NORTEL

Nortel Communication Server 1000

Branch Office Installation and Commissioning

Release: 5.5
Document Revision: 02.09

www.nortel.com

NN43001-314

Contents

Emergency Services configuration   **167**

Basic Emergency Services When VO Logged Out   **181**

Maintenance and diagnostics   **189**

New in this release

The following sections detail what's new in *Branch Office Installation and Commissioning* (NN43001-314) for Release 5.5.

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

Features

This release contains no new features.

Other changes

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

Revision history

April 2009	Standard 02.09. This document is up-issued to include technical updates in the section *Connecting the MG 1000B Core to the network*.
January 2009	Standard 02.08. This document is up-issued to add attention in the section *Converting a small system to a Branch Office.*.
January 2009	Standard 02.07. This document is up-issued to reflect the technical changes in the section *Adding the Branch Office endpoints to the NRS database*.
August 2008	Standard 02.06. This document is up-issued to include information on Installing a DSP Daughterboard.
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 in the section Examples of Alternative Call Routing for NBWM in operation.
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: (553-3001-314).
September 2006	Standard 5.00. This document is up-issued with an update to Procedure 23 Configuring the MG 1000B zone, which resulted in no remote access over IP Network to CS.
January 2006	Standard 4.00. This document is up-issued with information on reconfiguring Call Server alarm notification levels if necessary when configuring Adaptive Network Bandwidth Management.
August 2005	Standard 3.00. This document is up-issued to support CS 1000 Release 4.5.
October 2003	Standard 1.00. This document is a new NTP for Succession 3.0. It was created to support a restructuring of the Documentation Library. This document contains information previously contained in the following legacy document, now retired: *Branch Office* (553-3023-221).

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.

Overview

Contents

This section contains information on the following topics:

What is Branch Office?

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

The Branch Office feature is implemented on a Media Gateway 1000B (MG 1000B) platform. The MG 1000B platform includes an MG 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 Media Gateway Controller (MGC) card in the 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.

The Media Gateway 1000B Branch Office can be configured with one of two following hardware platforms:

- A Call Processor Pentium Mobile and Media Gateway Controller using the Large System Release 5.5 or later software stream (l s c u)

- An SSC card using the Small System Release 4.5 software stream (c u)

For both hardware platforms the main office must be using a CS 1000E system or a CS 1000M CP PII or CP PIV system running Release 5.5 or later software. The main office can support a mixture of up to 255 of the two Branch Office hardware platforms.

For small configurations, the Survivable Remote Gateway provides the same functionality and benefits as the Branch Office.

You can implement the Branch Office feature as a new hardware configuration. It can also be created by converting an existing Small System to an MG 1000B platform (see "Converting a small system to a Branch Office" (page 81)). The functionality is the same in both configurations.

A Branch Office is designed to work with a main office only if the two offices use a common dialing plan. Any other configuration is not guaranteed to work properly.

Figure 1 "Branch Office associated with a CS 1000E main office" (page 17) shows a Branch Office network.

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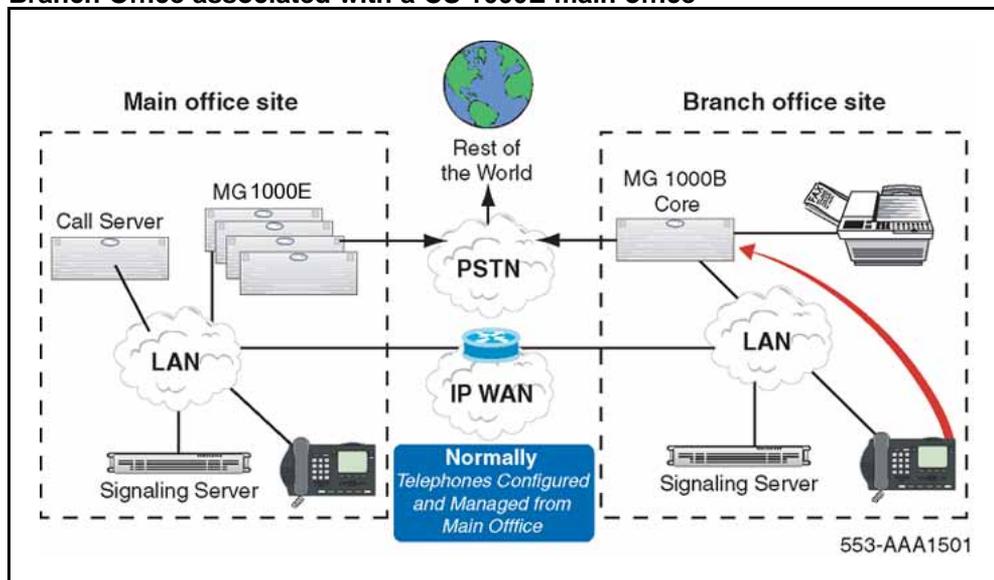
Main Office and Branch Office Migration

All Main Office Call Servers in CS 1000 Release 5.5 are large system software stream based. The Main Office TN (MOTN) in a Branch Office will always be set to the large system software stream MOTN.

In a Branch Office where the Main Office has been migrated from a SSC to CP PM call server, the LD 20 PRT on the branch will not correctly display the MOTN using the small system TN format until the branch has been migrated or upgraded. In the case where the branch is SSC based, the LD20 PRT will remain incorrect until the Branch Office Call Server has been migrated to a CP PM call server.

MG 1000B (MGC) compared to the MG 1000B (SSC)

The MG 1000B with MGC has a number of differences in hardware capability when compared with older Branch Offices.

The MGC has six Ethernet interfaces for connecting to external networking equipment. Three are reserved for ELAN connections and three are reserved for TLAN connections. The six external Ethernet interfaces on the MGC are set to Auto Negotiate mode by default. You can change the settings for ports 1E, 2T, E and T to 100 Mbps full duplex by using the mgcsetup command. With a properly designed data network, the multiple ELAN and TLAN interfaces can be used to implement a dual homed configuration for the MG 1000B with MGC.

Four of these interfaces are accessed by using RJ45 connectors on the faceplate. Two are reserved for ELAN and two are reserved for TLAN.

Two additional Ethernet connections are available if an Option 11C cabinet is used. One is reserved for ELAN and one is reserved for TLAN.

For the Option 11C cabinets, to break out the two additional 100BaseT Ethernet connections, you need to use the MGC 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 for network redundancy, previously know as dual-homing on older Branch Offices.. The MGC Ethernet interface failover is accomplished with the embedded Ethernet switch. The Ethernet interface failover feature requires no special network configuration to function. The end customer decides if two separate Layer 2 switches are used to implement the feature to minimize the service outage. For more information see the Communication Server 1000E: Installation and Configuration (NN43041-310) NTP.

Also, you can use the broadcast and multi cast rate limiting features of the embedded Ethernet switch on the MGC to reduce the susceptibility of the Call Server to broadcast storms and similar network issues, if you directly cable the Call Server to the MGC.

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

The MGC has two conference loops with thirty units each. The maximum number of participants in a conference is thirty. On the SSC, the maximum number of conference loops was four with sixteen units in each loop. The maximum number of participants in a conference was six.

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

The MGC 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 MGC 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.

MGC Serial Ports

Each MGC installed in a MG 1000B provides the opportunity for 3 remote Serial Data Interfaces (SDI). The maximum number of TTYs does not change. Therefore, after you configure the maximum TTYs , no additional TTYs are supported.

The MGC 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 MGC, 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 used).

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

Unlike the NTDK20xx SSC card, all SDI ports on the MGC are configured by using shipped software. No DIP switches are on the MGC 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 Call Server TTY ports or the MGC remote TTY ports.

MGC serial port default configuration

The default settings for the serial ports are

- Baud rate = 9600

- Number of data bits = 8

- Number of stop bits = 1

- Parity = none

- Flow control = none

MGC serial ports configuration change in Overly 17

If you configure the serial ports on an MG 1000B with MGC 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.

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

CEMux Support

Support of the Option 11C CS 1000M cabinet and chassis CEMux type cards are additions to the MG 1000B with an MGC with the CP PM. The list of supported cards is as follows:

Table 1
CEMux Packs and daughter boards supported in MG 1000B with MGC

Pack	Daughterboard	IP Expansion CEMux Application
1.5MB DTI/PRI (NTAK09)	DCHI (NTAK93)	non-downloadable DCH
	DDCH (NTBK51)	downloadable DCH
	CC (NTAK20)	clock controller (stratum 3/4)
1.5MB TMDI (NTRB21)	CC (NTAK20)	downloadable DCH, clock controller (stratum 3/4)
2.0MB DTI (NTAK 10)	n/a	clock controller (stratum 3/4)
2.0MB PRI (NTAK79)	n/a	clock controller (stratum 3/4), non-downloadable DCH

2.0MB 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

Standard Option 11C minimum vintages apply to all packs and daughter boards.

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

Support of CEMux requires CS 1000 Release 5.5 Softswitch software and a Media Gateway Controller Card (MGC). 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 CS 1000 Release 5.5, matches that of the CS 1000M large systems.

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

Clock References

With CEMux support, you can configure digital trunks and clock controller configuration in the IPMG. Each IPMG that contains a digital trunk card requires a clock controller on that shelf. You cannot use Clock references across IPMGs, and you can configure only one clock controller per shelf.

Main office hardware description

The main office must be one of the following systems:

- CS1000E;

- CS1000MCabinet;

- CS1000MChassis;

- CS1000MHalf;

- CS1000MSingle;
- CS1000MMulti;

The diagrams throughout this document show a CS 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 system has been enhanced for CS 1000 Release 5.5 Branch Office. The CP PM Call Server and MGC replace the SSC (Motorola) used in earlier MG 1000B. The Media Card is still supported however, the DSPs are also available on the MGC.

Two DSP Daughterboards are included in the CS 1000 portfolio of products. The daughterboards are available in two different sizes, a 32-port daughterboard and a 96-port daughterboard. These daughterboards are located on the Media Gateway Controller (MGC) card to provide DSP resources for connecting IP and TDM devices. These daughterboards eliminate the need to install the Media Cards within the CS 1000E Media Gateways (MG 1000B) chassis, to save slots and reduce cost over the current Media Card solution. The addition of the DSP Daughterboards into a MG 1000B system does not limit the use of Media Cards, either for DSP-only functionality or for the full IP Line application within the same system. The MGC is used only in the Media Gateway chassis or Option 11C-style cabinets. From a functional perspective, the DSP Daughterboards behave in a similar manner as the current Voice Gateway (VGW) application on the Media Card.

Support exists for the following configurations:

- a system with only Media Cards
- a system with only DSP DBs
  - a 32-port daughterboard in daughterboard position 1
  - a 32-port daughterboard in daughterboard position 2
  - A 32-port daughterboard in daughterboard position 1 and a 32-port daughterboard in daughterboard position 2
  - a 96-port daughterboard in daughterboard position 1
  - a 96-port daughterboard in daughterboard position 1 and a 32-port daughterboard in daughterboard position 2
- a system with DSP DBs (all of the position combinations described above) and Media Cards.

The basic hardware of an MG 1000B platform includes the MG 1000B Core and the Signaling Server.

Figure 2
CS 1000 Release 5.5 MG 1000B System
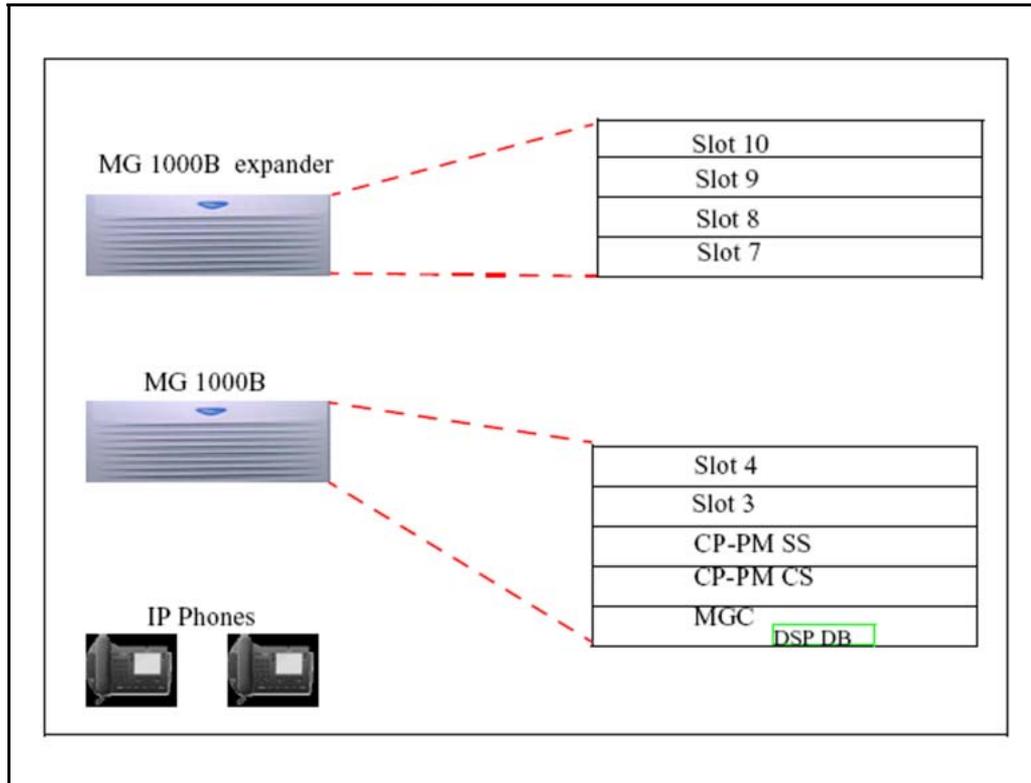
CS 1000 Release 5.5 continues to support the existing Branch Office configuration that uses the SSC processor and Release 4.5 or 5.0 software, but Nortel no longer offers sales of the SSC based Branch Office.

CS 1000 Release 5.5 provides various hardware versions of the Signaling Server, the existing ISP1100 signaling servers, the CP PM Signaling Servers, or the commercial off-the-shelf (COTS) HP and IBM servers.

Author's note: This HW platform information was in the SIP Line SID and FD for this NTP. Is information appropriate for the SS supported hardware or should it be referring to ?

With CS 1000 Release 5.5 Branch Office, the hardware configuration includes a CP PM call processor card with the MGC, as well as a CP PM Signalling Server. If the CP PM Signalling Server configuration cannot be used, the option exists to use the Signaling Server on COTS.

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 81) for more information.

After conversion to 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 an MG 1000B Cabinet or MG 1000B Chassis for a converted small system, unless otherwise indicated. Likewise, 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.

Where required, the MG 1000B Core is connected by copper wire to the MG 1000B Expander for added capacity.

The MG 1000B Core must contain a CP PM Call Server. The CP PM Call Server provides telephony services to elements at the Branch Office, such as digital telephones, analog devices, digital trunks, and analog trunks. It 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 MGC. The software feature set on the CP PM can differ from that of the Call Server at the main office.

Figure 3 "MG 1000B Core/MG 1000B Expander" (page 25) shows an MG 1000B Core/MG 1000B Expander.

Figure 3
MG 1000B Core/MG 1000B Expander
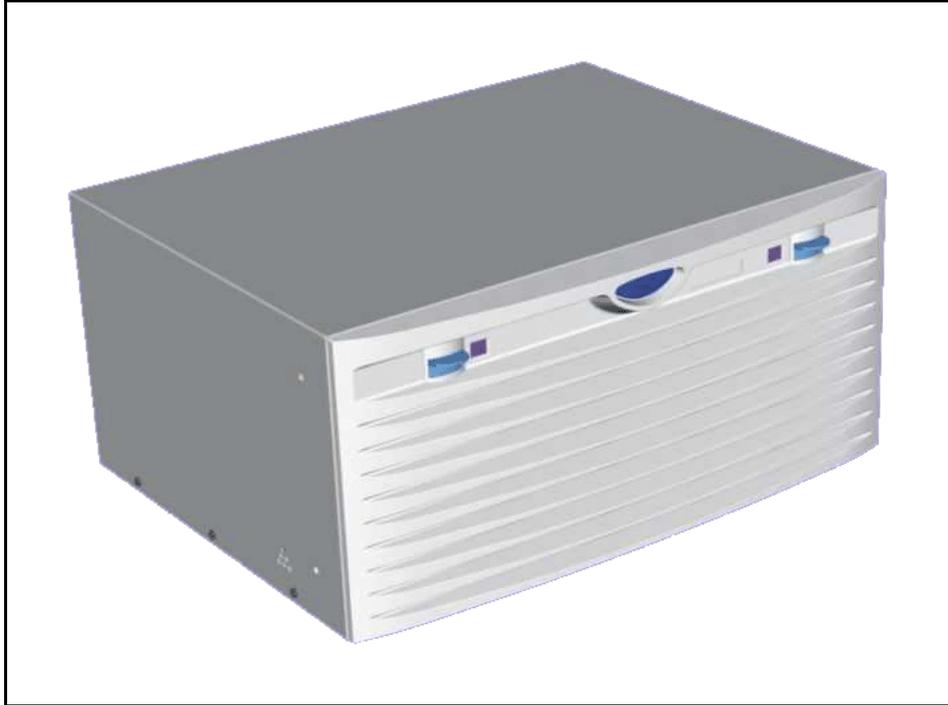
MG 1000B Chassis
CEMux packs are supported in card positions 1 to 4 of an MG 1000B chassis. They are not supported in the MG 1000B expander chassis.

Card slots
Table 2 "Card slots for MG 1000B Core and MG 1000B Expander" (page 26) shows the card slot assignments for all configurations of the MG 1000B Core and MG 1000B Expander (discussed in "MG 1000B Expander" (page 27)).

Table 2
Card slots for MG 1000B Core and MG 1000B Expander

MG 1000B Configuration	MG 1000B Core				MG 1000B Expander	
	Total slots	Slot # for MGC	Slot # for 48-port DLC	Usable slot #s	Total slots	Usable slot #s
MG 1000B Core	5	0	Not used	1-4	4	7-10
MG 1000B Cabinet	11	0	Not used	1-10 (see Note 1)	N/A	N/A
MG 1000B Chassis	5	0	4 (see Note 2)	1-3	4	7-10 (see Note 1)
Note 1: **For converted small systems only, the Meridian Mail card must be installed in slot 10 if Meridian Mail is to be supported.** *Note 2:* **On converted CS 1000 Mini Systems, slot 4 must remain unused if the 48-port Digital Line Card (DLC) is not used. However, it can be covered by a double-slot card inserted in slot 3.**						

In Table 2 "Card slots for MG 1000B Core and MG 1000B Expander" (page 26), 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:

- 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
- CP PM Call Server card
- CP PM Signalling Server card

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

MG 1000B Expander

The MG 1000B Expander can be used with all MG 1000B platform configurations except the MG 1000B Cabinet. The MG 1000B Expander is identical to the MG 1000B Core with the following exceptions:

- 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 3 "MG 1000B Core/MG 1000B Expander" (page 25) shows the MG 1000B Expander. Table 2 "Card slots for MG 1000B Core and MG 1000B Expander" (page 26) gives the card slots for the MG 1000B 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.

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 Installation and Commissioning;* ((NN43001-312)) . For more information on SIP, H.323, and overlap signaling, refer to *IP Peer Networking Installation and Commissioning* .

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 58) and "Adding the Branch Office endpoints to the NRS database" (page 137).

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 CS 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), Subscriber Manager (SM), or Telephony Manager 3.1 (TM 3.1).

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 *IP Line Fundamentals;* ((NN43100-500)) .

Media Card

For CS 1000 Release 5.5, the new Media Card 32S (MC32S) fully replaces the functionality of the current VGMC pack NTVQ01BB. The MC32S also adds SRTP security. For an MGC-based MG 1000B, the sets are configured in four-field format. For additional information, see the *IP Line Fundamentals;* ((NN43100-500)) NTP or the *Circuit Card Reference* ((NN43001-311)) NTP.

The Media Card acts as a Media Card, providing 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.

Media Cards provide echo cancellation, compression, and decompression of voice streams. For more information about DSP resources residing on the MGC 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 CS 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 "Media Card DSP capacity" (page 38).

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 an MGC communicates with the Main Office Call Server using the built-in 100BaseT Ethernet Interface on the MGC. The ethernet ports on the MGC are

- CE: Connection to CP PM Call Processor ELAN port

- CT: Connection to CP PM Signaling Server TLAN port

- 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

You must connect the MGC 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 MGC 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 MGC ethernet ports do not auto-negotiate to 100 Mb Full Duplex, an alarm occurs. A CLI command is also available on the MGC 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 MGC.

MG 1000B Data Network Topology illustrates a typical robust network topology.

Figure 4
MG 1000B Data Network Topology
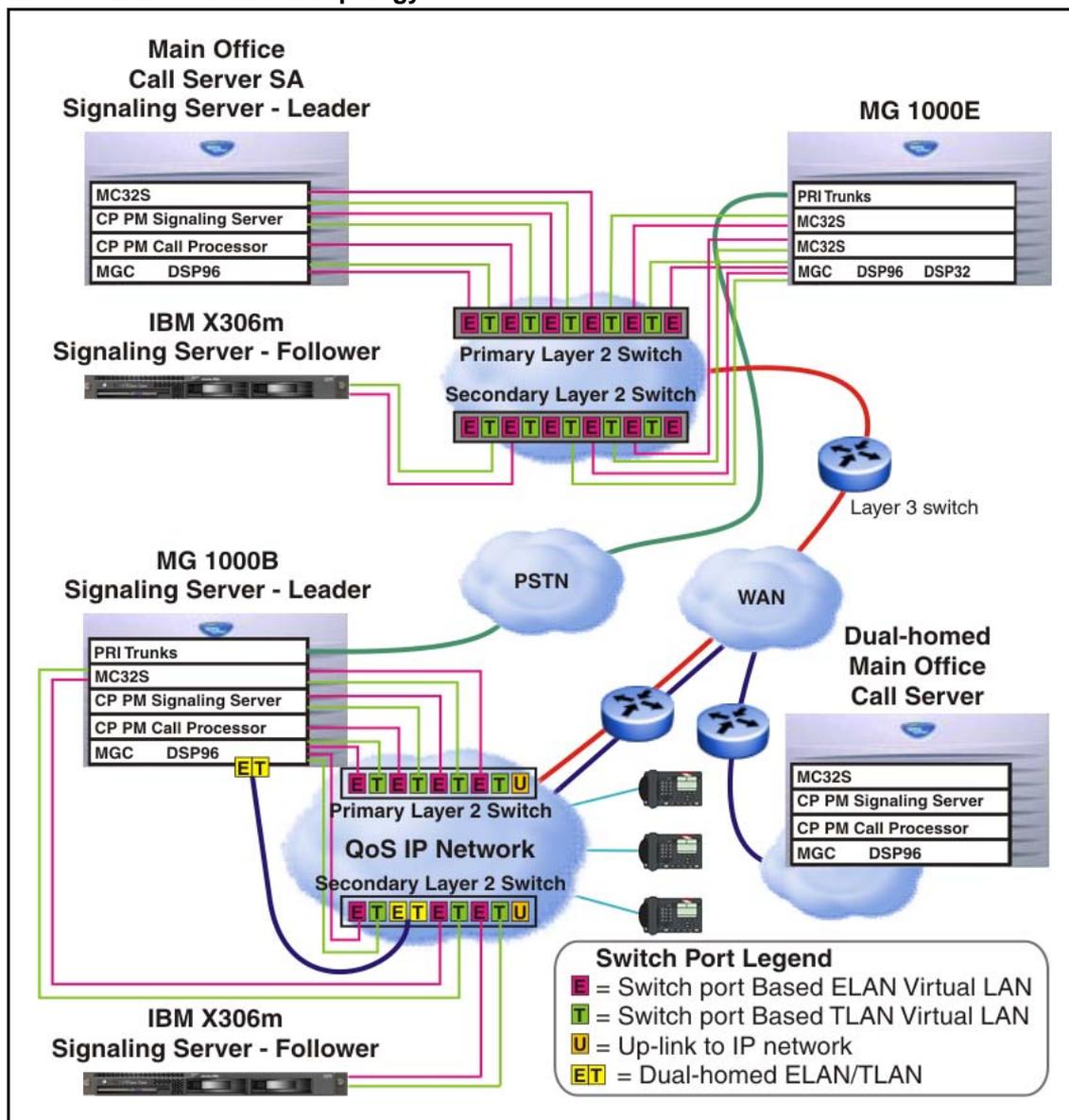
MGC Network Connections

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 MGC are the only embedded Ethernet ports that allow a direct connection to another device, and the only cards supported for this direct connection is the CP PM Call Server or the CP PM Signalling 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 5
Single server port network connections (no dual-homing)
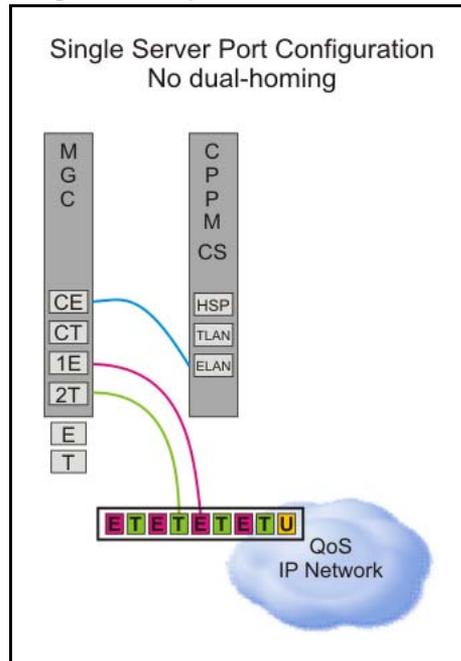
The following figure illustrates a typical network configuration that supports the dual-homed feature. With this configuration, however, a single Layer 2 switch remains a single point of failure.

Figure 6
Single server port network connections (dual-homing - non distributed)
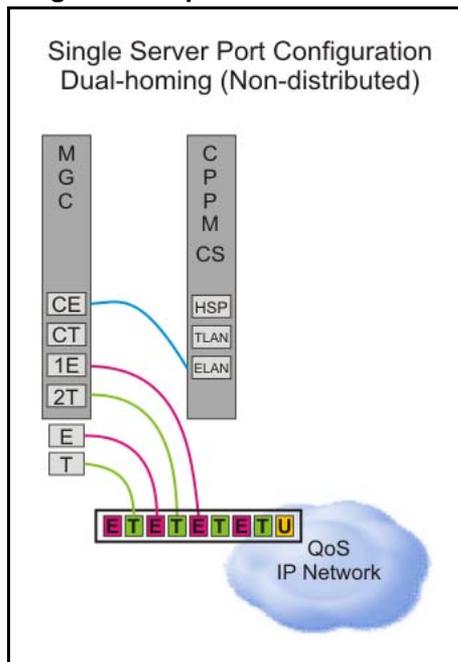
The following figure illustrates a typical network configuration that supports dual homing of both the ELAN and TLAN. Multiple Layer 2 switches ensure there isn't a single point of failure. Nortel recommends this configuration for the highest reliability in a single CPU Call Server configuration. You must partition the layer 2 switch into separate VLANs to keep the ELAN and TLAN traffic on separate subnets

Figure 7
Single server port network connections (dual-homing - distributed)
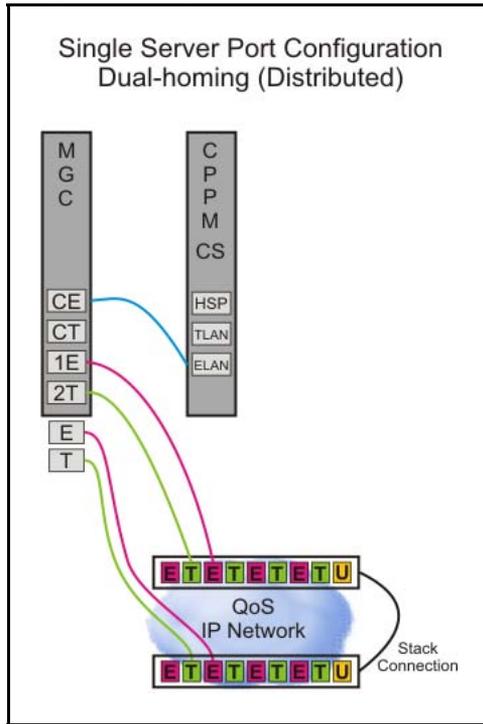
MG 1000B platform configuration overview

In each MG 1000B Core, one CP PM and MGC is required. The three remaining slots (nine in an MG 1000B Cabinet) can contain analog line cards, analog trunk cards, digital line cards, or digital trunk cards. Refer to Table 2 "Card slots for MG 1000B Core and MG 1000B Expander" (page 26) for a summary of the allowable card slots.

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

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

There are two configurations for the MG 1000B platform:

- without an MG 1000B Expander

- with an MG 1000B Expander

MG 1000B platform without an MG 1000B Expander

Figure 8 "MG 1000B platform without MG 1000B Expander" (page 36) shows an MG 1000B platform configured without an MG 1000B Expander. This configuration has a single MG 1000B Core.

Figure 8
MG 1000B platform without MG 1000B Expander

This MG 1000B platform configuration requires at least one Media Card or an MGC card with associated DSP daughterboards. The additional slots can be used for any combination of the following:

- trunk card

- analog or digital line card

- second Media Card

- Nortel Integrated Conference Bridge card

- Nortel Integrated Recorded Announcer card

- cards to support CallPilot Mini or CallPilot 201i

- Meridian Mail card (for converted small systems only)

For more information on the Media Card configuration, refer to *IP Line Fundamentals; ((NN43100-500))* . For more information on Integrated Conference Bridge, refer to *Integrated Conference Bridge Service Implementation Guide (NN43001-558).*

MG 1000B platform with an MG 1000B Expander

shows an MG 1000B platform configured with an MG 1000B Expander. With the addition of an MG 1000B Expander, you have additional usable slots. There must be at least one Media Card (32-port cards with IP Line 5.5) or an MGC with the associated DSPs (32-96) daughter boards for the MG 1000B core. If more than one Media Card is used, the cards may be located in the chassis or expander.

The MG 1000B Expander does not support digital trunks.

Figure 9
MG 1000B platform with MG 1000B Expander
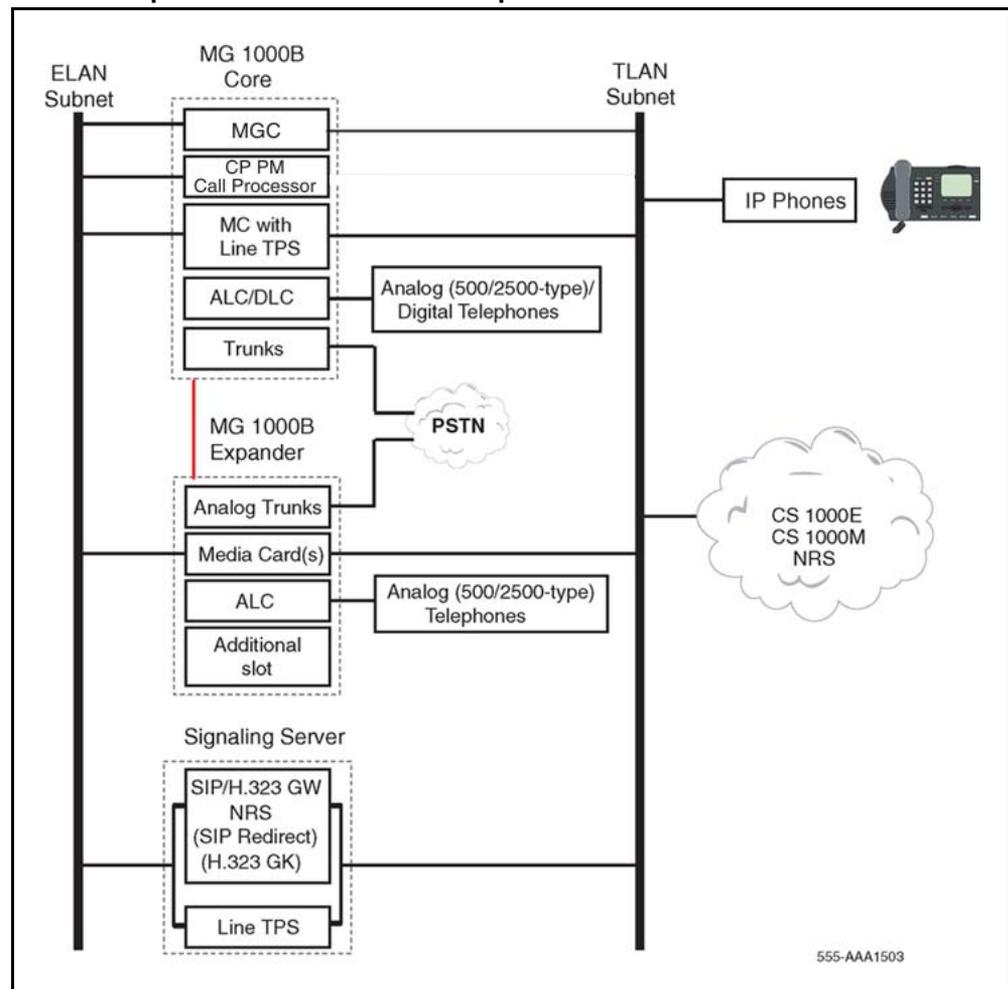
Capacity

Each CS 1000 main office can support up to 255 branch offices. Each Branch Office supports up to 400 IP Phone 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)) .

The configuration of an MG 1000B platform depends on:

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

Media Card DSP capacity

The number of DSP ports to provision depends on the trunk-to-telephone ratio. A rule-of-thumb is to have the number of ports greater than or equal to the number of trunks configured. See *Communication Server 1000E Planning and Engineering* ((NN43041-220)) for more information.

If digital telephones and analog (500/2500-type) telephones are equipped at the Branch Office, additional DSP ports are needed 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. The user can engineer fewer DSP ports depending on their desired 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 and .

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 always 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. With the main office running CS 1000 Release 5.5 software the Branch Office must run CS 1000 Release 5.5, Release 5.0 or Release 4.5.

Indefinite operation with a mixed-software configuration of CS 1000 Release 4.5 and CS 1000 Release 5.0 Branch Offices with a CS 1000 Release 5.5 main office is supported.

Consider this mixed software policy when planning your system upgrade. Branch Offices must be at CS 1000 Release 4.5 or later prior to upgrading the main office to CS 1000 Release 5.5 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.

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.

For information on upgrading software, refer to "Upgrading to CS 1000 Release 5.5" (page 87).

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 CS 1000 Release 5.5 and the Branch Office is on CS 1000 Release 4.5, features introduced in Release 5.5 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 CS 1000 Release 5.5 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 still permitted to order a Branch Office running CS 1000 Release 5.0 if their main office is running CS 1000 Release 5.0, They are also permitted to order a Branch Office running CS 1000 Release 4.5/4.0 if the main office is running CS 1000 release 4.5/4.0, They are also permitted to order a Branch Office running CS 1000 release 3.0 if the main office is running CS 1000 3.0 until the CS 1000 release 3.0 is MD.

IP Phone firmware

When you add a new CS 1000 Release 5.5 Branch Office to a network that has CS 1000 Release 4.5, or CS 1000 Release 5.0 Branch Offices, 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 *IP Line Fundamentals;* ((NN43100-500)) .

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 introduction of Enhanced UNIStim Firmware Download feature for Release 4.5, IP Phone firmware at the Branch Office is automatically downloaded from the main office.

Package Combinations

The MG 1000B with MGC requires existing packages 402 SOFTSWITCH, 403 IPMG, and Branch Office Package 390.

Package combinations supported using the Rls 4.5 MG 1000B are supported by the MG 1000B with MGC.

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 TM 3.1, 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 CS 1000 Release 5.5.

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 CS 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 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 Signalling Server, the NCS de-registers the Main Office from its database. Therefore, redirection from local mode cannot be completed. If the alternative Signalling 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 Signalling 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, unless it is already acting as the Primary or Alternate 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
All IP Phones excluding Phase 1/0 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 *IP Line Fundamentals;* ((NN43100-500)) .

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:

- Relaxed node ID 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 CS 1000E system.

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

For further information on this configuration and its limitations, see "Configuring non-zero S2 IP Addresses" (page 53).

Patch Management Enhancements

The changes completed under this feature are applicable to Call Server, Media Cards (ITG SA and MC32S) and Media Gateway Controller.

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 section contains information on the following topics:

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* () . 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.

Figure 8
MG 1000B platform without MG 1000B Expander

This MG 1000B platform configuration requires at least one Media Card or an MGC card with associated DSP daughterboards. The additional slots can be used for any combination of the following:

- trunk card

- analog or digital line card

- second Media Card

- Nortel Integrated Conference Bridge card

- Nortel Integrated Recorded Announcer card

- cards to support CallPilot Mini or CallPilot 201i

- Meridian Mail card (for converted small systems only)

For more information on the Media Card configuration, refer to *IP Line Fundamentals; ((NN43100-500))* . For more information on Integrated Conference Bridge, refer to *Integrated Conference Bridge Service Implementation Guide (NN43001-558)*

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. The Main Office can accept only an IP Phone 2004 compatible phone following a Branch Office redirection. If the redirected phone is not 2004 compatible (such as 2007 or 1140), an Invalid Set Type message is displayed.

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.

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 CS 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.*

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.*

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 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 Peer Networking Installation and Commissioning* ((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 local 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 systems supports up to 30 parties with the addition of the MGC as the gateway controller for the MG 1000B.

In a CS 1000E system, the MGC acts as the controllers for the MG 1000Bs:

- 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 MGC, the Group Call feature supports 20 group members.

If the MG 1000B system has a MGC as the 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 of IP Phones

If the MG 1000B IP Phone loses communication with the main office, the Call Server in the MG 1000B Core provides the call processing for the telephone. While the MG 1000B IP Phones are being provided with service at the Branch Office, the telephone display shows "Local Mode".

When an MG 1000B telephone is in Local Mode, the user has full access to services configured at the Branch Office (analog or digital devices, analog or digital trunks) and to other IP Phones registered to the MG 1000B Call Server. With proper ESN configuration, the Branch User can also access IP Phones at the main office or other branch offices by routing through the local PSTN.

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 140)

Configuring non-zero S2 IP Addresses

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 and any associated Media Cards in the MG 1000B Core are 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 10 "Configuration using S2 IP Address" (page 54) shows a typical configuration using the S2 IP Address.

Figure 10
Configuration using S2 IP Address
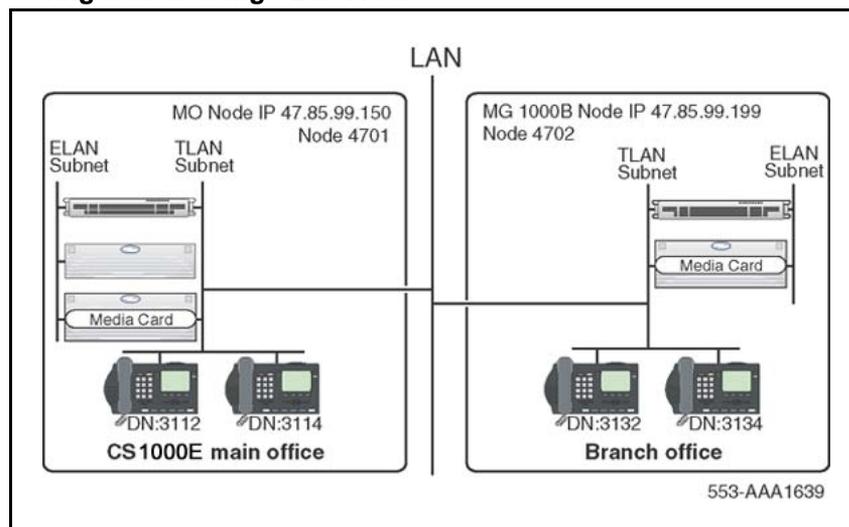
Points to remember

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, relaxed node ID checking must be used. Four digits must be configured for the Node IP Address 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 on the IP Phones.

- 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 TSP or MGC becomes unavailable, MG 1000B IP Phones registered to the main office TPS (in Normal Mode) are unaffected. MG 1000B IP Phones that are rebooted try to register using S1, or S2 if programmed.

- The main office can be either a CS 1000M Large System or a CS 1000E. If the main office is any system other than a CS 1000M Large System or a CS 1000E, a TN mismatch occurs and redirection from Branch Office to main office is not successful.

- 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 MGC and CP PM at the Branch Office are initialized or rebooted simultaneously, 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.

- If the main office contains a survivable remote gateway, then MG 1000B IP Phones can register successfully using either S1 or S2 when the main office Call Server becomes unavailable.

- 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 189).

- 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 CP PM processes incoming calls from a local trunk or from an analog (500/2500-type) or digital telephone, the CP PM 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 CP PM 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.

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 CP PM 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 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 for more information on ESA and SPN configuration.

Configuring ESA for emergency services

Beginning with CS 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. Refer to *Emergency Services Access Fundamentals* ((NN43001-613)) for complete information.

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 CP PM, or alternately, the Number Plan Area (NPA) code of the MG 1000B CP PM 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 *Software Input Output Reference - Maintenance;* ((NN43001-711)) .

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 CS 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 CS 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 (CS 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 CS 1000/2100. With this solution, you can register a number of IP sets with the CS 1000 and to receive telephony services from it. Other IP sets are normally registered with a remote CS 1000/2100 to receive telephony services from the 2100/CS 1000. In the case the link to the remote CS 1000/2100 or to the remote 2100/CS 1000 itself goes down, the IP telephones survive by registering with the local CS 1000, which provides telephony services while the link to the CS 1000/2100 or the CS 1000/2100 itself is down. When the link to the remote 2100/CS 1000 or to the remote CS 1000/2100 itself is restored, the IP telephones are automatically redirected back to the remote CS 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/CS 1000.

The Network Music feature connects a Central Audio Server attached to a CS 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 CS 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 11
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 section contains information on the following topics:

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 64).

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 64).

For more information about CDP, refer to *Dialing Plans Reference;* .   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 64).

Emergency Services

To understand Emergency Service Access (ESA), see "Emergency services" (page 56). 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 167).

Central Deployment Model

The following components interact with this feature:

- CLID
- Features which depend on CLID
- DAPC
- Keymap download
- LNR
- ISDN (new CDM 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 Central Deployment Model (CDM) functionality the numbering zone and zone-based flexible dial plan concepts 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 numbering zone to process 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)* NTP.

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.

There is a procedure in TM 3.1 to transfer IP Phone data from the main office to the Branch Office.

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 3 "Example dialing string, area codes, and Access Codes" (page 65) uses the following configuration at the main office for MG 1000B telephones to reach the PSTN.

Table 3
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.)

For other examples, such as calls between different NPAs within the same city, refer to the Dialing plan configuration.

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 4 "LD 117 Zone configuration example." (page 66)

Table 4
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.
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 CP PM is available through Ethernet connection or remote login through a dial-up modem.

Element Manager

The Element Manager application:

- configures the Media Card for IP Line 5.5
- configures the IP Phone Terminal Proxy Server (TPS)
- configures the Virtual Trunks
- upgrades the 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

Telephony Manger 3.1

TM 3.1 supports all Windows and web-based applications for the Branch Office feature, similar to the CS1000E; and CS1000M; systems. TM 3.1 allows customers to configure IP Phone data for use in survivable mode.

When using TM 3.1 Station Administration for IP Phones, it is possible to copy and paste an IP Phone from one system to another. This can be useful for provisioning the IP Phone data on both the main office and Branch Office.

Set-Based Installation for IP Phones

Nortel recommends using Set-Based Installation for MG 1000B IP Phones. Set-Based Installation takes less time than traditional telephone installation.

The procedure for Set-Based Installation enables the delegation of telephone installation to trusted users. To have a trusted user perform this function, configure a Temporary IP Phone Installer's Password for the system. "IP Phone passwords and parameters" (page 91) To proceed with Set-Based Installation, see Procedure 12 "Using Set-Based Installation" (page 143).

Automatic Set Removal

The Automatic Set Removal feature enables the technician or a trusted user to remove the IP Phone configuration from the system. This feature requires a Flexible Feature Code (FFC) and a set relocation password. The FFC code is Automatic Set Removal (AREM) in LD 57, and the set relocation password is the Set Relocation Security Code (SRCD) in LD 15.

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 *System Management Reference;* ((NN43001-600)) . This is required reading for any Branch Office administrator. Refer to *Access Control Management Reference* ((NN43001-602)) 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 198)

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.

Patch Management

Dependencies and restrictions on this feature include:

- Linux dependency: This feature does not support Linux SS.

- The Pentium processor is the only platform supported for call server. (CPPIV, CPPM and CoRes). The CPPII and SSC are no longer supported as of CS 1000 Release 6.0.

- The SSC Media Gateways and ITG Pentium are not supported.

- This feature is not backward compatible.

- This feature is not applicable for Loadware PEP's.

- Special Instructions are displayed only by using PLIS command and cannot be viewed using overlay commands.

Adding a Branch Office

Contents

This section contains information on the following topics:

Introduction

To install a Branch Office:

Step	Action
1	Upgrade the main office to CS 1000 Release 5.5 software. For more information, refer to *Communication Server 1000E - Software Upgrades* ((NN43041-458)) or *CS 1000M and Meridian 1 Large System Upgrades Overview* ((NN43021-458)) .
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 CS 1000 Release 5.5 Branch Office can only be added to a CS1000E; or 1000M main office running CS 1000 Release 5.5 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 0000000000000000IP 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 189) 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)* ((NN43001-579)) for more information on these features.

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

- Network Speed Call (NSC) package 39. This package is required for SRG 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 SRG 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 22). 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.*

- 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.

When using Set-Based Installation at the MG 1000B, install the following:

- Set Relocation (SR) package 53

- Flexible Feature Code (FFC) package 139

- Automatic Installation (AINS) package 200

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 CS 1000 Branch Office:

Step	Action
1	At the main office:

a Upgrade the main office software to CS 1000 Release 5.5. Refer to , *Communication Server 1000E - Software Upgrades;* ((NN43041-458)) or *CS 1000M and Meridian 1 Large System Upgrades Overview;* ((NN43021-458)) .

Upgrade the main office software to CS 1000 Release 6.0. Refer to , *Communication Server 1000E - Software Upgrades;* ((NN43041-458)) or *CS 1000M and Meridian 1 Large System Upgrades Overview;* ((NN43021-458))

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.*

c Configure the Branch Office zones. See Configuring ESN and MG 1000B zones.

d Configure the Branch Office dialing plan. See Dialing plan configuration.

e Configure the IP Phone passwords. See Procedure 3 "Setting and changing the Station Control Password Configuration" (page 92).

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 97).

b Install the MG 1000B Signaling Server. See Installing a Signaling Server.

c Install the Branch Office software, starting with CP PM Call Server and MGC.

Software for the MG 1000B CP PM Call Server and MGC comes with preprogrammed data that can be selected during the installation procedure. For more information, see "Preprogrammed data" (page 205).

d Configure the Branch Office (Customer Data Block and ELAN subnet). See Configuring the MG 1000B zone.

e Configure the Branch Office dialing plan. See Dialing plan configuration.

f Configure the Media Cards. Refer to *IP Line Fundamentals;* ((NN43100-500)) .

Use the same zone for DSP physical TNs and IP Phone TNs. The zone number must match that at the main office. Refer to *IP Line Fundamentals;* ((NN43100-500)) .

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

h If applicable, configure Abbreviated Dialing. See Abbreviated Dialing configuration.

i Provision the Virtual Trunks. Refer to *IP Peer Networking Installation and Commissioning.*

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 and the media cards use the same H.323 ID. This ensures that the Branch User will be properly redirected to the main office. Refer to "Adding the Branch Office endpoints to the NRS database" (page 137) for more information.

j Install MG 1000B telephones, starting with "Installing and configuring IP Phones" (page 140).

--End--

Adding a CS 1000 Release 5.5 Branch Office to a Main Office with a previous software release

The CS 1000 Release 5.5 Branch Office feature requires a main office running Nortel Communication Server 1000 Release 5.5. Therefore, the main office must be upgraded to CS 1000 Release 5.5 before a CS 1000 Release 5.5 Branch Office can be added.

Two options are available when an existing Succession Release 3.0 Main Office, CS 1000 Release 4.0 Main Office, or a CS 1000 Release 5.0 Main Office requires the addition of a new Branch Office. These options are:

1. Upgrade the entire network to CS 1000 Release 5.5, and then add the new Branch Office (see "Upgrade the entire network to CS 1000 Release 5.5" (page 77)).

2. Upgrade only the main office to CS 1000 Release 5.5, and then add the new Branch Office (see "Upgrade only the main office to CS 1000 Release 5.5" (page 77)).

If, in a given network, there is one or more Succession 3.0 Branch Offices, all Branch Offices must be upgraded to CS 1000 Release 4.5 before you can upgrade the main office to CS 1000 Release 5.5

For further information on upgrading the IP Phone firmware, refer to *IP Line Fundamentals;* ((NN43100-500)) . For information on upgrading and reconfiguring the Signaling Server software, refer to *Signaling Server Installation and Commissioning;* ((NN43001-312)) .

Upgrade the entire network to CS 1000 Release 5.5

To upgrade the entire network to CS 1000 Release 5.5:

Step	Action
1	At the main office:
	a Upgrade the Call Server software to CS 1000 Release 5.5.
	b Upgrade the main office Signaling Servers software to CS 1000 Release 5.5 with the Automatic Firmware Upgrade set.
	c Reconfigure the main office Signaling Server to configure the NRS.
	d Upgrade the main office Media Cards to CS 1000 Release 5.5.
2	At each existing CS 1000 4.5 or CS 1000 5.0 Branch Office:
	a Upgrade the Small System Controller to CP PM Call Server and MGC (CS 1000 Release 5.5).
	b Upgrade the MG 1000B Signaling Servers software to CS 1000 Release 5.5 with the Automatic Firmware Upgrade set.
	c Reconfigure the MG 1000B Signaling Servers to configure the NRS.
	d Upgrade the MG 1000B Media Cards to CS 1000 Release 5.5.
3	Execute the `umsUpgradeAll` command on the main office Signaling Servers, or Media Cards, if necessary.
4	Install the new CS 1000 Release 5.5 Branch Office as described in "Implementation summary" (page 74).

--End--

Upgrade only the main office to CS 1000 Release 5.5

> **ATTENTION**
> A mixed software configuration between the main office and branch offices running CS 1000 Release 4.5, CS 1000 Release 5.0 or CS 1000 Release 5.5, is permitted. In this case, indefinite operation with a mixed software configuration is supported.

If you choose to upgrade only the main office to CS 1000 Release 5.5, 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 or CS 1000 Release 5.0 Branch Offices (see "Upgrade main office with IP Phone firmware upgrade" (page 78)).

2. Do not upgrade the IP Phone firmware in the existing CS 1000 Release 4.5 or CS 1000 Release 5.0 Branch Offices (see "Upgrade main office without IP Phone firmware upgrade" (page 79)).

Upgrade main office with IP Phone firmware upgrade
To upgrade the main office to CS 1000 Release 5.5 and upgrade the IP Phone firmware in CS 1000 Release 4.5 or CS 1000 Release 5.0 branch offices to CS 1000 Release 5.5:

Step	Action
1	At the main office:
	a Upgrade the Call Server software to CS 1000 Release 5.5.
	b Upgrade the main office Signaling Server(s) software to CS 1000 Release 5.5 with the Automatic Firmware Upgrade set.
	c Reconfigure the main office Signaling Server to configure the NRS.
	d Upgrade the main office Media Cards to CS 1000 Release 5.5.
	e If necessary, execute the `umsUpgradeAll` command on the main office Signaling Server(s) or Media Card(s).
2	At each existing CS 1000 Release 4.5 or CS 1000 Release 5.0 Branch Office:
	a Upgrade the IP Phone firmware to CS 1000 Release 5.5 IP Phone firmware.
3	Execute the `umsUpgradeAll` command on the main office Signaling Server(s), or Media Card(s) if necessary.
4	Install the new CS 1000 Release 5.5 Branch Office as described in "Implementation summary" (page 74).

--End--

Upgrade main office without IP Phone firmware upgrade

To upgrade the main office to CS 1000 Release 5.5 without upgrading the IP Phone firmware in the existing CS 1000 Release 4.5 or CS 1000 Release 5.0 branch offices:

Step	Action
1	At the main office:
	a Upgrade the Call Server software to CS 1000 Release 5.5.
	b Upgrade the main office Signaling Server software to CS 1000 Release 5.5 with the Automatic Firmware Upgrade set.
	c Reconfigure the main office Signaling Server to configure the NRS.
	d Upgrade the main office Media Cards to CS 1000 Release 5.5.
2	At each existing CS 1000 Branch Office:
	a If necessary, execute the `isetResetAll` command on the MG 1000B Signaling Server(s) or Media Card(s).
3	Install the new CS 1000 Release 5.5 Branch Office, as described in "Implementation summary" (page 74).

--End--

Converting a small system to a Branch Office

Contents

This section contains information on the following topics:

Introduction

Customers with a CS1000M; 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 helps the customer how to upgrade CS1000M 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 21).

The following small systems can be converted to a Branch Office:

- single-cabinet Meridian 1 Option 11C/CSM1Cabinet;

- single-chassis Meridian 1 Option 11C Mini/CSM1Chassis; with or without a chassis expander

- single-cabinet CS1000MCabinet;

- single-chassis CS1000MChassis; with or without a chassis expander

Only single-cabinet and single-chassis systems (with or without a chassis expander) can be converted. Multiple-cabinet and multiple-chassis Small Systems must first be reduced to single cabinets or chassis.

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

- a system controller card that meets the requirements for CS 1000 Release 5.5 software, specifically:

  — NTDW60BA or newer Media Gateway Controller (MGC)

- at least one Media Card, running IP Line 5.5 software. This card can be an 8- or 24-port Media Card (which occupies one slot) or have DSP resources available through the DSP daughterboard(s) on the Media Gateway Controller card.

- a Signaling Server

  — If a Signaling Server is added to a previously CISPR Class B system (previously used in some specific countries), the system is now compliant to Class A, as noted in the front and back pages of this document.

Refer to *Communication Server 1000E - Software Upgrades;* ((NN43041-458)) for information on preparing a small system for conversion.

Conversion

A main office must exist before a small system can be converted to a Branch Office. The main office must be a CS1000M; or CS1000E; system.

If necessary, refer to *CS 1000M and Meridian 1 Large System Upgrades Overview;* ((NN43021-458)) or *Communication Server 1000E - Software Upgrades;* ((NN43041-458)) for instructions on upgrading an existing system to CS 1000 Release 5.5 software. Refer to *Signaling Server Installation and Commissioning;* ((NN43001-312)) for instructions on installing a Signaling Server.

If a Signaling Server is added to a previously CISPR Class B system (previously used in some specific countries), the system is now compliant to 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 89) 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 74)," 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 an MGC card with DSP daughterboard(s).

d Add a CP PM Call Server card with security dongle.

e Install a Media Card if required. Refer to *IP Line Fundamentals;* ((NN43100-500)) .

If the small system already has a Media Card, upgrade it to IP Line 5.0. Refer to *IP Line Fundamentals;* ((NN43100-500)) .

f Install a Signaling Server if required. Follow the procedures in Installing a Signaling Server.

A Signaling Server must be installed on an Meridian Option 11C/CSM1Cabinet;, or Meridian Option 11C Mini/CSM1Chassis; system. A CS1000MSS; 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. Refer to *IP Line Fundamentals;* ((NN43100-500)) .

h Install the Branch Office software, using the Branch Office keycodes. Configure the MGC card.

The software for a Branch Office is significantly different from the software for a small system.

i Configure the Branch Office (Customer Data Block and ELAN subnet). See Configuring the MG 1000B zone.

j Configure the Branch Office dialing plan. See Dialing plan configuration.

k Configure the Media Cards. Refer to *IP Line Fundamentals;* ((NN43100-500)) .

Use the same zone for DSP physical TNs and IP Phone TNs. The zone number must match that at the main office. Refer to *IP Line Fundamentals;* ((NN43100-500)) .

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. See Abbreviated Dialing configuration.

n Provision the Virtual Trunks. Refer to *IP Peer Networking Installation and Commissioning* .

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. Refer to "Adding the Branch Office endpoints to the NRS database" (page 137) for more information.

o   Configure the IP Phones as Branch Users. Refer to "Branch User Config" (page 146) for details on Branch User Config.

--End--

Upgrading to CS 1000 Release 5.5

Contents

This section contains information on the following topics:

Introduction

This chapter describes upgrading an existing main office and its associated branch offices from CS 1000 Release 4.5 or CS 1000 Release 5.0 to CS 1000 Release 5.5.

If, in a given network there is one or more Succession Release 3.0 CS 1000 or Release 4.0 CS 1000 Branch Offices, all Branch Offices must be upgraded to CS 1000 Release 4.5 before upgrading the main office to CS 1000 Release 5.5.

When the Branch Office is being upgraded, the following components are not affected:

- 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

Selecting to migrate your system to an MG 1000B will mean you are effectively decommissioning your existing system software. Once your order is processed, your existing system Site ID/Serial number will be marked as decommissioned in Nortel's software history database. The purchased software licenses on your existing system (and the "right-to-use" for the software) can be transferred to the target CS 1000E main system. You can also transfer your Applications to the target CS 1000E as part of this process if you wish (assuming they are supported). If you want to move some Applications to a different system, please do that in advance using the regular Applications Transfer process.

Upgrading to CS 1000 Release 5.5

If the main office has not already been upgraded to CS 1000 Release 5.5, begin with step 1. If the main office has been upgraded to CS 1000 Release 5.5, begin with step 2.

Step	Action
1	At the main office:
	a Upgrade the Call Server software to CS 1000 Release 5.5.
	b Upgrade the main office Signaling Server(s) software to CS 1000 Release 5.5 with the Automatic Firmware Upgrade set.
	c Configure the main office Signaling Server(s) to access the NRS.
	d Upgrade the main office Media Card(s) to CS 1000 Release 5.5.
2	At each existing CS 1000 Release 4.5, or CS 1000 Release 5.0 Branch Office:
	a Upgrade the Small System to CS 1000 Release 5.0.
	b Upgrade the MG 1000B Signaling Server software to CS 1000 Release 5.5 with the Automatic Firmware Upgrade set.
	c Configure the MG 1000B Signaling Server(s) to access the NRS.
	d Upgrade the MG 1000B Media Card(s) to CS 1000 Release 5.5.
3	Execute the `umsUpgradeAll` command on the main office Signaling Servers, or Media Cards, if necessary.

--End--

Main office configuration

Contents

This section contains information on the following topics:

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 135).

Branch Office dialing plan configuration in the main office and Branch Office is described in Dialing plan configuration.

Configuration of PVQ alarms, thresholds, and notification levels is discussed in Proactive Voice Quality management and "Maintenance and diagnostics" (page 189).

For more information on main office configuration, refer to *IP Peer Networking Installation and Commissioning* .   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)) as appropriate for the system.

IP Telephony Nodes

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

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

Procedure 1
Adding a Node to the Call Server

Step	Action
1	Log in to Element Manager.
2	From the navigation pane, select **System** , **IP Network** , and then **Nodes: Serves, Media Cards** to display the **IP Telephony** page.
3	Click **Add** to add a new Node to the Call Server.

| **--End--** |

For more information on the IP Telephony Management, see *Element Manager System Reference - Administration* (NN43001-632) .

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 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.

AUTHOR'S NOTE: Is Node Management the proper terminology; for consistency's sake?

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

SIP Line Gateway

The SIP Line Gateway parameters are configured and the application is enabled on all the elements that are part of the Node.

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

AUTHOR'S NOTE: Is this the correct book to reference or should it be the SIP Line Fundamentals NTP.

UNIStim LTPS

Enable thee UNIStim LTPS application on every application server that is part of the Node.

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)

AUTHOR'S NOTE: Should import and export configurations be included sections in this NTP.

IP Phone passwords and parameters

Procedure 2 "Setting the IP Phone Installers Password" (page 91) enables any trusted user to install a telephone from its keypad interface. Both main office and branch passwords are required.

Procedure 2
Setting the IP Phone Installers Password

Step	Action

The IP Phone Installer's Password is configured on one Signaling Server or Media Card 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 5 "IP Phone node passwords" (page 91).

Table 5
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.

Table 5
IP Phone node passwords (cont'd.)

Command	Description
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 *IP Line Fundamentals;* ((NN43100-500)) .

--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, such as the Set-Based Removal feature prompts SRCD (LD 15) and AREM (LD 57). The actual SCPW password configuration takes place while configuring the telephone data through the overlays. Telephone data is discussed in "MG 1000B telephones" (page 139).

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 3
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 6
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 7
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
	0-31	Range for small system and Media Gateway 1000B
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 8
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
CODE	AREM	Automatic Set Removal
- AREM	xxxx	Code to invoke Automatic Set Removal
CODE	SCPC	Station Control Password Change
- SCPC	xxxx	Code to invoke password change

4 The SCPW itself is configured during IP Phone configuration, either using TM 3.1 (see "MG 1000B IP Phone configuration using TM 3.1" (page 94)) or overlays (see Procedure 4 "Configuring MG 1000B IP Phones at the main office using LD 11" (page 94)).

--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 TM 3.1 (see "MG 1000B IP Phone configuration using TM 3.1" (page 94)) or LD 11 (see Procedure 4 "Configuring MG 1000B IP Phones at the main office using LD 11" (page 94)).

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 MGCs. For details on transferring the data from the main office to the Branch Office see "Transferring IP Phone data using TM 3.1" (page 150).

MG 1000B IP Phone configuration using TM 3.1

At the main office, TM 3.1 can be used to configure MG 1000B IP Phones. Use **Telephone Pages** to configure the telephones to include the following:

- Terminal Type
- TN
- Customer Number
- Branch Office Zone
- Prime DN corresponding to the BUID

Refer to *Telephony Manager 3.1 System Administration;* ((NN43050-601)) for details.

MG 1000B IP Phone configuration using LD 11

Use Procedure 4 "Configuring MG 1000B IP Phones at the main office using LD 11" (page 94) at the main office to configure MG 1000B IP Phones.

Procedure 4
Configuring MG 1000B IP Phones at the main office using LD 11

Step	Action
1	Configure the Branch Office zones and dialing plan. See Configuring ESN and MG 1000B zones.
2	Configure the following telephone data in LD 11: • Terminal type • Customer Number • TN • Zone • Prime DN to correspond to BUID

Table 9
LD 11 Provision Branch User and SCPW at the main office

Prompt	Response	Description
REQ:	NEW CHG	Add new data, or change existing data.

Table 9
LD 11 Provision Branch User and SCPW at the main office (cont'd.)

Prompt	Response	Description
TYPE:	a...a	Terminal type.
		Type **?** for a list of possible responses.
CUST	xx	Customer number as defined in LD 15.
ZONE	0-255	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** 1100 Series sets are also supported.
...		
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 section contains information on the following topics:

Installing an MG 1000B Core

For CS 1000 Release 5.5, the MG 1000B Core must contain a Call Processor Pentium Mobile (CP-PM) CS and a Media Gateway Controller (MGC) card. The chassis can contain the following interface cards:

- 8-port or 32-port 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)

The MG 1000B Expander will support digital trunks if configured with a media gateway controller.

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 that can be installed in the same rack as the MG 1000B Core and MG 1000B Expander or an option CP PM Signaling Server that can be installed in any slot of the platform (excluding slot 0). The MG 1000B Expander is optional and follows the same installation procedure as the MG 1000B Core. A CP PM Signaling Server can also be installed in any slot of the platform (excluding slot 0).

Readiness checklist

Before starting the installation, use the checklist in to make sure you are ready.

Table 10
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 11 "Tools checklist" (page 99) are available before assembling the components.

Table 11
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 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 Core or MG 1000B Expander
Items required

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

- equipment layout plan (discussed in *Communication Server 1000E: Installation and Configuration (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 5
Mounting the MG 1000B Core or MG 1000B Expander in a 19-inch rack

Step	Action

References to "MG 1000B Core" in the following steps also apply to the MG 1000B Expander.

1   Fasten the right guide bracket to the right rack support.

   a Insert two #12-24 self-tapping screws into the two middle slots in the guide bracket and into the respective holes in the right rack support.

   b Tighten the screws. See Figure 12 "Guide bracket installed in a rack" (page 100).

Figure 12
Guide bracket installed in a rack
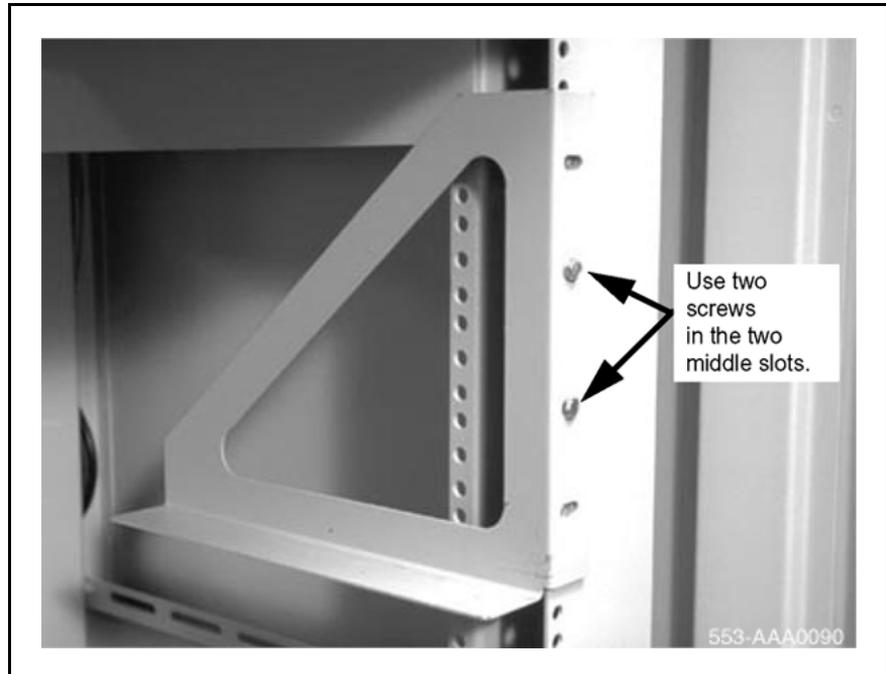
The guide brackets guide the MG 1000B Core into place and enable one person to install the MG 1000B Core in the rack.

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

   a Insert two #12-24 self-tapping 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 Core. See Figure 13 "Right ear bracket installed on the MG 1000B Core" (page 101).

   a Use two #8-32 machine screws.

   b Position the ear bracket so that the four holes on the bracket flange are nearer to the back of the MG 1000B Core. 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 Core.

Figure 13
Right ear bracket installed on the MG 1000B Core

Bracket flange marked with an "R". Attach this ear bracket to the right-hand side of the MG 1000B Core.

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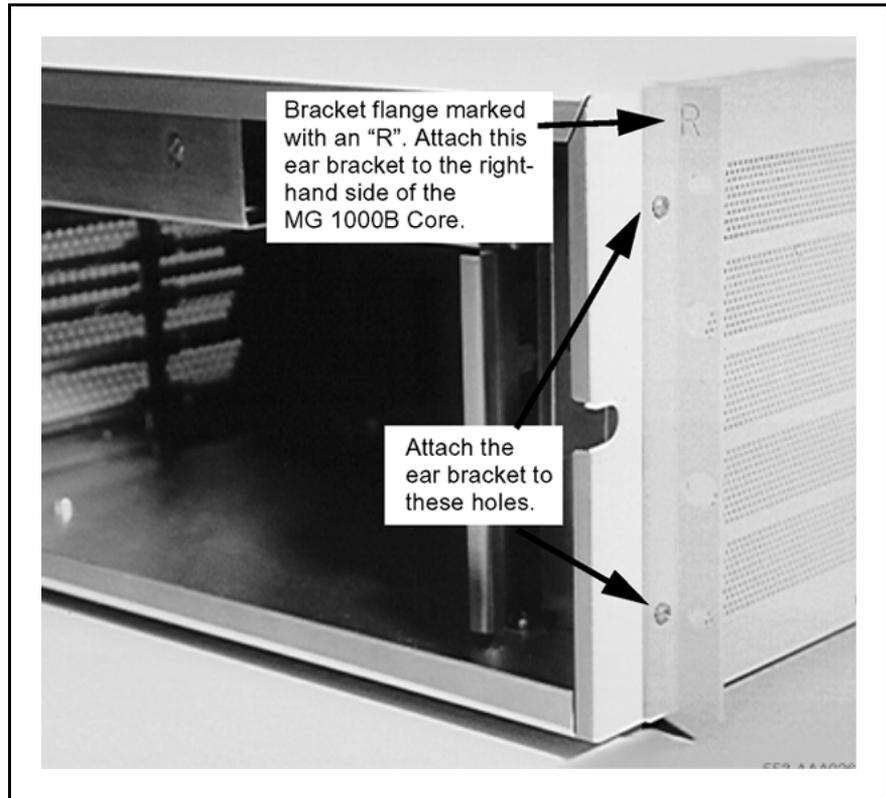
4 Attach the left ear bracket (marked with an "L") to the holes on the left side of the MG 1000B Core (near the front).

   a Use two #8-32 machine screws.

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

> ⚠️ **WARNING**
> The MG 1000B Core and MG 1000B Expander each weigh approximately 30 lb. (13.5 kg) with circuit cards installed, or 26 lb. (12 kg) without circuit cards installed. If necessary, get assistance when lifting the equipment.

5 Place the MG 1000B Core on the guide brackets. Carefully slide the MG 1000B Core into the rack until the ear brackets come to rest against the rack support.

6 Use the four remaining #12-24 self-tapping screws to fasten the MG 1000B Core to the rack supports (two screws on each side).

7   Make sure that the back of the MG 1000B Core is on the guide brackets. See Figure 14 "MG 1000B Core and MG 1000B Expander installed in a rack" (page 102).

Figure 14
MG 1000B Core and MG 1000B Expander installed in a rack
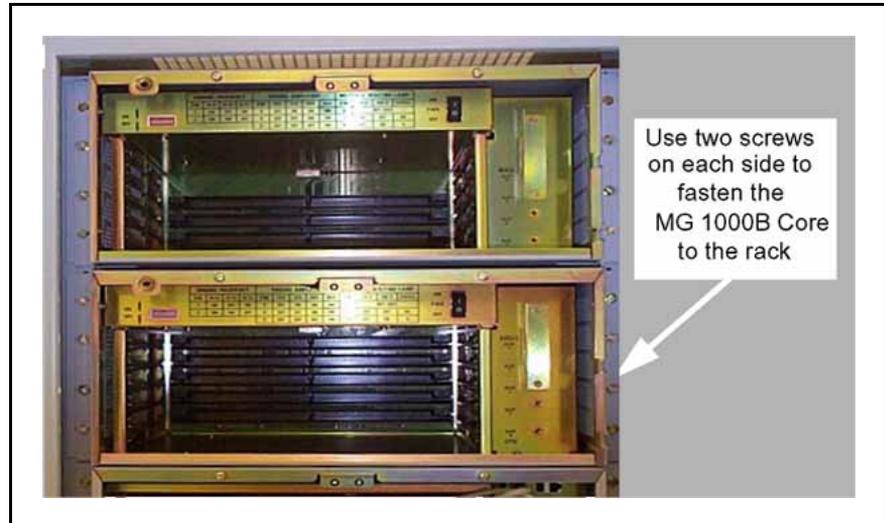
8   Install the equipment ground wires for the MG 1000B Core, MG 1000B Expander, and Signaling Server. See *Communication Server 1000E: Installation and Configuration (NN43041-310).*

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

10   In the MG 1000B Core do the following:

   a   Install the DSP software daughterboards on the MGC card.

   b   Install the MGC card in the chassis.

   c   Install the security dongle on the CP-PM Call Server card.

   d   Set the S5 dip switch to position 0.

   e   Install the CP PM Call Server card in the chassis.

   f   Install the Signaling Server hardware

   • If you are using a CP PM Signalling 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, rackmount the signalling server as per the vendor's directions.

11   Install circuit cards in the MG 1000B Core and the MG 1000B Expander. See *Communication Server 1000E Installation and Commissioning* ((NN43041-310)) .

12   Make the Ethernet connections. Configure the Ethernet port to enable TM 3.1 and Element Manager connectivity as required.

    a See Procedure 7 "Connecting the Ethernet ports" (page 120).

    b Follow the instructions in *Telephony Manager 3.1 Installation and Commissioning;* ((NN43050-300)) .

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

13 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)) .

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

Figure 15
Power switch on the front of the MG 1000B Core
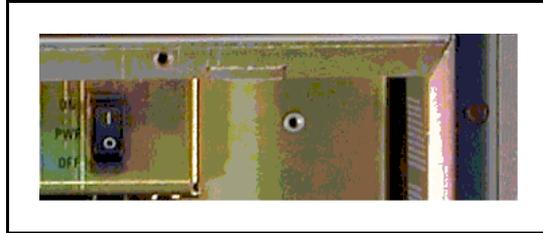
15 Install any remaining equipment, such as alarms. See *Communication Server 1000E: Installation and Configuration (NN43041-310)* .

16 Reinstall the front covers on the MG 1000B Core and MG 1000B Expander.

--End--

Installing cards

In the MG 1000B, install Media Cards. To install and configure the 8- or 32-port Media Card (see Figure 16 "Media Card" (page 103)) refer to *IP Line Fundamentals;* ((NN43100-500)) .

Figure 16
Media Card
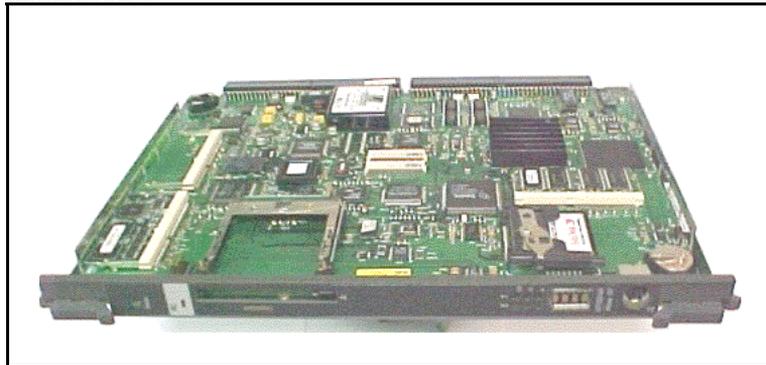
Install a trunk card to connect with the PSTN and an analog or digital line card to connect with local resources. Consult *Circuit Card Reference* ((NN43001-311)) for specific details and installation procedures of the various interface cards of the MG 1000B Core.

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 104).

- Power down the chassis.

- Remove the SSC card.

- Destroy or return the SSC security device to your local Nortel Repairs/ Returns center.

- Install the DSP Daughterboard on the MGC card as described in "Installing a DSP Daughterboard" (page 107).

- Install the MGC card as described in "Installing the MGC card" (page 108).

- Install the CP PM as described in "Installing the CP PM card" (page 108).

- Cable the cards as shown in "MGC Network Connections" (page 32).

- Power up the MG 1000B.

- Enter the 'mgcsetup' menu and configure the IP parameters, then reboot the MGC.

If the Centralized Software Upgrade (CSU) feature is enabled on the Call Server, the firmware for the MGC 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 CF card into the active CP PM Call Server RMD slot to back up the database.
3	Load the Equipment Data Dump Program (LD 43). At the prompt, enter

Table 12
LD 43 – Load program

LD 43	Load program.
.	EDD

4 When EDD000 appears on the terminal, enter:

Table 13
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 14
Exit program

****	Exit program

--End--

Installing the cards

The following sections describe the process required to install the MGC
and CP PM cards.

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 15
DSP Daughterboard configurations

Position 1	Position 2
DB32 (card slot 11)	None
None	DB32 (card slot 0)
DB32 (card slot 11)	DB32 (card slot 0)
DB96 (card slot 11, 12 &13)	None
DB96 (card slot 11, 12 &13)	DB32 (card slot 0)

> **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 (ie unit 0 of card 0 in the first IPMG) <supl sh> = 000 0) is not available.
>
> A single channel (unit 0) is not available on the first IPMG 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 MGC card.

Figure 17
DSP Daughterboard
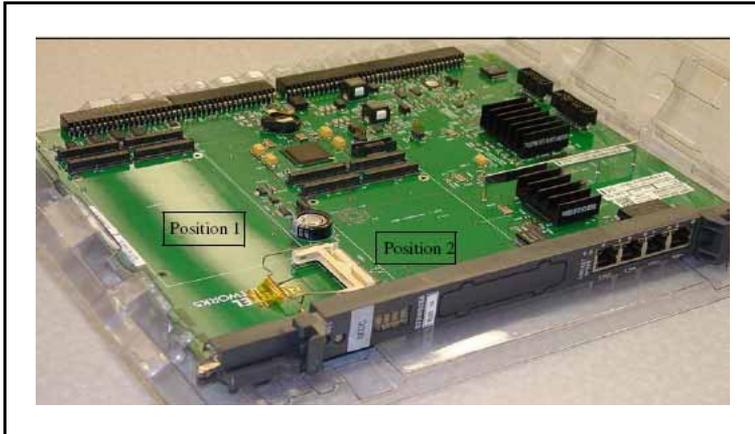
Installing a DSP Daughterboard

Step	Action
1	Place the MGC on a safe ESD surface.
2	Place the DSP Daughterboard in either Daughterboard position 1 (for DSP DB-96) or Daughterboard position 2 (for DSP DB-32), depending on how the Daughterboard will be configured from a TN perspective.
3	Ensure the DSP Daughterboard is securely attached to the MGC. (using supplied screws).

--End--

Installing the MGC card

Table 16
MGC 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)

Installing the MGC card

Step	Action
1	Insert the MGC into Slot 0 of the Chassis.

> **ATTENTION**
> You must ensure that all dongles for the CP PM card are correctly identified.
>
> Please DESTROY or RETURN the SSC dongle to your local Nortel Repairs/Returns center.
>
> For the CP PM call server, you must use the dongle provided in the software kit. Chassis Expander dongles may be disposed of, as they are no longer needed.

Step	Action
2	The existing 3-port SDI cable (NTBK48AA) is reused. It connects to the SDI port on the Chassis.

--End--

Installing the CP PM card

The following procedure describes how to install the CP PM card in a Chassis.

Ensure that the S5 switch is set to position 0 for the CP PM Call Server card.

Installing the CP PM card

Step	Action
1	Ensure that the security dongle (the one that comes as part of the software kit) is inserted on the CP PM call processor.
2	Slide the CP PM call processor into Slot 1 (or higher) of the Chassis.
3	Lock the card into the faceplate latches.
4	Attach the SDI cable. The 50-pin Amphinol connects to the back of the CP PM call server.

Figure 18
SDI cable

--End--

The preceding steps enable users to upgrade the system one MG 1000B at a time. For each additional IPMG, repeat Procedure 3 (Removing the SSC card) to Procedure 5 (Installing the CP PM card).

Upgrading the CP PM software

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	Call up the Software Installation Program during a SYSLOAD. During SYSLOAD, the following prompt appears:

Table 17
SYSLOAD

```
Read boot parameters from:
F: Faceplate compact flash
H: Hard Drive
0 [H]
```

	Press F to boot from the compact flash (which contains the software).
5	Enter <CR> at the Install Tool Menu.

Table 18
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 CS 1000 system, complete the following checklist.

Table 19
Installation checklist

Have you:
Received all server equipment and peripherals? • For an IBM X306m (NTDU99AAE5) or HP DL320-G4 (NTDU97AA) 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 CS 1000E Nortel CP PM Signaling Server (NTDW61BAE5): — NTDW6102E5 - CP PM Signaling Server Hard Drive kit — N0118766 - CP PM Signaling Server Hard Drive Installation instructions — NTAK19ECE6 - CP PM Signaling Server 2 port SDI Cable assembly kit — NTDU0606E6 - CP PM Signaling Server 25cm RJ45 Ethernet Cable kit — a 25-pin to 9-pin straight-through serial cable (not supplied) *Note:* Save the packaging and packing materials in case you must reship the equipment or peripherals.
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* ((553-3041-210)) ?

Installing a CP PM Signaling Server

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

Installation in a MG 1000B system   The NTDW61BAE5 model of the CP PM Signaling Server is designed for use in a CS1000E; system. The first task that must be performed is to install the hard drive shipped with the server. For instructions, see Procedure 6 "Replacing the hard drive on a CP PM Signaling Server" (page 112).

You can insert the NTDW61BAE5 model of the CP PM Signaling Server into any slot of a MG 1000B or 11C cabinet or chassis, except slot 0. Slot 0 is reserved for a Media Gateway Controller (MGC) card. Keying prevents the CP PM Signaling Server from being inserted into this slot.

Procedure 6 "Replacing the hard drive on a CP PM Signaling Server" (page 112)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 6
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 19
CP PM hard drive jumper
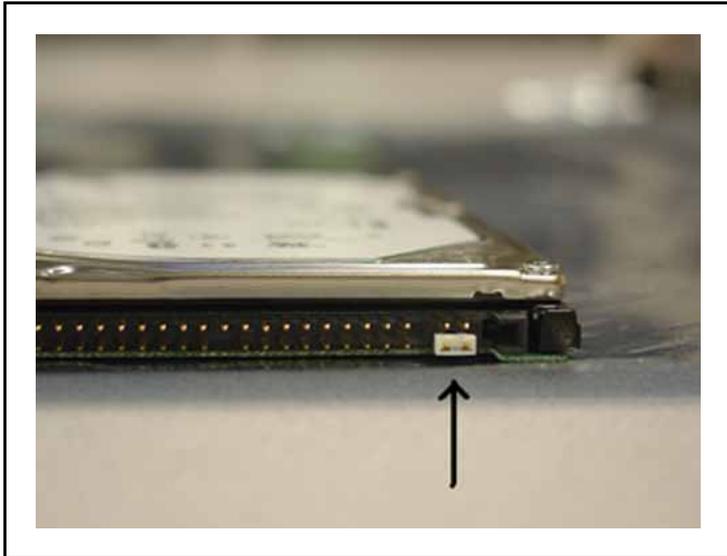
2   Place hard drive on printed circuit board and slide to mate with
            connector J32.

Figure 20
CP PM hard drive and connector J32

3   Secure hard drive from the bottom side with the included screws.

Figure 21
Securing CP PM hard drive to circuit board
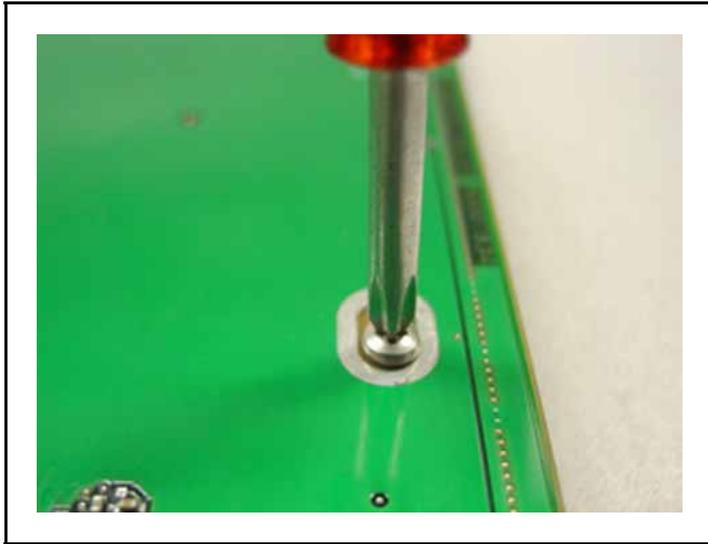
4 Place Dip Switch S5 in position 2 to select HD Master option.

Figure 22
CP PM Signaling Server FMD dip switch
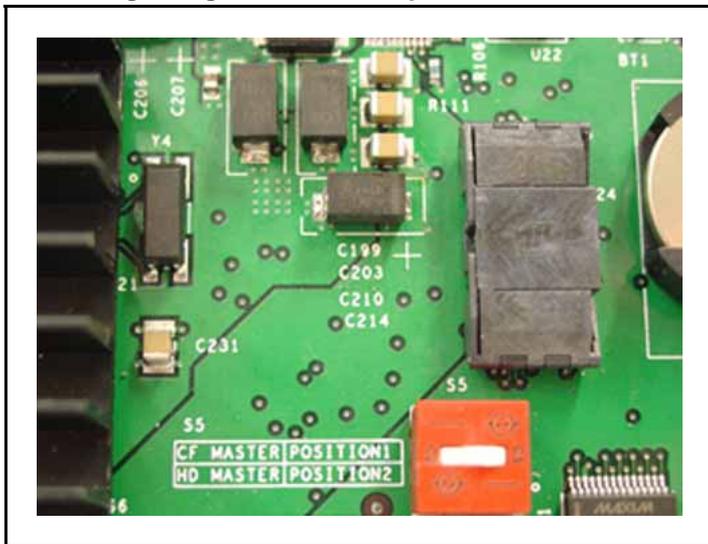
ATTENTION
A CP PM circuit card has an on-board switch (S5) for designating the internal hard drive (HD) or internal Compact Flash (CF) drive as the Fixed Media Device (FMD) for the Signaling Server. You must configure the on-board FMD switch (S5) to position 2 to designate the HD as the FMD for the Signaling Server.

5 Remove on-board compact flash retainer clip if populated.

Figure 23
CP PM Signaling Server internal CF card retainer clip

--End--

MG 1000B software installation

Contents

This section contains information on the following topics:

Installing MG 1000B software

Installing MGC software

For details on installing software on an MGC card refer to *Communication Server 1000E Installation and Commissioning;* ((NN43041-310)) .

Installing CP PM software

For details on installing software on a CP PM card refer to *Communication Server 1000E Installation and Commissioning;* ((NN43041-310)) .

Upgrading MGC software

For details on upgrading software on an MGC card refer to *Communication Server 1000E - Software Upgrades* ((NN43041-458)) .

Upgrading CP PM software

For details on upgrading software on a CP PM card refer to *Communication Server 1000E - Software Upgrades;* ((NN43041-458)) .

Connecting the MG 1000B Core to the network

The MG 1000B Core has two 100BaseT ports (1and 2) for Ethernet connection to the network. See Figure 86 "Ethernet connections for CP PM Signaling Server" (page 241).

Figure 24
Branch Office Ethernet connections
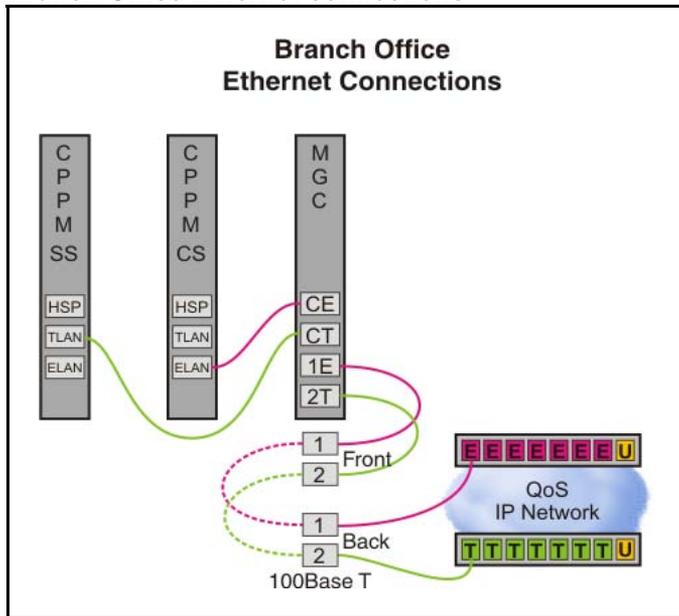
From the Media Gateway Card, connect two short Ethernet cables between the Media Gateway bulkhead and the two 100BaseT ports at the top right corner of the MG 1000B Core. The TLAN network interfaces exist only on the MG 1000B Media Cards, IP Phones, and the Signaling Server, as shown in Figure 8 "MG 1000B platform without MG 1000B Expander" (page 36) and Figure 9 "MG 1000B platform with MG 1000B Expander" (page 37).

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 whether the route is network based or host based.

Note 6: INI is required for the activation of subnet Mask.

--End--

Procedure 7
Connecting the Ethernet ports

Step	Action

To configure the TLAN and ELAN network interfaces at the MG 1000B Core and enable traffic over the LAN/WAN, connect the CAT5 cables and configure the data connectivity.

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 MGC card on the CE port and then make the ELAN connection from the 1E port of the MGC 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 97).

--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 25 "Confirm IP telephony node values H.323 Gatekeeper" (page 122)):

  — 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.

- under SIP GW Settings (see):

— 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;* ((NN43001-312)) .

To configure an Alternate and Failsafe (if required) NRS, refer to the corresponding procedures in *IP Peer Networking Installation and Commissioning.*

Figure 25
Confirm IP telephony node values H.323 Gatekeeper

Figure 26
Confirm IP telephony node values SIP Redirect Server

Signaling Server software installation

Software for the Signaling Server is installed using the Install Tool, which runs from the Signalling Server Software CD-ROM or Compact Flash card for the CP PM Signaling Server. The Install Tool program also upgrades existing Signaling Server software to the latest version. The Signaling Server is out-of-service during software installation or upgrade.

To perform a software installation or upgrade, reboot the Signaling Server with the CD-ROM in its drive or bootable Compact Flash card inserted in the CP PM Signaling Server.

The Install Tool installs all Signaling Server software, including the operating system, applications, and web files. The Install Tool also copies software files for the Media Cards and IP Phones, which are used to upgrade these components. For a new Signaling Server, the Install Tool prompts for IP telephony parameters to perform basic system configuration.

After the Signaling Server software is installed, further system configuration is performed using Element Manager and NRS Manager.

For more information about the Signaling Server, refer to *Signaling Server Installation and Commissioning;* ((NN43001-312)) .

Materials required

To install the software, you need:

1. A power cable, serial cable, and CAT5 cables for networking.

2. The Signaling Server Software CD-ROM or compact flash (CF) card. Order or download the software from the Nortel Electronic Software Download site if you do not have the latest version in the shipment.

Creating a Signaling Server software compact flash card

This section describes the steps necessary to create a Signaling Server Software CF Card. A Signaling Server software CF card is necessary to load the Signaling Server Software Installation Tool, along with the Signaling Server software, operating system, and web files onto a CP PM Signaling Server.

Use the following procedure to create a Signaling Server Software CF Card.

Procedure 8
Creating a Signaling Server Software CF Card

Step	Action
1	Navigate to the folder on your local PC into which you downloaded the CP PM Signaling Server Load zip file.
2	Unzip the Signaling Server Software Load zip file.

This results in:

- parent directory (cf:\)
- six child directories (plus other required loadware files)
  - \licenses
  - \load
  - \mkboot
  - \opensrc
  - \ssexxxxx.p
    Where "xxxxx" identifies the current release of Signaling Server software.
  - \symtabs

Step	Action
3	Open the **\mkboot** directory and locate the mkbootrmd.bat file.

This batch file is used to format the CF card.

Step	Action
4	Insert the CF card into a PCMCIA adapter and insert it into your PC.

> **ATTENTION**
> The CF card must be 512Mb (CPC# A0548249).

Step	Action
5	Click on **My Computer** to verify the drive letter assigned to the CF drive.

The **My Computer** screen appears.

Figure 27
My Computer
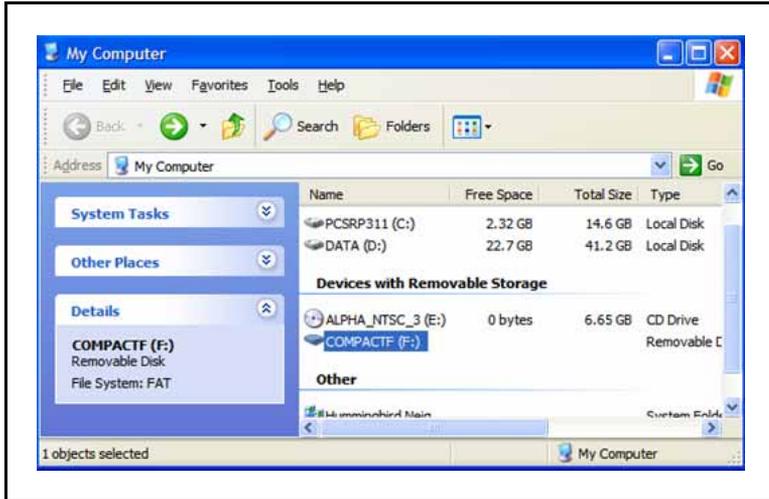
In this example, drive F: is assigned to the CF drive.

6   Navigate to the **Temp** folder on your local PC ((or the folder into which you downloaded the CP PM Signaling Server Load zip file).

7   Open the \mkboot folder and locate the mkbootrmd.bat file.

The following is an example of what you should see on the screen.

Figure 28
Run mkbootrmd.bat
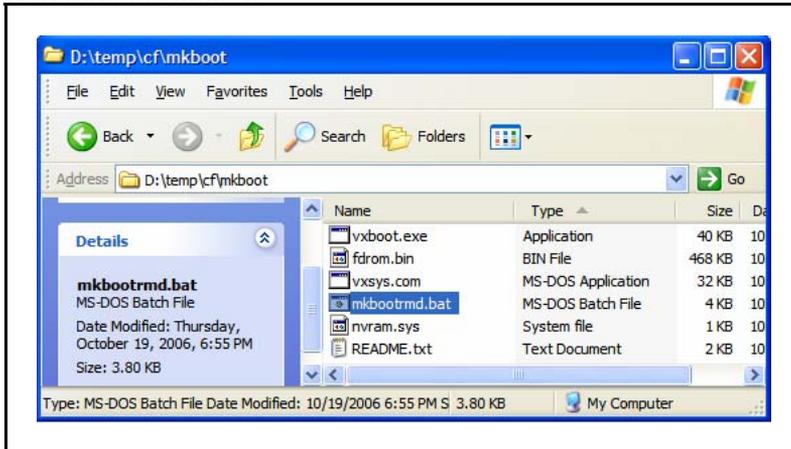
8   Double click the mkbootrmd.bat file to start the application (this batch file is used to format the CF card).

You can press any key to continue when prompted.

The line asking you to enter a CF drive letter appears on the screen.

Figure 29
Enter CF drive letter
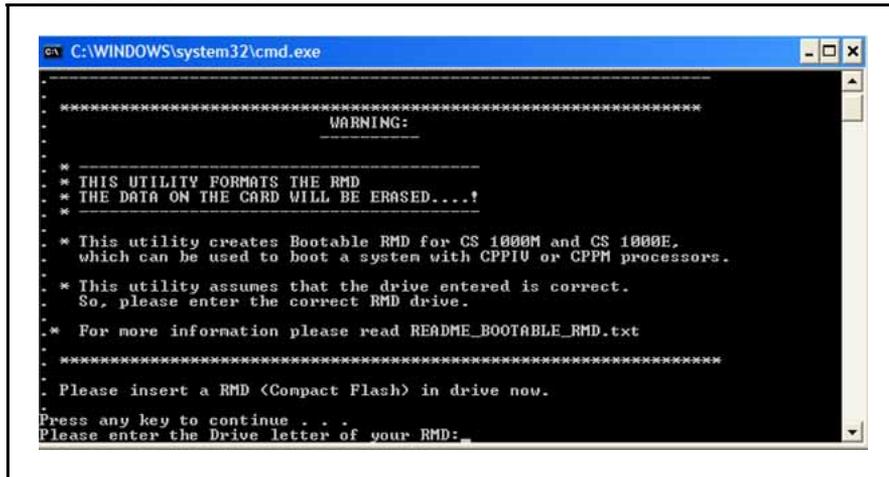
> **CAUTION**
> The mkbootrmd.bat file does not verify the drive
> assignment; it is possible to format other drives on
> your PC or Laptop.

9 Enter the drive letter assigned to the CF drive on your PC.

A line asking you to insert a new CF card in the CF drive
appears on the screen.

Figure 30
Insert new CF card in drive
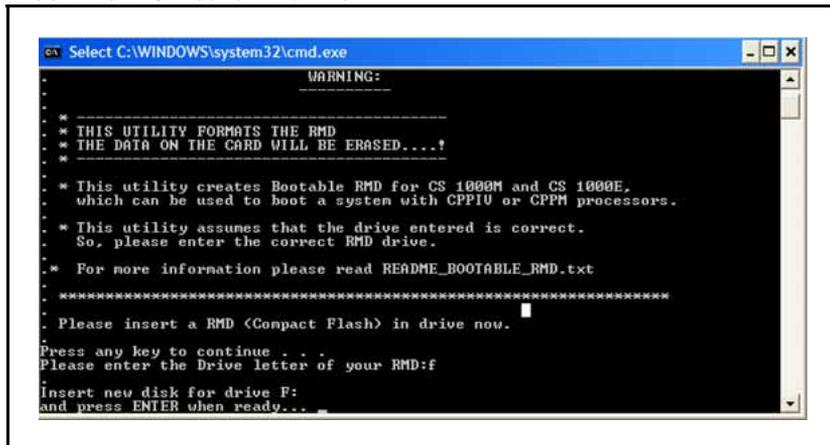
Although a CF card is already in the CF drive, you are requested
to insert a new CF card in the drive. Ignore this request and
proceed to the next step.

10 Press **Enter** to start formatting the CF card.

The Start of CF card formatting process screen appears.

Figure 31
Start of CF card formatting process
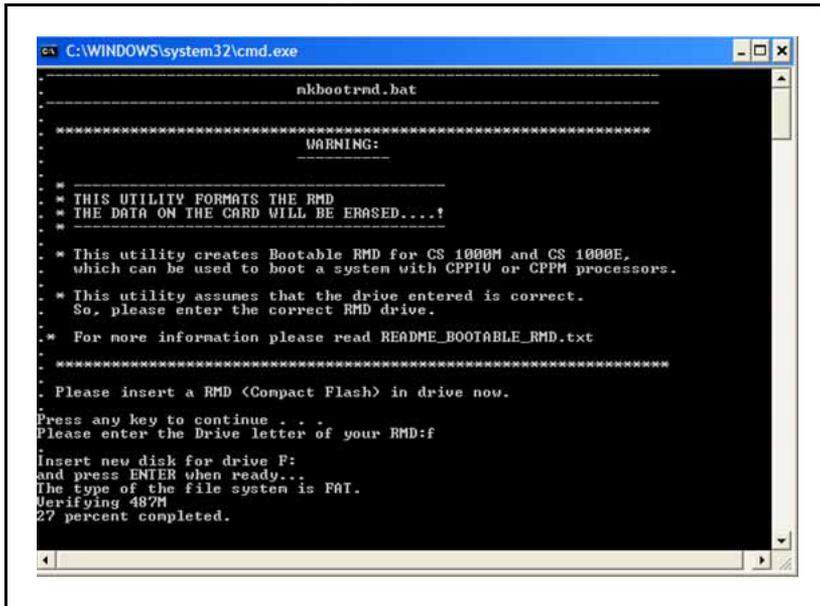
When the formatting process is almost complete, the End of CF card formatting process screen appears.

Figure 32
End of CF card formatting process
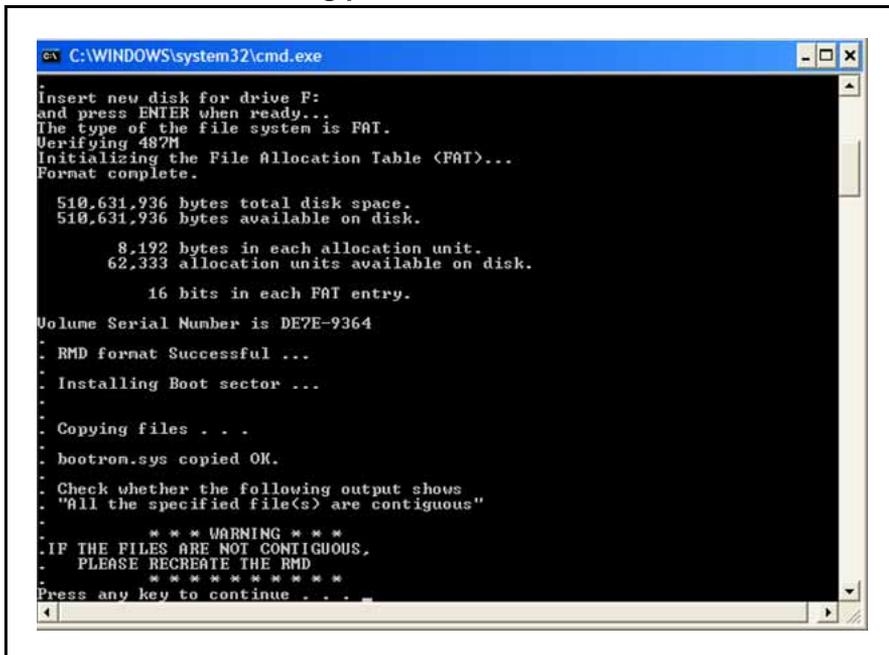
You see the following messages (among others):

`RMD format Successful ...` (after the Volume Serial Number string)

`bootrom.sys copied OK.`

You should also see a very important warning message:

`Check whether the following output shows
"All the specified file(s) are contiguous".`

11 Press any key to continue.

The Verify CF card formatting process screen appears.

Figure 33
Verify CF card formatting

Look for the following message near the bottom of the screen:

`All specified files are contiguous.`

This message indicates that the CF card formatting process has ended successfully and the CF card is now ready to be loaded with the Signaling Server Software and system components.

12 Press any key to close the batch file and associated MS-DOS window.

13 **Click** on **My Computer** to verify that the CF drive has been renamed to **CS1000BOOT**.

The following is an example of what you should see on the screen.

Figure 34
CF drive renamed to CS1000BOOT
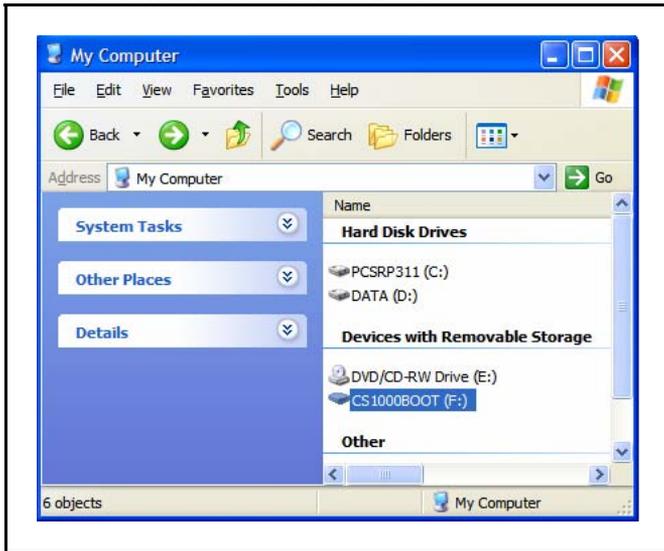
14   Double click the CF drive to verify that it contains the
             bootrom.sys and nvram.sys files.

             The following is an example of what you should see on the
             screen.

Figure 35
Verify contents of CS1000BOOT
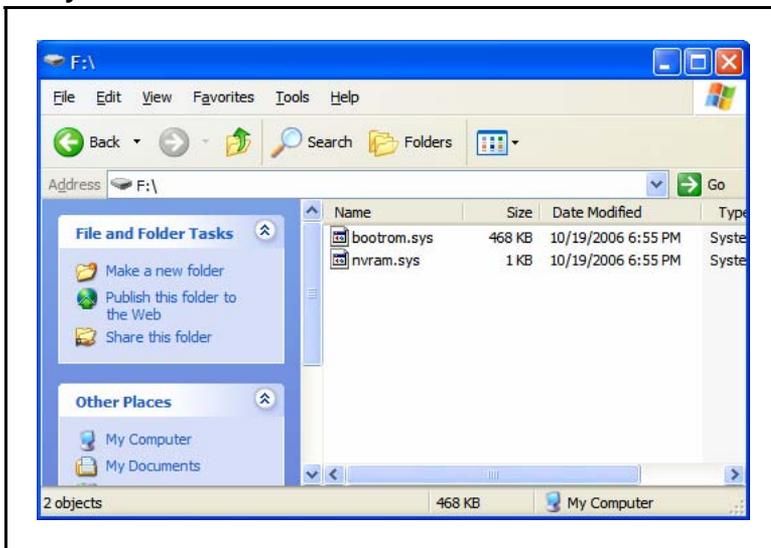
15   Navigate to the **Temp** folder on your local PC (or the folder into
             which you downloaded the CP PM Signaling Server Load zip
             file).

16 Copy all of the subfolders and files from the parent directory (\cf) to the CF drive.

> *Note:* This can take up to 12 minutes depending on the speed of your computer. You are copying files from the hard drive on your local PC to the CF card in the CF drive.

When all subfolders and files are copied successfully to the CF card, it can be used to install and upgrade Signaling Server software on a CP PM Signaling Server.

17 Remove the CF card from the CF drive and label it appropriately.

An example for a label is, Signaling Server, sse-x.xx.xx, where x.xx.xx represents the Signaling Server software version.

--End--

When all Signaling Server Software and system components are loaded successfully onto the Signaling Server Software CF Card, it can be used to install Signaling Server software and system components onto a CP PM Signaling Server.

Installing the Signaling Server software

If you are installing the software on a new Signaling Server, or If you are upgrading the software, refer to *Signaling Server Installation and Commissioning;* ((NN43001-312)) .

Upgrading the Signaling Server software

Use the Signaling Server Install Tool to upgrade the Signaling Server software, refer to *Signaling Server Installation and Commissioning;* ((NN43001-312))

To upgrade the Signaling Server software, the IP Phone firmware, and the Media Card loadware, select option **a** in the Main Menu of the Install Tool To upgrade only the Signaling Server software, select option **b** in the Main Menu.

Refer to *Signaling Server Installation and Commissioning;* ((NN43001-312)) for more information on upgrading and rec-onfiguring the Signaling Server.

Signaling Server tools

See Procedure 9 "Viewing the Tools Menu" (page 131) to access the options in the Signaling Server Install Tools menu.

Procedure 9
Viewing the Tools Menu

Step	Action

Use this option to set the date and time on the Signaling Server. This is also where you can reset the shell login names and passwords (if you forgot them or simply want to restore the initial defaults).

1   Enter **t** at the **Main Menu** to access the Tools menu. **The Tools Menu** appears as shown.

Figure 36
Tools menu

```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
============================================================

                 T O O L S   M E N U

This is the Tools Menu. Please select one of the options below.

          Please enter:
<CR> -> <a> - To set system date and time.
        <b> - To re-partition and re-initialize the hard disk.
        <c> - To reload Default Accounts.
        <d> - To test the hard disk.
        <e> - To change the web server security flag.
        <f> - To initialize unprotected (/u) partition.
        <g> - Clear the boot sector to allow re-installation of the previous release
        <h> - Copy the IP configuration from the removable media to the hard disk
        <i> - Backup the IP configuration from the hard disk to the removable media
        <j> - To replace CPU board BIOS.
        <m> - To return to the Main Menu.

        Enter Choice>
```

2   Under the **Tools Menu**:

a   Set the date and time (default).

b   Repartition and reinitialize the hard disk.

c   Delete the Administrator login and password.

d   Test the hard disk.

e   Change the web server security flag.

f   Initialize the unprotected partition (/u).

> ⚠️ **WARNING**
>
> Option f (Initialize unprotected partition [/u]) deletes the database, reports, and all other files and directories on partition **u**. Back up the database before selecting this option.
>
> Option b (Partition and initialize the hard disk), results in a reboot. Leave the Signaling Server Software CD-ROM in the drive so that the Install Tool can restart. Then, reinstall the Signaling Server software, as described.

--End--

Signaling Server port speed

Use to change the initial port speed of the Signaling Server for a maintenance terminal connection. This procedure is optional.

Procedure 10
Changing the Signaling Server port speed

Step	Action
1	Make sure the DTE–DTE null modem cable (supplied with the Signaling Server) runs from the back port of the Signaling Server to the maintenance terminal.

> *Note:* The CP PM Signalling Server does not require a null modem.

2	Press <CR> to see the login prompt. The Signaling Server must boot successfully before the user can log in.
3	Log in to the Signaling Server.

> **ATTENTION**
> If the Signaling Server has connected to the Call Server (the startup messages indicate whether or not the link is up), use the PWD1 login to access the Signaling Server.

The default Signaling Server Command Line Interface (CLI) login and password is:

- Login = `admin1`
- Password = `0000`

The system immediately prompts a change to the default password.

> **ATTENTION**
> If you forget the password, reset it from the **Tools Menu** (see).

> *Note:* Steps 4 though 7 can vary based on what type of Signaling Server you use. The information shown in steps 4 through 7 are for an ISP1100 Signaling Server.

4	Enter `stty 9600` to change the port speed to 9600 baud.

Acceptable values for the maintenance port speed are 9600, 19 200, 38 400, and 115 200.

> *Note:* Steps 4 through 7 vary, depending on the type of Signaling Server used. The instructions shown in this procedure are for an ISP 1100 Signaling Server.

5   Change the port speed on the terminal, terminal emulator, or workstation (which can require a terminal emulator reset).

6   Press <CR> several times to make sure the command line prompt is visible at the new speed.

7   Enter **exit** to log out of the CLI.

--End--

After installing software and configuring basic information about the Signaling Server, the Signaling Server components can be configured using the web-based Element Manager interface. See *Element Manager System Reference - Administration;* ((NN43001-632)) .

Verifying a successful configuration

To ensure that ELAN and TLAN network interfaces on the Signaling Server are configured correctly, perform a ping test at each interface.

Procedure 11
Verifying successful configuration

Step	Action
1	Log on to the Signaling Server. For details on logging on to the Signaling Server see *Signaling Server Installation and Commissioning* ((NN43001-312)) .
2	From the Call Server, in LD 117, enter: **ping <ip address>**
3	From the Media Card, log in to the Media Card and enter: **ping "ip address",3**
4	From the Signaling Server, log in and enter: **ping "ip address",3**

--End--

Refer to LD 117 in *Software Input Output Reference - Maintenance;* ((NN43001-711)) for IP connectivity information.

Configure login names and pseudo terminals (PTYs) for TM 3.1 and Element Manager connectivity. You need three PTYs for Element Manager. For the configuration procedure, see *Telephony Manager 3.1 Installation and Commissioning;* ((NN43050-300)) .

The default login is

> User ID: `admin1`
> Password: `0000`

This is a Level 1 password. For more information, refer to *System Management Reference;* ((NN43001-600)) .

Branch Office configuration

Contents

This section contains information on the following topics:

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 117)), 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 Branch Office dialing plan (see Dialing plan configuration).
3	Configure the CDM (see Configuring the CDM).
4	Configure Media Cards as voice gateways (see "Configuring the Media Cards" (page 137)).
5	Configure trunks and lines (see "Configuring the trunks and lines" (page 137)).

6   Configure IP Phones (see).

--End--

Configuring the Central Deployment Model

To configure zone based parameters, the Central Deployment Model (CDM) 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 20
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	
CDM	(NO) YES	CDM 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 CDM. For more information on the CDM, see *Dialing Plans Reference* (NN43001-283) .

Step	Action
1	Enable the **Central Deployment Model** option in **OVL15**,
2	Set the **dial plan** option to the appropriate dial plan **PUB** or **PRV**.
3	Configure the numbering zones for sets
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--

Configuring the Media Cards

The Media Cards (see Figure 16 "Media Card" (page 103)) 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 Media Card operating system and application files. The workfile is a single packed and compressed file.

For more information on configuring the Media Card, see *IP Line Fundamentals;* ((NN43100-500))

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 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 install and configure Virtual Trunks on the Branch Office, refer to *IP Peer Networking Installation and Commissioning.*

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 (CDP_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 section contains information on the following topics:

Overview

After the Branch Office zones and passwords are provisioned, the MG 1000B IP Phones must be provisioned. They can be provisioned using TM 3.1, LD 11, or Set-Based Installation.

The IP Phones or devices that are supported in the MG 1000B include:

- IP Phones – "Installing and configuring IP Phones" (page 140)

- Analog (500/2500-type) telephones and devices – "Analog devices" (page 163)

- Digital telephones and devices – "Digital devices" (page 164)

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 93)). 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. However, refer to "Transferring IP Phone data using TM 3.1" (page 150)for procedures to transfer IP Phone data from the main office to the MG 1000B.

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:

- Set-based installation - Use the keypad interface on the IP Phone to enter the data.

  — Enter the IP Phone data (follow the procedure Procedure 12 "Using Set-Based Installation" (page 143)).

  — Enter the Branch User-specific data (follow the procedure Procedure 13 "Configuring a Branch User" (page 147)).

- Use TM 3.1 or LD 11 to enter all data.

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 three ways: Set-Based, TM 3.1, or 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 *CS 1000E Installation and Configuration NTP (NN43041-310).* If the Branch Office is a converted small system, refer to *Communication Server 1000M and Meridian 1 Small System Installation and Commissioning* ((NN43011-310)) .

To install an IP Phone at the Branch Office using Set-Based Installation, 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 2 "Setting the IP Phone Installers Password" (page 91) 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 141).

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	Provision the basic Terminal Number (TN), Directory Number (DN), and node data through the Set-Based Installation procedure (Procedure 12 "Using Set-Based Installation" (page 143)). This makes the set operational and provides basic provisioning for survivability. Nortel recommends that the DN be the same at both the main office and the Branch Office.
3	Configure the Branch User ID (BUID) and its Main Office TN (MOTN) through Procedure 13 "Configuring a Branch User" (page 147).

--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 12 "Using Set-Based Installation" (page 143). 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 Configuration NTP (NN43041-310)* for more detail), verify that the network has DHCP enabled. Refer to *Converging the Data Network with VoIP Fundamentals;* ((NN43001-260)) 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 12
Using Set-Based Installation

Step	Action

This procedure installs IP Phones at the Branch Office and main office. If necessary, the administrator can perform a Set-Based 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 37 "Set-Based Installation Step 1" (page 143).

Figure 37
Set-Based Installation Step 1


```
Connect SVC              Jan 01 12:17am

  Node : ____

  Password : _____

  OK      BKSpace      Clear      Cancel
```

2   Enter the TN and press the OK soft key, as shown in Figure 38 "Set-Based Installation Step 2" (page 144).

Figure 38
Set-Based Installation Step 2
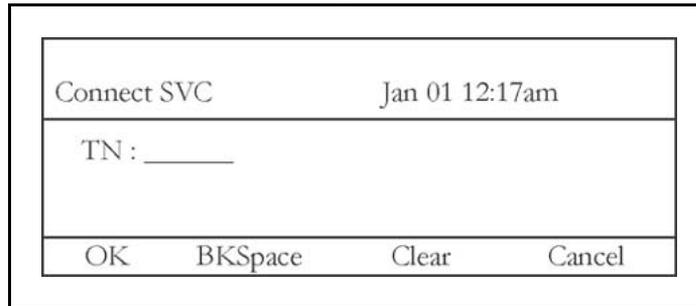
3   Wait for the default key map to download. The screen appears as shown in Figure 39 "Set-Based Installation Step 3" (page 144).

Figure 39
Set-Based Installation Step 3
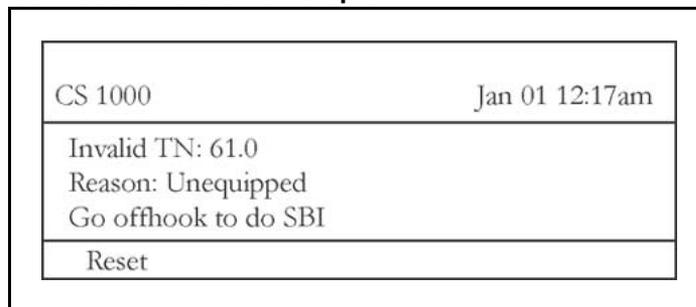
4   Lift the handset and listen for the continuous dial tone. The **Model** prompt is displayed as shown in Figure 40 "Set-Based Installation Step 4" (page 144).

Figure 40
Set-Based Installation Step 4
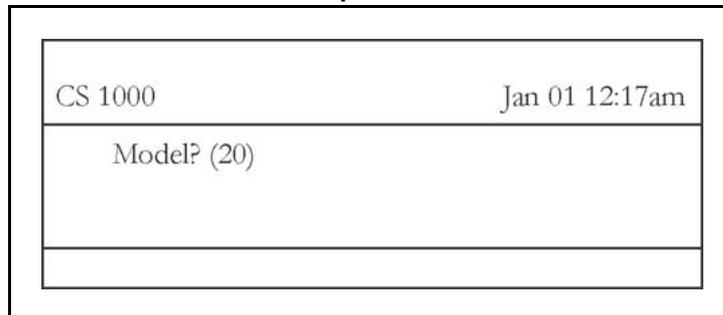
5   Press the **#** key to select the default model, or enter the model number and press **#**.

6   Listen for a special tone. The prompt appears as shown in Figure 41 "Set-Based Installation Step 6" (page 145). Enter the zone number as assigned in the branch zone data at the main office. Press **#**.

Figure 41
Set-Based Installation Step 6

CS 1000   Jan 01 12:17am

    OK, ZONE?(0)
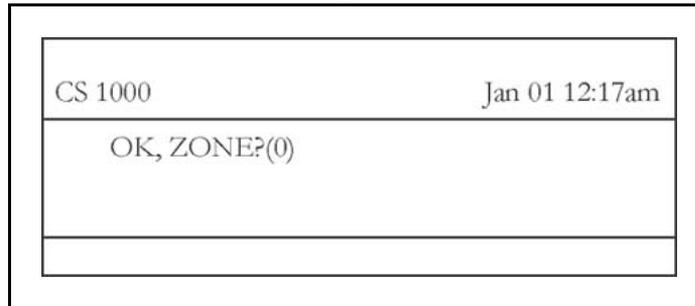
7   Enter the extension number as prompted by the screen shown in
, and press
#.
Figure 42
Set-Based Installation Step 7

CS 1000   Jan 01 12:17am

    OK, EXTENSION? 2244
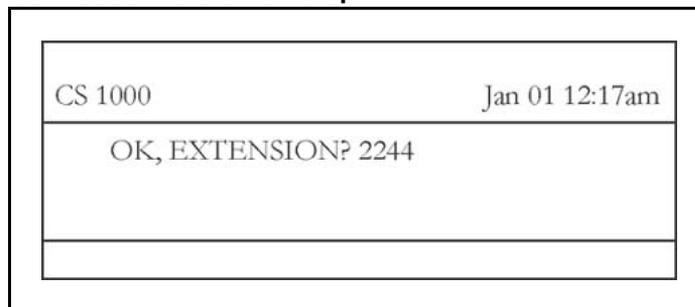
8   Replace the handset when you hear a relocation tone and see
"OK" on the screen display.

9   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 43
Set-Based Installation complete

CS 1000   Jan 01 12:17am

    Local Mode

Trans   Conf   Forward   More...
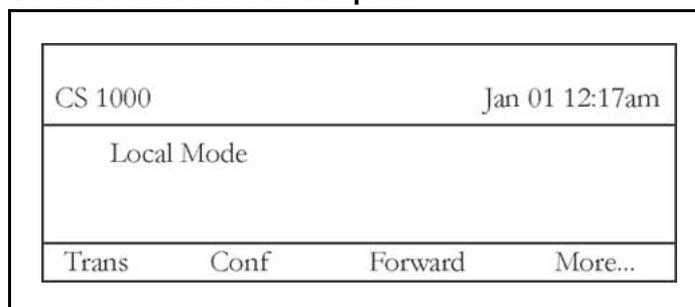
10   Test for survival functionality by making and receiving a call on
the telephone.

11 The telephone is now configured for basic operation and survivability. To configure the Branch User, see "Branch User Config" (page 146).

--End--

You must also configure the Set-Based Removal feature prompts SRCD (LD 15) and AREM (LD 57) by following Procedure 3 "Setting and changing the Station Control Password Configuration" (page 92).

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 141).

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 29 "Normal Operation troubleshooting" (page 193)).

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 44 "Options menu" (page 146).

Figure 44
Options menu
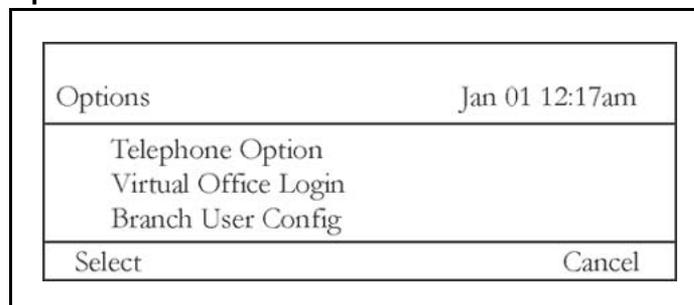
If an SCPW has been configured, "Password Admin" appears in the list as the second option, forcing the "Branch User Config" option to scroll out of sight. Use the navigation keys to scroll down to "Branch User Config".

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 either CSLS; format (four fields) or small system format (two fields). 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 91).

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 29 "Normal Operation troubleshooting" (page 193) 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 13
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 Virtual Office Login and Branch User Config options are displayed.

2 Select **Branch User Config**, as shown in Figure 51 "Options menu" (page 158).

3 Enter the Branch User ID, that is a dialable DN of the main office. See Figure 45 "Branch User ID" (page 148).

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 45
Branch User ID

```
┌─────────────────────────────────────────┐
│                                          │
│  ┌───────────────────────────────────┐   │
│  │ CS 1000              Jan 01 12:17am │  │
│  │                                    │   │
│  │   Enter Branch User ID:            │   │
│  │                                    │   │
│  │                                    │   │
│  └───────────────────────────────────┘   │
│   Select    Delete    Clear    Cancel    │
└─────────────────────────────────────────┘
```

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 46 "Branch password" (page 148).

Figure 46
Branch password

```
┌─────────────────────────────────────────┐
│                                          │
│  ┌───────────────────────────────────┐   │
│  │ CS 1000              Jan 01 12:17am │  │
│  │                                    │   │
│  │   Enter Branch Password:           │   │
│  │                                    │   │
│  │                                    │   │
│  └───────────────────────────────────┘   │
│   Select    Delete    Clear    Cancel    │
└─────────────────────────────────────────┘
```

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 CSLS; format (four fields), and press **Select**.

The default value is the Branch Office TN in CSLS; format (four fields). See Figure 47 "Main Office Terminal Number" (page 149), which shows an example of the display of a TN in small system format.

Figure 47
Main Office Terminal Number

```
CS 1000                              Jan 01 12:17am

    Enter Main Office TN:
    6 2   1 0


 Select      Delete        Clear        Cancel
```

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 48 "Main office password" (page
149).

Figure 48
Main office password

```
CS 1000                              Jan 01 12:17am

    Enter Main Office Password:



 Select      Delete        Clear        Cancel
```

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--

Transferring IP Phone data using TM 3.1

Provisioned data for MG 1000B IP Phones can be transferred directly from the main office to the branch office using TM BUID and MOTN values are then added. This transfer can be done by:

Using the Reports and Import Facility in TM

Step	Action
1	Create a report file to contain the exported station data:
	• In TM WebStation, choose **Telephones > Reports**.
	• In the Reports page, choose **Customize**.
2	Configure the report file in the Customize a Report page:
	• Under Field Selection, choose fields that have been configured in the IP Phone.
	• Under Custom Criteria, enter criteria **SYNCSTATUS = Transmitted**.
	• Under Report Format, choose **CSV**.
	• Under Format Options, enter a file name.
	• Under Save Report Definition, enter a report name.
	• Click **Save** to save the report configuration.
3	Generate the report file.
	• Under Site/System Selection, choose the main office system.
	• Click **View Data** to generate the report.
	• When prompted to Open or Save the file, click **Save**.

4   Create the import file.

- In a text editor, open the report file generated in Step 3.

- Add the fields MOTN and BUID to the end of first line, separating fields with commas.

- Add the values for MOTN and BUID to the end of the rest of the lines, separating fields with commas.

- Save the file.

5   Import the data:

- In TM Web Station, choose **Telephones > Import**.

- In the Import page, choose branch office Site – System and click **Import**.

- Select the import file created in Step 4 and click **OK**.

- Click **Close** in the Import Status window when the import process is done.

6   Verify the results:

- In the Import page, click **View Log** to check the details of each telephone imported.

- In TM WebStation, choose **Telephones > Search**.

- In the Search Telephones page, choose the **Branch Office Site – System**.

- Enter search criteria Sync Status = All and click **Search**.

- All the imported telephones are listed, click on a few telephones to verify the attributes.

- Select all the telephone(s) imported and click**Transmit** to synchronize with the PBX and test appropriately.

--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 or TM 3.1. 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 either 2 or 4-fields TN format) and then press the **Select** softkey.

Figure 49
Entry of Main Office TN
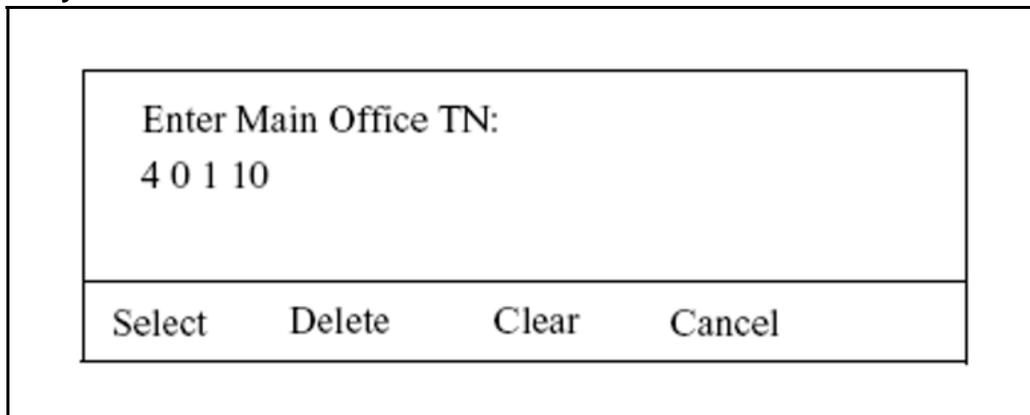
Validation of MOTN input from Branch User Config is limited to preliminary range checks. The input string is converted to a packed TN and the MOTN and MOTN type are set as either small or large system.

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 21
LD 11 Branch Office changes for Internet Telephones

Prompt	Responses	Description	Pkg#
REQ	NEW/CHG		
TYPE	2004P1, 2004P 2/2050PC, 205 0MC/2002P1,2 002P2/2001P2, 1110,1120,1140, 1150, 2007,2033	Internet telephones.	
CUST	<num>	Customer number.	
TN	c u , l s c u	With CS 1000 Release 5.0 MG 1000B with MGC, 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	c u , l s c u	Main Office TN The default is the Branch Office TN entered above, which for CS 1000 Release 5.0 MG 1000B with MGC, will be 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 50
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 for details on testing Local Mode functionality.

Procedure 14
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 3
"Setting and changing the Station Control Password Configuration" (page
92) 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 15 "Installing IP Phones through overlays" (page 155) describes
the general method of installing a Branch User IP Phone through LD 11.

> **ATTENTION**
> If the installation technician uses TM 3.1 or 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 15
Installing IP Phones through overlays

Step	Action
1	Configure the Branch Office zones and dialing plan. See Configuring the MG 1000B zone. 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 22
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.
	c u	Format for small system, Media Gateway 1000B, where c = card and u = unit.
ZONE	0-255	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 23
LD 11 Enable/disable Virtual Office (optional).

Prompt	Response	Description
REQ:	NEW CHG	Add new data, or change existing data.

Table 23
LD 11 Enable/disable Virtual Office (optional). (cont'd.)

Prompt	Response	Description
TYPE:	a...a	Terminal type. Type **?** for a list of possible responses.
CLS	(VOLA) VOLD	Allow Virtual Office operation from this TN. Deny Virtual Office operation from this TN.
CLS	VOUA	Allow Virtual Office login onto this TN using other telephone (destination of Virtual Office login).
	(VOUD)	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 .

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 .

--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 and to *IP Phones Fundamentals;* ((NN43001-368)) . You can also test the telephone. Refer to .

Changing the SCPW

Use to change the SCPW of a telephone at any time.

Procedure 16
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 17
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 51
Options menu


```
Options                        Jan 01 12:17am

    Telephone Option
    Virtual Office Login
    Test Local Mode

Select                               Cancel
```
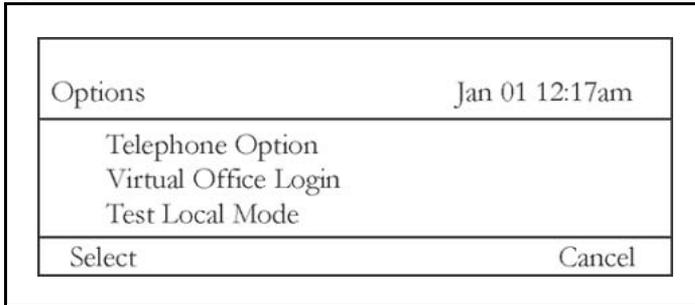
The Virtual Office Login option only appears if VOLA CLS is configured.

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 18
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 51 "Options menu" (page 158)).

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 52 "Virtual Office - logged in" (page 160).

Figure 52
Virtual Office - logged in
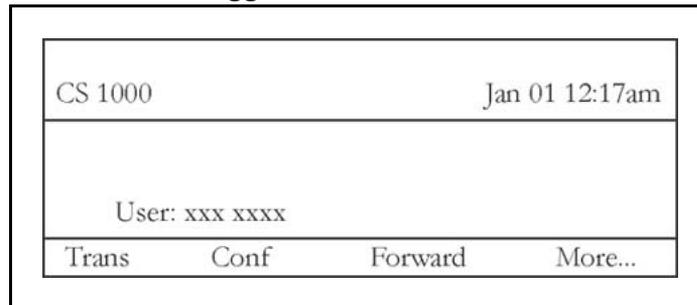
7   To log out of Virtual Office:

a   Press the **Services** key to display the Options menu.

b   Use the navigation keys to highlight Virtual Office Logout.

See Figure 53 "Virtual Office application menu" (page 160).

Figure 53
Virtual Office application menu
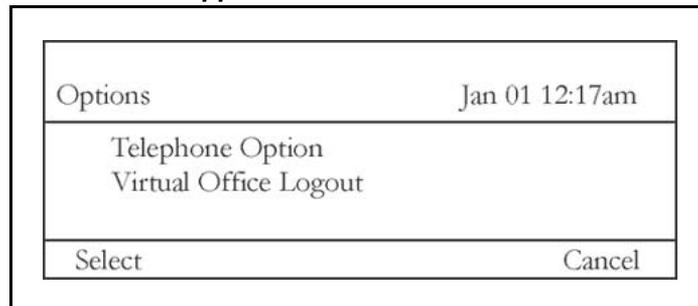
c   Press the **Select** soft key.

--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 54 "Virtual or Branch soft key display" (page 161)). The IP Phone is not operational in this mode. The user must log in to bring the IP Phone back into service.

Figure 54
Virtual or Branch soft key display
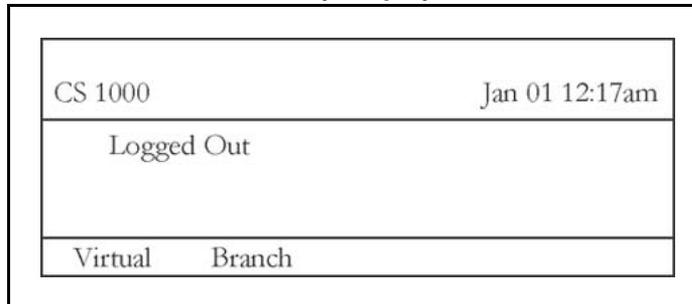
The Virtual and Branch soft keys are provided to reset the IP Phone to operational:

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 54 "Virtual or Branch soft key display" (page 161). 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 44 "Options menu" (page 146). 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 19
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, or TM 3.1, and is operating in Normal Mode.

1   Press the **Services** key (the key with the Globe icon).

The Options menu is displayed (see).

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 55
      Resume Normal Mode
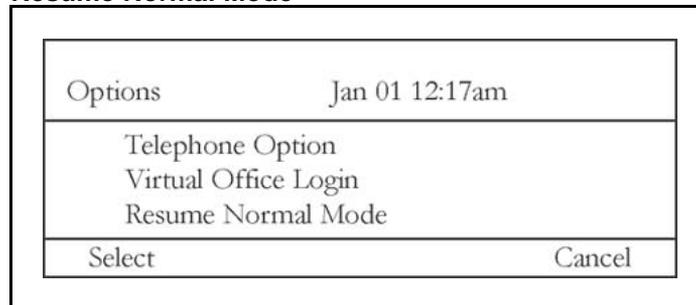
    The Virtual Office Login option only appears if VOLA CLS is configured.

    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 only when in Normal Mode.

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 *IP Line Fundamentals;* ((NN43100-500)) .

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 20
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:

- Set-Based Installation
- Overlays (locally or remotely through a modem or Ethernet connection). For more information, see Procedure 15 "Installing IP Phones through overlays" (page 155).
- TM 3.1

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:

- Set-Based Installation (not for M3900-series telephones)
- Overlays (locally or remotely through a modem or Ethernet connection). For more information, see Procedure 15 "Installing IP Phones through overlays" (page 155).
- TM 3.1

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.

Activating analog (500/2500-type) and digital telephones

Activate each telephone using the Automatic Set Configuration feature. This feature is described in . If the Branch Office is a converted small system, refer to *Communication Server 1000M and Meridian 1 Small System Installation and Commissioning* ((NN43011-310)) .

To program a telephone with the data feature, configure the Data Class of Service parameter in LD 11. Refer to *Software Input Output Administration;* ((NN43001-611)) .

Emergency Services configuration

Contents

This section contains information on the following topics:

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 21
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** 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.*

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 24
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
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 25
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.

Command	Description
	• 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.*

        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 26
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)-999	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

Table 26
LD 86 Configure Digit Manipulation Index. (cont'd.)

Prompt	Response	Description
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 27
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	CDP and BARS
	0-255	NARS
	0-999	FNP
ENTR	0-63	Entry number for NARS/BARS Route List
	0-6	Route List entry number for CDP
	X	Precede with X to remove
LTER	NO	Local Termination entry
ROUT		Route number
	0-511	Range for CSLS; and CS1000E; system
	0-127	Range for small system and Media Gateway 1000B
DMI	(0)-999	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 28
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

Table 28
LD 90 Configure ESN Special Number and Digit Manipulation. (cont'd.)

Prompt	Response	Description
	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.
…		
- RLI		Route List Index to be accessed
	0-127 0-255 0-999	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 1-999	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 22
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**.*

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 23
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 21 "Configuring the main office" (page 171), 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. Refer to Dialing plan configuration.

--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.*

Testing the number
Use Procedure 24 "Testing ESDN using an MG 1000B Telephone" (page 177) to test the ESDN number from any telephone in the Branch Office.

Procedure 24
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 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--

Element Manager ESA configuration

From Element Manager, you can configure ESA. From the **Zone List** window in Element Manager (see Branch Office-specific zone configuration), select the **Branch Office Emergency Service** option, and enter the necessary information. Refer to .

Figure 56
Zone Emergency Service Information

Managing: **192.167.100.3**
    IP Telephony » Zones » Zone 0 » Zone Emergency Service Information

Zone Emergency Service Information

Input Description	Input Value
Zone Number (ZONE):	0
Route number (ESA_ROUT):	▼
ESA Access Code (ESA_AC):	None (AC0) ▼

[Submit]   [Refresh]   [Cancel]

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).

To configure Emergency Service using SPN, follow the process outlined in Dialing plan configuration. 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 199) 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 57
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

Basic Emergency Services When VO Logged Out

Contents

Overview

Overview

Before the introduction of the Basic Emergency When VO Logged out feature, logged out phones could not be used for basic telephony function - making and receiving calls. The reason was that the basic telephony function was controlled by the central Call Server. The logged out phones were not registered with the Call Server and thus the user could not make and receive calls.

New functionality is introduced: to provide the ability for the logged out phone to make ESA calls and receive callbacks, temporarily register with the Call Server. The registration begins as the user tries to make a call from the logged out phone by going off hook or pressing the primary key, or using the handsfree or headset.

Making an ESA Call From a Logged Out Phone
The Call Server is provisioned with a pool of Emergency Terminal Numbers (TNs) referred to as Emergency Services Access Terminal Number (ESTN) in this document. The ESTN is allocated from this pool to register the logged out phone.

As the logged out phone registers with the Call Server using the allocated ESTN, the key presses are transmitted to the Call Server according to the existing operation, so the Call Server is fully responsible for initiating the call. The Call Server normally provides the dial tone and collects the digits.

The logged out phone can make ESA calls only. The configured ESTNs are fully restricted. As the Directory Number (DN) translation is complete, the Call Server checks the type of the DN and proceeds with the call only if an Emergency Services Access Directory Number (ESDN) or other locally routed emergency DNs as defined per ESA feature is dialed.

Scenario: Process Event In *VO Logout* State

Receiving ESA Callback
After the ESA call is complete (released by one of the parties), the logged out phone registers with the Call Server for a preconfigured period of time (20 minutes by default). During this time the phone continues to use the ESTN allocated for the ESA call.

The logged out phone can receive calls from any source during this period, which makes it possible to receive ESA callbacks from PSAP or local security service.

As the preconfigured time out is complete, the Call Server unregisters the phone. The phone moves to the original logged out state and the phone ESTN becomes available to other ESA calls from any other VO logged out phone.

ESA Call Processing

The ESA call from the logged out phone is processed in the same way as the ESA call from a normally registered phone. The information configured in the emergency TN block is provided to the OSN phone/terminal. This includes

- Name: *LoggedOut.*

- CPND block: uses the English string *VOLO* and is automatically configured against the primary key of all the emergency TNs.

- DES: All the emergency TNs have the *ESTN* designator.

- DN: The emergency DN configured by administrator. The primary DN, that is configured by the administrator, is sent to the OSN phone/terminal, so that callback to this phone is possible.

CLID Composition

In Release 4.5 and earlier, the CLID configuration is static. The static CLID entry is configured in LD 15 and associated with the phone in overlays 10 and 11.

Such a static CLID may not correctly identify the physical location of the logged out phone. The pool of emergency TNs is shared by all phones configured in the system, so any phone can use the same CLIDentry.

To identify the physical location of the logged out phone using its CLID, the *Location Auto Update* mechanism, introduced by the ESA Client Mobility feature is required.

ESA VO Logout Timer

A special *ESA VO Logout* timer is created for every logged out phone with the emergency TN allocated. The emergency TN is released and the phone returns to the original logged out state when this timer expires.

The timer is created and set to 60 seconds as soon as the emergency TN is allocated. The timer stops only after the user completes dialing the ESA number.

In other words, the user has a maximum of 1 minute to dial an ESA number. After the 1 minute, all key presses are lost and you must re-initiate the call. The ESA VO Logout Timer also includes the case when user dials a wrong number, in which they will receive overflow tone and *Release and try again message* on phone display.

The *Release and try again message* prevents the ESTN from abnormally remaining on the call server, for example, due to the accidental pressing the primary key or dropping the handset.

- The timer stops upon initiation of the ESA call (for example, while waiting for answer and connect phases).

- The timer restarts as the user completes the ESA call. The timer is set to a preconfigured period (20 minutes by default) so the user can receive a callback during that period.

- The timer restarts again if the user makes another ESA call.

- If the timer expires but the phone is involved in a call, the time out event is ignored. When this call is finished, the 20 minute timer reloads.

Provisioning, Administration and Maintenance

The Basic Emergency Services When VO Logged Out feature is provisioned like follows:

Step	Action
1	First, specify the number of emergency TNs in the pool and specify the range of the emergency pool in LD 24.
2	Then go to LD 11 and configure emergency TNs.
	Enter the new VOLO response for the type prompt. Very limited information is prompted for the ESTN (basically, only the DN used for the call is required).
	The system saves the VOLO TNs in a new, fully restricted data block similar to IP Phone 2001. Because these TNs are fully restricted to provide only one DN to access emergency numbers while the set is in VOLO state, Emergency TNs do not use up any user licences (ISMs).
3	Use LD 117 to print the used emergency TNs.
4	The *isetShow* command output displays if the logged out phone is registered with the Call Server, and uses emergency TN.
5	LD 32 idu command shows a different type of TN (VOLO) when queried.
6	LD 80 trak command shows a different type of TN (VOLO) when printing TN info.

--End--

Because the emergency TNs are stored with no features configured, the only primary key label downloaded to the logged out phone is for making a call. The soft keys, feature keys, and information area of the display are emptied as the set registers.

Keeping Logged Out State
The remote user, who logged on to the TN that the emergency call was made from, may go back to its home TN during this time. According to the existing functionality, this forces the logged out phone to reregister with its home TN as well.

The use case *Scenario: Keep Logged Out State* provides the requirement to prevent the logged out phone registered with the Call Server for ESA from reregistering.

When this scenario occurs, the VOLO phone will sustain it's *Awaiting Callback* state until the ESAVOLO timer expires, and returns to it's original *Logged Out* state, to give you the chance to go back to normal registration by using the soft key provided.

Configure ESA Data Block
Configure the VOLO BLOCK only for the lowest customer number. If you configure a low customer number after you configure the VOLO BLOCK for a higher customer, the number is not handled. The VO set cannot register as the configuration of the VOLO TN cannot occur in LD24 under such a situation. The VO set that tries to register in this case receives the prompt *Service Not Available*.

Because you can define the ESA data block for any customer, you can define the ESTN pool for any customer as well. The ESTN pool will only be required for customers that have access to the VO Login feature (lowest customer number for the time being).

Sysload
Scenario: Load ESA VO Logout Settings

- This scenario begins when the system starts loading the configuration database from disk

- The ESA VO Logout data configured in the Manage ESA Data and Manage ESTN Data scenarios.

Warm Start
An active call to or from PSAP survives a warm start. In *Awaiting Callback* state, the VOLO set will be able to register back to Call Server with the same VOLO TN. But since it will loose it's VOLO timer, and it is not

possible to distinguish between this situation and a first time registration, it is not possible to reload the timer. To avoid this scenario, the Signalling Server must deregister the phone and put it back to "Logged out" state.

Emergency Services For Client Mobility

The Emergency Services Access feature is composes a CLID that identifies the physical location of the logged phone. If a system is configured with an internal LIS server, the location update might not happen right after the set registers.

The call to PSAP occurs immediately after the set registers, requiring the correct location information; This is not desired. Special handling may be required, possibly by directly calling background LIS for the VOLO TN.

Active Call Fail Over

Interactions with Active Call Fail over can be considered under the following possible scenarios:

- ELAN failure happens for less than 10 minutes:
  — The ESA VOLO phone is on a call.

    The call must remain up since TPS keeps the set registered till 10 minutes. The TN synchronization after ELAN goes up must be completed without any errors.

  — ESA VOLO phone is in *Waiting to Callback* and *Awaiting Callback* status.

    The ESTN VOLO timer can expire during this period, causing the ESTN to be released. If the ELAN Signalling Server sends the TN online for the logged out phone with the TN previously used, that ESTN may already be assigned to another phone. The result can be unpredictable.

    To avoid this situation, the LTPS must move the phone to its original logged out state, and allow the Call Server to release the ESTN and its associated timer.

- ELAN/TLAN failure happens for more than 10 minutes when:
  — The ESA VOLO phone is on a call.

    As a result, the ACF timer or PSAP will release the call register. In this case, the ESA VOLO timer should be removed. Nevertheless, the active call should survive. The phone returns to its original logged out state, but according to ACF feature, the TPS closes

the audio path if the phone goes on-hook or you press the release button.

— ESA VOLO phone is in *Waiting to Callback* status.

This is the same as 2a case, when the phone looses it's ESTN info after reregistering and will go back to it's original logged out state. This needs additional implementation on Call Server to free up reserved ESTN and it's timer.

Context Sensitive Soft Keys

This will work for the original soft keys that came from Call Server, but there are two extra callers and redial soft keys that are added on the TPS. It needs an extra check on the TPS to prevent these two soft keys on a VOLO set.

Element Manager

Element Manager supports the following configuration, provisioning and maintenance aspects of the Basic Emergency Services When VO Logged Out Feature.

- Configuration: Changes in ESA data block in LD 24.
- Diagnostics: A new command PRT ESALO is added in LD 117.

Maintenance and diagnostics

Contents

This section contains information on the following topics:

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, and IP Phone 1150E. It does not apply to the IP Phone KEM, Expansion Module for IP Phone 1100 Series, IP SoftPhone 2050, WLAN 2210/2211 or SIP Phones.

Enhanced UNIStim Firmware Download for IP Phones

CS 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 (or the Media Card) 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 *IP Line Fundamentals* ((NN43100-500)) .

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 58 "Required firmware version" (page 191)).

Figure 58
Required firmware version
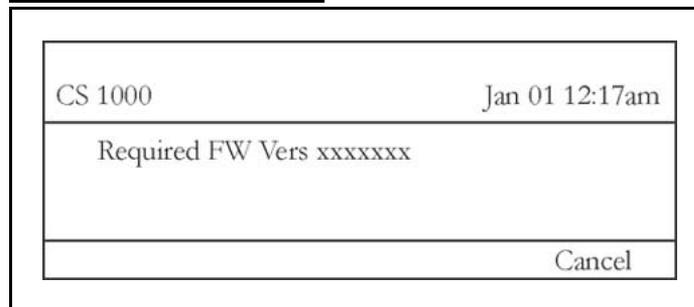
This figure shows a screen display from an IP Phone 2004. The display on another model of IP Phone may differ.

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.

Procedure 25
Upgrading firmware for CS 1000 Release 5.5

Step	Action

Upgrade procedures are generally found in the **Communication Server 1000E: Installation and Configuration NTP (NN43041-310)**. *Relevant information can be found in* **IP Line: Description, Installation, and Operation (NN43100-500)**.

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 FTP 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--

For Branch Office systems running CS 1000 Release 4.5 or CS 1000 Release 5.0 software, always upgrade the MG 1000B TPS before the main office TPS. Otherwise, the MG 1000B TPS does not have the required version of firmware for upgrading the telephone. The IP Phone stays in Local Mode with the required firmware files displayed (see). The system administrator has two options:

- Upgrade the firmware at the Branch Office, in which case the IP Phones are redirected to the main office after the upgrade.

- Issue the `isetResetAll` command on the MG 1000B Signaling Server maintenance terminal to redirect the IP Phones to the main office.

Procedure 26
Upgrading firmware for CS 1000 Release 4.5 or CS 1000 Release 5.0

Step	Action
1	At the Branch Office, upgrade the IP Phone firmware on the Signaling Server. For instructions to upgrade the IP Phone firmware on the Signaling Server, refer to *Communication Server 1000E: Upgrade Procedures (NN43041-458)* .
2	Issue the CLI command `umsUpgradeAll` at the Branch Office. IP Phones that are registered in Local Mode are upgraded.
3	At the main office, upgrade the firmware on the Signaling Server.
4	IP Phones registered to the main office are upgraded. MG 1000B telephones are redirected back to the TPS with the required version of firmware.

--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 inTable 31 "Branch appears on the telephone display, there can be more than one reason.

Table 29
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.
Local Mode 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.	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.

Table 29
Normal Operation troubleshooting (cont'd.)

Message	Probable Cause	Actions
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 30
Legend for LD 32 STAT command Login status

Number	Description
0	Initialize status
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)

Table 30
Legend for LD 32 STAT command Login status (cont'd.)

Number	Description
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 31
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.

Table 31
Branch User Config troubleshooting (cont'd.)

Message	Probable Cause	Actions
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 Password entered three times.	Wait one hour for the lock to clear automatically, or disable and enable the Main Office TN in LD 32 to clear the lockout.
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.

Table 31
Branch User Config troubleshooting (cont'd.)

Message	Probable Cause	Actions
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.
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.

Table 31
Branch User Config troubleshooting (cont'd.)

Message	Probable Cause	Actions
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 Installation and Commissioning* ((NN43001-312)) 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 32
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
	l s c u	Format for Large System and CS 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 21 "Configuring the main office" (page 171), step 5).

- If ESA is not enabled, the CLID is the same as the CLID entry composed in LD 15 (see Configuring ESN and MG 1000B zones, step 1).

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 (see Configuring the MG 1000B zone, Step 2).

Refer to *Emergency Services Access: Description and Administration (NN43001-613)* () for more information on this feature.

Print Branch Office zone information

LD 117 contains commands to view Branch Office zones at the main office Call Server.

Table 33
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>]	
	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 0-255	Print zone information for a specific zone.

Table 33
LD 117 Print zone information. (cont'd.)

Command	Description
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/disable Branch Office zone features

LD 117 contains commands to enable and disable features for the Branch Office zones.

Table 34
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 35
LD 117 Display zone status.

Command	Description
STAT ZONE [<Zone>]	
	Display zone status table
STAT ZBR [<Zone>]	
	Display status of Branch Office zones.

Change/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 toProactive Voice Quality management and *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 36
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 toProactive Voice Quality management and *Converging the Data Network with VoIP (NN43001-260).*

Table 37
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 Call Server or CP PM. This includes IP Phones registered by a Virtual Office and Branch Office logins at the main office Call Server. At the CP PM, inventory only includes IP Phones registered at the MG 1000B MGC, 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 161).

LD 117 contains inventory commands. These commands include the registered IP Phones.

Table 38
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 39
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

Appendix Preprogrammed data

Contents

This section contains information on the following topics:

Introduction

To install a CS 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.

This chapter contains the following preprogrammed data:

Passwords and codes

Table 40 "Passwords and codes" (page 206) lists each function and its default password or code. The user may be prompted to change the password upon first entry.

Table 40
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 CS 1000E to automatically configure telephones.

First digits

Table 41 "Default numbering plan First digit" (page 207) shows the default numbering plan for a Branch Office.

Table 41
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
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 CS 1000E system.

Important extension numbers

Table 42 "Default numbering plan important extension numbers" (page 208) lists important extension numbers.

Table 42
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."Flexible Feature Codes" (page 208) lists the FFCs for the CS 1000E system.

Table 43
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
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 MGC.Table 44 "Pre-configured SDI ports" (page 209) shows the default SDI port configuration. The value for "XX" is set on the faceplate of the CP PM.

Table 44
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 45
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 MGC) and programmed for Maintenance (MTC), Service Change (SCH), and BUG messages.

ESDI settings

Table 46 "ESDI settings" (page 209) lists the preset ESDI settings.

Table 46
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

Table 46
ESDI settings (cont'd.)

Setting	Code
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

shows preprogrammed trunk route information that you must have to activate and modify trunks.

Table 47
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

Table 47
Preprogrammed trunk route information (cont'd.)

Route	Type	Access Code	Mode	Interface
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

"System parameters" (page 211) provides the default system parameter values for the system.

Table 48
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;* ((NN43031-220)) 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 49
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
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

Table 49
Preprogrammed trunk route information (cont'd.)

Mode	Card	Model	Signaling	DIP or DTN	BIMP and TIMP
		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
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	-

Table 49
Preprogrammed trunk route information (cont'd.)

Mode	Card	Model	Signaling	DIP or DTN	BIMP and TIMP
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

Telephone models

Define four models (model# 20) for IP Phone 2001, IP Phone 2002, IP Phone 2004, IP Phone 1110, IP Phone 1120E, IP Phone 1140E, IP Phone 1150E, and IP Softphone 2050 with KEY 0 SCR, VOLA CLS, and VOUA CLS.

Define model# 20 for analog (500/2500-type) telephones.

Appendix
Branch Office engineering example

Contents

This section contains information on the following topics:

Introduction

This chapter provides sample engineering calculations for a Branch Office with a CS1000M; or CS1000E; main office.

The following abbreviations are used in formulas:

- IT = IP Phone

- AT = analog (500/2500-type) telephone

- MC = Media Card

Assumptions

Equipment characteristics
Assume the Branch Office has the equipment characteristics provided in "Equipment characteristics" (page 215).

Table 50
Equipment characteristics

Number	Type
120	IP Phones
36	Analog (500/2500-type) telephones

Traffic characteristics

Assume the Branch Office has the traffic characteristics provided in "Traffic characteristics" (page 216).

Table 51
Traffic characteristics

Number	Comments
6 CCS	For each IP Phone, 50% of calls go to other IP Phones, and 50% of calls go to analog (500/2500-type) telephones and PRI trunks.
5 CCS	For each analog (500/2500-type) telephone, 40% of calls go to PRI trunks, and 60% of calls go to IP Phones.
120 seconds	The average holding time for each call.

Conference traffic is generally 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% of IP Phone traffic), traffic should be included in the LAN/WAN bandwidth calculation.

Required calculations

The following is a summary of the required calculations:

- number of Virtual Trunks to the main office

- number of Media Cards

- real-time load for the Call Server

- bandwidth for WAN

- bandwidth for LAN

Calculations

Figure 59 "Branch Office traffic flow" (page 217) 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 59 "Branch Office traffic flow" (page 217).

Figure 59
Branch Office traffic flow
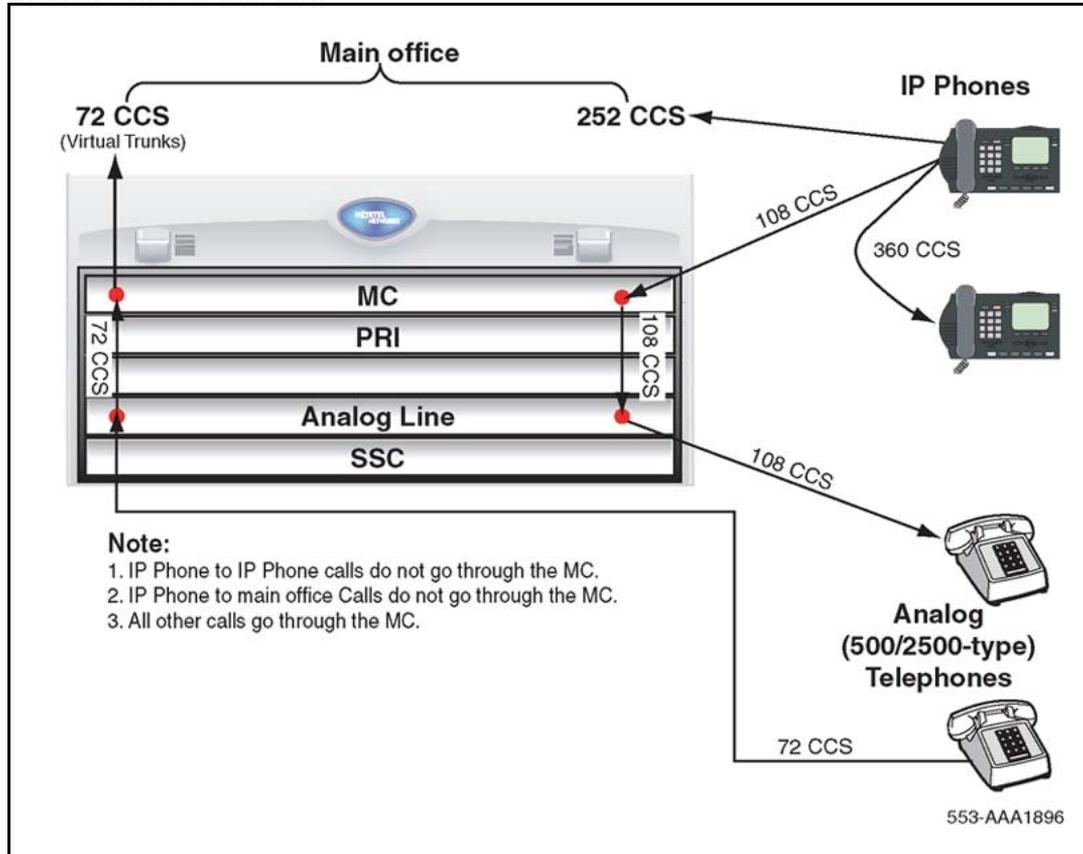
Procedure 27
Calculating traffic

Step	Action
1	Calculate the IP Phone to IP Phone traffic (intra-IP Phone traffic does not go through the MC):
	Total IT x IT CCS x % calls to Intra-IT calls = Intra-IT traffic
	120 x 6 x 0.5 = 360 CCS
2	Calculate the IP Phone traffic to analog (500/2500-type) telephones:
	Number of ATs x CCS for each AT x % of calls to ITs = IT traffic to analog (500/2500-type) telephones

36 x 5 x 0.6 = 108 CCS (this traffic is part of MC traffic)

3 Calculate the IP Phone traffic to main office resources (MOR):

Total ITs x IT CCS - Intra-IT traffic - IT traffic to analog (500/2500-type) telephones = IT traffic to MOR

120 x 6 - 360 - 108 = 252 CCS

4 Calculate the analog (500/2500-type) telephone traffic to Virtual Trunks (IPPT):

Number of ATs x CCS for each AT x % of calls to Virtual Trunks = Analog (500/2500-type) traffic to IPPT

36 x 5 x 0.4 = 72 CCS (this traffic is part of MC traffic)

This is the total IPPT traffic.

5 Calculate total IP traffic to the LAN:

a Total ITs x IT CCS + analog traffic to IPPT = Total CCS

120 x 6 + 72 = 792 CCS

b Total CCS ÷ 36 = Erlangs

792 ÷ 36 = 22 Erlangs

6 Calculate the MC traffic from analog (500/2500-type) telephones to IP Phones and Virtual Trunks:

IT traffic to analog (500/2500-type) telephones + Analog traffic to IPPT = MC traffic

108 + 72 = 180 CCS

--End--

MG 1000B Core and MG 1000B Expander requirements

shows the number of cards required and the devices on those cards.

Table 52
MG 1000B Core and MG 1000B Expander card type, number and devices

Card type	Number of cards	Devices on cards
MC	1	32 DSP channels
XALC	3	36 Analog (500/2500-type) telephones

One MG 1000B Core has four slots available, and an MG 1000B Expander is required for additional cards.

Requirement: one MG 1000B Core

An Analog Line card or Digital Line card has 16 ports. If 36 digital telephones are used instead of 36 analog (500/2500-type) telephones, the resulting calculation would yield the same number of cards: three XDLC cards, taking the place of three XALCs. The total number of card slots and MG 1000B Core requirements are the same.

Procedure 28
Calculating Call Server Loading

Step	Action

Only the CCS from one terminating end of a connection is used in the Call Server loading calculation. For example, a call from one IP Phone to another includes the CCS from both telephones. The Call Server loading calculation divides the CCS by two.

1   Calculate the IP Phone to IP Phone calls:

IT to IT CCS x 100 seconds ÷ average hold time ÷ 2 = IT to IT calls

360 x 100 ÷ 120 ÷ 2 = 150 calls

Dividing by 2 is only required for IT-to-IT traffic. Intra-IT CCS is double counted in relation to the number of calls. For example, one call lasting 100 seconds appears as one CCS on the originating telephone, one call on the CPU, and one CCS on the terminating telephone. Two CCS on telephones must be divided by two to get the correct number of calls.

2   Calculate the IP Phone to main office resources (MOR) calls:

IT to IT CCS x 100 seconds ÷ average hold time = IT to MOR calls

252 x 100 ÷ 120 = 210 calls

3   Calculate the IP Phone to analog (500/2500-type) telephones:

IT to AT CCS x 100 seconds ÷ average hold time = IT to AT calls

108 x 100 ÷ 120 = 90 calls

4   Calculate the analog (500/2500-type) telephone to Virtual Trunks (IPPT) calls:

AT to IT CCS x 100 seconds ÷ average hold time = AT to IPPT calls

72 x 100 ÷ 120 = 60 calls

5   Calculate the Call Server loading in EBC:

IT to IT calls x (1+f1) + IT to MOR calls x (1+f2) + IT to AT calls x (1+f3) + AT to IPPT calls x (1+f4) = Call Server EBC

150 x 2.15 + 210 x 1.68 + 90 x 1.48 + 60 x 1.18 = 879.3 EBC

6   Calculate the Call Server loading in percent:

Call Server loading ÷ CS maximum EBC = % loading

879.3 ÷ 35000 = 3%

Requirement: The loading of this configuration for Call Server is very low at 3%. This Call Server can be located at the Branch Office or anywhere within the zone.

--End--

Appendix
On-net dialing plan configuration examples

Contents

This section contains information on the following topics:

Introduction

This section contains configuration examples for the following on-net (or private) dialing plans:

- Figure 60 "Coordinated Dialing Plan (CDP)" (page 222)
- Figure 61 "Uniform Dialing Plan (UDP)" (page 226)
- Figure 62 "Group Dialing Plan (GDP)" (page 232)
- "Transferable DN" (page 239)

The configuration examples in this chapter are for an H.323 system, using only the H.323 Gatekeeper in the NRS. Configuration of a SIP system with a SIP Redirect Server, whether alone or with an H.323 Gatekeeper, is similar.

Coordinated Dialing Plan

Figure 60 "Coordinated Dialing Plan (CDP)" (page 222) shows a sample Coordinated Dialing Plan (CDP) configuration.

Figure 60
Coordinated Dialing Plan (CDP)
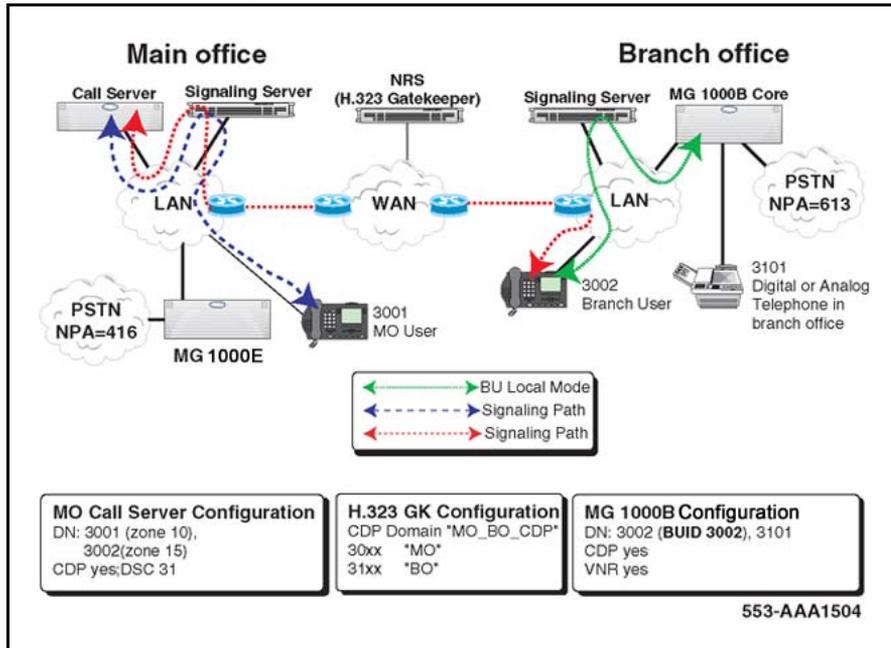
Call Scenarios
This section describes the following call scenarios, all based on Figure 60 "Coordinated Dialing Plan (CDP)" (page 222):

- "*From main office to Branch Office*" (page 222)

- "*From Branch Office to main office*" (page 223)

- "*When the Branch User telephone is in Local Mode*" (page 223)

From main office to Branch Office   In this scenario, the following occurs:

- DN 3001 (in the main office) or 3002 (in the Branch Office) dials DN 3101 (a TDM telephone in the MG 1000B).

- The main office Call Server recognizes the first two digits "31" as a CDP DSC. It accesses the RLI appropriate for that steering code and uses the Virtual Trunk specified for that route.

- The NRS is queried for a destination node IP address with which to route the call over the Virtual Trunk. Because "31" is registered with the Branch Office, the Branch Office node IP address is returned.

- The MG 1000B Core terminates the incoming Virtual Trunk call to DN 3101.

- The Voice Gateway channel in the Branch Office provides IP-TDM transcoding.

From Branch Office to main office   In this scenario, the following occurs:

- DN 3101 (in the Branch Office) dials DN 3001 (or 3002 - both are registered with the main office).

- The Branch Office recognizes 3001 as a vacant number. Since VNR is enabled, the call is routed using the RLI defined for VNR, using the Virtual Trunk specified for that route.

- The NRS is queried for the destination node IP address with which to route the call over the Virtual Trunk. Because "30" is registered to the main office, the main office node IP address is returned.

- The main office Call Server terminates the incoming Virtual Trunk call to DN 3001 (or 3002).

- The Voice Gateway channel in the Branch Office provides IP-TDM transcoding.

When the Branch User telephone is in Local Mode   In this scenario, the following occurs:

- The MG 1000B Core handles the call processing of DN 3002.

- If no network outage or Signaling Server/NRS failure occurs, DN 3002 can call any telephone in the Branch Office and main office.

- However, DN 3002 cannot be reached from the main office by using CDP, because the DN is not registered at the main office as it would be in Normal Mode.

Configuration example
Main office   To configure CDP at the main office, do the following:

Step	Action
1	Configure ESN Control Block for CDP.

```
>LD 86
REQ NEW
CUST 0
FEAT ESN
CDP YES
MXSC 50
NCDP 4
DLTN YES
```

2   Configure CDP Distant Steering Code

```
>LD 87
REQ NEW
CUST 0
FEAT CDP
TYPE DSC
DSC 31
FLEN 4
RLI 12
```

Refer to *IP Peer Networking Installation and Commissioning* ((NN43001-313)) for more information.

--End--

NRS configuration   To configure the NRS, do the following:

Step	Action
1	Create CDP Domain: "MO_BO_CDP".
2	Create H.323 endpoints: "MO", "BO".
3	Create Numbering Plan entries in CDP Domain:
	a Add "31" for endpoint "BO".
	b Add "30" for endpoint "MO".

--End--

Refer to *IP Peer Networking Installation and Commissioning* ((NN43001-313)) for more information.

Branch Office   To configure CDP at the Branch Office, do the following:

Step	Action
1	Configure ESN Control Block for CDP

```
>LD 86
REQ NEW
CUST 0
FEAT ESN
CDP YES
MXSC 50
NCDP 4
DLTN YES
```

2	Configure Branch User.

```
> LD 11
REQ: NEW
TYPE: 2004P1, 2004P2
TN 61 0
CUST 0
BUID 3002
```

--End--

Refer to Procedure 15 "Installing IP Phones through overlays" (page 155) and *IP Peer Networking Installation and Commissioning* ((NN43001-313)) for more information.

Uniform Dialing Plan

Figure 61 "Uniform Dialing Plan (UDP)" (page 226) shows a sample Uniform Dialing Plan (UDP) (Access Code + LOC + DN) configuration.

Figure 61
Uniform Dialing Plan (UDP)
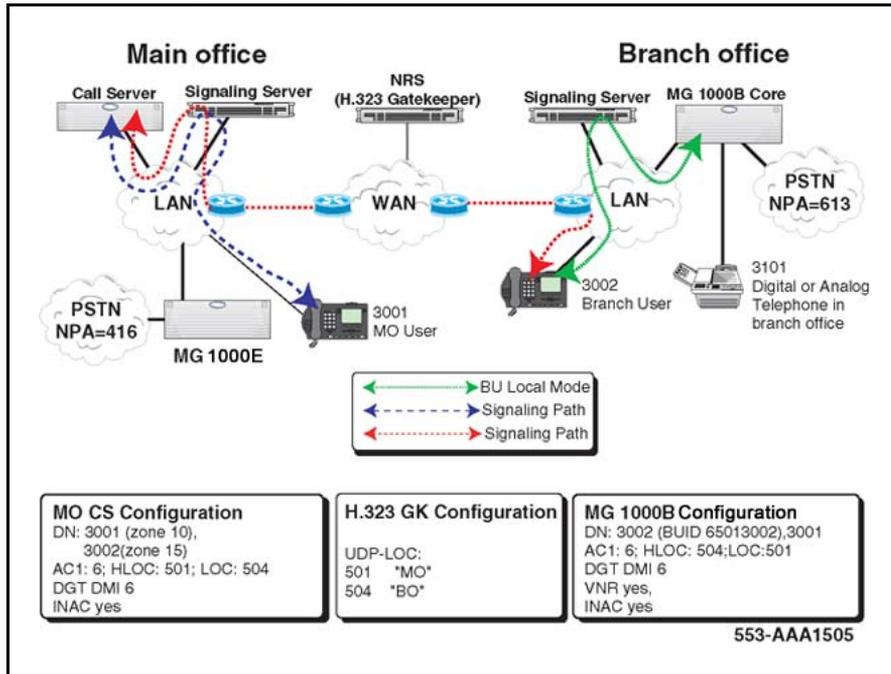
Call Scenarios

This section describes the following call scenarios, all based on Figure 61 "Uniform Dialing Plan (UDP)" (page 226):

- "*From main office to Branch Office*" (page 226)

- "*From Branch Office to main office*" (page 227)

- "*When the Branch User telephone is in Local Mode*" (page 227)

From main office to Branch Office
In this scenario, the following occurs:

- DN 3001 or 3002 dials DN "65043101" (a digital telephone in the Branch Office).

- The main office Call Server recognizes the digit "6" as AC1 and the digits "504" as LOC. It accesses the associated RLI and uses the defined Virtual Route and Virtual Trunk.

- The NRS is queried for the destination node IP address with which to route the call over the Virtual Trunk. Because "504" is registered to the Branch Office, the Branch Office node IP address is returned for "ESN 504 3101".

- The MG 1000B Core terminates the incoming Virtual Trunk call to DN 3101, since "504" matches the HLOC of the Branch Office.

- The Voice Gateway channel in the Branch Office provides IP-TDM transcoding.

From Branch Office to main office
In this scenario, the following occurs:

- DN 3101 dials DN "65013001" (or "65013002").

- The MG 1000B Core recognizes the first digit "6" as AC1. It accesses the RLI appropriate for the LOC of "501" and uses the Virtual Trunk specified for that route.

- The NRS is queried for a destination node IP address with which to route the call over the Virtual Trunk. Because "501" is registered to the main office, the main office node IP address is returned.

- The main office Call Server terminates the incoming Virtual Trunk call to DN 3001 (or 3002) because "501" matches the HLOC of the main office.

- The Voice Gateway channel in the Branch Office provides IP-TDM transcoding.

When the Branch User telephone is in Local Mode
In this scenario, the following occurs:

- The MG 1000B Core handles the call processing of DN 3002.

- If no network outage or Signaling Server/NRS failure occurs, DN 3002 can still make and receive a call to or from any telephone in the Branch Office or main office using UDP.

- However, dialed in/out digits are different from those used in Normal Mode because the LOC is changed. For example:

    — DN 3001 can call DN 3002 by dialing "65043002", instead of the "3002" dialed in Normal Mode.

    — DN 3101 can call DN 3002 by dialing "3002", instead of the "65013002" dialed in Normal Mode.

    — DN 3002 can call DN 3001 by dialing "65013001", instead of the "3001" dialed in Normal Mode.

    — DN 3002 can call DN 3101 by dialing "3101", instead of the "65043101" dialed in Normal Mode.

Configuration example

Main office

To configure UDP at the main office, do the following:

Step	Action
1	Configure ESN Control Block for UDP.

```
>LD 86
REQ NEW
CUST 0
FEAT ESN
AC1 6
```

2	Configure Digit Manipulation (DGT).

```
>LD 86
REQ NEW
FEAT DGT
DMI 6
DEL 3
```

3	Configure UDP LOC.

```
>LD 90
REQ NEW
FEAT NET
TRAN AC1
TYPE LOC
LOC 504
FLEN 7
RLI 12
LDN 0
```

4	Configure UDP HLOC.

```
>LD 90
REQ NEW
FEAT NET
TRAN AC1
TYPE HLOC
HLOC 501
DMI 6
```

5	Configure HLOC in Customer Data Block.

```
>LD 15
REQ: CHG
TYPE: CDB
NET_DATA YES
ISDN YES
CLID YES
ENTRY <xx>
HLOC 501
```

6   Configure Virtual Trunk route.

```
>LD16
REQ NEW
TYPE RDB
CUST 00
ROUT 120
DES VTRKNODE51
TKTP TIE
VTRK YES
ZONE 101
NODE 51
PCID H323
ISDN YES
MODE ISLD
DCH 12
IFC SL1
INAC YES
```

--End--

Refer to *IP Peer Networking Installation and Commissioning*
((NN43001-313)) for more information.

NRS configuration
To configure the NRS, do the following:

Step	Action

1   Create H.323 endpoints: "MO", "BO".

2   Create Numbering Plan entries.

    a   Choose type "UDP-LOC".

    b   Add "504" for endpoint "BO".

    c   Add "501" for endpoint "MO".

--End--

Refer to *IP Peer Networking Installation and Commissioning* ((NN43001-313)) for more information.

Branch Office
To configure UDP at the Branch Office, do the following:

Step	Action
1	Configure ESN Control Block for UDP.

```
>LD 86
REQ NEW
CUST 0
FEAT ESN
AC1 6
```

2	Configure Digit Manipulation.

```
>LD 86
REQ NEW
FEAT DGT
DMI 6
DEL 3
```

3	Configure UDP LOC.

```
>LD 90
REQ NEW
FEAT NET
TRAN AC1
TYPE LOC
LOC 501
FLEN 7
RLI 1
LDN 0
```

4	Configure UDP HLOC.

```
>LD 90
REQ NEW
FEAT NET
TRAN AC1
TYPE HLOC
HLOC 504
DMI 6
```

5	Configure HLOC in Customer Data Block.

```
>LD 15
REQ: CHG
TYPE: CDB
NET_DATA YES
ISDN YES
CLID YES
ENTRY <xx>
HLOC 50
```

6   Configure Branch User.

```
>LD 11
REQ: NEW
TYPE: 2004P1, 2004P2
TN 61 0
CUST 0
BUID 65013002
```

7   Configure Virtual Trunk Route

```
>LD 16
REQ NEW
TYPE RDB
CUST 00
ROUT 120
DES VTRKNODE53
TKTP TIE
VTRK YES
ZONE 104
NODE 53
PCID H323
ISDN YES
MODE ISLD
DCH 12
IFC SL1
INAC YES
```
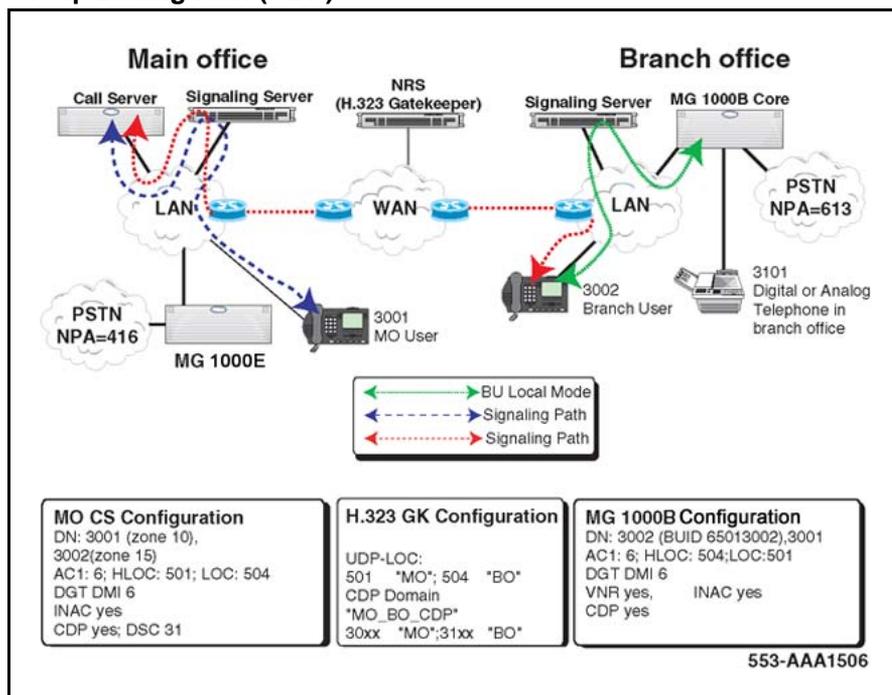
Refer to Procedure 15 "Installing IP Phones through overlays" (page 155) and *IP Peer Networking Installation and Commissioning* ((NN43001-313)) for more information.

--End--

Group Dialing Plan

Figure 62 "Group Dialing Plan (GDP)" (page 232) shows a sample Group Dialing Plan (GDP) configuration.

Figure 62
Group Dialing Plan (GDP)

Call Scenarios

This section describes the following call scenarios, all based on Figure 62 "Group Dialing Plan (GDP)" (page 232):

- "*From main office to Branch Office using CDP*" (page 232)

- "*From main office to Branch Office using UDP-LOC*" (page 233)

- "*From Branch Office to main office using CDP*" (page 233)

- "*From Branch Office to main office using UDP-LOC*" (page 234)

- "*Branch User telephone (DN 3002) is in Local Mode*" (page 234)

From main office to Branch Office using CDP
In this scenario, the following occurs:

- DN 3001 or 3002 dials a number "3101".

- The main office Call Server recognizes the digits "31" as a CDP DSC. The Call Server accesses the RLI appropriate for that DSC and uses the Virtual Trunk specified for that route.

- The NRS is queried for a destination node IP address with which to route the call over the Virtual Trunk. Because "31" is registered to the Branch Office, the Branch Office node IP address is returned.

- The MG 1000B Core terminates the incoming Virtual Trunk call to DN 3101.

- The Voice Gateway channel in the Branch Office provides IP-TDM transcoding.

From main office to Branch Office using UDP-LOC
In this scenario, the following occurs:

- DN 3001 or 3002 dials a number "65043101".

- The main office Call Server recognizes the digit "6" as AC1. The Call Server accesses the RLI appropriate for the LOC "504" and uses the Virtual Trunk specified for that route.

- The NRS is queried for a destination node IP address with which to route the call over the Virtual Trunk. For "ESN 504 3101", the Branch Office node IP address is returned since "504" is registered to the Branch Office.

- The MG 1000B Core terminates the incoming Virtual Trunk call to DN 3101 because "504" matches the HLOC of the Branch Office.

- The Voice Gateway channel in the Branch Office provides IP-TDM transcoding.

From Branch Office to main office using CDP
In this scenario, the following occurs:

- DN 3101 dials a number "3001"(or "3002").

- The MG 1000B Call Server recognizes the number as a vacant number. Because VNR is enabled, it uses the Virtual Trunk specified for that route according to the RLI defined for VNR.

- The NRS is queried for a destination node IP address with which to route the call over the Virtual Trunk. The main office IP address is returned because "30" is registered to the main office.

- The main office Call Server routes the incoming Virtual Trunk call to DN 3001 (or 3002).

- The Voice Gateway channel in the Branch Office provides IP-TDM transcoding.

From Branch Office to main office using UDP-LOC
In this scenario, the following occurs:

- DN 3101 dials a number "65013001"(or "65013002").

- The MG 1000B Core recognizes the first digit "6" as AC1. The MG 1000B Core accesses the RLI appropriate for LOC "501" and uses the Virtual Trunk specified for that route.

- The NRS is queried for a destination node IP address with which to route the call over the Virtual Trunk. The main office node IP address is returned because "501" is registered to the main office.

- The main office Call Server terminates the incoming Virtual Trunk call to DN 3001 (or 3002) because "501" matches the HLOC of the main office.

- The Voice Gateway channel in the Branch Office provides IP-TDM transcoding.

Branch User telephone (DN 3002) is in Local Mode
In this scenario, the following occurs:

- The MG 1000B Core handles the call processing of DN 3002.

- If no network outage or Signaling Server/NRS failure occurs, DN 3002 can still make or receive a call to or from any telephones in the Branch Office and main office using UDP. However, DN 3002 cannot be reached from the main office by using CDP. Refer to Local Mode scenarios for CDP ("*When the Branch User telephone is in Local Mode*" (page 223)) and UDP .

- By having UDP and CDP working together, GDP provides the convenience of CDP and the flexibility of UDP.

Configuration example
Main office
To configure GDP at the main office, do the following:

Step	Action
1	Configure ESN Control Block for CDP and AC1.

```
>LD 86
REQ NEW
CUST 0
FEAT ESN
CDP YES
MXSC 50
NCDP 4
AC1 6
DLTN YES
```

2   Configure Digit Manipulation.

```
>LD 86
REQ NEW
FEAT DGT
DMI 6
DEL 3
```

3   Configure Route List Block (RLB). For more information, refer to Configuring ESN and MG 1000B zones.

```
>LD 86
REQ NEW
FEAT RLB
RLI 12
ENTR 0
ROUT 120
DMI 0
```

4   Configure CDP Distant Steering Code (DSC).

```
>LD 87
REQ NEW
CUST 0
FEAT CDP
TYPE DSC
DSC 31
FLEN 4
RLI 12
```

5   Configure UDP LOC.

```
>LD 90
REQ NEW
FEAT NET
TRAN AC1
TYPE LOC
LOC 504
FLEN 7
RLI 12
LDN 0
```

6   Configure UDP HLOC.

```
>LD 90
REQ NEW
FEAT NET
TRAN AC1
TYPE HLOC
HLOC 501
DMI 6
```

7   Configure HLOC in CDP.

```
>LD 15
REQ: NEW
TYPE: CDB
NET_DATA YES
ISDN YES
CLID YES
ENTRY <xx>
HLOC 501
```

8   Configure Virtual Trunk Route.

```
>LD 16
REQ NEW
TYPE RDB
CUST 00
ROUT 120
DES VTRKNODE51
TKTP TIE
VTRK YES
ZONE 101
NODE 51
PCID H323
ISDN YES
MODE ISLD
DCH 12
IFC SL1
INAC YES
```

--End--

Refer to Configuring ESN and MG 1000B zones in this document and
IP Peer Networking Installation and Commissioning ((NN43001-313)) for
more information.

NRS configuration
Configure the following in the NRS:

- CDP domain: "MO_BO_CDP"

- H.323 endpoints: "MO", "BO"

- Numbering Plan entries

  — in CDP domain "MO_BO_CDP"

    – add "31" for endpoint "BO"

    – add "30" for endpoint "MO"

  — for type "UDP-LOC"

    – add "504" for endpoint "BO"

    – add "501" for endpoint "MO"

Refer to *IP Peer Networking Installation and Commissioning*
((NN43001-313)) for more information.

Branch Office
To configure GDP at the Branch Office, do the following:

Step	Action
1	Configure ESN Control Block for CDP and AC1.

```
>LD 86
REQ NEW
CUST 0
FEAT ESN
CDP YES
MXSC 50
NCDP 4
AC1 6
DLTN YES
```

2	Configure Digit Manipulation.

```
>LD 86
REQ NEW
FEAT DGT
DMI 6
DEL 3
```

3	Configure UDP LOC.

```
>LD 90
REQ NEW
FEAT NET
TRAN AC1
TYPE LOC
LOC 501
FLEN 7
RLI 1
LDN 0
```

4   Configure UDP LOC.

```
>LD 90
REQ NEW
FEAT NET
TRAN AC1
TYPE HLOC
HLOC 504
DMI 6
```

5   Configure HLOC in CDP.

```
>LD 15
REQ: CHG
TYPE: CDB
NET_DATA YES
ISDN YES
CLID YES
ENTRY <xx>
HLOC 504
```

6   Configure Branch User.

```
>LD 11
REQ: NEW
TYPE: 2004P1, 2004P2
TN 61 0
CUST 0
BUID 65013002
```

7   Configure Virtual Trunk Route.

```
>LD 16
REQ NEW
TYPE RDB
CUST 00
ROUT 120
DES VTRKNODE53
TKTP TIE
VTRK YES
ZONE 104
NODE 53
PCID H323
ISDN YES
MODE ISLD
DCH 12
IFC SL1
INAC YES
```

--End--

Refer to Procedure 15 "Installing IP Phones through overlays" (page 155) in this document and *IP Peer Networking Installation and Commissioning* ((NN43001-313)) for more information.
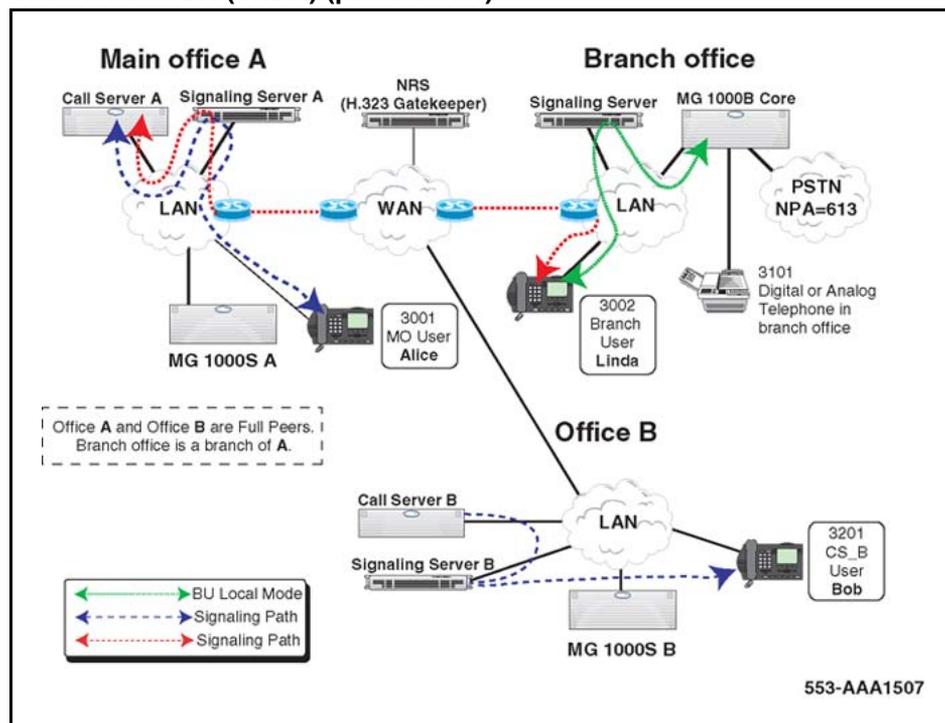
Transferable DN

Overview
Transferable DN (TNDN) allows a user to retain their DN when they move to a different office, whether the new "office" is a Branch Office or a full peer.

Original configuration (pre-transfer) Figure 63 "Transferable DN (TNDN) (pre-transfer)" (page 240) shows a sample of a TNDN configuration before the move.

Figure 63
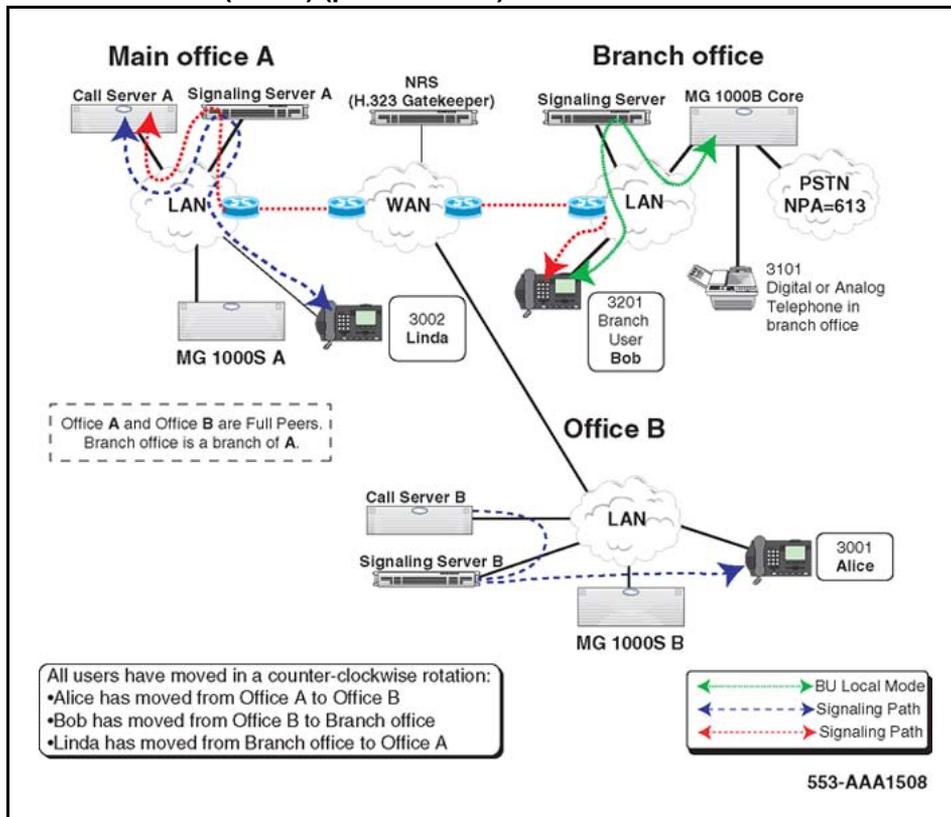**Transferable DN (TNDN) (pre-transfer)**

The components are configured as follows:

- Main office Call Server A
  — DN: 3001 (zone 10), 3002 (zone 15)
  — VNR: YES

- Call Server B
  — DN: 3201 (zone 20)
  — VNR: YES

- MG 1000B Call Server
  — DN: 3002 (zone 15, BUID 3002), 3101
  — VNR: YES

- NRS
  — CDP Domain "TNDN"
  — 3001 "MO"
  — 3002 "MO"
  — 3101 "BO"
  — 3201 "CS_B"

The Move   Alice is transferred from main office A to Office B. Bob is transferred from Office B to the Branch Office. Linda is transferred from the Branch Office to main office A. All three users want to keep their existing telephone numbers.

New configuration (post-transfer)   The TNDN configuration after the transfer is shown in Figure 64 "Transferable DN (TNDN) (post-transfer)" (page 241).

Figure 64
Transferable DN (TNDN) (post-transfer)

After the transfer, the components are configured as follows:

- Main office Call Server A
  — DN: 3002 (zone 10), 3201 (zone 15)
  — VNR: YES
- Call Server B
  — DN: 3001 (zone 20)
  — VNR: YES
- MG 1000B Call Server

— DN: 3201 (zone 15, BUID 3201), 3101

— VNR: YES

- NRS

  — CDP Domain "TNDN"

  — 3001 "CS_B"

  — 3002 "MO"

  — 3101 "BO"

  — 3201 "MO"

Call Scenario
The following is a general example of a call scenario after the move has occurred, based on :

- Alice (at Office B) calls Bob (at the Branch Office) by dialing DN 3201.

- The Call Server of Alice's current office (Office B) recognizes 3201 as a vacant number. VNR is enabled, so according to the RLI defined for VNR, it uses the Virtual Trunk specified for that route.

- The NRS is queried for a destination node IP address with which to route the call over the Virtual Trunk. Because the NRS has been updated to reflect the current location of "3201", the corresponding node IP address of main office A is returned.

- The Destination Call Server terminates the incoming Virtual Trunk call to DN 3201.

Configuration for TNDN
To configure TNDN, do the following:

Step	Action
1	Configure VNR. VNR must be enabled at all Call Servers and MG 1000B SSCs. ``` >LD 15 REQ: CHG TYPE: CDB NET_DATA YES VNR YES RLI 12 ```
2	Remove the TN at Office A when the user has moved from office A to office B.

```
>LD 11
REQ: OUT
TYPE: 2004P1, 2004P2
TN 61 0
```

3 Add the new TN at Office B using a new telephone with the same DN.

```
>LD 11
REQ: NEW
TYPE: 2004P1, 2004P2
TN 62 8
```

4 Configure the NRS as follows:

a CDP Domain: "TNDN".

b H323 endpoints: "MO", "BO", "Call Server_B"

c Numbering Plan Entry: In CDP domain "TNDN", keep the configuration updated to reflect the current location of the DNs.

--End--

Refer to *IP Peer Networking Installation and Commissioning* ((NN43001-313)) for more information.

Appendix
Off-net dialing plan configuration example

Contents

This section contains information on the following topics:

Introduction

This section contains an example of how to configure a dialing plan for a call from a Branch User in Normal Mode to the local PSTN. This example will walk you through the steps outlined in Dialing plan configuration.

The configuration example in this chapter is for an H.323 system, using only the H.323 Gatekeeper in the NRS. Configuration of a SIP system with a SIP Redirect Server, whether alone or with an H.323 Gatekeeper, is similar.

Call scenario

shows the call scenario for the example.

Figure 65
Off-net dialing plan example - call scenario.
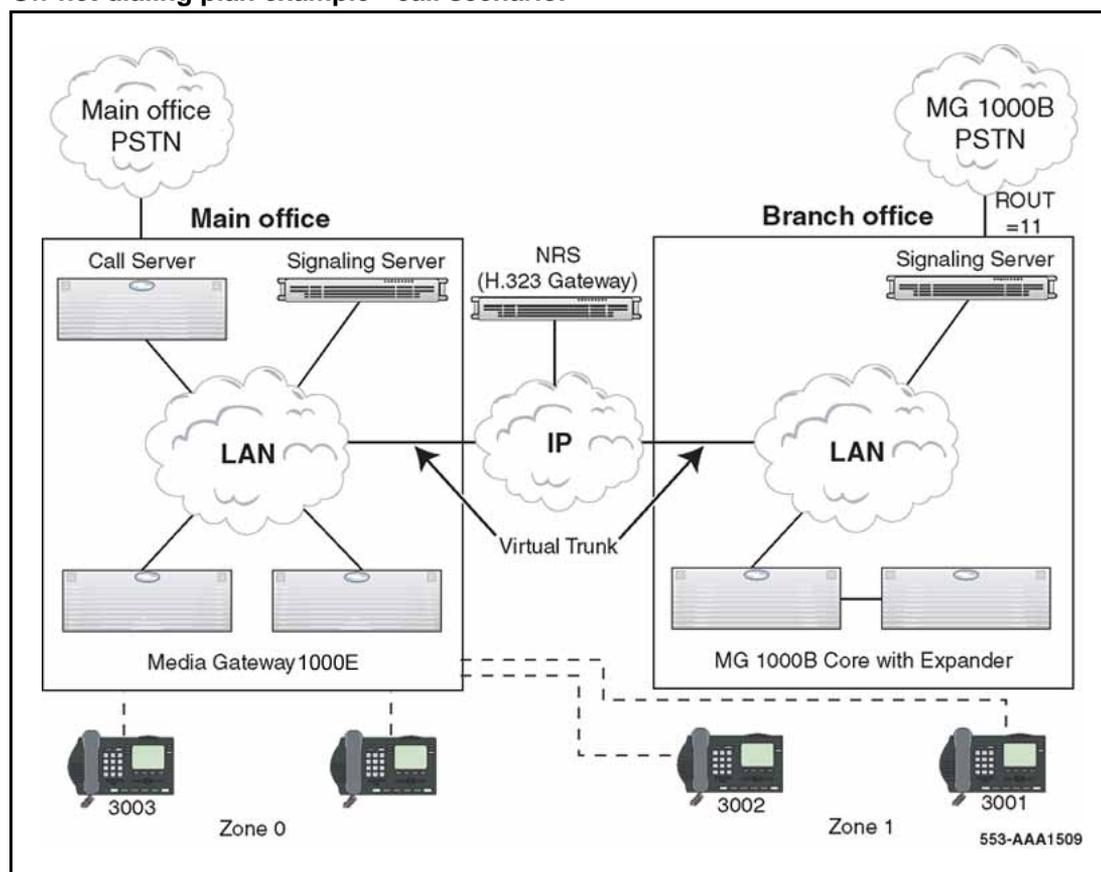
Provisioning
Main office

At the main office Call Server, the following is provisioned:

- AC1 = 1, and AC2 = 2
  ```
  >LD86REQ PRTCUST 0FEAT ESN
  MXLC 50
  ...
  NCDP 4
  AC1 1
  AC2 2
  DLTN YES
  ...
  TGAR NO
  ```

- For Zone 1, ZACB = ALL, and ZDP = 101
  ```
  >LD 117
  => PRT ZACB 1
  ```

```
_____|
| | Access Code Behavior || Zone |State|-----------------
---------------|| | | | | | Dialed | New || # DES | | DC1 | DC2
| DC3 | AC | AC ||------------------------------------------
--------------- || 1 BRANCH_ZONE | ENL | 101 | | | ALL | AC1
||------------------------------------------------------ |
Number of Zones configured = 2
=>
```

- DMI = 10, with DEL = 0 and CTYP = INTL

  ```
  >LD86REQ PRTCUST 0FEAT DGTDMI 10
  DMI 10
  DEL 0
  ISPN YES
  CTYP SPN
  ```

- RLI = 1, with DMI = 10 and ROUT = 18, where this is the route number
  for the Virtual Trunk

  ```
  >LD86REQ PRTCUST 0FEAT RLBRLI 1
  RLI 1
  ...
  ROUT 18
  ...
  DMI 10
  ...
  ```

- SPN = 101, with CLTP = INTL and RLI = 1

  ```
  >LD90REQ PRTCUST 0FEAT NETTRAN AC1TYPE SPNSPN 101
  SPN 101
  FLEN 0
  ITOH NO
  CLTP INTL
  RLI 1
  SDRR NONE
  ITEI NONE
  ```

NRS

In the NRS database, a Numbering Plan entry that associates the SPN
101 with the Branch Office endpoint is provisioned.

The Numbering Plan entry is provisioned in NRS Manager, as shown in
and
.

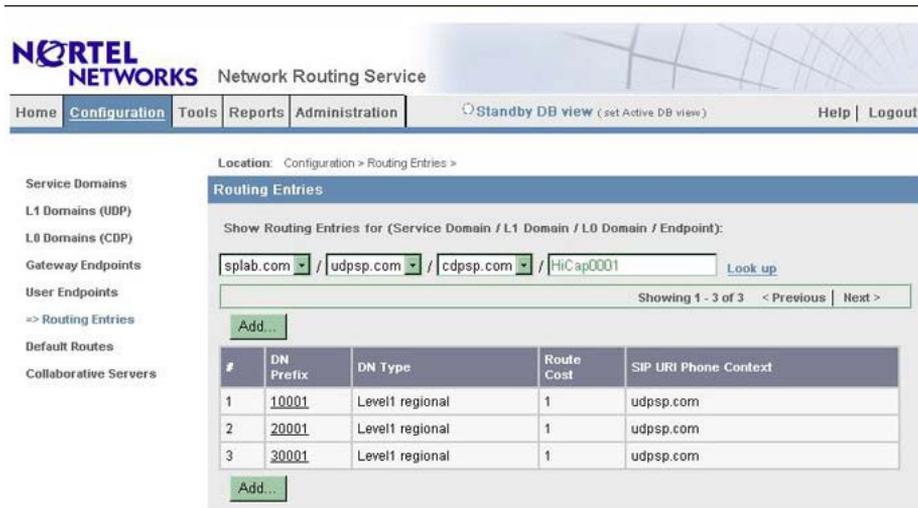**Figure 66**
NRS Routing Entries window

Figure 67
NRS Add Routing Entry

Branch Office

At the MG 1000B Small System Controller, the following is provisioned:

- DMI = 12 with DEL = 3 to remove the ZDP digits added in the main office
  ```
  >LD86 REQ PRTCUST 0 FEAT DGT DMI 12
  ```

```
DMI 12
DEL 3
ISPN NO
CTYP INTL
```

- RLI = 4, with DMI = 12 and ROUT = 11, where this is the route number for the PSTN Trunk

```
>LD86REQ PRTCUST 0FEAT RLBRLI 4
RLI 4
...
ROUT 11
...
DMI 12
...
```

- SPN = 101, with CLTP = INTL and RLI = 4

```
>LD90REQ PRTCUST 0FEAT NETTRAN AC1TYPE SPNSPN 101
SPN 101
FLEN 0
ITOH NO
CLTP INTL
RLI 4
SDRR NONE
ITEI NONE
```

Call example

This section describes what happens when Branch User 3001 is in Normal Mode and dials "1 87654321", using the configuration provisioned in the previous section.

Main office

At the main office Call Server:

1. The call is recognized as originating from a Branch User in Zone 1.

2. Based on the ZACB property, the Call Server recognizes that the call has been dialed with AC1, and that zone-based digit manipulation must be performed.

3. The ZDP digits are inserted after the Access Code, changing the digit string to "1 101 87654321".

4. The digits are translated by the ESN feature.

    a. ESN recognizes that the number has been dialed using AC1, so "101" is a Special Number.

    b. RLI "1" is associated with SPN "101", so route "18" and DMI "10" should be used.

    c. DMI "10" sets the call type to SPN. Because ISPN=YES for DMI "10", CLID is based on the call type defined by the CLTP field in SPN "101", which is INTL.

5. The call is routed to route "18", the Virtual Trunk. The digit string sent by the Call Server is "101 87654321", as the Access Code is not sent out.

NRS

The NRS recognizes the digits "101" and call type of PrivateSpecial, and identifies the endpoint as the Branch Office. It then routes the call to the Branch Office.

Branch Office

At the MG 1000B Small System Controller:

1. The call comes in on the Virtual Trunk. The INAC field in the Route Block of the Virtual Trunk is configured as "YES", and call type SPN is associated with ACI in configuration of NET_DATA (LD 15). AC1 is inserted at the beginning of the digit string, changing the digit string to "1 101 87654321".

2. The digits are translated by the ESN feature.

    a. ESN recognizes that the number begins with AC1, so "101" is a Special Number.

    b. RLI "4" is associated with SPN "101", so route "11" and DMI "12" should be used.

    c. DMI "12" deletes the first three digits of the digit string, and sets the call type to International.

3. The call is routed to route "11", the PSTN trunk.

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, consult *Dialing Plans Reference;*.

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 on the pertinent Small System Controller.

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, Media Card, and TM 3.1 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.

ITG-P

Internet Telephony Gateway-Pentium. The ITG-P card has a Pentium processor and 24 Digital Signal Processor (DSP) channels. It occupies two slots in an MG 1000B Core or MG 1000B Expander. It provides the same functionality as the Media Card when equipped with the IP Line 3.1 application. See Voice gateway.

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 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 with an emergency backup on the Media Card.

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 Media Cards also provide echo cancellation and compression and decompression of voice streams. The voice gateway software can run on an 8- or 32-port Media Card or the 24-port ITG-P card. Within the MG 1000B Core, both of these cards register the voice channels to the MG 1000B Small System Controller 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

NORTEL