usage of Virtual Office. For more information on the Virtual Office feature, refer to *Features and Services Fundamentals* (NN43001-106-B1).

Table 27
LD 11 Enable/disable Virtual Office (optional).

Prompt	Response	Description
REQ:	NEW CHG	Add new data, or change existing data.
TYPE:	a...a	Terminal type. Type ? for a list of possible responses.

Table 27
LD 11 Enable/disable Virtual Office (optional). (cont'd.)

Prompt	Response	Description
CLS	(VOLA) VOLD	Allow Virtual Office operation from this TN. Deny Virtual Office operation from this TN.
CLS	VOUA (VOUD)	Allow Virtual Office login onto this TN using other telephone (destination of Virtual Office login). Deny Virtual Office login onto this TN using other telephone (destination of Virtual Office login).

4 Provision the Station Control Password (SCPW) if the Virtual Office feature is desired in Local Mode due to LAN/WAN or main office failure. See Procedure 8 "Setting and changing the Station Control Password Configuration" (page 127).

5 Perform a manual or automatic installation of the MG 1000B IP Phone according to instructions in *IP Phones Fundamentals* (NN43001-368).

WARNING
After all telephones are installed, perform a datadump (using LD 43 or NRS Manager) on the MG 1000B Call Server. Refer to the *Communication Server 1000E: Installation and Configuration NTP (NN43041-310)*.

6 Test the IP Phones for survivability using Procedure 23 "Testing the telephone for survivability" (page 188).

--End--

Using the IP Phones

An MG 1000B IP Phone is operational immediately after configuration. You can learn more about its services by referring to "Telephone Options" (page 192) and to *IP Phones Fundamentals* (NN43001-368). You can also test the telephone. Refer to "Test Local Mode" (page 195).

Changing the SCPW

Use Procedure 24 "Installing IP Phones through overlays" (page 189) to change the SCPW of a telephone at any time.

Procedure 25
Changing the SCPW

Step	Action
1	Dial the SCPC code followed by the current Station Control Password.

An FFC tone is given at this point.

2 Enter the new password.

The new password must be the same length as SCPL.

3 Wait for the FFC tone and enter the new password again.

If the new password is accepted, another FFC tone is given. If the new password is not accepted, an overflow tone is given.

--End--

Telephone Options

The IP Phone Options feature is described in *IP Phones Fundamentals* (NN43001-368).

Procedure 26
Using the Telephone Options feature

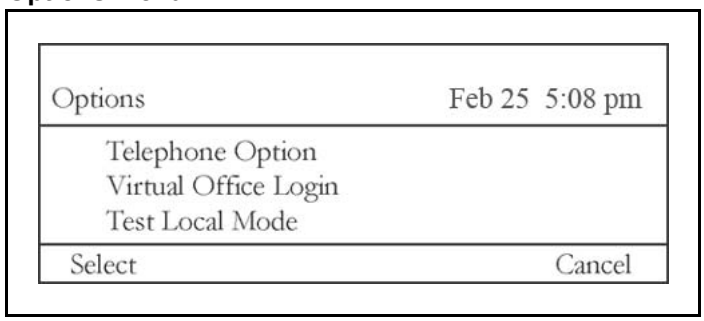
Step	Action

This procedure explains how to use IP Phone Options features. The IP Phone has been configured using Branch User Config and is operating in Normal Mode.

1 Press the **Services** key (the key with the Globe icon).

The **Options** menu is displayed (see Figure 60 "Options menu" (page 192)).

Figure 60
Options menu



The Virtual Office Login option only appears if VOLA CLS is configured.

2 Use the navigation keys to highlight **Telephone Option**.

3 Press the **Select** soft key to activate the feature.

4 Use the **Up** or **Down** keys to select an option.

The available options will differ depending on the type of IP Phone in use. The options include:

- Volume adjustment
- Contrast adjustment

- Language
- Date and time
- Display diagnostics
- Local dialpad tone
- Set info
- Ring type
- Call timer
- Onhook default path
- Change Feature Key label

5 Press the **Select** soft key.

6 Follow the screen prompts to enter data as required.

7 Press the **Services** key or the **Cancel** soft key to exit the Services menu.

--End--

Virtual Office Login on the Branch Office

The Virtual Office Login feature is described in *IP Phones Fundamentals* (NN43001-368).

Procedure 27
Using the Virtual Office Login feature

Step	Action

This procedure explains how to log in to and log out of Virtual Office. The IP Phone has been configured using Branch User Config and is operating in Normal Mode or Local Mode.

1 Press the **Services** key (the key with the Globe icon).

The **Options** menu is displayed (see Figure 60 "Options menu" (page 192)).

2 Use the navigation keys to highlight **Virtual Office Login**.

3 Press the **Select** soft key.

The screen prompts for the User ID.

4 Enter the User ID, the user's dialable DN with the Access Code.

ATTENTION
The User ID must be an ESN number.

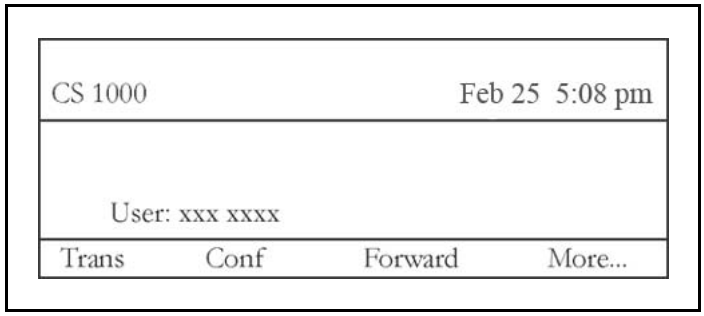
5 Press the **Select** soft key.

6 Enter the Station Control Password for the destination IP Phone.

"Locating Remote Server" appears on the display.

When logged into Virtual Office, the telephone display appears as shown in Figure 61 "Virtual Office - logged in" (page 194).

Figure 61
Virtual Office - logged in



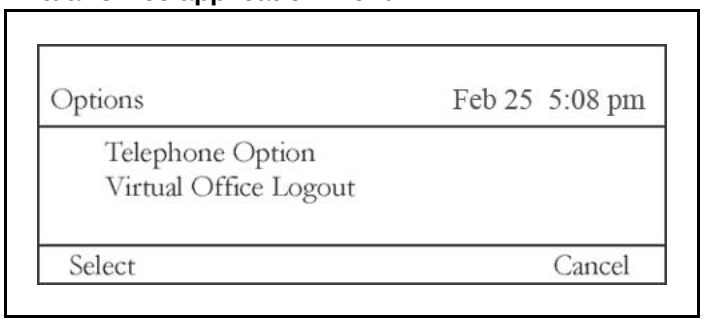
7 To log out of Virtual Office:

a Press the **Services** key to display the Options menu.

b Use the navigation keys to highlight Virtual Office Logout.

See Figure 62 "Virtual Office application menu" (page 194).

Figure 62
Virtual Office application menu



c Press the **Select** soft key.

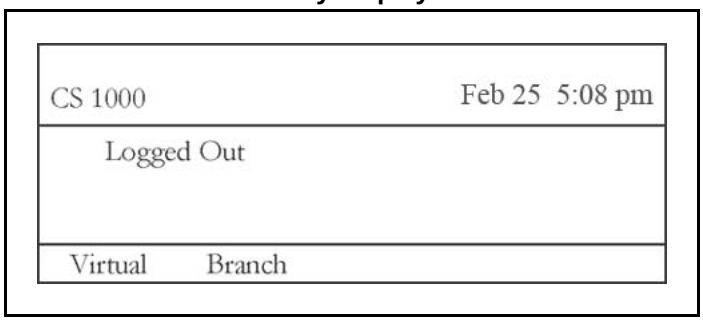
--End--

Feature interactions between Branch User and Virtual Office logins

When an MG 1000B IP Phone user travels to the main office or another network location, the user can access their own Main Office TN from an IP Phone at the visited location by using the Virtual Office feature. The IP Phone at the Branch Office is forced to log out after the Virtual Office feature is activated.

If the IP Phone has been forced- to log out, the Virtual or Branch User soft key shows on the IP Phone display area (see Figure 63 "Virtual or Branch soft key display" (page 195)). The IP Phone is not operational in this mode. The user must log in to bring the IP Phone back into service.

Figure 63
Virtual or Branch soft key display



The Virtual and Branch soft keys are provided to reset the IP Phone to operational:

1. Press the Branch soft key to register the IP Phone to the main office.
2. Press the Virtual soft key to activate Virtual Office Login.

In either case, the user is prompted for the User ID and the SCPW.

When a Branch User IP Phone re-powers, it registers with the MG 1000B Call Server, and is automatically redirected to the main office. If another IP Phone has already occupied the Main Office TN using the Virtual Office login, the re-powered IP Phone is logged out at the main office Call Server with the screen shown in Figure 63 "Virtual or Branch soft key display" (page 195). The IP Phone remains registered to the main office TPS and is listed with the **`isetShow`** command.

Test Local Mode

A user in Normal Mode can test the survivability functionality by entering the Test Local Mode command, as shown in Figure 53 "Options menu" (page 182). This results in the IP Phone registering to the MG 1000B Call Server. The user should make a call and receive an MG 1000B-based or PSTN-based call in Test Local Mode to be sure that the telephone works in the event of a LAN/WAN failure.

Procedure 28
Using the Test Local Mode feature

Step	Action

This procedure explains how to test the IP Phone for Local Mode operation. The IP Phone has been configured using Branch User Config, overlays, and is operating in Normal Mode.

1 Press the **Services** key (the key with the Globe icon).

The Options menu is displayed (see Figure 60 "Options menu" (page 192)).

2 Use the navigation keys to highlight **Test Local Mode**.

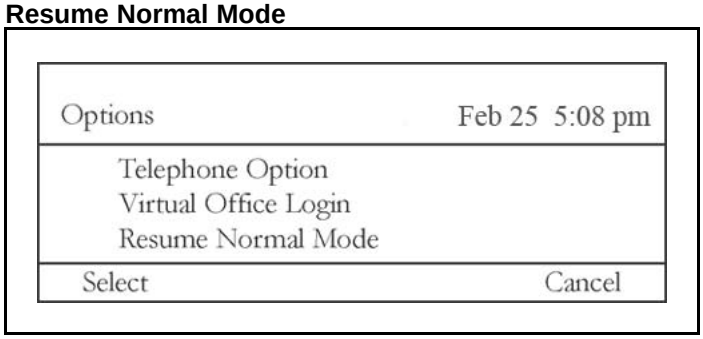
3 Press the **Select** soft key.

The IP Phone displays "Local Mode".

4 To register again at the main office:

a Press the **Services** key to display the menu in Figure 64 "Resume Normal Mode" (page 196).

Figure 64
Resume Normal Mode



The Virtual Office Login option only appears if VOLA CLS is configured.

b Use the Navigation keys to highlight **Resume Normal Mode**.

c Press the **Select** soft key.

--End--

If you fail to resume Normal Mode, Test Local Mode lasts for ten minutes, and then automatically redirects the telephone to the main office Call Server.

Personal Directory, Callers List, Redial List

The Personal Directory feature permits users to configure and maintain a Personal Directory of telephone numbers. The system also automatically creates the following lists:

- Callers List — a list of calls to the user
- Redial List — a list of numbers dialed by the user

Entries in the Personal Directory, Callers List, and Redial List are stored on the Application Server on a Signaling Server at the main office. Therefore, Branch Users can access their lists in Normal Mode only.

As per PD/CL/RI, Personal Directory, Callers List, and Redial List are not supported in Local Mode (on MG1000B) . As previously stated, these features are available in Normal mode only.

Branch Users access their Personal Directory, Callers List, and Redial List using the SCPW.

For more information on the Personal Directory, Callers List, and Redial List features, refer to *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

Set-Based Removal

The following procedure can be used by an administrator or a trusted user to remove the system provisioning for an IP Phone or analog (500/2500-type) or digital telephone.

Procedure 29
Using the Set-Based Removal feature

Step	Action
	When the Automatic Set Removal (AREM) feature is enabled and you have a Set Relocation Security Code (SRCD), follow these steps:
1	Lift the handset or press the DN key of the IP Phone to be removed.
2	Key in the AREM code after hearing the dial tone.
3	Enter the SRCD.
4	Hang up, or press the Release key.

--End--

Analog and digital devices in the Branch Office

Analog devices

Analog (500/2500-type) telephones are supported in the Branch Office, but are not centrally managed from the main office. Instead, they are managed at each Branch Office. When a call is between an analog (500/2500-type) telephone and an IP Phone, a DSP resource is required. Therefore, when analog (500/2500-type) telephones are located in the Branch Office, allow for additional voice gateway channels to support IP-TDM connections.

Analog (500/2500-type) telephones at a Branch Office can be configured using overlays (locally or remotely through a modem or Ethernet connection). For more information, see Procedure 24 “Installing IP Phones through overlays” (page 189).

Analog devices supported by the Branch Office feature include analog (500/2500-type) telephones, fax machines, and modems.

Digital devices

Digital telephones and attendant consoles are supported in the Branch Office, but are not centrally managed from the main office. Instead, they are managed at each Branch Office. When a call is between a digital telephone and an IP Phone, a DSP resource is required. Therefore, when digital telephones are located in the Branch Office, allow for additional voice gateway channels to support IP-TDM connections.

Digital telephones at a Branch Office can be configured using overlays (locally or remotely through a modem or Ethernet connection). For more information, see Procedure 24 “Installing IP Phones through overlays” (page 189).

Digital devices supported by the Branch Office feature include digital telephones, consoles, and a CallPilot Mini or CallPilot 201i.

M3900-series digital telephones also have a Virtual Office feature. This feature is not network-wide, like the Virtual Office feature on the IP Phones. For an M3900-series telephone, a Virtual Office login enables a registration to another TN within the MG 1000B CP PM.

Emergency Services configuration

Contents

This chapter contains the following topics:

"Overview" (page 199)

"Emergency Services Access (ESA)" (page 199)

"Emergency Service using Special Numbers (SPN)" (page 211)

"CLID verification (CLIDVER)" (page 212)

"Networked M911" (page 212)

Overview

For MG 1000B applications, Nortel recommends two alternative general methods to specify which digit string results in a call to emergency services:

- Use the Emergency Services Access (ESA) feature. This is the preferred method in North America, the Caribbean and Latin America (CALA), and in those countries that are members of the European Union (EU). ESA provides specific features and capabilities required by legislation in these jurisdictions.
- Use of a special dialing sequence, such as a Special Number (SPN) in the Network Alternate Route Selection (NARS) data block. This method is also used where ESA is available, but the ESDN at the main office does not match the ESDN at the Branch Office.

Either of these methods have a Branch Office implementation which triggers the main office Call Server to forward emergency services calls to the MG 1000B PSTN. Calls are redirected over a Virtual Trunk using the services of the NRS.

Emergency Services Access (ESA)

Routing ESA calls

ATTENTION
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 routing 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 CS1000E; node, the only tandem trunks are IP Peer trunks. There is no way to specify the appropriate rerouting digits (that is, Prepend Digits) to reroute 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.

Emergency call routing

A Call Server can provide service to IP phones across multiple emergency jurisdictions. This can also occur with traditional non-IP equipment in the form of remote peripheral equipment (for example, Carrier Remote, Fiber Remote).

An emergency call should be handled by the designated means for the phone location (for example, local security desk or local PSAP). The emergency call should be routed to a service at the current location of the phone.

PSTN routing: Enhanced 911 versus Basic 911

Currently, no industry-standard (wireline) solution exists for routing an emergency call to an arbitrary PSAP, and delivering location data. With Enhanced 911 (E911), multiple Emergency Service Zones (PSAP areas) are connected by an E911 Tandem system. The PSTN first routes an emergency call to the E911 Tandem, which contains a Selective Router. The Selective Router looks up the caller's ANI in its Selective Routing Data Base (which is synchronized with the ALI database) to determine the correct PSAP and then routes the emergency call appropriately. Hence, the call can be routed to any CO in the correct E911 Tandem area. The Selective Router automatically routes the call to the appropriate PSAP based on the ANI.

In areas that support Basic 911, the route to the PSAP is determined by the PSTN access point. Hence, the call must be routed to the nearest CO to the caller. ESA can specify a route for each ERL, which meets the more

stringent requirement of Basic 911. In areas with Enhanced 911, system administrators have more flexibility in how to route their emergency calls to the PSTN.

Configuring ESA for the Branch Office

For ESA, the main office Call Server forwards the call to the Branch Office for termination. Calls are redirected over a Virtual Trunk using the NRS services. The NRS routes the calls using a special number, referred to in this section as the ESA Special Number.

ESA must be configured and tested on each call processor (the main office Call Server and each MG 1000B CP PM) to differentiate between emergency calls originating from IP Phones at each location and calls originating on trunks.

The steps to configure ESA for emergency access at each location are:

Step	Action
1	Determine the dialing plan for ESA calls.
2	Configure the main office emergency trunk (CAMA or PRI).
3	Configure the Virtual Trunk at the main office.
4	Configure ESN at the main office.
5	Configure ESA at the main office.
6	Configure the branch zone on the main office.
7	Configure the ESA Special Number on the main office.
8	Test ESDN using a main office telephone.
9	Configure the MG 1000B emergency trunk (CAMA or PRI).
10	Configure the Virtual Trunk at the MG 1000B.
11	Configure ESN at the Branch Office.
12	Configure ESA at the Branch Office.
13	Configure the Branch Office zone on the Branch Office.
14	Configure the ESN SPN on the Branch Office.
15	Configure the NRS for the ESA Special Number used.
16	Test ESDN using an MG 1000B IP Phone.
17	Test ESDN using an analog (500/2500-type) or digital telephone located at the Branch Office.

--End--

Reregistering to minimally configured branch

A Branch User in Local Mode but not physically at the branch may get incorrect emergency service handling. A Branch Office (for example, Survivable Branch Office or Survivable Remote Gateway) may not be provisioned with knowledge of all the ERLs in the enterprise. In this case, one of two scenarios occurs if an IP phone reregisters to the branch (either by VO ESA redirection or by fallback to Local Mode):

- If the local TN is provisioned as Manual Update, then the phone inherits the static location data. The static location data probably indicates basic ESA processing (per LD 24) if this is a small branch.
- If the local TN is provisioned as Auto Update, then cached location data in the phone is rejected if undefined locally, and unknown location values (ERL = 0, ECL = 0, LocDesc = Unknown) are assigned. Unknown location indicates default (basic) emergency processing (per LD 24), which is acceptable for a small branch. A system message is also generated to indicate that the phone location data was actually unknown and defaults were used, but emergency calls should be handled correctly.

Minimally configured branches (without LIS support) should be configured as *manual update*.

Determining the dialing plan for ESA calls

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.

ESA for international deployment must support the standard emergency number "112" and any emergency numbers in use prior to the EU directive.

The basic ESA feature only provides for a single ESA route per system. Since all IP Phones are associated with the same main office, all ESA calls therefore go to the same Public Safety Answering Point (PSAP) regardless from which Branch Office they originated. This is not satisfactory if the branch offices are widely dispersed.

In general, ESA calls should leave the network through a trunk at the Branch Office where the originating telephone is located. To enable this, it is necessary for telephones at each Branch Office 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 Branch Office. This prefix can be configured with the zone data for the MG 1000B telephones. The provisioning of this prefix is an enhancement for Branch Office.

While a variety of numbering schemes are available, Nortel recommends that customers use "0" + the ESN location code of the MG 1000B + ESDN, where ESDN is:

- for North America and CALA — "911"
- for members of the European Union — "112" and any other emergency numbers in use prior to the EU directive

This number, referred to here as the ESA Special Number, is configured as a special number (SPN) in the NRS so that the Virtual Trunk routes the call to the Branch Office.

Procedure 30
Configuring the main office

Step	Action

You can use Element Manager or the Command Line Interface for this procedure. Refer to IP Peer Networking Installation and Commissioning (NN43001-313) *for details.*

1 Configure the main office emergency trunk (CAMA or PRI).

Configure either analog CAMA or digital PRI to correctly signal the call identification.

ESA overrides all security features. Configure the trunk with restrictions so that other features cannot access the trunk.

2 Configure the Virtual Trunk using the procedure from *IP Peer Networking Installation and Commissioning* (NN43001-313).

The Virtual Trunk must be configured to enable emergency calls originating from MG 1000B IP Phones registered at the main office to reach the Branch Office.

3 Configure ESN.

ESA uses a route number rather than ESN route list index. However, ESN is required at the Branch Office.

4 Configure Emergency Services Access (ESA) in LD 24.

Configure an ACD number as an Emergency Services Directory Number.

Table 28
LD 24 Configure Emergency Services Access.

Prompt	Response	Description
REQ	NEW CHG	Add new data, or change existing data.
TYPE	ESA	Emergency Services Access data block
CUST	xx	Customer number as defined in LD 15

Table 28
LD 24 Configure Emergency Services Access. (cont'd.)

Prompt	Response	Description
ESDN	xxxx	Emergency Services DN (for example, 911). Up to four digits are accepted.
ESRT		ESA route number
	0-511	Range for CSLS; and CS1000E; system
	0-127	Range for small system and Media Gateway 1000B
DDGT	x…x	Directing Digits (for example, 1, 11, or 911). Up to four digits are accepted.
DFCL	x…x	Default ESA Calling Number. 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. The input must be a valid single appearance internal DN.

5 Configure the Branch Office zone on the main office.

a Configure the Branch Office zone's ESA dialing information in LD 117.

Table 29
LD 117 Configure Branch Office zone ESA route.

Command	Description
CHG ZESA <Zone><ESA Route #><AC><ESA Prefix><ESA Locator>	
	Defines the ESA parameters for the Branch Office zone, where: • Zone = Zone number for the Branch Office. • ESA Route # = Virtual Trunk route to MG 1000B Core. • 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 = Digit string added to start of ESDN. This is a unique prefix in the NRS. Nortel recommends that users use "0" + ESN location code of the Branch Office node. An example for location code 725 would be: 0725. • ESA Locator = Direct Inward Dial telephone number to be sent as part of ANI for use by the PSAP to locate the source of the call.

b Enable the Branch Office zone ESA in LD 117

ENL ZBR <Zone> ESA

6 Configure the ESA Special Number at the main office.

a Configure the ESA Special Number in the NRS. Using NRS, configure the ESA Special Number defined for the Branch Office zone. Refer to *IP Peer Networking Installation and Commissioning* (NN43001-313).

Nortel recommends that customers use "0" + the ESN Location code + ESDN. An example for location code 725 would be 0725911. The zero is recommended to prevent a collision in the ESN data with the HLOC entry.

b Configure the ESN Special Number at the main office.

1. Configure the Digit Manipulation Index in LD 86 with the DGT feature.

Table 30
LD 86 Configure Digit Manipulation Index.

Prompt	Response	Description
REQ	NEW	Add new data.
CUST	xx	Customer number as defined in LD 15
FEAT	DGT	Digit manipulation data block
DMI		Digit Manipulation Index numbers
	(0) (0)-31 (0)-255 (0)-1999	No digit manipulation required CDP NARS and BARS 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. DMI is not prompted if route TKTP = ADM.
DEL	(0)-19	Number of leading digits to be deleted
INST	x…x	Insert. Up to 31 leading digits can be inserted.
CTYP	<cr>	Call type to be used by the manipulated digits. This call type must be recognized by the far-end switch.

2. Configure the Route List Index in LD 86 with the RLB feature.

Table 31
LD 86 Configure Route List Index.

Prompt	Response	Description
REQ	NEW	Add new data.
CUST	xx	Customer number as defined in LD 15
FEAT	RLB	Route List data block
…		
RLI		Route List Index to be accessed
	0-127 0-255 0-1999	CDP and BARS NARS FNP
ENTR	0-63 0-6 X	Entry number for NARS/BARS Route List Route List entry number for CDP Precede with X to remove
LTER	NO	Local Termination entry
ROUT		Route number
	0-511	Range for CSLS; and CS1000E; system
DMI	(0)-1999	Digit Manipulation Index number, as previously defined in LD 86, FEAT = DGT (step i on page 381)

3. Configure the ESN Special Number and Digit Manipulation in LD 90.

Table 32
LD 90 Configure ESN Special Number and Digit Manipulation.

Prompt	Response	Description
REQ	NEW	Add new data.
CUST	xx	Customer number as defined in LD 15
FEAT	NET	Network translation tables
TRAN		Translator
	AC1 AC2	Access Code 1 (NARS/BARS) Access Code 2 (NARS)
TYPE	SPN	Special code translation data block
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.

Table 32
LD 90 Configure ESN Special Number and Digit Manipulation. (cont'd.)

Prompt	Response	Description
…		
- RLI		Route List Index to be accessed
	0-127 0-255 0-1999	CDP and BARSNARS FNP
…		
- SDRR		Supplemental Digit Restriction or Recognition
	ALOW ARRN DDD DENY DID ITED LDDD LDID STRK <cr>	Allowed codes Alternate Routing Remote Number Recognized remote Direct Distance Dial codes Restricted codes Recognized remote Direct Inward Dial codes Incoming Trunk group Exclusion Digits Recognized Local Direct Distance Dial codes Recognized Local Direct Inward Dial codes For ADM/MDM trunk groups Return to SPN
- - DMI	1-255 1-1999	Digit Manipulation Index Digit Manipulation Index with FNP DMI is only prompted when the Directory Number Expansion (DNXP) package 150 is equipped and SDRR = LDID.

ATTENTION
The Branch Office must recognize incoming digits on the Virtual Trunk and remove all but the ESDN.

7 Test ESDN using a main office telephone to confirm that main office calls go out the main office trunks.

If OSDN is used, the ESA route number must be blank to make test calls without using any trunk resources. It the route number has been configured, remove it by entering "x" at the prompt.

--End--

Procedure 31
Configuring the Branch Office

Step	Action

You can use Element Manager or the Command Line Interface for this procedure. Refer to IP Peer Networking Installation and Commissioning (NN43001-313).

1 Configure an emergency trunk (CAMA or PRI).

2 Configure the Virtual Trunk.

Before a call can come in on the Virtual Trunk, the Virtual Trunk must be configured.

3 Configure ESN.

A Special Number (SPN) is configured at the Branch Office. The SPN contains the digits sent to the NRS to route the emergency call from the main office to the Branch Office.

The SPN must use:

- A Route List Index (RLI) with local termination
- A Digit Manipulation Index (DMI)
  The system deletes the routing digits, leaving only the Emergency Services DN (ESDN).

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:

- telephones to connect to the MG 1000B Call Server (digital devices, analog devices, attendant consoles) and to dial the ESDN
- the Virtual Trunk (and any other trunks) to tandem a call to ESA

--End--

Procedure 32
Configuring the Branch Office zone

Step	Action
1	Configure the Branch Office zone on the Branch Office. In the Branch Office, only the zone number and bandwidth/codec selection is configured. Use the same zone number between the Branch Office and main office. The main office configuration (Procedure 30 “Configuring the main office” (page 203), step 5) provides the Branch Office zone characteristics (local time, local dialing, and ESA).
2	Configure the ESN SPN. The Branch Office must recognize the incoming digits on the Virtual Trunk and remove all but the ESDN. The call is routed to

a local termination. ESA recognizes the call as an emergency call and selects the correct route.

--End--

Configuring the NRS

The NRS must be configured for the ESA Special Number (SPN). The NRS uses the ESA SPN to route the emergency call from the main office to the Branch Office.

Nortel recommends that a consistent pattern be followed for all ESA calls. For example, use "0" + ESN Location code of the Branch Office node + the ESDN. An example for location code 725 would be: 0725911. The zero is recommended to prevent a collision in the ESN data with the HLOC entry.

For more information, refer to *IP Peer Networking Installation and Commissioning* (NN43001-313).

Testing the number

Use Procedure 33 “Testing ESDN using an MG 1000B Telephone” (page 209) to test the ESDN number from any telephone in the Branch Office.

Procedure 33
Testing ESDN using an MG 1000B Telephone

Step	Action
1	For IP Phones:
	a Dial the ESDN on an MG 1000B IP Phone in Local Mode. Use Procedure 28 “Using the Test Local Mode feature” (page 195) to enter Local Mode. The calls must go out on the emergency trunks in the Branch Office.
	b Dial the ESDN on an MG 1000B IP Phone in Normal Mode. The calls must tandem over the Virtual Trunk to the Branch Office and go out on the emergency trunks in the Branch Office. The following configuration problems can occur: • The call can receive overflow tones. Use LD 96 to view the digits sent to the Virtual Trunk (ENL MSGO dch#). • If the digits look correct on the main office, the NRS might not be properly configured. If the NRS rejects the call, a diagnostic message is displayed on the NRS console. • If the call makes it to the correct Branch Office (check that it is not going to the wrong node if the NRS is configured incorrectly) the Branch Office is probably rejecting it

because it does not know the digit string. Use LD 96 to view the digits (ENL MSGI {dch#}).

2 For analog (500/2500-type) or digital telephones, dial the ESDN on an MG 1000B analog (500/2500-type) or digital telephone.

The calls must go out on the emergency trunk(s) in the Branch Office.

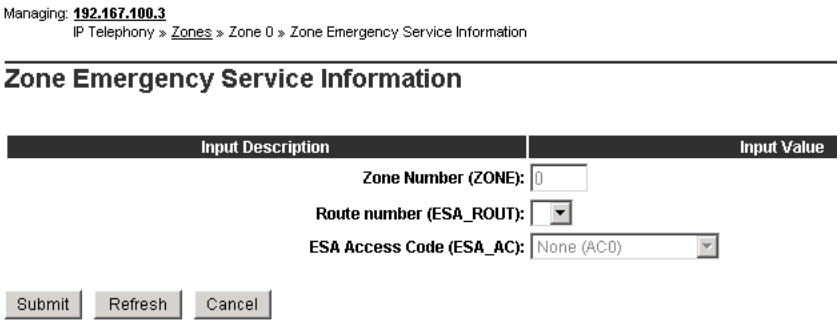
--End--

Configuring ESA in Element Manager

From Element Manager, you can configure ESA. From the **Zone List** window in Element Manager.

select the **Branch Office Emergency Service** option, and enter the necessary information. Refer to Figure 65 "Zone Emergency Service Information" (page 210).

Figure 65
Zone Emergency Service Information



Provisioning ESA calls for a central deployment

The challenge for provisioning ESA calls for a central deployment is that there are not enough ESDNs available for addressing the need of different ESDNs for a large number of sites. There had been only one ESDN available per system. The number was increased to 16 since Release 5.0 but is still not enough for larger deployments.

To resolve this issue, some digit manipulation is required. One ESDN is configured with a number that is not a real emergency number and is not conflicting with other DNs, 111 for example. Then, when a local emergency number is dialed (911, 999, 112, and so on) it is converted to 111 and the ESA processing engages. Based on the ERL number configured for the originating set, the route list is retrieved from the

corresponding ERL table. In that route list, 111 is changed back to the local emergency number before it is sent to the PSAP. The process is illustrated in the following example:

Call scenario: Dial local ESN 911 from DN 3013100 Houston.

1. Configure ESA with ESDN = 111 in LD 24
2. Configure ESDN conversion in the ZFDP table from 911 to 111 for the originating site

   Chg ZFDP 1 911 ESDN 111 LEN 3 ‘Houston Emergency Services DN”

3. Configure a route list in LD 86 as follows. This route list is going to be entered in the ERL table for routing the ESA call over a trunk.

   RLI 8
   Route 3 (route to PSAP)
   DEL 3
   INST <AC1/AC2>911

   For routing the call to a gateway, the route list is configured as follows:

   RLI 8
   Route 2 (route over VTRK to GW)
   DEL none
   INST 00301

   The call is routed to the gateway (GW) as 00301111. The GW converts the number to 911 with the following SPN:

   SPN 00301111
   RLI 9
   LTER = YES
   DEL 8
   INST 911

   911 is configured in the GW as an Emergency Service DN (ESDN) and the call is routed to the Public Safety Answering Point (PSAP).

Emergency Service using Special Numbers (SPN)

Determining the dialing plan for emergency access calls is critical.

In many jurisdictions, the emergency number is a fixed number (for example, "112" or "999"). The call processor (main office Call Server or MG 1000B CP PM) cannot have a DN that conflicts with these digits. To

dial the emergency number in this configuration, a Branch Office user must dial the appropriate Access Code. For example, if AC2 is 9, then the user must dial "9 999" to make a call to emergency services.

Access to Emergency Service using SPN should be configured in the following circumstances:

- When the Emergency Service number at the Branch Office is different from that at the main office.
- When there is more than one number used for accessing Emergency Service; for example, when there are different numbers for Police, Fire, and Ambulance services.
- In markets where the ESA feature is not available (outside of North America and CALA).

If MG 1000B PSTN access is correctly configured, Emergency Service from the Branch Office will already be present.

Branch Office access to Emergency Service using SPN must be configured and tested on each call processor (the main office Call Server and the MG 1000B Call Server) to differentiate between emergency calls originating from IP Phones at each location and emergency calls originating on trunks.

CLID verification (CLIDVER)

Use the CLIDVER prompt in LD 20 to verify that the ESA or non-ESA (SPN) emergency number is properly composed and configured. Refer to “Verify CLID” (page 224) for more information.

Networked M911

The Networked M911 feature introduces a new trunk subtype 911P exclusively for 911 calls redirected over an MCDN Network. A new prompt, 911P, is introduced in the Route Data Block for TIE trunks only. This prompt, if set to YES, signifies that the trunks associated with these routes are 911P trunks. All incoming 911 calls to the tandem M1 are redirected to the target M1 over 911P trunks. At the target node, these calls will be treated in respect the same as incoming calls on 911E/ 911T trunks.

A new trunk subtype is introduced in the Route Data Block exclusively for TIE trunks. All the prompts specific to 911 are prompted in the RDB if the TKTP prompt value is TIE. In case of TIE trunks, the M911_TRK_TYPE prompt does not appear and is replaced by the newly introduced prompt 911P. The M911_ANI, M911_NPID_FORM and NPID_TBL_NUM are not prompted in the RDB. If the 911P prompt is set to YES, IFC prompt is set to SL1 by default since 911P trunks are supported only over MCDN.

Figure 66
New and changed prompts and responses in LD 16

PROMPT	RESPONSE	DESCRIPTION
req	new/chg	
type	rdb	Route Data Block
cust	0-99	
.....		
tktp	TIE	Trunk Type
911P	**(NO)/YES**	**M911 Trunk Type for MCDN Network.**
M911_ABAN	**(NO)/YES**	optional call abandon treatment YES = abandoned call treatment for route NO = no abandoned call treatment for route
M911_TONE	**(YES)/NO**	optional call abandon tone YES = tone given on answer NO= silence given on answer

Maintenance and diagnostics

Contents

This chapter contains the following topics:

"Firmware downloads" (page 215)

"Troubleshooting" (page 218)

"Signaling Server CLI commands" (page 223)

"Call Server commands" (page 224)

"Co-resident Call Server and Signaling Server restart commands" (page 228)

Firmware downloads

ATTENTION
This section applies only to the IP Phone 2001, IP Phone 2002, IP Phone 2004, IP Phone 2007, IP Phone 1110, IP Phone 1120E. IP Phone 1140E, IP Phone 1150E, IP Phone 2033, and IP Phones 1210, 1220, 1230. It does not apply to the IP Phone KEM, Expansion Module for IP Phone 1100 Series, IP SoftPhone 2050, WLAN 2210/2211, WLAN 61xx, or SIP Phones.

Enhanced UNIStim Firmware Download for IP Phones

Communication Server 1000 Release 4.5 introduced Enhanced Firmware Download for IP Phones. The Branch Office IP Phone firmware is automatically downloaded from the main office to the Branch Office

The administrator enters **`umsUpgradeAll`** command at the main office. The firmware version on the Normal Mode Branch Office IP Phone is compared to the firmware policy of the main office. If the firmware is the same as the main office, no firmware update is required. If the firmware is different, the IP Phones are redirected to the Branch Office.

The firmware files are transferred from the main office to the Branch Office by FTP. Once the files have successfully been transferred to the Branch Office, the **`umsUpgradeAll`** command is invoked on the Branch Office. All IP Phones waiting for the firmware are automatically upgraded and returned to the main office.

The firmware retrieval mechanism for the Branch Office TPS retrieves only firmware files it finds missing.

It does not compare the list of firmware on the Branch Office TPS with the main office TPS to determine whether the Branch Office has the latest firmware, nor does it perform any automatic compare and update operations. The Branch Office TPS only receives firmware files when the **umsUpgradeAll** command is issued on the main office TPS. When an IP Phone registers with a TPS, the TPS checks the firmware version in the IP Phone. If the firmware version differs from that required by the Signaling Server and the firmware upgrade policy requires an upgrade, the firmware is downloaded to the telephone. The telephone reboots after the firmware download is complete and registers with the TPS again.

When the IP Phone firmware in the TPS is upgraded, the IP Phones that registered with the Call Server before the upgrade are not affected. The system administrator must execute the CLI command **umsUpgradeAll** to download the firmware to all registered IP Phones that do not have the latest firmware files. However, firmware download is automatic for IP Phones that register to the TPS after the upgrade.

Firmware download does not happen when Internet Telephones register to the LTPS by a Virtual Office Login or Branch Office redirection to the Main Office. Instead, Branch Office Internet Telephones are redirected back to the Branch Office LTPS for firmware upgrade. This redirection occurs only if the **umsUpgradeAll** command is issued from the Main Office LTPS, and the current firmware version does not match the Main Office LTPS firmware policy.

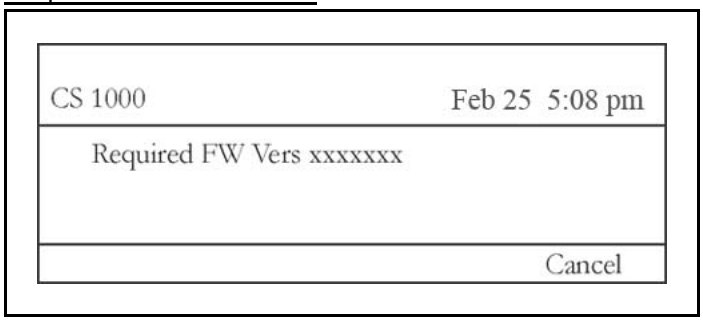
If an IP Phone is in use when the **umsUpgradeAll** command is issued, the call is not interrupted. Its firmware version is checked against the main office TPS firmware policy, and if there is no match, the IP Phone is flagged, then redirected to the MG 1000B TPS when the call is completed.

The **umsUpgradeAll** command has no immediate impact on IP Phones that are logged in or out by Virtual Office. However, the firmware files may be upgraded, if required, when the Virtual Office session is terminated.

For information on Enhanced UNIStim Firmware, refer to *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

Each IP Phone that is redirected back to the Branch Office has its firmware version checked against the MG 1000B TPS firmware policy. If there is no match, the firmware is upgraded automatically and the IP Phone is redirected back to the main office. If there is a match, the IP Phone stays in Local Mode, and "Required firmware <version> is displayed on the telephone screen (see Figure 67 "Required firmware version" (page 217)).

Figure 67
Required firmware version



This figure shows a screen display from an IP Phone 2004. The display on another model of IP Phone may differ.

This display can only be cleared by pressing the Cancel key. While this display appears, the user can only receive calls; they cannot make outgoing calls.

Upgrade procedures can be found in *Signaling Server IP Line Applications Fundamentals* (NN43001-125). Relevant information can be found in *IP Line: Description, Installation, and Operation* (NN43100-500).

Procedure 34
Upgrading firmware for Communication Server 1000 Release 7.0

Step	Action
1	At the Main Office, upgrade IP Phone firmware on the Signaling Server. For instructions, see the chapter "Uploading software upgrade files" in *Communication Server 1000E: Upgrade Procedures (NN43041-458)* ().
2	Issue the CLI command **`umsUpgradeAll`** at the main office.
3	The Branch Office IP Phones that are in Normal Mode (for example, IP Phones registered to the main office Call Server) are checked to see if they require a firmware upgrade. If the IP Phones require a firmware upgrade, the IP Phones are redirected back to the Branch Office.
4	The Branch Office checks its own firmware version and compares it with the firmware version which is required by the IP Phone. If the Branch Office does not have the required firmware, then the Branch Office automatically initiates an File Transfer Protocol (FTP) or Secure File Transfer Protocol (sFTP) session to the main office and retrieves the required firmware.

5 Issue the CLI command **umsUpgradeAll** at the Branch Office. The IP Phones that are waiting in Local Mode receive the firmware upgrade and are redirected back to the main office.

--End--

Troubleshooting

This section contains error messages and troubleshooting information for IP Phone operation.

When a login is attempted and one of the messages provided in Table 33 "Normal Operation troubleshooting" (page 218) through Table 35 "Branch User Config troubleshooting" (page 221) appears on the telephone display, there can be more than one reason.

Table 33
Normal Operation troubleshooting

Message	Probable Cause	Actions
Local Mode	Test Local mode	Press **Services** key (key with Globe icon), and select **Resume Normal Mode**. Use the STAT c u command in LD 32 to show the reason why the Branch User stays in Local Mode.
Local Mode Server Unreachable (1)	Incorrect Primary or Alternate NCS IP address configured.	Correct Primary or Alternate NCS IP address.
	Primary or Alternate NCS IP address unreachable from this endpoint.	Check network configuration and update as required.
	NCS port number is not properly configured.	Correct main office and MG 1000B NCS port numbers.
	NCS is down.	Restore NCS.
	Link to NCS is down.	Possible additional action required. The Branch office is not registered with the NCS; Check virtual trunks configuration, H.323 ID for each server and/or NCS configuration.

Table 33
Normal Operation troubleshooting (cont'd.)

Message	Probable Cause	Actions
Local Mode Ser ver Unreachable (2)	Main office TPS is unreachable from the MG 1000B TPS.	Check network configuration, and update as required.
	Main office TPS is down.	Restore main office Signaling Server.
	Link to main office TPS is down.	Restore Link to main office TPS.
	Main office Call Server is down.	Restore main office Call Server.
	Main office node is not registered as a SIP or H.323 endpoint to the NCS.	Register the main office node to the NCS.
Local Mode Invalid ID (1)	Branch User ID endpoint is not in NCS database.	Check NRS database and update as required.
	Incorrect Branch User ID configured.	Correct Branch User ID configuration in Branch Office TN.
Local Mode Invalid ID (2)	Branch User ID not found in any equipped TN.	Check main office Branch User configuration, and update as required.
	Incorrect Branch User ID configured.	Correct Branch User ID configuration in Branch Office TN.
Local Mode Invalid ID (3)	NCS database has Branch Office as endpoint for Branch User ID.	Correct NRS database configuration to have main office as Branch User ID endpoint.
	Incorrect Branch User ID configured.	Correct Branch User ID configuration in Branch Office TN.
Required FW Vers	Firmware incompatible with main office TPS.	Upgrade IP Phone firmware at the MG 1000B TPS. Nortel recommends that customers upgrade all MG 1000B TPSs before they upgrade the main office TPS during firmware upgrade. The IP Phones are directed to the Branch Office for firmware upgrade, and then redirected to the main office automatically.

Table 34
Legend for LD 32 STAT command Login status

Number	Description
0	Initialize status

Table 34
Legend for LD 32 STAT command Login status (cont'd.)

Number	Description
1	Branch User Login
2	Branch User Local Mode Test
3	Branch User Config
5	Branch User Forced Logout (F/W Download)
6	Branch User No Branch Password Provisioned
7	Branch User Locked from Branch Password Retry
10	Branch User NRS Unreachable
11	Branch User NRS User Unknown (user id - TN combination unknown)
12	Branch User main office unreachable, or Main office is not registered with the NRS as an endpoint.
13	Branch User main office User ID Unknown, or Branch User main office User ID and Main Office TN Combination does not exist, or IP Phone telephone type and Main Office TN telephone type do not match.
14	Branch User Firmware Out of Sync
15	Another Branch User already logged in the User ID at the main office and is active on a call
16	Branch User ID entry in NRS database has MG 1000B as endpoint
30	Virtual Office Login
32	Virtual Office Locked from Login

Table 35
Branch User Config troubleshooting

Message	Probable Cause	Actions
Busy, try again	Main office TN already equipped and active on a call.	Identify duplicate Branch User ID allocation, and correct the configuration accordingly.
	Incorrect Branch User ID entered.	Retry with correct Branch User ID.
Invalid ID (1)	Incorrect Branch User ID entered.	Retry with correct Branch User ID.
	Branch User ID not in NRS database.	Update NRS database to include Branch User ID.
Invalid ID (2)	Incorrect Branch User ID entered.	Retry with correct Branch User ID.
	No Main Office TN associated with Branch User ID configured.	Configure Main Office TN to associate with Branch User ID.
	Main Office TN associated with the Branch User ID and the programmed TN on the IP Phone does not match.	Configure a Main Office TN to match the IP Phone TN. Branch User in which the TN Main Office configured is the same as the Branch User TN. Configure a new Branch Office TN and IP Phone TN to match the Main Office TN.
Invalid ID (3)	NRS database has Branch Office as endpoint for Branch User ID.	Correct NRS database configuration to have main office as Branch User ID endpoint.
	Incorrect Branch User ID entered.	Retry with correct Branch User ID.
Locked from Login	Incorrect MG 1000B TPS IP Phone Installer's Password, or Temporary IP Phone Installer's Password entered three times.	Wait one hour for the lock to clear automatically, or use the clearLockout command on the MG 1000B IPL maintenance terminal to clear the lockout.
	Incorrect Main Office TN Station Control Password, main office IP Phone Installer's Password, or main office Temporary Telephone Installer's	Wait one hour for the lock to clear automatically, or disable and enable the Main Office TN in LD 32 to clear the lockout.

Table 35
Branch User Config troubleshooting (cont'd.)

Message	Probable Cause	Actions
	Password entered three times.	
Permission Denied (1)	IP Phone Installer's Password or Temporary IP Phone Installer's Password at the MG 1000B TPS not configured or disabled.	Set or enable the IP Phone Installer's Password or Temporary IP Phone Installer's Password at the MG 1000B TPS.
Permission Denied (2)	Incorrect Branch User ID entered.	Retry with correct Branch User ID.
	IP Phone Installer's Password at the main office TPS not configured or disabled and the Branch User ID is already assigned to a user in another Branch Office.	Identify duplicate Branch User ID allocation, and make correction.
Permission Denied (3)	Incorrect Branch User ID entered.	Retry with correct Branch User ID.
	Incorrect IP Phone Installer's Password at the main office TPS entered.	Retry with correct IP Phone Installer's Password at the main office TPS.
	Station Control Password not configured in Main Office TN.	Add Station Control Password to the Main Office TN.
Permission Denied (4)	Terminal type configured in the Main Office TN does not match the type of the MG 1000B IP Phone.	Change the terminal type in the Main Office TN to match the type of the MG 1000B IP Phone, or change the terminal type in the Branch Office TN to match the type in the Main Office TN, and replace the MG 1000B IP Phone with the correct type.

Table 35
Branch User Config troubleshooting (cont'd.)

Message	Probable Cause	Actions
Permission Denied (6)	Incorrect Branch User ID entered.	Retry with correct Branch User ID.
	Incorrect Branch Office IP Phone Installer's Password or Temporary IP Phone Installer's Password entered.	Retry with correct Branch Office IP Phone Installer's Password or Temporary IP Phone Installer's Password.
	Incorrect main office IP Phone Installer's Password or Station Control Password entered.	Retry with correct main office IP Phone Installer's Password or Station Control Password.
Server Unreachable (1)	Incorrect Primary or Alternate NRS IP address configured.	Correct Primary or Alternate NRS IP address.
	Primary or Alternate NRS IP address unreachable from this endpoint.	Check network configuration and update as required.
	NCS port number is not properly configured.	Correct main office and MG 1000B NCS port numbers.
	NRS is down.	Bring NRS into service.
	Link to NRS is down.	Restore Link to NRS.
Server Unreachable (2)	Main office TPS is unreachable from the MG 1000B TPS.	Check network configuration, and update as required.
	Main office TPS is down.	Bring main office Signaling Server into service.
	Link to main office TPS is down.	Restore link to main office TPS.
	Main office Call Server is down.	Bring main office Call Server into service.
	Main office node is not registered as a SIP or H.323 endpoint to the NRS.	Register the main office node to the NRS.

Signaling Server CLI commands

This section describes Command Line Interface (CLI) commands on the Signaling Server specific to the MG 1000B.

Refer to *Signaling Server IP Line Applications Fundamentals* (NN43001-125) for a complete list of all CLI commands available on the Signaling Server.

isetShow

The isetShow command shows the type of IP Phone registration and the registration status. This command displays general information for all registered IP Phones.

clearLockout TN or IP

A registration lock is placed at the TPS after three consecutive failed attempts to enter either the IP Phone Installer's Password or the Temporary IP Phone Installer's Password.

The lockout affects the Virtual Office login or Branch User Config and lasts for one hour. This lockout does not survive re-registration of the IP Phone. However, the installation technician can issue the **`clearLockout`** command to clear the lockout for a particular telephone.

This command has one parameter the TN or IP address of the telephone.

Call Server commands

This section contains LD commands on the Call Server applicable to the Branch Office feature.

Verify CLID

LD 20 contains the CLIDVER prompt, which is used to verify the proper composition and configuration of the Calling Line ID (CLID) for ESA and non-ESA calls. The prompt simulates a call without actually making it and generates a report showing the CLID, zone numbers, and other information.

Table 36
LD 20 Generate a CLIDVER report.

Prompt	Response	Description
REQ:	PRT	Print
TYPE:	CLIDVER	CLID Verification
CUST	xx	Customer number as defined in LD 15.
SORTBY	(DN) TN"	The output/report will be sorted based on this flag. If the response is DN, the LD prompts the user to enter the DN, and the output is sorted by the DN. If the response is TN, the LD prompts the user to enter the TN, and the output is sorted by the TN.
DN	x...x,	Directory Number. If no value is entered, the report includes all Directory Numbers.
TN		Terminal Number

Table 36
LD 20 Generate a CLIDVER report. (cont'd.)

Prompt	Response	Description
	l s c u	Format for Large System and Communication Server 1000E system, where l = loop, s = shelf, c = card, and u = unit
ESA_ONLY	(YES) NO	Flag used to decide if the report should contain information for ESA call type only or for all call types. If the ESA package is not enabled, this input prompt does NOT appear. The report contains non-ESA data only.
SHORT	(YES) NO	Flag to decide if the output report should be a Short Report or a Long Report.

The CLIDVER report contains the CLID composed for the Branch User. If the report is generated on the main office Call Server, the CLID is composed as follows:

- If ESA is enabled in the Branch Office, the CLID is the same as the value entered for the ESA Locator parameter in the CHG ZESA command in LD 117 (see Procedure 30 "Configuring the main office" (page 203), step 5).
- If ESA is not enabled, the CLID is the same as the CLID entry composed in LD 15.

If the CLIDVER report is generated on the MG 1000B CP PM, the CLID is the same as the CLID entry composed in LD 15'

For more information about this feature, see *Emergency Services Access: Description and Administration* ((NN43001-613)).

Print Branch Office zone information

LD 117 contains commands to view Branch Office zones at the main office Call Server.

Table 37
LD 117 Print zone information.

Command	Description
PRT ZACB [<Zone>]	
	Print a table of Branch Office zone dialing plan entries.
PRT ZBW [<Zone>]	
	Print a table of zone bandwidth utilization.
PRT ZDES [<DESMatchString>]	

Table 37
LD 117 Print zone information. (cont'd.)

Command	Description
	Print a table of the zone description entries.
PRT ZDP [<Zone>]	
	Print a table of Branch Office zone dialing plan entries.
PRT ZDST [<Zone>]	
	Print a table of Branch Office zone time adjustment properties entries.
PRT ZESA [<Zone>]	
	Print a table of Branch Office zone Emergency Services Access parameters.
PRT ZONE ALL	Print zone information for all zones.
PRT ZONE 0-8000	Print zone information for a specific zone.
PRT ZTDF [<Zone>]	
	Print a table of Branch Office zone time adjustment properties entries.
PRT ZTP [<Zone>]	
	Print a table of Branch Office zone time adjustment properties entries.

Enable and disable Branch Office zone features

LD 117 contains commands to enable and disable features for the Branch Office zones.

Table 38
LD 117 Enable/Disable Branch Office zone features.

Command	Description
ENL ZBR [<Zone>] [ALL] [LOC] [ESA] [TIM]	
	Enable features for the Branch Office zone. If no specific features are specified, ALL is assumed.
DIS ZBR [<Zone>] [ALL] [LOC] [ESA] [TIM]	
	Disable features of the Branch Office zone. If no specific features are specified, ALL is assumed.

View status of Branch Office zone at main office Call Server

LD 117 contains commands to view the status of Branch Office zones at the main office Call Server.

Table 39
LD 117 Display zone status.

Command	Description
STAT ZONE [<Zone>]	
	Display zone status table
STAT ZBR [<Zone>]	
	Display status of Branch Office zones.

Change and print PVQ notification levels

The notification level can be changed on a zone-by-zone basis so that a particular zone, such as a Branch Office zone, is monitored more closely than others. LD 117 contains commands for changing and viewing the notification level for a zone. For more information on PVQ, refer to *Converging the Data Network with VoIP* (NN43001-260).

ATTENTION
The notification level for a Branch Office zone must be configured the same at both the main office and the Branch Office.

Table 40
LD 117 Change/print PVQ notification levels.

Command	Description
CHG ZQNL ALL <Level>	
	Change the notification level for all zones.
CHG ZQNL <Zone> <Level>	
	Change the notification level for the specified zone.
PRT ZQNL ALL	Print a table of the notification level for all zones.
PRT ZQNL <Zone>	
	Print a table of the notification level for the specified zone.

Print PVQ statistics

LD 117 contains a command to print PVQ statistics for the Branch Office zone. For more information on PVQ, refer to *Converging the Data Network with VoIP (NN43001-260)* ().

Table 41
LD 117 PVQ statistics.

Command	Description
PRT ZQOS <Zone>	
	Print the PVQ statistics for the Branch Office zone.

Print inventory

The inventory (generated in LD 117) is for all IP Phones registered to the Server. This includes IP Phones registered by a Virtual Office and Branch Office logins at the main office Call Server. At the Server, inventory only includes IP Phones registered at the MG 1000B Gateway Controller, not all the IP Phones physically located at the Branch Office.

To get an inventory of all IP Phones at a Branch Office, execute the **INV GENERATE** command at the Branch Office with all Branch Users in Local Mode.

ATTENTION
Do this only during a maintenance window.

To register all IP Phones at the CP PM, disconnect the LAN/WAN connection to the main office (not recommended) or individually log out the IP Phones from the main office. See "Test Local Mode" (page 195).

LD 117 contains inventory commands. These commands include the registered IP Phones.

Table 42
LD 117 Print inventory.

Command	Description
INV PRT	Print STATUS, CARDS, SETS or ALL.
INV GENERATE	Generate inventory CARDS, SETS, ALL or ABORT.
INV MIDNIGHT	Generate inventory CARDS, SETS, ALL, OFF or STATUS.

Print MG 1000B software and system information

When the Branch Office (SBO) package 390 is equipped, the **ISS** and **ISSP** commands in LD 22 display system and software information for the Branch Office. If the SBO package is restricted, the two commands provide information about the Call Server.

Table 43
LD 22 Print MG 1000B software and system information.

Prompt	Response	Description
REQ	ISS ISSP	Print issue and release Print system, DepList, and patch information

Co-resident Call Server and Signaling Server restart commands

The following restart commands are supported on the Co-resident Call Server and Signaling Server.

Table 44
Restart commands

From	Command	Description
Linux Bash Shell	Reboot	Shut down all processes and restart Linux OS End result for the Call Server is equivalent to a cold start.
Call Server Overlay 135	ini active	Invoke Call Server warm start only. No impact to other Linux processes.
	Sysload active	Invoke Call Server cold start No impact to other Linux processes.
Call Server PDT1/PDT2	Reboot	Invoke Call Server warm start No impact to other Linux processes.
	Reboot -1	Invoke Call server cold start No impact to other Linux processes.
Call Server VxWorks Shell (su)	Reboot	Invoke Call server warm start No impact to other Linux processes.
	Reboot -1	Invoke Call Server cold start No impact to other Linux processes.

Appendix Preprogrammed data

Contents

This chapter contains the following topics:

“Introduction” (page 231)
“Passwords and codes” (page 231)
“Default numbering plan” (page 232)
“Flexible Feature Codes” (page 233)
“SDI ports” (page 234)
“Trunk routes” (page 236)
“System parameters” (page 236)
“Customer data” (page 237)
“Trunk models” (page 237)

Introduction

To install a Communication Server 1000E system as a Branch Office, you must first enter customer data in overlays. For example, you must assign features to the telephone keys.

For software installation, it is not necessary to program data for the Call Server in advance. The Call Server can be programmed with the minimum number of files to enable the Branch Office feature to operate.

Passwords and codes

Table 45 "Passwords and codes" (page 232) lists each function and its default password or code. The user may be prompted to change the password upon first entry.

Table 45
Passwords and codes

Function	Code or extension
TTY password (For access to TTY system overlays)	0000
Level 1 login name access	ADMIN1
Level 1 password access	0000
Level 2 login name access	ADMIN2
Level 2 password access	0000
Administration telephone password	1234
Administration telephone FFC	*41
SPRE code	1
Telephone relocation Flexible Feature Code	*40
Telephone Removal Flexible Feature Code	*42
Telephone relocation password (SRCD)	1234

Default numbering plan

The default numbering plan for a Branch Office is based on the following guidelines:

- The default numbering plan uses four digits and starts at 2200.
- The prime extension number (DN) for each telephone is in the range 2200-2XXX. The value of "XXX" varies depending on the number of telephones in the system. Secondary extension numbers use numbers outside this range. This arrangement enables the Communication Server 1000E to automatically configure telephones.

First digits

Table 46 "Default numbering plan First digit" (page 232) shows the default numbering plan for a Branch Office.

Table 46
Default numbering plan First digit

First digit	Preprogrammed use for digit
1	SPRE code
2	Not used
3	Not used
4	Not used
5	Not used

Table 46
Default numbering plan First digit (cont'd.)

First digit	Preprogrammed use for digit
6	Not used
7	COT/TIE/DID/WATS/FEX/RAN/MUS/AWR/Paging Trunk Access Codes and attendant DN, Call park DNs
8	Not used
9	Not used
0	Attendant extension

The first number of the default numbering plan is preprogrammed as 2200. The remaining numbers are assigned in software. These numbers do not become active until you select the numbers during the telephone activation procedure.

The digit "7" in the default numbering plan is programmed with many system features to help you configure the Communication Server 1000E system.

Important extension numbers

Table 47 "Default numbering plan important extension numbers" (page 233) lists important extension numbers.

Table 47
Default numbering plan important extension numbers

Extension	Use
Attendant extension	0
Call park extensions	7900-7919

Flexible Feature Codes

Many administrative procedures use Flexible Feature Code (FFC) data. Table 48 "Flexible Feature Codes" (page 233) lists the FFCs for the Communication Server 1000E system.

Table 48
Flexible Feature Codes

FFC Prompt	FFC	Definition
ASRC	*40	Automatic Set Relocation
AREM	*42	Automatic Set Removal Code
ADMN	*41	Administration Set Access Code
CFWA	#1	Call Forward All Calls Activate
CFWD	#1	Call Forward All Calls Deactivate

Table 48
Flexible Feature Codes (cont'd.)

FFC Prompt	FFC	Definition
C6DS	*70	6 Party Conference Code
HOLD	#4	Permanent Call Hold
MNTC	*43	Maintenance Access Code
PUGR	*71	Pick-up Group Code
RDLN	*72	Last Number Redial
RDST	*73	Store Last Number Redial
RGAA	*74	Ring Again Activate
RGAD	*75	Ring Again Deactivate
RGAV	*77	Ring Again Verify
SPCC	#2/*80	Speed Call Controller Code
SPCU	#3/*81	Speed Call User Code
SSPU	*89	System Speed Call User Code

SDI ports

The minimum port configuration for the Branch Office is three SDI ports, all of which are on the Gateway Controller. Table 49 "Pre-configured SDI ports" (page 234) shows the default SDI port configuration. The value for "XX" is set on the faceplate of the Server.

Table 49
Pre-configured SDI ports

TTY Number	Card	Port	Use	Configuration
0	0	0	MTC/SCH/BUG	XX/8/1/NONE
1	0	0	MTC/SCH/BUG	1200/8/1/NONE
2	0	1	CTY	1200/8/1/NONE

Table 50
Pre-configured PTY ports

TTY Number	Card	Port	Use
14	0	0	MTC/SCH/BUG
15	0	1	MTC/SCH/BUG

Modem port

The pre-configured modem port enables the remote maintenance modem to be connected without additional system programming. This port is pre-configured as TTY 0 (port 0 on the) and programmed for Maintenance (MTC), Service Change (SCH), and BUG messages.

ESDI settings

Table 51 "ESDI settings" (page 235) lists the preset ESDI settings.

Table 51
ESDI settings

Setting	Code
BPS	4800
CLOK	EXT
IADR	003
RADR	001
T1	10
T2	002
T3	040
N1	128
N2	08
K	7
RXMT	05
CRC	10
ORUR	005
ABOR	005
USER	CMS
ENL	NO

Telephone tones

The telephone tones in North America are as follows:

- **Dial tone:** A continuous tone.
- **Special dial tone:** Three beeps followed by continuous dial tone.
- **Overflow tone:** Like a busy tone, except faster and higher.
- **Relocation tone:** A short high-pitched beep that continues for 4 seconds, followed by silence.

Trunk routes

Table 52 "Preprogrammed trunk route information" (page 236) shows preprogrammed trunk route information that you must have to activate and modify trunks.

Table 52
Preprogrammed trunk route information

Route	Type	Access Code	Mode	Interface
00 *	COT	7100	IAO	-
01 *	COT	7101	ICT	-
02 *	COT	7102	OGT	-
03	TIE	7103	IAO	-
04	TIE	7104	ICT	-
05	TIE	7105	OGT	-
06	DID	7106	ICT	-
07	WAT	7107	IAO	-
08	WAT	7108	ICT	-
09	WAT	7109	OGT	-
40	MUS	7140	OGT	-
41	AWR	7141	-	AUD
42	RAN	7142	-	DGT
43	RAN	7143	-	AUD
44	PAG	7144	OGT	-
50	FEX	7150	IAO	-
51	FEX	7151	ICT	-
52	FEX	7152	OGT	-

Trunk routes marked with an asterisk (*) are configured to support Call Detail Recording (CDR) output. CDR is pre-configured in LD 16 as follows:

```
CDR     YES
INC     YES
OAL     YES
AIA     YES
```

System parameters

Table 53 "System parameters" (page 237) provides the default system parameter values for the system.

Table 53
System parameters

Parameter	Value
Low Priority Input Buffers (LPIB)	450
High Priority Input Buffers (HPIB)	450
Number of Call Registers (NCR)	300
Multiple Appearance Redirection Prime (MARP) feature allowed	YES

Refer to "Capacity Engineering" in *Communication Server 1000S: Planning and Engineering* (NN43041-220) for further information on buffer sizes.

The preprogrammed data also include virtual superloops 96, 100, 104, 108, and 112.

Customer data

The default customer number used in the preprogrammed data is zero (0).

Trunk models

Do not use the DIP Class of Service for Model 19 of TIE trunk mode. The correct Class of Service for model 19 of TIE trunk mode is DTN.

All trunks are programmed as immediate start/ supervision = YES, with the exception of trunks with an asterisk (*). Trunks marked with an asterisk (*) are set for wink start/ supervision = YES.

Table 54
Preprogrammed trunk route information

Mode	Card	Model	Signaling	DIP or DTN	BIMP and TIMP
COT	XUT	1	GRD	DIP	3COM/600
		2	LOP	DIP	3COM/600
		3	GRD	DTN	3COM/600
		4	LOP	DTN	3COM/600
		5	GRD	DIP	3COM/900
		6	LOP	DIP	3COM/900
		7	GRD	DTN	3COM/900
		8	LOP	DTN	3COM/900

Table 54
Preprogrammed trunk route information (cont'd.)

Mode	Card	Model	Signaling	DIP or DTN	BIMP and TIMP
TIE	XUT	1	OAD	DIP	3COM/600
		2	LDR	DIP	3COM/600
		3	OAD	DTN	3COM/600
		4	LDR	DTN	3COM/600
		5	OAD	DIP	3COM/900
		6	LDR	DIP	3COM/900
		7	OAD	DTN	3COM/900
		8	LDR	DIP	3COM/900
TIE	XEM	16	EAM	DIP	-/600
		17	EM4	DIP	-
		18	EAM	DTN	-/600
		19	EM4	DTN	-
DID	XUT	1	LDR Wink Start Supv = YES	DIP	3COM/600
		2	LDR Wink Start Supv = YES	DTN	3COM/600
		3	LDR Wink Start Supv = YES	DIP	3COM/900
		4	LDR Wink Start Supv = YES	DTN	3COM/900
		5*	LDR Wink Start Supv = YES	DIP	3COM/600
		6*	LDR Wink Start Supv = YES	DTN	3COM/600
		7*	LDR Wink Start Supv = YES	DIP	3COM/900
		8*	LDR Wink Start Supv = YES	DTN	3COM/900

Table 54
Preprogrammed trunk route information (cont'd.)

Mode	Card	Model	Signaling	DIP or DTN	BIMP and TIMP
WAT	XUT	1	GRD	DIP	3COM/600
		2	LOP	DIP	3COM/600
		3	GRD	DTN	3COM/600
		4	LOP	DTN	3COM/600
		5	GRD	DIP	3COM/900
		6	LOP	DIP	3COM/900
		7	GRD	DTN	3COM/900
		8	LOP	DTN	3COM/900
MUS	XUT	1			3COM/600
AWR	XUT	1			600/1200
RAN	XUT	1			600/1200
PAG	XUT	1	LDR	DIP	3COM/600
		2	OAD	DIP	3COM/600
		3	LDR	DTN	3COM/600
		4	OAD	DTN	3COM/600
		5	LDR	DIP	3COM/900
		6	OAD	DIP	3COM/900
		7	LDR	DTN	3COM/900
		8	OAD	DTN	3COM/900
PAG	XEM	16	EAM	DIP	-/600
		17	EM4	DIP	-
		18	EAM	DTN	-/600
PAG	XEM	19	EM4	DTN	-
FEX	XUT	1	GRD	DIP	3COM/600
		2	LOP	DIP	3COM/600
		3	GRD	DTN	3COM/600
		4	LOP	DTN	3COM/600
		5	GRD	DIP	3COM/900
		6	LOP	DIP	3COM/900
		7	GRD	DTN	3COM/900
		8	LOP	DTN	3COM/900

Appendix
Branch Office engineering example

Introduction

This chapter provides sample engineering calculations for a Branch Office with a Communication Server 1000M or Communication Server 1000E Main Office.

Assumptions

The following section assumes the equipment and traffic characteristics of the Branch Office.

Equipment characteristics

Assume the Branch Office possesses the equipment characteristics as follows:

- One MG 1000B chassis, with an card, 128 DSP ports (fully populated DSP daughter cards), and one MB 1000B expander chassis.
- CP PM Co-resident Call Server and Signaling Server
- One PRI span (either T1 or E1)
- 120 UNIstim IP phones
- 48 TDM telephones, comprised of Digital telephones

Traffic characteristics

Assume the Branch Office has the following traffic characteristics:

- UNIStim IP telephone CCS: 6 CCS
- TDM telephone CCS: 5 CCS
- Average Hold time: 120 seconds
- Traffic Distribution:

- UNIStim telephones: forty-five per cent to other UNIStim telephones (Intra-IP calls), fifty-five per cent to Branch Office TDM telephones and TDM trunks.
- TDM telephones: forty per cent of calls to TDM trunks, sixty per cent of calls to UNIStim telephones.

- No trunk traffic between Branch Office TDM resources and Main Office.

Conference traffic is usually not singled out for calculation in traffic engineering. When a Branch Office does not have conference capability, conference call participants must use the LAN/WAN to reach the Main Office to join conferences. However, if the traffic is significant (a rough guide is more than 10 per cent of IP Phone traffic), include traffic in the LAN/WAN bandwidth calculation.

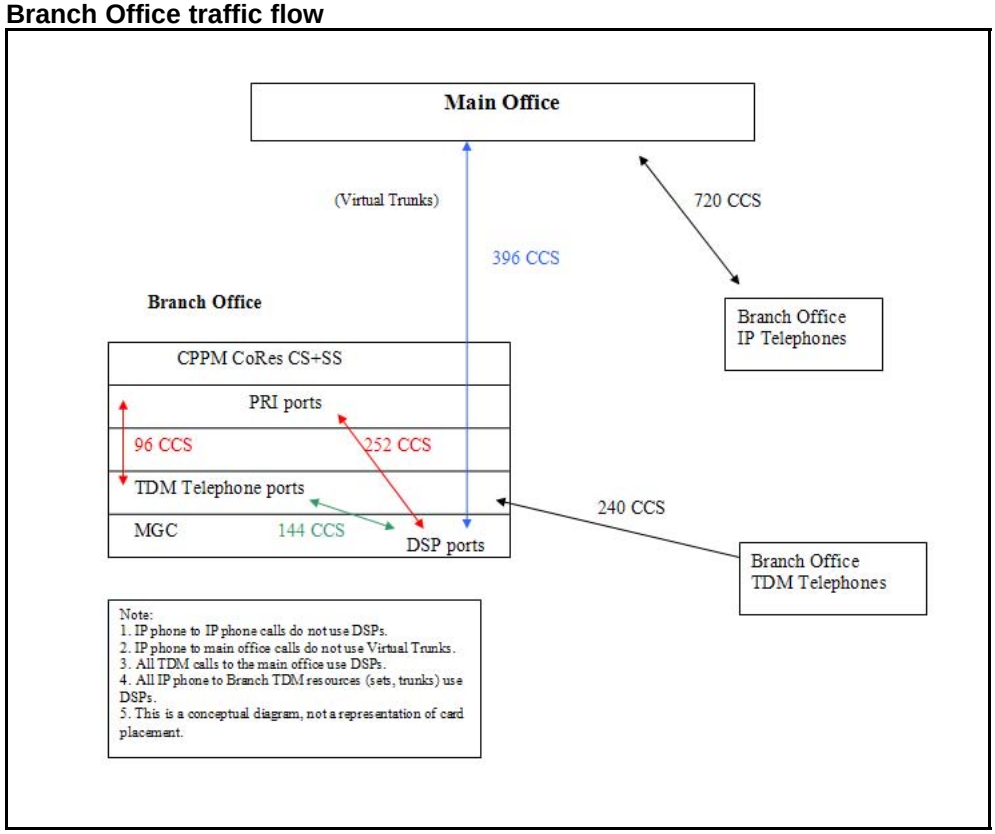
Calculations

Figure 68 "Branch Office traffic flow" (page 243) is a conceptual representation of an MG 1000B Core. An actual system could require different types and numbers of cards.

Traffic

Traffic calculations are based on the traffic flows shown in Figure 68 "Branch Office traffic flow" (page 243).

Figure 68
Branch Office traffic flow



Procedure 35
Calculating traffic

Step	Action
1	Calculate the total Branch Office IP Phone traffic. Total_IP_CCS = Branch IP sets x Branch IP CCS rate = 120 x 6 = 720 CCS
2	Calculate the total Branch Office TDM Phone traffic. Total_TDM_CCS = Branch TDM sets x Branch TDM CCS rate = 48 x 5= 240 CCS
3	Calculate the IP Phone to IP Phone traffic (intra-IP Phone traffic does not require DSPs). Intra_IP_CCS = Branch IP sets x Branch IP CCS rate x % calls to Intra-IP calls = 120 x 6 x 0.45 = 324 CCS
4	Calculate the IP telephone to Branch Office traffic (requires DSPs and Virtual trunks). VTRK_CCS = Total_IP_CCS – Intra_IP_CCS = 720 – 324 = 396 CCS
5	Calculate the TDM telephone to Branch Office IP telephone traffic (requires DSPs).

TDM_IP_CCS = Total_TDM_CCS x % of calls to IP telephones
= 240 x 0.6 = 144 CCS

6 Calculate the Branch Office IP telephone to PRI.
PRI_IP_CCS = VTRK_CCS – TDM_IP_CCS
396 – 144 = 252 CCS

7 Calculate the TDM telephone to PRI traffic:
PRI_TDM_CCS
= Total_TDM_CCS – TDM_IP_CCS

--End--

DSP requirements

You must calculate the DSP port requirement in increments of 32.

The CP MG, , MC32, and MC32S provide DSPs in groups of 32. When DSP calculations refer to a Voice Gateway Media Card, it is a bank of 32 DSPs which are either an MC32, MC32s, CP MG 32, CP MG 128, or DSPs from a DSP daughterboard. Therefore, an card that is fully populated with 256 DSPs is equivalent to 8 Voice Gateway Media Cards.

Table 55 "Erlang B and Poisson values in 32-port increments" (page 244) 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.

Table 55
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	132
64	1822	64	1687
96	2891	96	2689
128	3982	128	3713
160	5083	160	4754
192	6192	192	5804

Procedure 36
Calculating Branch Office DSP requirements

Step	Action
1	Calculate the DSP traffic (see step 4 of the Calculating traffic procedure). Total_DSP_CCS = VTRK_CCS ***Note:*** This is also equal to TDM_IP_CCS + PRI_IP_CCS = 396 CCS
2	Calculate the number of DSPs required to support this level of traffic by using Table 55 "Erlang B and Poisson values in 32-port increments" (page 244), Erlang B P.01 columns to determine the number of DSPs required at the Branch Office. ***Note:*** The Total DSP is 396 CCS, therefore this can be easily sustained by 32 DSP ports (396 is less than 794). BO_DSPs = 32

--End--

Virtual Trunk requirements

Procedure 37
Calculating Virtual Trunk requirements

Step	Action
1	Calculate the Virtual Trunk traffic. VTRK_CCS = VTRK_CCS (see step 4 of the Calculating traffic procedure) = 396 CCS
2	Calculate the number of Virtual Trunks required to support this level of traffic by using Table 55 "Erlang B and Poisson values in 32-port increments" (page 244), Poisson P.01 columns to determine the number of Virtual Trunks required to the Branch Office. ***Note:*** The Virtual trunk CCS is 396, therefore this can be easily sustained by 32 Virtual Trunk ports (396 is less than 732).

Virtual Trunks to Branch Office = 32

Note: To get a more granular relationship of trunk CCS to ports required, use a general Poisson P.01 table. For more information about Trunk traffic Poisson 1 percent blocking table, see *Communication Server 1000E — Planning and Engineering* (NN43041-220).

--End--

Call Server Real-time usage

The following is a simplified engineering example of a Communication Server 1000E. For more information about engineering a Communication Server 1000E , see *Communication Server 1000E — Planning and Engineering* (NN43041-220).

When a branch is operating in a normal branch mode, the Main Office handles the local UNIStim IP traffic, therefore only inbound virtual trunk traffic affects the branch.

When a branch operates in local mode (the link to Main Office is down), the local UNIStim IP traffic occurs at the branch, but there are no Virtual Trunks involved.

This example assumes the branch runs in standard branch mode.

Procedure 38
Calculating Call Server Loading

Step	Action
1	Calculate the TDM Phone to TDM Trunk calls PRI_TDM_calls = PRI_TDM_CCS x 100 seconds ÷ average hold time (PRI_TDM_CCS, from procedure Calculating traffic, step 7) = 96 x 100 ÷ 120 = 80 calls
2	Calculate the TDM telephone to IP telephone calls (these use virtual trunks). TDM_IP_calls = TDM_IP_CCS x 100 seconds ÷ average hold time (TDP_IP_CCS, from procedure Calculating traffic, step 5) = 144 x 100 ÷ 120 = 120 calls
3	Calculate the IP telephone to PRI Trunk calls (these use virtual trunks) PRI_IP_calls = PRI_IP_CCS x 100 seconds ÷ average hold time (PRI_IP_CCS, from procedure Calculating traffic, step 6) = 252 x 100 ÷ 120 = 210 calls

4 Calculate the total number of calls at the Branch Office.
Total_calls = PRI_TDM_calls + TDM_IP_calls + PRI_IP_calls
= 80 + 120 + 210 = 410 calls per hour

5 Calculate the Call Server real-time multipler.

- System RTM = 1+ [(PRI_TDM_calls ÷ Total_calls) x f10] + [(TDM_IP_calls ÷ Total_calls) x f9] + [(PRI_IP_calls ÷ Total_calls) x f4] + error_term
- System RTM = [(80 ÷ 410) x 4.36] + [(120 ÷ 410) x 3.95] + [(210 ÷ 410) x 3.65) = 1+ 0.851 + 1.156 + 1.87 + 0.25 = 5.127

Note: For more information about real time factors (f4, f9, f10, error_term), see *Communication Server 1000E — Planning and Engineering* (NN43041-220). Use the Communication Server 1000E Co-resident Calling Server and Signaling Server column.

6 Calculate the Call Server loading in EBC.
System EBC = Total_Calls x System RTM
= 410 x 5.127 = 2102

7 Calculate the Call Server loading in percent.
Real Time Usage = System EBC ÷ rated EBC x 100
= 2102 ÷ 150000 x 100 = 1.4%

Note: For more information about the rated EBC, see *Communication Server 1000E — Planning and Engineering* (NN43041-220). Use the Communication Server 1000E Co-resident Calling Server and Signaling Server value.The configuration loading for the Call Server is very low at 1.4 per cent. Locate this Call Server at the Branch Office or anywhere within the zone.

--End--

MG 1000B Core and MG 1000B Expander requirements

Table 56 "MG 1000B Core and MG 1000B expander card type, number and devices" (page 247) shows the number of cards required and the devices on those cards.

Table 56
MG 1000B Core and MG 1000B expander card type, number and devices

Card type	Number of cards	Devices on cards
MC	0	DSPs supplied by card
XDLC	4	48 Digital telephones

PRI	1	< 23 ports required
CPPM CS+SS	1	
	1	DSP daughter cards; this goes into slot 0 of the MG 1000B core

The MG 1000B Core has four slots available. An MG 1000B Expander is required for additional cards. Digital Trunk cards, such as PRI/DTI/TMDI, are only supported in slots 1 to 4 of the MG 1000B Core chassis.

The proposed system would require an MG 1000B core and MG 1000B Expander.

Bandwidth requirement for Branch Office LAN/WAN

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.

Procedure 39
Calculating MG 1000B bandwidth with Virtual Trunk

Step	Action
1	Calculate the Virtual Trunk traffic. VTRK_CCS = VTRK_CCS (from procedure, Calculating traffic, step 4) = 396 CCS
2	Calculate the IP Set to Main Office traffic . Intra_IP_CCS = Intra_IP_CCS (from procedure, Calculating traffic, step 3) = 324 CCS
3	Calculate total LAN/WAN traffic. Total_WAN_CCS = Intra_IP_CCS + VTRK_CCS Total_WAN_CCS = 396 + 324 = 720 CCS
4	Convert Total WAN CCS to Erlangs. Branch Office Bandwidth Erlangs = Total_WAN_CCS ÷ 36 ***Note:*** 36 CCS = 1 Erlang = 720 ÷ 36 = 20 Erlangs

--End--

See the Branch Office Bandwidth Erlangs number, in the bandwidth table, to find the corresponding bandwidth required to carry the traffic to the Main Office. For information about the bandwidth table and calculating

LAN/WAN bandwidth requirements, see *Converging the Data Network with VoIP Fundamentals* (NN43001-260). The codec selection greatly impacts the bandwidth requirements.

List of terms

CDP

Coordinated Dialing Plan. Under the recommended Coordinated Dialing Plan, the Branch User ID can be an extension (for example, 4567). For more information about CDP, see *Dialing Plans Reference* (NN43001-283).

datadump

A datadump, or Equipment Datadump (EDD), is performed on the Call Server to save the active database to backup and to copy the database to static memory.

DSP

Digital Signal Processing, which refers to manipulating analog information, such as sound or photographs that has been converted into a digital form. DSP also implies the use of a data compression technique.

When used as a noun, DSP stands for Digital Signaling Processor, a special type of coprocessor designed for performing the mathematics involved in DSP. Most DSPs are programmable, which means that they can be used for manipulating different types of information, including sound, images, and video.

ELAN subnet

Embedded Local Area Network subnet. This isolated subnet connects the Call Server, Signaling Server, Voice Gateway Media Card for system communication purposes.

gateway

In networking, a combination of hardware and software that links two different types of networks. Gateways between e-mail systems, for example, enable users on different e-mail systems to exchange messages.

H.323

A standard approved by the International Telecommunication Union (ITU) that defines how audiovisual conferencing data is transmitted across networks. In theory, H.323 enables users to participate in the same conference even though they are using different videoconferencing applications. Although most videoconferencing vendors have announced that their products conform to H.323, it is too early to say whether such adherence actually results in interoperability.

IP

Abbreviation of **Internet Protocol**, pronounced as two separate letters. IP specifies the format of packets, also called datagrams, and the addressing scheme. Most networks combine IP with a higher-level protocol called Transport Control Protocol (TCP), which establishes a virtual connection between a destination and a source.

IP by itself is something like the postal system. It enables you to address a package and drop it in the system, but there's no direct link between you and the recipient. TCP/IP, on the other hand, establishes a connection between two hosts so that they can send messages back and forth for a period of time.

LAN

Local Area Network.

Layer 2 switching

Packets are forwarded according to the destination's MAC address. The switch automatically determines which switch port must be used to send the packet, according to the destination's MAC address. The MAC address location was determined from incoming packets from that MAC address received on that port.

Layer 3 switching

Packet traffic is grouped according to the source and destination addresses. The first packet in a flow is routed by a software-based algorithm. Subsequent packets with the same source and destination addresses are switched according to the destination's MAC address (hardware mechanism). This is similar to multi-layer routing and routers with hardware assist.

NAT

Network Address Translation. It is defined as an internet standard that lets a LAN use both internal and external IP addresses. This protects an internal IP address from being accessed from outside.

NAT translates the internal IP addresses to unique IP addresses before sending out packets. NAT is practical when only a few users in a domain need to communicate outside of the domain at the same time.

NCS

Short for Network Connection Server. It provides a TPS interface to the NRS, allowing the TPS to query the NRS using the UNIStim protocol. It is a remote system node IP based on BUID (Branch Office), virtual office user (network wide virtual office login), and NUID (Geographic Redundancy). It also checks remote system status and provides it to the TPS for further analysis. The NCS is required only for set redirection, while the rest of the NRS requires for calls. It is part of NRS H.323 Gatekeeper and is not part of NRS SIP proxy. It is required to support the MG 1000B, Virtual Office, and Geographic Redundancy features.

NRS

Short for Network Routing Service, which refers to the software application where all systems in the network are registered. The NRS consists of the Session Initiation Protocol (SIP) Redirect Server and the H.323 Gatekeeper, which includes the Network Connection Service (NCS).

PSTN

Short for Public Switched Telephone Network, which refers to the international telephone system based on copper wires carrying analog voice data. This is in contrast to newer telephone networks based on digital technologies, such as ISDN and FDDI.

Telephone service carried by the PSTN is often called plain old telephone service (POTS).

QoS

Short for **Quality of Service**, a networking term that specifies a guaranteed throughput level. One of the biggest advantages of ATM over competing technologies, such as Frame Relay and Fast Ethernet, is that it supports QoS levels. This enables ATM providers to guarantee to their customers that end-to-end latency does not exceed a specified level.

There are several methods to provide QoS, as follows:

- high bandwidth
- packet classification
- DiffServ

- IP fragmentation
- traffic shaping
- use of the platform's queuing mechanisms

routing

The process of selecting the correct path for packets transmitted between IP networks by using software-based algorithms. Each packet is processed by the algorithm to determine its destination.

SIP

Short for Session Initiation Protocol. SIP is a protocol standard used for establishing, modifying, and terminating conference and telephony sessions in IP networks. A session can be a simple two-way telephone call or it can be a collaborative multi-media conference session. SIP initiates real-time, multimedia sessions which can integrate voice, data, and video. The protocol's text-based architecture speeds access to new services with greater flexibility and more scalability.

TDM

Short for Time Division Multiplexing, a type of multiplexing that combines data streams by assigning each stream a different time slot in a set. TDM repeatedly transmits a fixed sequence of time slots over a single transmission channel.

Within T-Carrier systems, such as T-1 and T-3, TDM combines Pulse Code Modulated (PCM) streams created for each conversation or data stream.

TLAN subnet

Telephony Local Area Network subnet. This subnet is separated from the rest of the network and connects the Voice Gateway Media Cards, the Signaling Server, and the IP Phones for telephony communication purposes.

TPS

IP Phone Terminal Proxy Server. This server controls the connection of IP Phones. It resides on the Signaling Server.

UDP

Uniform Dialing Plan. Each location within the network is assigned a Location Code, and each telephone has a Directory Number that is unique within the network. Under the Uniform Dialing Plan (UDP), the Branch User ID is the user's main office Directory

Number (DN) with the Access Code (for example, 6 343-5555). For details of other Numbering Plan options, see *Communication Server 1000E Planning and Engineering (NN43041-220)* ().

Voice gateway

The voice gateway application is used any time an IP and TDM device are connected together. The cards are equipped with DSPs to perform media transcoding between IP voice packets and TDM-based devices. The Voice Gateway Media Cards also provide echo cancellation and compression and decompression of voice streams. The voice gateway software can run on an MC, MC32s, and 32/96 ports daughter board. Within the MG 1000B Core, these cards register the voice channels to the MG 1000B Call Server when they are configured.

WAN

Wide Area Network. A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs).

Computers connected to a wide-area network are often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites. The largest WAN in existence is the Internet.

Nortel Communication Server 1000

Branch Office Installation and Commissioning

Release: 7.0
Publication: NN43001-314
Document revision: 04.02
Document release date: 11 June 2010