Nortel Communication Server 1000

Communication Server 1000E Maintenance

Release: 7.0
Document Revision: 04.01

www.nortel.com

NN43041-700

Nortel Communication Server 1000
Release: 7.0
Publication: NN43041-700
Document release date: 4 June 2010

Contents

New in this release

The following sections details what's new in *Communication Server 1000E Maintenance* (NN43041-700) for Nortel Communication Server 1000 Release 7.0.

Navigation

Feature changes

Following are the feature changes for this release:

Other changes

Revision History

June 2010

Standard 04.01. This document is up-issued to support Communication Server 1000 Release 7.0.

October 2009

Standard 03.14. This document is up-issued to reflect changes in technical content for Communication Server 1000 Release 6.0. "NTDW20 Media Gateway Extended Peripheral Equipment Controller (MG XPEC)" (page 42) provides information about MG XPEC.

October 2009

Standard 03.13. This document is up-issued to update the section Software maintenance tools.

August 2009
Standard 03.12. This document is up-issued to support the new MG 1010 media gateway.

June 2009
Standard 03.11. This document is up-issued to support Communication Server 1000 Release 6.0.

May 2009
Standard 03.10. This document is up-issued to support Communication Server 1000 Release 6.0. Following are the other changes done for this Release:

- UNIStim with DTLS
- SSC is not supported in CS 1000 Release 6.0
- patch conflict management
- supported Ciphers and advanced cryptography for DTLS
- transfer using SFTP client by default during Linux upgrades and installations
- memshow command changed to free –b –t -o

May 2009
Standard 03.09. This document is up-issued to support Communication Server 1000 Release 6.0. This NTP may contain information on or refer to products and naming conventions that are not supported in this release. This information is included for legacy purposes and convenience only. This includes but is not limited to items, such as: SSC; ISP 1100; ITG Pentium cards; and Media Cards running certain IP Line applications.

July 2008
Standard 02.04. This document is issued to support Communication Server 1000 Release 5.5.

June 2008
Standard 02.03. This document is issued to support Communication Server 1000 Release 5.5.

February 2008
Standard 02.02. This document is issued to support Communication Server 1000 Release 5.5.

December 2007
Standard 02.01. This document is issued to support Communication Server 1000 Release 5.5.

October 2007
Standard 01.03. This document is issued to support Communication Server 1000 Release 5.0. Changes to address CR Q01766330.

June 2007
Standard 01.02. This document is issued to support Communication Server 1000 Release 5.0. Procedures for adding and replacing a CP PM Call Processor card and a Media Gateway Controller card are added.

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 documents, now retired: *Communication Server 1000E: Maintenance* NN43041-700 and *Communication Server 1000S: Maintenance* NN43041-500.

January 2007
Standard 4.00. This document is up-issued to reflect addition of technical content due to CR Q01542505.

July 2006
Standard 3.00. This document is up-issued with corrections from CR Q01324850.

August 2005
Standard 2.00. This document is up-issued for Communication Server 1000 Release 4.5.

September 2004
Standard 1.00. This document is issued for Communication Server 1000 Release 4.0.

How to get help

Contents

This section contains the following topics:

Getting help from the Nortel web site

The best way to get technical support for Nortel products is from the Nortel Technical Support web site:
www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. 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:
www.nortel.com/callus

Getting help from a specialist by using an Express Routing Code

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

Getting help through a Nortel distributor or reseller

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

Overview

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

Subject

This document describes system maintenance for the CS 1000E system.

Note on legacy products and releases

This NTP contains information about systems, components, and features that are compatible with Nortel Communication Server 1000 Release 7.0 software. For more information about legacy products and releases, click the **Technical Documentation** link under **Support** on the Nortel home page:

www.nortel.com

Applicable systems

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

Intended audience

This document is intended for individuals who configure, maintain, and troubleshoot CS 1000E systems.

Conventions

In this document, the Communication Server 1000E (CS 1000E) is referred to generically as system.

In this document, the following Chassis or Cabinets are referred to generically as Media Gateway:

- Option 11C Mini Chassis (NTDK91) and Chassis Expander (NTDK92)
- Option 11C Cabinet (NTAK11)

- MG 1000E Chassis (NTDU14) and Expansion Chassis (NTDU15)
- Media Gateway 1010 (MG 1010) (NTC310)

In this document, the following hardware is referred to generically as Server:

- Common Processor Pentium Mobile (CP PM) card
- Common Processor Media Gateway (CP MG) card
- Common Processor Dual Core (CP DC) card
- Commercial off-the-shelf (COTS) servers
  - IBM x306m server (COTS1)
  - HP DL320 G4 server (COTS1)
  - IBM x3350 server (COTS2)
  - Dell R300 server (COTS2)

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

In this document, the following hardware is referred to as Gateway Controller:

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

Note: Gateway Controllers run a common MGC loadware. The MGC maintenance commands are supported on all Gateway Controller platforms unless otherwise indicated.

Co-res CS and SS is not supported on COTS1 servers. You can deploy a COTS1 server as a stand-alone Signaling Server.

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

Table 1
Hardware platform supported roles

Hardware platform	VxWorks Server	Linux Server	Co-res CS and SS	Gateway Controller
CP PIV	yes	no	no	no

Hardware platform	VxWorks Server	Linux Server	Co-res CS and SS	Gateway Controller
CP PM	yes	yes	yes	no
CP DC	no	yes	yes	no
CP MG	no	no	yes (see note)	yes (see note)
MGC	no	no	no	yes
MG XPEC	no	no	no	yes
COTS1	no	yes	no	no
COTS2	no	yes	yes	no

Note: The CP MG card functions as the Co-resident Call Server and Signaling Server, and the Gateway Controller while occupying slot 0 in a Media Gateway.

Related information

This section lists information sources that relate to this document.

NTPs

The following NTPs are referenced in this document:

- *Unified Communications Management Common Services Fundamentals* (NN43001-116)
- *Signaling Server IP Line Applications Fundamentals* (NN43001-125)
- *Network Routing Service Fundamentals* (NN43001-130)
- *Converging the Data Network with VoIP Fundamentals* (NN43001-260)
- *Circuit Card Reference* (NN43001-311)
- *SIP Line Fundamentals* (NN43001-508)
- *Co-resident Call Server and Signaling Server Fundamentals*(NN43001-509)
- *Signaling Server IP Line Applications Fundamentals* (NN43001-125)
- *IP Phones Fundamentals* (NN43001-368)
- *Software Input/Output Administration* (NN43001-611)
- *Web Services API Administration* (NN43001-640)
- *Element Manager System Reference – Administration* (NN43001-632)
- *Software Input/Output Reference – Maintenance* (NN43001-711)

- *Software Input/Output Reference – System Messages* (NN43001-712)
- *Communication Server 1000 Fault Management – SNMP* (NN43001-719)
- *Traffic Measurement: Formats and Outputs Reference* (NN43001-750)
- *Communication Server 1000E Planning and Engineering* (NN43041-220)
- *Communication Server 1000E Installation and Commissioning* (NN43041-310)
- *Communication Server 1000E Software Upgrades* (NN43041-458)
- *Communication Server 1000E Hardware Upgrades* (NN43041-464)

Online

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

www.nortel.com

CD-ROM

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

Precautions

Contents

This section contains the following topics:

General precautions

CS 1000 equipment is based on solid state circuitry that is sensitive to static electricity and environmental conditions. Follow the precautions in this chapter to avoid personal injury and equipment damage.

DANGER
To avoid the danger of electric shock, be careful when working with power equipment and connections. Warning notices are displayed and must be heeded.

Wear an antistatic wrist strap when handling circuit cards to prevent damage caused by static electricity.

Circuit cards

Handle the circuit cards as follows:

- Wear an antistatic wrist strap before handling circuit cards.
- Handle the cards by the card stiffeners and edges only. Do not touch the contacts or components.
- Keep the cards installed in the system as much as possible to avoid dirty contacts and unnecessary wear.
- Set the cards on a protective antistatic bag. If an antistatic bag is not available, hold the card, or set it in a card slot unseated from the connectors.
- Unpack or handle the cards away from electric motors, transformers, or similar machinery.

- Store the cards in protective packing. Do not stack cards on top of each other unless they are packaged.
- Store the cards in a dry dust-free area.

During repair and maintenance procedures:

- Turn off the power switch, if there is one.
- Software-disable the cards, if applicable, before they are removed or inserted.
- Hardware-disable the cards, whenever there is an enable/disable switch, before they are removed or inserted.
- Insert the cards into compatible slots only.
- Return defective or heavily contaminated cards to a repair center; do not try to repair or clean them.

Communicating with the system

Contents

This section contains the following topics:

Introduction

Send maintenance commands and receive system messages (status and error messages) by communicating with the system through one or more of the following input/output devices or management tools:

- TTY or VDT terminal as an input/output device
- PC running terminal emulation software
- RS-232-C compatible printer as an output-only device
- Maintenance telephone as an input-only device
- Element Manager

See *Communication Server 1000E Installation and Commissioning* NN43041-310 for information about how to connect these devices and management tools.

System terminal access for CP PIV Call Processors

Terminal Server

Because each CS 1000E Core Call Server provides only two ports for serial devices, the Terminal Server is used to provide the necessary standard serial ports for applications and devices that require them, such as printers and Call Detail Recording (CDR). The Terminal Server is also used to connect maintenance terminals and modems for support staff.

The Terminal Server provides an rlogin service that allows serial devices to establish dedicated connections to pseudo TTY (PTY) ports on the Call Server. (The Terminal Server therefore serves the same purpose as Serial Data Interface [SDI] and Multipurpose Serial Data Link [MSDL] cards in Large Systems.) You can telnet through the Terminal Server to individual components on the ELAN subnet, and therefore obtain maintenance access for each device. You can also access the Terminal Server from a remote PC by dialing the onboard modem.

As the Terminal Server is configured to automatically log in to the active Call Server upon startup, only one Terminal Server is required for each Call Server pair.

While the Terminal Server is needed for serial port access to the Call Server, it can also be optionally configured to provide access to Media Gateway 1000T (MG 1000T) serial ports for maintenance purposes.

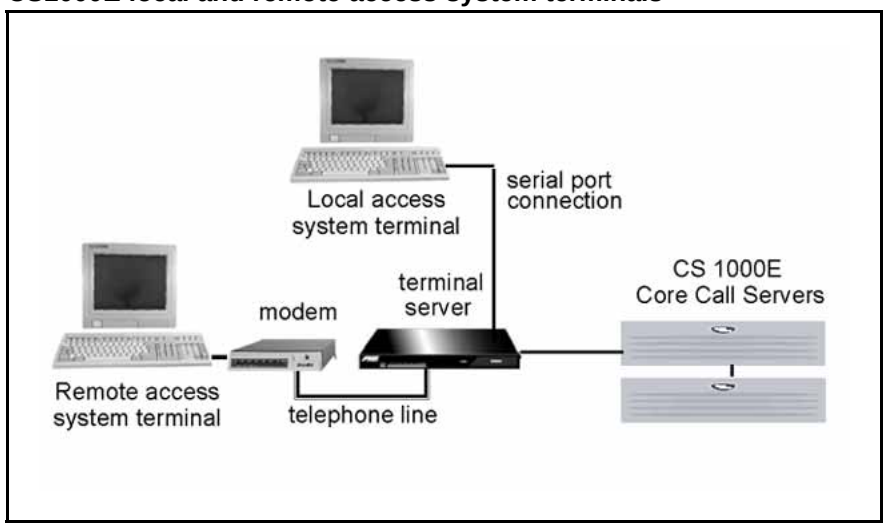
For more details on installing and configuring the Terminal Server, see *Communication Server 1000E Installation and Commissioning .*

System terminal

When a system terminal is installed locally, it is typically connected to a serial port on the Terminal Server. This ensures continued access to the active Call Server. When a system terminal is installed at a remote location, a modem and a telephone line are required between the system terminal and the Terminal Server.

Figure 1 "CS1000E local and remote access system terminals" (page 20) shows a typical system terminal configuration to the Call Servers.

Figure 1
CS1000E local and remote access system terminals



With the CS 1000E, a system terminal can also connect directly to the Call Server, Signaling Server, Media Cards, and Media Gateway 1000T (MG 1000T).

When a system terminal is installed directly on the CP PIV Call Processor, it connects to the com 1 port.

When a system terminal connection is made to a CP PM Call Processor, the com (SDI) port is routed through the backplane of the shelf to the 50 pin MDF connector. The NTAK19EC cable ships with the CP PM that adapts the 50 pin MDF to a 25 pin DB connector for connectivity. A 25 pin null modem cable is required to adapt the SDI port to a typical PC serial port. Port0 is used for maintenance access. Port1 is for an external modem connection.

When a system terminal is installed on the Signaling Server, the rear serial port is the primary port for maintenance and administration.

System terminal access for Gateway Controllers

Each Gateway Controller installed in a CS 1000E has 3 serial ports: SDI0, SDI1, and SDI2. SDI2 is not available during system initialization and therefore cannot be used to access installation menus.

The Gateway Controller serial ports can be used for local debug purposes or configured as system terminals in LD 17. Unlike the Small System Controller (SSC) SDI ports, all Gateway Controller SDI ports are configured through software. The Gateway Controller does not have DIP switches. Furthermore, the remote SDI feature of the Gateway Controller eliminates the need for a terminal server or TTY on a system with Gateway Controllers.

See *Communication Server 1000E Installation and Commissioning* for more detail about configuring Gateway Controller serial ports.

MG 1000E 10BaseT port

The MG 1000E 10BaseT Ethernet port defaults to the disabled state. To use the 10BaseT Ethernet port, assign the port a unique IP address, and enable the port from the Call Server. The MG 1000E 10BaseT Ethernet port can run in Normal or Survival mode. In Normal mode, the MG 1000E does not provide access to maintenance or alarm management.

MG 1000E card slot assignment

The MG 1000E contains physical card slots numbered 1 to 10. When configuring the CS 1000 system, the physical card slot numbers must be transposed to loop, shelf, card.

Connecting to the Media Card RS-232 maintenance port

Connect a serial cable either to the rear P2 connector or to the faceplate connector, but not both. The card's hardware cannot support two devices connected at the same time.

The terminal device should be configured to 9600, 8, N, 1. Configure the flow control to "None" or a similar setting.

If the hardware flow control is enabled, you see information from the card but the card does not respond to any keystrokes. If this happens, ensure the flow control is set to "None", close the session, and reopen it.

Element Manager

Element Manager is a web-based interface that supports a broad range of system management tasks, including:

- configuration and maintenance of IP Peer and IP telephony features
- configuration and maintenance of traditional routes and trunks
- configuration and maintenance of numbering plans
- configuration of Call Server data blocks (such as configuration data, customer data, Common Equipment data, D-channels)
- maintenance commands, system status inquiries, backup and restore functions
- software download, patch download, patch activation

The Element Manager web server resides on the Signaling Server and can be accessed directly through a web browser.

For more information about Element Manager, see *Element Manager System Reference – Administration.*NN43001-632.

Accessing the system

Use maintenance commands to disable, enable, and test system components. To perform system maintenance on the CS 1000E, use the following:

- SDI system terminal using command line inputs.
- Element Manager. For details on Element Manager, see *Element Manager System Reference – Administration* NN43001-632 and *Signaling Server IP Line Applications Fundamentals* (NN43001-125).
- Maintenance Telephone.

Access through an SDI system terminal

Send maintenance commands and receive system messages by accessing the Call Server, through an RS-232 device, such as a VDT or TTY.

On the Call Server, the device can be connected through the Terminal Server or through a Com port. If the RS-232 device is connected directly to the Call Server Com port, a separate terminal is required to communicate with each Call Server in the Core.

When you access the system through a system terminal, a login procedure is required. All system passwords are initially set to"0000". Change passwords in the Configuration Record in LD 17. If a system reload (sysload) occurs before the new password is saved in a data dump, the last active password remains valid.

Accessing the system from an SDI system terminal

To access the system from an SDI system terminal, follow the steps in Procedure 1 “Accessing the system from an SDI system terminal” (page 23).

Procedure 1
Accessing the system from an SDI system terminal

Step	Action
1	Connect port 0 of the SDI cable to call server and terminal server. Route RS232 cable to the call server and the other cable to terminal server.
2	Press **Return**. **a** If the response is `OVL111 nn IDLE` or `OVL111 nn BKGD`, you are ready to log into the system. Go to step 2. **b** If the response is `OVL000 >` , you are already logged into the system. Go to step 4. Responses vary with different Background Terminal packages.
3	Enter **`LOGI ADMIN1`** and press **Return**. The normal response is `PASS?`. If there is any other response, see *Software Input/Output Reference – Maintenance* NN43001-711.
4	Enter either the level 1 or level 2 password and press **Return**. If the password is correct, the system responds with the prompt `>`.
5	Enter **`LD xx`**, where xx represents the number of the program.
6	Perform tasks.

7 To end the program, enter four asterisks (****).

8 To end the login session, enter **LOGO**.

--End--

Access through the maintenance telephone

The Call Server can be accessed using a maintenance telephone. A telephone functions as a maintenance telephone when the class-of-service is defined as Maintenance Telephone Allowed (MTA) in LD 11.

Using a maintenance telephone, you can send a subset of commands. The maintenance telephone takes priority over a system terminal and logs the terminal out.

Specific commands for testing tones and outpulsing through the maintenance telephone are given in the Tone and Digit Switch and Digitone Receiver Diagnostic (LD 34).

Specific commands for testing trunk connections through the maintenance telephone are given in the Trunk Diagnostic (LD 36).

The following Maintenance Overlays are accessible from an IP Phone operating as a maintenance telephone: 30, 32, 33, 34, 36, 37, 38, 41, 42, 43, 45, 46, 60, and 62.

Maintenance Overlay operations are supported on IP Phones except for the Tone and Digit Switch (TDS) commands of LD 34 and TONE commands of LD 46.

To use the maintenance telephone, the Terminal Number (TN) for that telephone must be operating.

To access the system using the maintenance telephone, a Special Service Prefix (SPRE) code, as defined in the Customer Data Block, is entered, followed by "91". See Procedure 2 “Accessing the maintenance telephone” (page 25) for details. To enter commands, press the keys that correspond to the letters and numbers of the command (for example, to enter "LD 42, Return", enter***53#42##***).

Table 2 "Translation from keyboard to dial pad" (page 25) shows the translation from a terminal keyboard to a telephone dial pad.

Table 2
Translation from keyboard to dial pad

Keyboard		Dial Pad
	1	1
A B C	2	2
D E F	3	3
G H I	4	4
J K L	5	5
M N O	6	6
P Q R S	7	7
T U V	8	8
W X Y Z	9	9
	0	0
Space or # (pound symbol)		#
Return		##

Accessing the maintenance telephone

To access the maintenance telephone, follow the steps in Procedure 2 “Accessing the maintenance telephone” (page 25).

Procedure 2
Accessing the maintenance telephone

Step	Action
1	Press the prime DN key.
2	Place the telephone in maintenance mode by entering **`xxxx91`**, where xxxx represents the customer SPRE code as defined in the Customer Data Block in LD 21. The SPRE code is typically "1", which means you enter **`191`** to place the telephone in maintenance mode.
3	To check for busy tone, enter Return (##) • If there is no busy tone, go to Step 4. • If there is a busy tone, a program is active. To end an active program and access the system, enter four asterisks (****).
4	Load a program by entering **`53#xx##`**, where xx represents the number of the program.
5	Perform tasks.

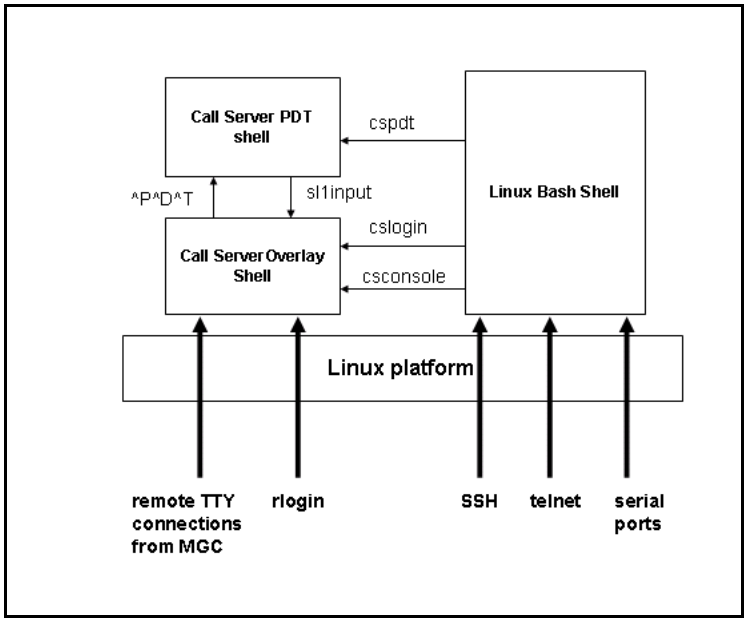
6 Press the release key to return the telephone to call processing mode. Background routines are then loaded automatically.

--End--

Access to the Co-resident platform

The CS 1000 Call Server, Signaling Server, and System Management applications operate on the CP PM hardware platform and the Linux operating system.

Access to each of the applications and the Linux Base shell can be selected. The following diagram shows the supported access mechanisms to the co-resident platform and how to navigate among components.



Access the Linux bash shells by using any of the following options:

- serial ports
- Telnet
- ssh
- rlogin
- remote TTY connections from Gateway Controller

Serial ports

Connecting to the serial ports on CP PM provides access to the Linux base bash shell directly. After logon at the shell and after the authorization, you can issue Linux base CLI commands and any appropriate Signaling Server application-related commands. If you choose to access the Call Server shell, issue the following commands:

- **`cslogin`** -- to switch into the Call Server overlay shell.
- **`cspdt`** -- to switch into the Call Server PDT shell
- **`csconsole`** -- to connect to the CPSI port 0

Co-resident Call Server and Signaling Server shells

Co-res CS and SS supports the following shells:

- **Linux Bash shell** --The Linux Bash shell is used for Linux Base and Signaling Server applications CLI commands.
- **Call Server Overlay shell** --The Call Server Overlay shells are used for the Call Server overlay commands.
- **Call Server PDT shell** --The PDT shells are used for the PDT commands.

Following commands are used to navigate between shells:

Table 3
Co-res CS and SS server shells navigation commands

From	To	Command
Linux Bash Shell	Call Server Overlay Shell	**`cslogin`** **`csconsole`**
Linux Bash Shell	Call Server PDT shell	**`cspdt`**
Call Server Overlay Shell	Linux Bash Shell	**`CTRL AD`**
Call Server Overlay Shell	Call Server PDT Shell	**`CTRL -PDT`**
Call Server PDT Shell	Call Server Overlay Shell	**`sllinput`**
Call Server PDT Shell	Linux Bash Shell	**`exit`**

Hardware maintenance tools

Contents

This section contains the following topics:

Introduction

Fault indicators and hardware features help perform maintenance tasks (particularly identifying and clearing faults). These maintenance tools include:

- circuit card features that include self-tests and status indicators
- LED indicators that identify Call Server power and temperature faults
- system alarms that categorize the severity of component failure

Alarm/fan module features

The NTDU64 alarm/fan module provides cooling for a CP PIV Call Processor. It also provides a thermostat to monitor the Call Server temperature.

If the Call Server temperature reaches 42°C (107°F), the fan units switch into high-speed mode. The fans revert to normal speed when the Call Server temperature falls below 37°C (98°F). Also, if one fan fails, the remaining two fans switch into high-speed mode indefinitely.

If the Call Server temperature exceeds 60°C (140°F), it triggers a major alarm. The Call Server continues to operate, provided it does not lose power.

The CP PM, CP MG, and CP DC cards do not have an alarm/fan module.

Alarm/fan LEDs

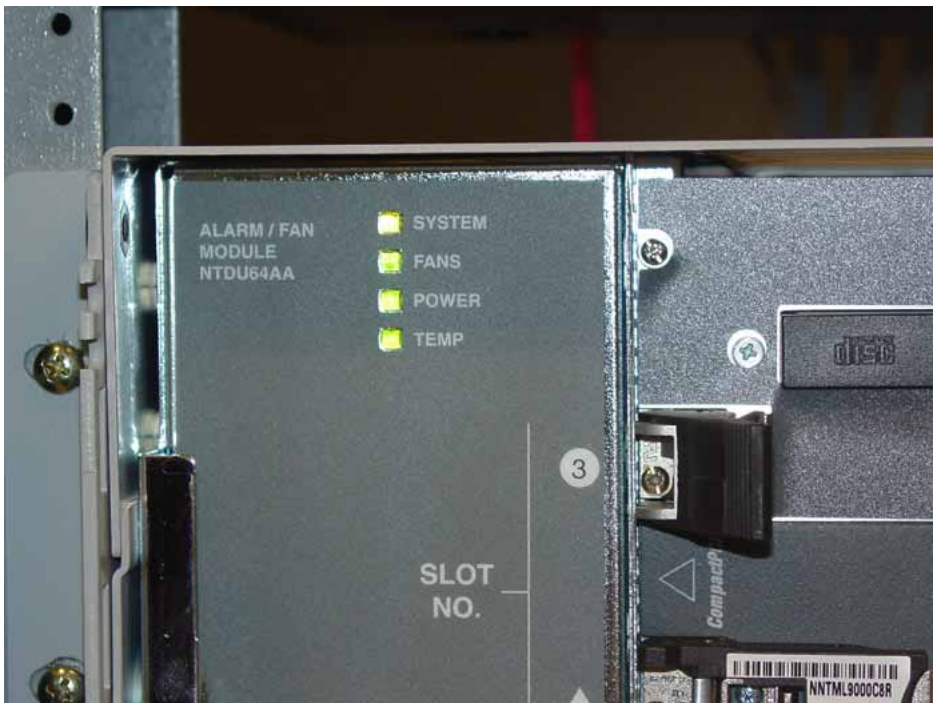
The alarm/fan module also provides status light emitting diode (LED) indicators for the following:

- system
- fans
- power
- temperature

For each LED, green indicates normal operations and red indicates faulty or disabled equipment.

Figure 2 "Alarm/fan module status LEDs" (page 30) shows the alarm/fan module green status LEDs during normal operations.

Figure 2
Alarm/fan module status LEDs



The system LED consolidates the status of the other three LEDs. If the fans, power, and temperature are all within normal operating parameters, the system LED is green. If any of the three other LEDs is red, indicating trouble, the system LED also appears red.

Figure 3 "Fan trouble LEDs" (page 31) shows the alarm/fan Module LEDs indicating fan trouble.

Figure 3
Fan trouble LEDs

Because the system LED shows the status of the other three LEDs, it is used to determine the overall status of the Call Server. It is visible through a light pipe in the Call Server front cover.

For information about replacing Call Server components, including the alarm/fan module and power module, see “Replacing equipment” (page 109).

Compact flash cards

The CP PM Call Processor has two compact flash (CF) sockets:

- one internal 1 GB Fixed Media Disk (FMD)
- one hot-swappable Removable Media Disk (RMD), accessible on the faceplate. The RMD contains the CP PM Call Processor software image.

Compact flash LEDs on the Call Server faceplate indicate the status of the CF devices.

Note: For the Signaling Server, the 40 GB hard drive is used as the primary storage device. However, 1 GB compact flash is used for additional data backup.

Fixed Media Disk

The Fixed Media Disk (FMD) is internal to the CP PM card, accessible only when the card is removed from the system. This flash card serves as a hard drive. The internal card connects directly to the Advanced Technology Attachment (ATA), also known as the hard drive controller in the chipset.

For CP PM Call Processor application, assign switch S5 to position 1. Position 1 indicates that a Compact Flash device is used for the FMD. For CP PM Signaling Server application, assign switch S5 to position 2.

Removable Media Disk

You can load CS 1000 software onto the CP PM Call Processor through the RMD.

To support hot insertion and removal, the faceplate card slot is controlled through a PCI-to-CF bridge, but is treated as a standard ATA device.

When you insert or remove the faceplate CF (RMD), SRPTxxxx information messages appear on the TTY and are written to the report log.

When you attempt to backup to the CF and the CF is missing from the faceplate, TEMUxxxx error messages are issued .

For more information about message details, see *Software Input/Output Reference – System Messages* NN43001-712.

Formatting a Removable Media Disk Compact Flash card

You can format the Removable Media Disk (RMD) CF card as a bootable or a nonbootable device.

From PDT1 or PDT2, issue the format command as follows: **formatCf2 {0,1}**.

where

0 = a nonbootable device
1 = a bootable device

You can format a compact flash on a PC (Microsoft Windows 98SE, Microsoft Windows 2000, or Microsoft Windows XP) for use as a compact flash in the RMD. You format the disk in FAT16 - DOS format.

Circuit card features

Circuit card features describes various circuit cards and features.

Self-tests

A self-test checks to see that a card is working correctly. Many cards perform a self-test on power-up. The software commands Disable and Enable force a card to self-test. The results of a self-test generally show whether or not there is a problem with the card.

NTDW53 Common Processor Dual Core card

The NTDW53 Common Processor Dual Core (CP DC) card includes the following components and features:

- AMD Athlon 64 X2 1.8 Ghz dual core processor
- 2 GB DDR2 RAM
- 160 GB SATA hard drive
- Three faceplate USB 2.0 ports for software installations, upgrades, patching, and USB keyboard and mouse support
- One faceplate VGA port for monitor support
- Two faceplate Gigabit Ethernet ports
- Faceplate status LED and card reset buttons

For more information about the CP DC card hardware, see *Circuit Card Reference* (NN43001-311).

You can use a USB 2.0 storage device to install or upgrade the Linux Base Operating System. The CP DC card does not support Compact Flash (CF) cards.

The CP DC Call Processor connects to the MG 1000E Media Gateway Controllers through Ethernet and therefore does not require backplane connectivity (other than power and a slot ID). The following rules apply to the preferential placement of the CP DC Call Processor in the MG 1000E:

- Do not install the CP DC Call Processor in slot 0 of any Media Gateway. This slot is reserved for the Gateway Controller.
- For ease of cabling, place the CP DC Call processor in slot 1 (slot 22 or 23 for MG 1010), next to the Gateway Controller.

CP DC faceplate

The CP DC card faceplate provides a reset button, status LEDs, three USB 2.0 ports, one VGA port, and two Gigabit Ethernet ports. The NTDW53 CP DC card faceplate is shown in Figure 4 "NTDW53 CP DC faceplate" (page 34).

Figure 4
NTDW53 CP DC faceplate

The VGA port provides monitor support. The three USB 2.0 ports provide USB keyboard, USB mouse, and USB 2.0 storage device support. You can use the USB 2.0 ports for software installations, upgrades, and patches.

The reset button provides a CP DC hardware reset. The reset button is recessed to prevent accidental resets. You must use a small blunt object to access the reset button. During a reset the status LED will flash red until the reset is complete. The CP DC card does not provide a faceplate INI button. To re-initialize a CP DC card, use the Command Line Interface (CLI) **`appstart cs restart`**command.

Status LED

The CP DC faceplate STS LED is a tri-color system status indicator. To determine the CP DC system status, see Table 4 "CP DC faceplate status LED" (page 34).

Table 4
CP DC faceplate status LED

LED color	CP DC system status
Green	Link is up
Flashing Green	Link is down
Orange	Linux applications loading
Flashing Orange	Linux applications load successful
Red	BIOS self test

LED color	CP DC system status
Flashing Red	Bootrom and Linux base loading
Off	No power

The CP DC faceplate RED LED is not active and is intended for future use The RED LED is a tri-color redundancy status indicator.

The HD ACT LED flashes during SATA hard drive activity.

CP DC serial data interface ports

The CP DC has two serial data interface (SDI) ports: Port 0 and Port 1. Both ports are standard RS232 DTE ports. They are routed through the backplane of the shelf to a 50-pin main distribution frame (MDF) connector on the back of the shelf. You require a NTAK19ECE6 cable to adapt the 50-pin MDF to a pair of 25-pin DB connectors. A 25-pin null modem is required to adapt an SDI port to a typical PC serial port. Port 0 is used for maintenance access. Port 1 is for an external modem connection.

You can change the baud rate of the CP DC card from the BIOS menu. The default serial connection baud rate of the CP DC card is 9600 bps, no parity, 1 stop bit.

The CP DC card serial port connection procedure remains the same as the CP PM card . For more information, see *Linux Platform Base and Applications installation and commissioning* (NN43001-315) .

CP DC media storage

The CP DC card contains a 160 GB SATA hard drive. The hard drive stores the Linux Base Operating System. If the hard drive fails, you can replace it by performing the CP DC hard drive replacement procedure, see *Circuit Card Reference* (NN43001-311).

NTDW61 Common Processor Pentium Mobile card

NTDW61 Common Processor Pentium Mobile (CP PM) card features include the following:

- Intel Pentium M 738 1.4 GHz
- two compact flash (CF) sockets
  - — one internal 1 GB Fixed Media Disk (FMD)
  - — one hot-swappable Removable Media Disk (RMD), accessible on the faceplate.
- 1 GB of DDR RAM, expandable to 2 GB
- two 100BaseT Ethernet ports

- — LAN 0 used for ELAN
- — LAN 1 not used on Call Server

- one 1 Gbps Ethernet port for HSP
- two SDI ports
- one USB port
- a reset (RST) button to cold start the Call Server
- an initialize (INI) button to warm start the Call Server
- an Active CPU or Call Server Redundancy (CS RED) LED

The CP PM Call Processor connects to the MG 1000E Media Gateway Controllers through Ethernet and therefore does not require backplane connectivity (other than power and a slot ID). The following rules apply to the preferential placement of the CP PM Call Processor in the MG 1000E:

- Do not install the CP PM Call Processor in slot 0 of any Media Gateway. This slot is reserved for the Gateway Controller.
- For ease of cabling, place the CP PM Call processor in slot 1 (slot 22 or 23 for MG 1010), next to the Gateway Controller.
- In a system configured for Campus Redundancy, place the two CP PM Call Processors in separate MG 1000E cabinets to increase potential survivability.

The CP PM has no power (PWR) LED.

The CP PM architecture has no system utility (Sys Util) card, so the display usually associated with the Sys Util card is not present.

Figure 5 "NTDW61 CP PM Call Processor" (page 36) shows the faceplate of the CP PM Call Processor card.

Figure 5
NTDW61 CP PM Call Processor

Initialize button

The manual initialize (Init) button associated with the active Call Server starts the Initialize program. The Initialize program can clear some equipment faults. It then rebuilds call-dependent data and generates system messages indicating the status of the system. This process is called an initialization.

CAUTION
SERVICE INTERRUPTION
Call processing is briefly interrupted during an initialization.

Reset button

You can cold restart the processor card with the Reset button. This is equivalent to a full power start up of the processor card. The System Loader initiates call processing and starts memory-checking diagnostics. This process is called a system reload or sysload.

CAUTION
SERVICE INTERRUPTION
During a sysload, active calls are disconnected and the system goes into an emergency line transfer state. Use the reset button only when specifically instructed to do so in an NTP.

CP PM Call Processor faceplate LEDs

The status LED indications of the NTDW61 CP PM Call Processor are as follows:

- Off: no power
- Red: BIOS self-test running
- Flashing red: bootrom and Operating System (OS) loading
- Yellow: sysload phase 1
- Flashing yellow: sysload phase 2
- Flashing green: SL1 loading on active core
- Green: normal operation

The Active CPU LED indications are as follows:

- Off: no power
- Green: redundant mode, active
- Flashing green: split mode, active
- Yellow: redundant mode, standby

- Flashing yellow: split mode, standby
- Red: single mode

The ELAN LED indications are as follows:

- LED1 Off: 10 Mbps
- LED1 Yellow: 100 Mbps
- LED2 Off: no link, no activity
- LED2 Green: link valid
- LED2 Blink: link valid and activity

The HSP LED indications are as follows:

- LED1 Off: 10 Mbps
- LED1 Yellow: 100 Mbps
- LED1 Green: 1000 Mbps
- LED2 Off: no link, no activity
- LED2 Green: link valid
- LED2 Blink: link valid and activity

NTDW61 CP PM Signaling Server

NTDW61 CP PM Signaling Server card features includes the following:

- Intel Pentium M 738 1.4 GHz processor
- one hard disk drive
- two compact flash (CF) sockets
  - one internal 1 GB Fixed Media Disk (FMD)
  - one hot-swappable Removable Media Disk (RMD), which is accessible on the faceplate.
- 1 GB of DDR RAM, expandable to 2 GB
- two 100BaseT Ethernet ports
  - LAN 0 used for ELAN
  - LAN 1 used for TLAN
- one 1 Gbps Ethernet port (not used on Signaling Server)
- two serial ports
- one USB port (not used on Signaling Server)

- a reset (RST) button to cold start the Signaling Server
- an initialize (INI) button to warm start the Signaling Server

CP PM Signaling Server LEDs

The status LED indications of the NTDW61 CP PM Signaling Server are as follows:

- Off: no power
- Red: BIOS self-test running
- Flashing red: bootrom and operating system (OS) loading
- Yellow: applications loading
- Flashing yellow: applications loaded successfully
- Green: pbxLink up
- Flashing green: pbxLink down

For more detailed information about the CP PM Signaling Server, see *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

NT4N39 PIV Call Processor features

Buttons on the NT4N39 PIV Call processor cards allow the administrator to initialize and reset the system.

Initialize button

The manual initialize (Init) button associated with the active Call Server starts the Initialize program. The Initialize program can clear some equipment faults. It then rebuilds call-dependent data and generates system messages indicating the status of the system. This process is called an initialization.

CAUTION
SERVICE INTERRUPTION
Call processing is briefly interrupted during an initialization.

Reset button

You can cold restart the processor card with the Reset button. This is equivalent to a full power start up of the processor card. The System Loader initiates call processing and starts memory-checking diagnostics. This process is called a system reload or sysload.

CAUTION
SERVICE INTERRUPTION
During a sysload, active calls are disconnected and the system goes into an emergency line transfer state. Use the reset button only when specifically instructed to do so in an NTP.

CP PIV faceplate LEDs

The CP PIV faceplate features the following 5 LEDs:

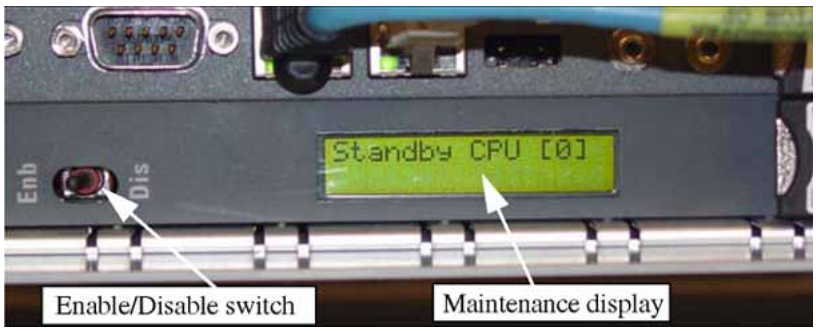
- PWR – Solid Green – Power Good
- CF – Flashing Green shows activity on compact flash cards CF1 or CF2.
- HDD – Flashing Green shows activity on secondary IDE bus (not used)
- LAN1 – ELAN Activity
- LAN2 – HSP Activity
  - — Flashing Yellow – 10 MB
  - — Flashing Green – 100 MB
  - — Flashing Amber – 1000 MB (1 GB)

CP PIV System Utility card features

The System Utility card maintenance display indicates the status of the CP PIV Call Processor, either active or standby. The display also provides an indication of normal and fault conditions as well as the progress of software upgrades and backups.

Figure 6 "System Utility card display for standby Call Processor" (page 40) shows the System Utility card display for a standby Call Processor.

Figure 6
System Utility card display for standby Call Processor



Interpretations of the maintenance display codes are listed in the *Software Input/Output Reference – System Messages* NN43001-712. Examine previous codes, system messages, and visual indicators with any current maintenance display codes to properly analyze faults.

Each new code shown on a maintenance display overwrites the one before it. However, all codes displayed are recorded. You can review them by printing the History File (in LD 22).

Figure 6 "System Utility card display for standby Call Processor" (page 40) also shows the location of the Enable/Disable (Enb/Dis) switch on the card. This switch enables and disables the hardware for that card.

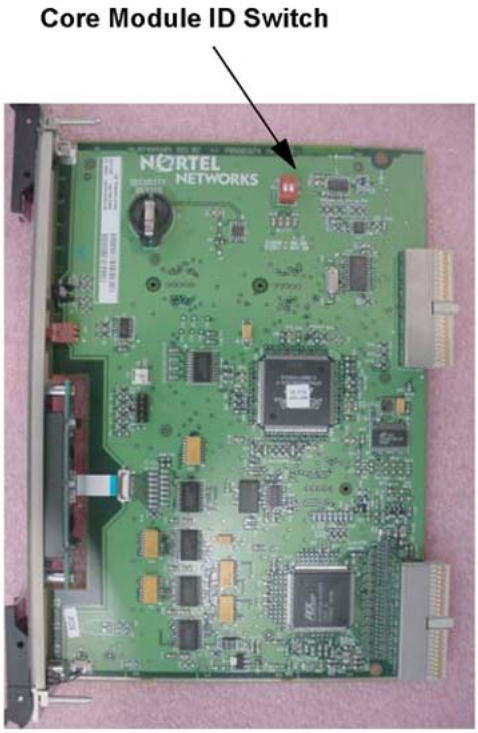
Table 5
Core module ID switch settings (System Utility card)

	Position 1	Position 2
Core 0	On	On
Core 1	Off	On

The System Utility card also contains DIP switches that specify the address of the card for Call Server 0 or Call Server 1. The Core ID switches are set in the factory.

Confirm that these settings match the identification labels for the module into which they will be installed. See Table 5 "Core module ID switch settings (System Utility card)" (page 41) and Figure 7 "Core Module ID switch" (page 42).

Figure 7
Core Module ID switch



NTDW20 Media Gateway Extended Peripheral Equipment Controller (MG XPEC)

The NTDW20 MG XPEC card replaces the NT8D01 controller card in the controller slot of a NT8D37 IPE module. The MG XPEC card is a dual card assembly that contains a motherboard and a daughterboard. Each board of the dual assembly contains non-removable Digital Signal Processor (DSP) daughterboards. The MG XPEC card provides the same hardware functions as the Media Gateway Controller (MGC) card in a traditional CS 1000E Media Gateway chassis or cabinet.

NTDW56 and NTDW59 Common Processor Media Gateway card

The Common Processor Media Gateway (CP MG) card functions as a gateway controller with DSP resources for IP Media Gateways in a CS 1000E system, and functions as a Co-resident Call Server and Signaling Server. The CP MG card occupies slot 0 in a Media Gateway. The CP MG card is available in two versions:

- NTDW56 - CP MG with 32 DSP ports
- NTDW59 - CP MG with 128 DSP ports

The Gateway Controller portion of the CP MG card is based on the same architecture as the Media Gateway Controller (MGC) card. For more information, see "NTDW60 Media Gateway Controller card" (page 43). The CP MG card contains non-removable DSP resources. MGC DSP daughterboards are not required for CP MG cards.

The Server portion of the CP MG card is based on the same architecture as the Common Processor Pentium Mobile (CP PM) card. For more information, see "NTDW61 Common Processor Pentium Mobile card" (page 35).

NTDW60 Media Gateway Controller card

The NTDW60 Media Gateway Controller (MGC) card provides a gateway controller for MG 1000E IP Media Gateways in a CS 1000E system. The MGC card functions as a gateway controller for CS 1000E Call Servers.

The MGC card has two expansion sites to accommodate Digital Signal Processor (DSP) daughterboards. The MGC card occupies slot 0 in a Media Gateway.

Excluding DSP daughterboards, MGC card features include:

- internal compact flash, which appears to the software as a standard hard disk drive
- six 100BaseT Ethernet ports
- three SDI ports
- four-character LED display

NTDW60 Media Gateway Controller LEDs

The Media Gateway Controller faceplate provides a 4-character LED display that indicates normal or abnormal situations during system initialization and regular operation of the MGC.

Media Gateway Controller LED display during system initialization

During system initialization, diagnostic information from the associated sanity tests appears on the MGC faceplate. The following table summarizes this information.

Table 6
MGC LED messages during system initialization

Message	Description
BOOT	The first message displayed when the system becomes active.
POST	Power-on self-test, displayed while the MGC carries out system hardware tests.
PASS	Power-on self-test pass.
Exxx	Error code, where xxx is a numeric value. The system has detected a serious error. See Table 8 "MGC LED error codes" (page 45) for error code details.
LOAD	Application software is loading.

In a successful initialization, the diagnostic messages appear in the following order: BOOT, POST, PASS, LOAD.

If a fatal error occurs during the self-test, an error code appears. The PASS and LOAD messages do not appear.

Media Gateway Controller LED display during normal operation

During normal operations, the MGC LED displays the IP Media Gateway (IPMG) superloop and MGC shelf number. If an error occurs, the display cycles between the shelf number and the error code. Each item appears for 20 seconds. The following table summarizes the information that appears on the LED display.

Table 7
MGC LED messages during normal operation

Message	Description
Exxx	Error code, where xxx is a numeric value. The system has detected a serious error. See Table 8 "MGC LED error codes" (page 45) for error code details.
LLL^{S}	IPMG super loop and MGC shelf number, where LLL is the superloop number and S is the shelf number (032^{0}, 120^{1}).

Media Gateway Controller LED error codes

The following table summarizes the error codes possible on the MGC LED display.

When the fault has been cleared, the error code is also cleared from the LED display and a corresponding MGCxxxx message is issued to the TTY, the LOG, and as SNMP traps.

Table 8
MGC LED error codes

LED code	Message	Severity	Description	Corrective action	Output
E001	MGC0001	Major	MGC <supl shelf> A DSP DB-96 is detected in DB position #2.	Remove the Media Gateway Controller from the chassis/ cabinet and move the DSP DB-96 from DB position #2 to DB position #1.	TTY LOG SNMP LED
E002	MGC0002	Critical	Unable to send MGC <supl shelf> registration request to Call Server	Check IP configuration and network connections.	TTY LOG SNMP LED
E003	MGC0011	Critical	MGC <supl shelf> link to Call Server is down	Check IP configuration and network connections.	TTY LOG SNMP LED

NTDW62, NTDW64, and NTDW78 DSP daughterboards

The NTDW60 Media Gateway Controller provides Digital Signal Processor (DSP) resources with the NTDW62 32-port DSP daughterboard, the NTDW64 96-port DSP daughterboard, and the NTDW78 128-port DSP daughterboard. These daughterboards transcode between IP and TDM devices in a CS 1000E. The daughterboards eliminate the need for Voice Gateway Media Cards in an MG 1000E, although the system can contain both DSP daughterboards and Voice Gateway Media Cards, if desired.

Two positions are available on the MGC card for DSP daughterboards. The following configurations of daughterboard placement on a Media Gateway Controller are possible:

- an NTDW62 32-port in position 1
- an NTDW62 32-port in position 2
- an NTDW62 32-port in position 1 and an NTDW62 32-port in position 2
- an NTDW64 96-port in position 1
- an NTDW64 96-port in position 1 and an NTDW62 32-port in position 2

- an NTDW78 128-port in position 1
- an NTDW78 128-port in position 1 and an NTDW78 128-port in position 2

Note: MGC cards provisioned with greater than 196 DSP ports are only supported in High Density Primary Rate Interface Media Gateways (HD PRI Gateway).

The following table summarizes where you can place the daughterboards and the card slots assigned to each card when it is in that position.

Table 9
DSP daughterboard placement and card slot assignment

Daughterboard	Position 1	Card slot	Position 2	Card slot
NTDW62 32-port	yes	11	yes	0
NTDW64 96-port	yes	11, 12, 13	no	-
NTDW78 128-port	yes	11, 12, 13, 14	yes	0, 9, 10, 15

The DSP daughterboards have no LEDs.

NTDW65 Voice Gateway Media Card

The NTDW65 MC32S Media Card provides 32 IP-TDM gateway ports. The MC32S replaces the previous media card or ITG card and runs on CS 1000 Release 5.5 and later software. Secure Real Time Protocol (SRTP) secures the IP media path to and from the DSP channels on the card.

Circuit card LEDs

Many circuit cards have one or more LEDs on the faceplate. The LED gives a visual indication of the status of the card or of a unit on a card.

When a green LED is steadily lit, the card is operating normally. When a green LED is off, the card is disabled or faulty.

When a red LED is steadily lit, the card, or a unit on it, is disabled, faulty or unequipped.

When a red LED is off and power is available to the card, the card is operating normally.

Media Card LEDs

The Media Card faceplate provides the following LEDs.

Status LED

The Media Card faceplate red LED indicates the following:

- the enabled/disabled status of the card
- the self-testing result during power up or card insertion into an operational system

Ethernet activity LEDs

The Media Card faceplate contains Ethernet activity LEDs for each subnet. The faceplate contains six Ethernet activity LEDs, three for the ELAN subnet and three for the TLAN subnet. The LEDs indicate the following links on the ELAN and TLAN subnets (in order from the top):

- 100 (100BaseT)
- 10 (10BaseT)
- A (Activity)

Maintenance hex display

The four-digit LED-based hexadecimal display provides the status of the Media Card at all times. The hex display provides an indication of fault conditions and the progress of PC Card-based software upgrades or backups. See Table 36 "Media Card faceplate maintenance display codes" (page 162) for a description of the hex display codes.

The Maintenance display also indicates the progress of the internal self-test in the form of T:xx.

ITG-P LED (Card Status)

The red status faceplate LED indicates the enabled or disabled status of the 24 card ports. The LED is on (red) during the power-up or reset sequence. The LED remains lit until the system enables the card. If the LED remains on, the self-test failed, the card is disabled, or the card rebooted.

NTAK10 faceplate LEDs

The NTAK10 2 Mb DTI circuit card has a total of six faceplate LEDs. Five of the LEDs are directly associated with the operation of the NTAK10 circuit card. The remaining LED is associated with the onboard clock controller.

The following table describes the NTAK10 LEDs.

Table 10
NTAK10 LEDs

LED	State	Definition
DIS	On (Red)	The NTAK10 2 Mb DTI circuit card is disabled.
	Off	The NTAK10 2 Mb DTI is not in disabled state.
OOS	On (Yellow)	The NTAK10 2 Mb DTI circuit card is in out-of-service state. No alarm states exist, the card is not disabled, nor is it in a loopback state.
	Off	The NTAK10 is not in an out-of-service state.
NEA	On (Yellow)	A near-end alarm state has been detected.
	Off	No near-end alarm.
FEA	On (Yellow)	A far-end alarm state has been detected.
	Off	No far-end alarm
LBK	On (Yellow)	The NTAK10 2 Mb DTI is in loopback mode.
	Off	The NTAK10 2 Mb DTI is not in loopback mode.
CC	On (Red)	The clock controller is switched on and disabled.
	On (Green)	The clock controller is switched on and is either locked to a reference or is in free-run mode.
	Flashing (Green)	The clock controller is switched on and is attempting to lock (tracking mode) to a reference. If the LED flashes continuously over an extended period of time, check the CC STAT in LD 60. If the CC is tracking, this can be an acceptable state. Check for slips and related clock controller error conditions. If none exist, this state is acceptable, and the flashing identifies jitter on the reference.
	Off	The clock controller is switched off.

NTAK79 faceplate LEDs

The NTAK79 2 Mb PRI circuit card has a total of seven faceplate LEDs. Five of the LEDs are directly associated with the operation of the Primary Rate interface (PRI). The remaining two LEDs are associated with the onboard Clock Controller and the onboard D-channel interface (DCHI).

The NTAK79 faceplate LEDs are described in Table 11 "NTAK79 LEDs" (page 49).

Table 11
NTAK79 LEDs

LED	State	Definition
OOS	On (Red)	The NTAK79 2 Mb PRI circuit card is either disabled or out-of-service state.
	Off	The NTAK79 2 Mb PRI is not in disabled state.
ACT	On (Green)	The NTAK79 2 Mb PRI circuit card is in active state.
	Off	NTAK79 2 Mb PRI is not in disabled state. The OOS LED is red.
RED	On (Red)	A red alarm state has been detected. This represents a local alarm state of: Loss of Carrier (LOS) Loss of Frame (LFAS), or Loss of CRC Multi-frame (LMAS).
	Off	No red (local) alarm.
YEL	On (Yellow)	A yellow-alarm state has been detected. This represents a remote alarm indication from the far end. The alarm can be either Alarm Indication (AIS) or Remote Alarm (RAI).
	Off	No yellow (remote) alarm.
LBK	On (Green)	The NTAK79 2 Mb PRI is in loopback mode.
	Off	The NTAK79 2 Mb PRI is not in loopback mode.
CC	On (Red)	The clock controller is switched on and disabled.
	On (Green)	The clock controller is switched on and is either locked to a reference or is in free run mode.
	Flashing (Green)	The clock controller is switched on and is attempting to lock (tracking mode) to a reference. If the LED flashes continuously over an extended period of time, check the CC STAT in LD 60. If the CC is tracking, this can be an acceptable state. Check for slips and related clock controller error conditions. If none exist, this state is acceptable, and the flashing identifies jitter on the reference.
	Off	The clock controller is switched off.
DCH	On (Red)	The DCHI is equipped and disabled.
	On (Green)	The DCHI is equipped and enabled, but not necessarily established.
	Off	The DCHI is switched off.

NTBK50 faceplate LEDs

The NTBK50 circuit card has a total of seven faceplate LEDs. Five of the LEDs are directly associated with the operation of the PRI. The remaining two LEDs are associated with the Clock Controller and DCHI/DDCH daughterboard.

The NTBK50 2 Mb PRI circuit card LEDs are described in Table 12 "NTBK50 faceplate LEDs" (page 50).

Table 12
NTBK50 faceplate LEDs

LED	State	Definition
OOS	On (Red)	The NTBK50 2 Mb PRI circuit card is either disabled or out-of-service. Also, the state of the card after power-up, completion of self-test, and exiting remote loopback.
	Off	The NTBK50 2 Mb PRI is not in disabled state.
ACT	On (Green)	The NTBK50 2 Mb PRI circuit card is in active state.
	Off	The NTBK50 2 Mb PRI is in disabled state. The OOS LED is red.
RED	On (Red)	A red-alarm state has been detected. This represents a local alarm state of Loss of Carrier (LOS), Loss of Frame (LFAS) or Loss of CRC Multi-frame (LMAS).
	Off	No red (local) alarm.
YEL	On (Yellow)	A yellow-alarm state has been detected. This represents a remote alarm indication from the far end. The alarm can be either Alarm Indication (AIS) or Remote Alarm (RAI).
	Off	No yellow (remote) alarm.
LBK	On (Green)	The NTBK50 2 Mb PRI is in loopback mode.
	Off	The NTBK50 2 Mb PRI is not in loopback mode.
CC	On (Red)	The clock controller is software-disabled.
	On (Green)	The clock controller is enabled and is either locked to a reference or is in free-run mode.
CC	Flashing (Green)	The NTAK20 is equipped and is attempting to lock (tracking mode) to a reference. If the LED flashes continuously over an extended period of time, check the CC STAT in LD 60. If the CC is tracking, this can be an acceptable state. Check for slips and related clock controller error conditions. If none exist, this state is acceptable, and the flashing identifies jitter on the reference.
	Off	The clock controller is not equipped.
DCH	On (Red)	The DCH is disabled.
	On (Green)	The DCH is enabled, but not necessarily established.
	Off	The DCH is not equipped.

NTAK09 and NTRB21 faceplate LEDs

The NTAK09/NTRB21 1.5 Mb DTI/PRI/DCH circuit cards have seven faceplate LEDs. Five LEDs are directly associated with the operation of the NTAK09/NTRB21 circuit cards. The remaining two LEDs are

associated with the optional daughterboards. The first of these LEDs indicates the status of the NTAK20 Clock Controller daughterboard. The second LED indicates the status of the D-channel interface.

Table 13 "NTAK09/NTRB21 LEDs" (page 51)describes the LEDs found on the NTAK09/NTRB21 DTI/PRI/DCH circuit cards. Only one of the five LEDs is on at one time.

Table 13
NTAK09/NTRB21 LEDs

Affected circuit card	LED	State	Definition
NTAK09 or NTRB21	DIS	On (Red)	The circuit card is disabled.
		Off	The circuit card is not in disabled state.
	ACT	On (Green)	The circuit card is in active state. No alarm states exist, the card is not disabled, nor is it in a loopback state.
		Off	An alarm state or loopback state exists, or the card is disabled. See other faceplate LEDs for additional information.
	RED	On (Red)	A red-alarm state is detected.
		Off	No red alarm.
	YEL	On (Yellow)	A yellow-alarm state is detected.
		Off	No yellow alarm.
	LBK	On (Green)	The card is in loopback mode.
		Off	The card is not in loopback mode.
	DCH	On (Red)	The D-channel is equipped and disabled.
		On (Green)	The D-channel is equipped and enabled.
		Off	The D-channel is not equipped.
NTAK20	CC	On (Red)	The NTAK20 is equipped and disabled.
		On (Green)	The NTAK20 is equipped and is either locked to a reference or is in free-run mode.
		Flashing (Green)	The NTAK20 is equipped and is attempting to lock (tracking mode) to a reference. If the LED flashes continuously over an extended period of time, check the CC STAT in LD 60. If the CC is tracking, this can be an acceptable state. Check for slips and related clock controller error conditions. If none exist, this state is acceptable, and the flashing is identifies jitter on the reference.
		Off	The NTAK20 is not equipped.

Table 13
NTAK09/NTRB21 LEDs (cont'd.)

Affected circuit card	LED	State	Definition
NTAK93 or NTBK51	DCH	On (Red)	The D-channel daughterboard is equipped and disabled.
		On (Green)	The D-channel daughterboard is equipped and enabled.
		Off	The D-channel daughterboard is not equipped.

Monitor jacks

The NTAK09, NTAK10, NTAK79, NTBK50, and NTRB21 have two bantam jacks (RCV and XMT) on the faceplate. They are used to monitor the performance of the carrier in the receive and transmit direction. The jacks allow the convenient connection of external T1/E1 test equipment and ISDN protocol analyzers.

Signaling servers for DTLS

The supported hardware for the Communication Server 1000 system with Datagram Transport Layer Security (DTLS) is as follows:

- Communication Server 1000E Call Processors
  - — Call Processor Pentium IV (CP PIV)
  - — Common Processor Pentium Mobile (CP PM)
  - — Co-resident Call Server and Signaling Server (all supported platforms)
  - — Gateway Controller
- CS 1000E Signaling Servers
  - — CP PM card
  - — Common Processor Dual Core (CP DC) card
  - — HP DL320 G4
  - — IBM x306m
  - — IBM x3350
  - — Dell R300
- IP Phones -- IP Softphone 1100, 1200, and Phase II series of Nortel IP Phones (including Nortel IP Phone 2007) support DTLS.

CP PM faceplates LEDs

There are two LEDs on CP PM faceplate:

- Status LED
  - Red indicates the power-up (by H/W) is on
  - Yellow indicates that the OS is loaded (by S/W)
  - Green indicates that "appstart" completed for software

- Redundancy LED
  - Red indicates boot up (by HW) is on.
  - Blank indicates when the OS starts (by S/W)

System alarms

Major and minor alarms can be displayed on the attendant console when connected to the system. However, attendant consoles cannot be connected to an MG 1000T and therefore cannot display MG 1000T alarms.

Major alarms

A major alarm indicates a fault that seriously interferes with call processing. The causes of major alarms are listed in Table 14 "Causes of major and minor alarms" (page 54).

When an MG 1000E is equipped with a power fail transfer unit (PFTU), a major alarm causes designated analog (500/2500-type) telephones to connect directly to Central Office trunks. This is called a line transfer.

Minor alarms

A minor alarm indicates that the system hardware or software has detected a fault requiring attention. The causes of minor alarms are listed in Table 14 "Causes of major and minor alarms" (page 54).

A minor alarm is indicated on attendant consoles in customer groups affected by the fault. A minor alarm indication on the console is an optional feature, enabled and disabled on a customer basis through data administration procedures.

Table 14
Causes of major and minor alarms

Alarm	Cause
Major	CPU or control bus failure Program failure when attempting to load the system System power faults Temperature fault (excessive heat)
Minor	Conference failure Digitone receiver failure More than one fault on different cards in one MG 1000E (indicated on affected customer console only) Serial Data Interface failure Memory failure Network failure (indicated on affected console only) Peripheral signaling failure Tone and digit switch failure

External alarms

A remote alarm, in the context of general maintenance, is the extension of a major alarm to another location or to an audible or visual indicator. The system generates a signal that indicates a major alarm condition and sends the alarm signal to a remote location, such as a monitoring center or test center, or to an indicator, such as a light or bell.

Line transfer

As an option, connect one or more PFTUs to the MG 1000Es. Each PFTU connects designated analog (500/2500-type) telephones to Central Office trunks. If call processing stops, those analog (500-2500-type) telephones are transferred through the PFTU to the Central Office so the outside connections are still available. A line transfer occurs:

- during a sysload (system reload)
- if there is a major power failure
- if call processing stops due to a Call Server failure

- if there is a loss of power to the MG 1000E
- if there is a loss of power to the PFTU
- if a line transfer switch on the attendant console is turned on

External power loss

You can connect reserve (backup) power supplies to the system, that is, uninterruptible power supplies (UPS) for AC-powered systems. If the main source of external power is lost, power to the system is maintained by the UPS.

Software maintenance tools

Contents

This section contains the following topics:

Introduction

Software maintenance tools help to identify and clear faults, and provide self-checking capabilities. Various software maintenance tools are available for the CS 1000:

- “Diagnostic programs” (page 58) monitor a variety of operations, detect faults, and initiate a corrective action during normal call processing.
- “Interactive diagnostics” (page 66) test hardware, isolate faults, and verify fault clearing.
- “Element Manager” (page 155) provides the means to check status and issue a variety of commands.

Maintenance applications

CS 1000 systems have over 600 overlay-based maintenance commands. To maintain a CS 1000 system using system terminals, you must remember, or look up, which overlay has the appropriate commands and the syntax of each command.

Element Manager (EM) eliminates the need to remember many of these commands by providing a subset of overlay functions for maintenance of the Call Server, MG 1000Es, Signaling Servers, and Voice Gateway Media Cards.

Diagnostic programs

Diagnostic software programs monitor system operations, detect faults, and clear faults. Some programs run continuously, while some are scheduled.

Diagnostic programs are resident or nonresident software programs. Resident programs, such as the Error Monitor and Resident Trunk Diagnostic, are always present in system memory. Nonresident programs, such as the Input/Output Diagnostic and Core Equipment Diagnostic, are used as Midnight and Background Routines or for interactive diagnostics. Nonresident programs are loaded from the system disk and are run as scheduled or upon request.

See *Software Input/Output Reference – Maintenance* NN43001-711 and *Software Input/Output Reference – System Messages* NN43001-712 for detailed information about all diagnostic programs.

Overlays

Nonresident programs are also called overlays or loads. They are identified by a title and a number preceded by the mnemonic for load (for example, Trunk Diagnostic — LD 36).

CS 1000E

The CS 1000E Core Call Server and MG 1000Es support the overlay commands and TN format (l s c u).

However, a number of maintenance commands are either not supported or not applicable to the MG 1000E. Table 15 "Unsupported overlay commands for MG 1000E" (page 58) lists the commands that are not supported in the MG 1000Es.

Table 15
Unsupported overlay commands for MG 1000E

LD	Unsupported commands
30	CPED, DISL, ENLL, LDIS, LENL, LOOP, RPED, SLFT, STEI, TIET, TTSM, and TTWI

Table 15
Unsupported overlay commands for MG 1000E (cont'd.)

LD	Unsupported commands
32	DISL, DISN, DLIF, DSCT, DSNW, DSPS, DSRB, DSTS, DSXP, ENLG, ENLL, ENLN, ENNW, ENPS, ENRB, ENTS, ESTU, FDIS, PCON, PERR, PLOG, PMES, PTAB, PTRF, RLBT, RLSU, SDLC, STAT NCAL, STAT loop, STAT NWK, STAT PER, IDC loop, IDCS, SUPL, XNTT, XPCT and XPEC
34	DTR and TDS Also, the following Maintenance Telephone commands are not supported: CDT, CMP, CUST, CWG, DRNG, DTD, ITN, JDRG, JIDT, ORD, PCRT and TST
38	DISX and ENLX
45	TEST
46	DISL, DISX, ENLL, ENLX and MFS
92	No supported commands (the Automatic Trunk Maintenance feature is not supported in CS 1000E)

Error Monitor

The Error Monitor is a resident program that continuously tracks call processing. The Error Monitor generates system messages if it detects invalid or incorrectly formatted call processing information.

System messages generated by the Error Monitor are preceded by the mnemonic ERR, which usually indicates hardware faults, or the mnemonic BUG, which usually indicates software problems.

With prompt ERRM in the Configuration Record (LD 17), instruct the system to print or not print ERR or BUG messages. If many similar BUG messages occur, consult the Technical Assistance Center.

Initialize Program

The Initialize Program momentarily interrupts call processing when it clears Core Equipment faults. It then rebuilds call-dependent data and generates system messages with the mnemonic INI, which indicate the status of the system.

CAUTION
SERVICE INTERRUPTION
Call processing is briefly interrupted during an initialization.

To activate an initialization (warm start) on the Call Server, press the initialize button on the CP card.

An initialization occurs automatically after the System Loader program runs, when a software or firmware fault is detected, and when a Core Equipment hardware fault is detected.

Midnight and Background Routines

In the Configuration Record (LD 17), select the nonresident software programs that run in the Midnight Routine and Background Routine. These routines automatically perform maintenance checks. Programs included in the Midnight Routine are defined with the prompt DROL (derived from "daily routine overlay"). Programs included in the Background Routine are defined with the prompt BKGD.

The Midnight Routine runs once every 24 hours. This routine is preset to run at midnight when a system is shipped. Assign a different time in the Configuration Record. When the Midnight Routine starts, the system cancels any other program.

A memory test runs once a day. The Core Equipment Diagnostic (LD 35) runs as part of the Midnight Routine, even if it is not programmed.

The Background Routine runs when no other program is loaded in the overlay area. The programs included in the Background Routine run in sequence repeatedly until there is another request to use the overlay area (for example, if you log on to check the status of a circuit card) or the Midnight Routine runs.

For the CS 1000E system, include the programs listed in Table 16 "Programs used in Midnight and Background Routines" (page 60) in Midnight and Background Routines. Software Audit (LD 44), and Network and Signaling Diagnostic (LD 30) should always be used in the Background Routine.

The maintenance requirements and the configuration of the system determine the other programs included in Midnight and Background Routines.

Table 16
Programs used in Midnight and Background Routines

LD	Program function
30	Network and Signaling Diagnostic
33	1.5 Mb/s Remote Peripheral Equipment Diagnostic
34	Tone and Digit Switch and Digitone Receiver
35	Core Equipment Diagnostic
36	Trunk Diagnostic 1

Table 16
Programs used in Midnight and Background Routines (cont'd.)

LD	Program function
37	Input/Output Diagnostic
38	Conference Circuit Diagnostic
40	Call Detail Recording Diagnostic
41	Trunk Diagnostic 2
43 (Midnight only)	Data Dump
44	Software Audit
46	Multifrequency Sender Diagnostic
60 (Midnight only)	Digital Trunk Interface Diagnostic
61 (Midnight only)	Message Waiting Lamp
135	Core Equipment Diagnostic
137	Input/Output Diagnostic

Overlay Loader

This resident program locates, loads, and checks all nonresident software programs. It automatically activates the Midnight and Background Routines. Load the Overlay programs manually by entering the commands through the system terminal or maintenance telephone. When the program is loaded, the program mnemonic (such as, TRK for Trunk Diagnostic) appears on the system terminal.

Overload Monitor

The volume of system messages is continuously monitored by the system. If too many error messages are detected from a line or trunk card, the system activates the Overload Monitor program. The Overload Monitor disables the faulty card and generates system messages with the mnemonic OVD.

Resident Trunk Diagnostic

This program automatically monitors all trunk calls and records apparent faults on each trunk. If the number of faults on a trunk exceeds the threshold for that trunk, the program generates a system message identifying the trunk and the type of fault.

A failure on a trunk can keep the trunk from detecting incoming calls. The threshold mechanism cannot detect such a failure, so this program also records the number of days since each trunk received an incoming call. If some incoming calls are not being processed, use the command LMAX in Trunk Diagnostic 1 (LD 36) to identify the trunk with the maximum idle days.

System Loader

The System Loader program loads all call processing programs and data and starts memory-checking diagnostics. After all required programs and data are loaded and all checks performed, the System Loader is erased from system memory, the Initialize Program runs, and normal call processing begins. This process is called a sysload (or system reload). The System Loader operates automatically on system power-up or if a core equipment or power fault destroys information in the system memory.

Unsuccessful DTLS negotiation

During unsuccessful DTLS negotiation, LTPS logs one of the following messages:

- “DTLS handshake error - bad server certificate. Client IP = xx.xx.xx.xx” --This log message is printed when the phone is not able to validate the server certificate or determines that the server certificate is not valid.
- “DTLS handshake failed - bad client certificate. Client IP = xx.xx.xx.xx” --This log message prints when the mutual authentication is turned on and the server cannot validate the client certificate or determine that the client certificate is not valid.

Diagnostics for Linux Base

In CS 1000, following diagnostic tools and capabilities are introduced for Linux Base systems:

- Wireshark (Ethereal) for Ethernet traffic sniffing
- Apparent Networks (Gryphon) Ethernet quality of service links monitoring
- system resource monitoring and alarming
- Linux OS level core dumps during abnormal OS or application failure
- MONIT applications register and set monitor thresholds and actions on error
- SNMP alarm generation and MIB-II support
- OMM reports and peg counters for each application
- Common Syslog logging infrastructure

The following table shows the diagnostic log files for Linux Base systems.

Table 17
Diagnostic log files for Linux Base

Message	Facility	Log file
SS	local0	ss_common.log
BRS	local1	nrs.log
Nortel MySQL	local2	nortel_MySQL.log
SNMP	local3	nortel_snmp.log
Reserved (SLP)	local4	N/A
NCGL	local5	ncgl_patch.log
CS	local6	callserver.log

All diagnostic files are in the **/var/log/nortel/** folder and Linux Base log files in **/var/log/nortel/linuxbase.log.**

Media Gateway Controller Local Diagnostic Shells

You can perform maintenance functions specific to the Media Gateway Controller (MGC) through Local Diagnostic Shell 1 (LDB1) and Local Diagnostic Shell 2 (LDB2). LDB1 provides MGC-specific functions similar to the PDT1 shell functions on the Call Server. LDB2 provides advanced functions similar to the PDT2 shell functions on the Call Server.

Access the LDB shells locally on an MGC serial port or remotely through rlogin, telnet, secure shell, or PPP. Passwords for the MGC platform are synchronized with passwords on the Call Server. Therefore, when logging on to LDB on the MGC, enter the Call Server PDT1 user name and password to access LDB1 and the Call Server PDT2 user name and password to access LDB2.

When you log on to the MGC, the following login banner appears:

```
Welcome to the Media Gateway Controller command line.
Firmware Version:<APPS FW version>
Management IP:<ELAN IP>
IPMG:<supl shelf>
Call Server IP Address:<CS IP address>
Installed daughterboards:<x> where x = 1 or 2
OS Time:  mm/dd/yyyy (hh:mm:ss)
Use "exit" to logout.
Idle session timeout = 20 minutes
mm/dd/yyyy hh:mm:ss MGCnnnn (None) (Info):  MGC <supl
shelf> - User <LDB1/LDB2> has logged into the card.
```

The following table summarizes the Local Diagnostic Shell CLI commands:

Table 18
Local Diagnostic Shell CLI commands

Command	Shell	Description
diskformat	LDB2	Format the internal compact flash card on the MGC.
diskshow	LDB1	Display the total used and available disk space on the internal compact flash card.
displayshow	LDB1	Display messages that currently appear on the LED of the MGC, except the superloop and shelf.
ethportdisable <port>	LDB2	Disables a port so that it can be used for mirroring.
ethportmirror <port1> <port2>	LDB2	Mirror an embedded Ethernet switch port. To disable mirroring of a port, use none for port2.
ethportreset	LDB2	Clears all port mirroring and reenables standard embedded Ethernet switch functionality.
ethportshow	LDB1	Displays Ethernet port settings for external and internal interfaces. The output includes autonegotiation settings, duplex, port speed, and port-mirroring status.
ethspeedshow	LDB1	Prints the current speed and duplex settings of the ports on the embedded Ethernet switch.
macshow	LDB1	Displays all MAC addresses associated with internal and external Ethernet ports on the embedded Ethernet switch.
memshow free –b –t -o	LDB1	Displays the total used and available RAM memory on the MGC.
mgcinfoshow	LDB1	Displays MGC information such as IP addresses, uptime, registration status, and superloop information.
mgcsetup	LDB1	Starts the setup menu. Change the local MGC configuration information, including local IP addresses, host name, and Call Server IP address.
rmonstatreset <port>	LDB1	Resets all RMON statistics counters for a port on the embedded Ethernet switch.
rmonstatresetall	LDB1	Resets all RMON statistics counters for all ports on the embedded Ethernet switch.
rmonstatshow <port>	LDB1	Displays RMON statistics collected by the embedded Ethernet switch for the port.
rmonstatshowall	LDB1	Displays RMON statistics collected by the embedded Ethernet switch for all ports.
swversionshow	LDB1	Displays the versions of all software and loadware currently in service on the MGC.

Local access to the MGC debug shell

For more detail about configuring MGC serial ports, see *Communication Server 1000E Installation and Commissioning* NN43041-310.

When you connect to an MGC TTY that is not configured as a system terminal, you receive no system prompt.

When you connect to an MGC TTY that is configured as a system terminal, you automatically connect to the Call Server SL1 shell.

In either situation, the commands in the following table provide access to the LDB and OAM shells.

Table 19
Accessing MGC debug shells

Command	Description
Ctrl+l, **Ctrl+d**, **Ctrl+b**	Obtain an LDB prompt.
Ctrl+o, **Ctrl+a**, **Ctrl+m**	Obtain an OAM prompt.
Ctrl+o, **Ctrl+a**, **Ctrl+m**	Obtain an OAM prompt from the LDS command line. The LDS session terminates after a successful logon to OAM.
Ctrl+l, **Ctrl+d**, **Ctrl+b**	Obtain an LDS prompt from the OAM command line. The OAM session terminates after a successful logon to LDB.
exit	Exit LDB or OAM.

To access the Call Server Problem Determination Tool (PDT), enter **Ctrl+p**, **Ctrl+d**, **Ctrl+t** on an MGC TTY configured as a system terminal.

Remote access to the MGC debug shell

CS 1000 supports rlogin, telnet, FTP, SFTP version 3.0 and secure shell (ssh) for remote access to the Media Gateway Controller.

For remote access to the MGC, initiate an rlogin or telnet session from the remote host to the ELAN address of the MGC.

The commands in Table 19 "Accessing MGC debug shells" (page 65) function remotely and locally.

Media Gateway Controller log file

A 1 MB circular log file accumulates system messages. The file, called Log0001.rpt, is stored in the MGC directory /u/rpt. Each record contains:

- timestamp
- message mnemonic
- message description
- severity
- if applicable, the four character LED message

Log0001.rpt is a report log file, similar to the log files on the Call Server and Signaling Server. The CLI commands to view and manage this file are identical to the commands on the Signaling Server platform.

Table 20
OAM DLOG commands

Command	Description
`activeDlogShow`	Display the current used firmware download file. See *IP Line Fundamentals*.
`inactiveDlogShow`	Display the inactive firmware download log file. See *IP Line Fundamentals*.
`dnldFailShow`	Display failed results in the active firmware download log file. See *IP Line Fundamentals.*

Interactive diagnostics

Load nonresident software programs into the memory through an SDI terminal. These programs, also called overlays or loads, are identified by a title and a number that is preceded by the mnemonic for load (for example, Trunk Diagnostic — LD 36).

The programs used in Midnight and Background Routines are also used manually as interactive diagnostic programs. See Table 16 "Programs used in Midnight and Background Routines" (page 60).

Nonresident programs are used interactively with a command and response format. In this format, enter a command that tells the system to perform a specific task. The system performs the task and sends system messages indicating status or errors back to you.

With interactive diagnostics you can:

- Disable, test, and enable specific equipment.
- Verify that a reported fault still needs to be cleared.
- Verify that a repair procedure has cleared a fault.

All maintenance programs, commands, and system messages are described in detail in *Software Input/Output Reference – Maintenance* NN43001-711 and in *Software Input/Output Reference – System Messages* NN43001-712.

Enhanced Maintenance feature

The system software sometimes requires modifications, called patches, which are provided by Nortel Technical Assistance Centers. The command ISS in Print Routine 3 (LD 22) prints the software generic and issue. A plus symbol (+) by the issue number means a patch is in service.

The Enhanced Maintenance feature provides the following:

- Enable patches to automatically survive a sysload.
- Enable patches on nonresident programs.
- Records all patches in the system.
- Enable data cartridges to be shipped with preloaded patches.

If a problem occurs with a patch, the CPU sends system messages, with the mnemonic EHM, to the system terminal or the history file.

Patch conflict issues can arise when you load individual patches or deplist patches. When you encounter a patch conflict, patch activation is aborted. CS 1000 Release 7.0 introduces a mechanism to handle conflicts. When you activate a patch, if any obsolete patches are in service, then all those patches are removed from the system.

> ***Note:*** In CS 1000 Release 7.0, deplist does not appear during a patch when the Deplist is empty.

Maintenance enhancement allows a technician to upgrade a site using the same software generic with new or replacement patches that are preloaded on the disk. Also, you can selectively dump specified patches from core memory to disk. You can use the dump patch facility for this purpose.

A maximum of 50 dummy globals are allowed for patches, instead of the normal five. Use of these globals are tracked, and you are given warning messages if attempting to use them for another patch.

Boot MGC to the Gold Image

To boot MGC to the Gold Image you must get to the MGC bootrom prompt, follow the steps Procedure 3 “Booting MGC to the Gold Image” (page 67) in to boot the MGC to Gold Image.

Procedure 3
Booting MGC to the Gold Image

Step	Action
1	Reboot MGC.
2	While booting, type **<CTRL B>** after the creation date is printed and the boot prompt is displayed.
3	At the prompt type **`test`**.
4	Select **`option b`** to change the boot options.
5	Select **`option 2`** to boot CSP from gold image once.

6 Select `option 0` to return to the previous menu.

7 Press the **return** key to exit menu and return to prompt.

8 Enter `@` at the prompt.

The MGC boots to the Gold Image.

--End--

Compact Flash Formatting with MGC Gold Image

To format the compact flash from the Gold Image, use Procedure 4 "Formatting Compact Flash with MGC Gold Image" (page 68).

Procedure 4
Formatting Compact Flash with MGC Gold Image

Step	Action
1	Type `<CTRL>I` when prompted during the MGC gold boot. This brings up a boot prompt.
2	At the prompt Enter `diskformat "all"`. This formats the MGCs internal compact flash.
3	Reboot the MGC and when it registers to the call server it gets automatically upgrade.

--End--

CS1000 Software Logs

The CS1000 logging infrastructure is comprised of a collection of log files that are created and archived across multiple elements that make up a CS1000 solution. The logs are intended to provide various levels of information related to specific events that have occurred during different operational states of the CS1000 solution. The collected information consolidated in the various logs includes information related to the following:

- status of software and hardware
- user administrative activity
- security events
- operational messages
- software debug messages

The collected information will have a variety of uses and apply to many aspects of system management. The users of this log information typically include network operations, security administrators, software developers, network engineering, and customer support.

For more information about logs, see System Management Reference (NN43001-600).

Supported DTLS Ciphers

Mocana DTLS stack supports the DTLS Ciphers and is compliant with RFC4347. Mocana DTLS supports the following DTLS ciphers:

- TLS-RSA-WITH-AES-256-CBC-SHA
- TLS-RSA-WITH-AES-128-CBC-SHA
- TLS-RSA-WITH-3DES-EDE-CBC-SHA
- TLS-RSA-WITH-DES-CBC-SHA
- TLS-DHE-RSA-WITH-AES-256-CBC-SHA
- TLS-DHE-RSA-WITH-AES-128-CBC-SHA
- TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA
- TLS-DH-ANON-WITH-DES-CBC-SHA
- TLS-PSK-WITH-AES-256-CBC-SHA
- TLS-PSK-WITH-AES-128-CBC-SHA
- TLS-PSK-WITH-3DES-EDE-CBC-SHA
- TLS-RSA-PSK-WITH-AES-256-CBC-SHA
- TLS-RSA-PSK-WITH-AES-128-CBC-SHA
- TLS-RSA-PSK-WITH-3DES-EDE-CBC-SHA
- TLS-DHE-PSK-WITH-AES-256-CBC-SHA
- TLS-DHE-PSK-WITH-AES-128-CBC-SHA
- TLS-DHE-PSK-WITH-3DES-EDE-CBC-SHA
- TLS-RSA-WITH-NULL-SHA
- TLS-RSA-WITH-NULL-MD5

Advanced Cryptography Support

Mocana DTLS library supports the following Advanced Cryptographies:

- Diffie-Hellman key exchange RSA
- PKCS #1, Version 1.5

- PKCS #5
- PKCS #7
- PKCS #8
- PKCS #10
- PKCS #12
- MD2
- MD4
- MD5
- SHA1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

Clearing faults

Contents

This section contains the following topics:

Fault clearing process

To clear a fault in the CS 1000, follow the steps in Procedure 5 "Clearing a fault in the CS 1000" (page 71).

Procedure 5
Clearing a fault in the CS 1000

Step	Action
1	Observe and record all fault indicators, system messages, and user reports.
2	Look up all system messages in *Software Input/Output Reference – System Messages* NN43001-712. The interpretation of the message can identify faulty equipment and tell you what action to take to clear the problem. If you cannot clear the fault using a Maintenance Application or through information in*Software Input/Output Reference – Maintenance*

NN43001-711, follow the process in this chapter to isolate and clear the fault.

3 If the system messages are not current or seem incomplete, review previous messages or initialize the system for information about the current status, as required.

4 Try to enable or test disabled equipment.

5 Software reenable cards by disabling and reenabling them. When the cause of a fault is not clearly evident, perform a software test to help identify the problem.

CAUTION
Working with ESDS devices
Wear an antistatic wrist strap when handling circuit cards to prevent damage caused by static discharge.

6 Software disable the circuit cards and hardware reenable them by unseating and reinstalling the cards. To unseat a circuit card, unscrew all faceplate screws holding the card in place. (Each circuit card has two screws except for the Drive Carrier card, which has four). Use the faceplate latches to eject the card. When reseating a circuit card, ensure to latch it and retighten all screws.

7 Replace equipment as necessary.

--End--

Verification

To verify that the system is operating properly and there are no remaining faults, follow the steps in Procedure 6 “Verifying operation” (page 72).

Procedure 6
Verifying operation

Step	Action
1	Ensure all LEDs on the alarm/fan module are green.
2	Make sure all circuit cards that could have been removed are reinserted in their assigned location and enabled.
3	Ensure the system utility card has the correct DIP switch settings for CPU 0 or CPU 1 as required. Also ensure that the enable/disable switch is configured to enable.
4	Make sure all wiring and connectors that could have been disconnected are reconnected.
5	Configure the midnight routine to run after logging out of the system by entering:

```
LD 135
MIDN
```

End the session in LD 135 and log out of the system by entering:

**** (four asterisks)

```
LOGO
```

The midnight routine runs now.

6 Check system messages produced when the midnight routine runs. Clear any faults indicated.

ATTENTION
Using the STAD command
Effective in CS 1000, Release 5.0, only users that have SEC_ADMIN privileges can change the system time and date. For more information about security enhancements, see *Security Management Fundamentals* (NN43001-604).

7 If a sysload occurred while clearing a fault, reset the correct time and date by entering:

```
LD 2
STAD (day) (month) (year) (hour) (minute) (second)
```

Check the time and date entered:

```
TTAD
```

End the session in LD 2 and log out of the system:
**** (four asterisks)

```
LOGO
```

8 Replace any covers that were removed.

9 Tag defective equipment with a description of the fault and return it to a repair center.

--End--

Fault indicators

When there is a fault in the system, you can receive notification by any combination of the following indicators:

- system messages
- visual fault indicators
- user reports

System messages

System messages are codes with a mnemonic and number, such as OVD0021. The mnemonic identifies a software program or a type of message. In this example, OVD indicates a message related to the Overload Monitor program. The number identifies the specific message.

Use system messages with other indicators, such as visual indicators, to identify and clear faults.

Table 21 "System message fault indicators and related fault types" (page 74) lists the most common fault-indicating messages and the type of fault they indicate. For a complete list and interpretation of system messages, see *Software Input/Output Reference – System Messages* NN43001-712.

Each type of fault indicator is described in Table 21 "System message fault indicators and related fault types" (page 74).

Table 21
System message fault indicators and related fault types

System messages	Type of fault
CCED messages CED messages CIOD messages HWR messages INI001, 002, 004, 005, 007 IOD006, 007, 060, 061, 291—297 NWS030, 102, 103, 142 SYS messages SRPT 181, Major failure	Call Server
CNF messages DTA, DTC, DTI messages ERR020, 120, 4060 INI003, 008—012 NWS101, 141, 201—204, 301, 401 OVD021, 022, 023, 031 SYS4696 TDS messages XMI messages	System resources
ERR4062 NWS301, 401, 501 OVD001—010, 024 XMI messages	Peripheral Equipment

Table 21
System message fault indicators and related fault types (cont'd.)

System messages	Type of fault
ERR090, 220, 270 OVD001—010 TRK messages	Trunk
ERR500 MWL500 NWS501 OVD001—010	Telephone

Visual fault indicators

To identify faults, use the following visual indicators:

- A major alarm display indicates a possible power, Call Server, or Small System Controller (SSC) card fault.
- Circuit card Light Emitting Diodes (LEDs) indicate a circuit card or a unit on a circuit card is disabled. For details on specific LEDs, see the following sections.
  - — "Circuit card features" (page 33)
  - — "NTDW60 Media Gateway Controller LEDs" (page 43)
  - — "Media Card LEDs" (page 46)

Clearing Core Call Server faults

CS 1000 Core Call Processor faults can disable the CP card and stop call processing. In addition, other equipment may not operate properly while a Call Processor fault is in the system.

When call processing stops on the Call Processor, you may need to replace the following equipment:

- CP PM Call Processor card (NTDW61)
- CP PM Signaling Server card (NTDW61)
- Media Gateway Controller card (NTDW60)
- Media Gateway Controller daughterboards (NTDW62, NTDW64, NTDW78)
- CP PIV Call Processor card (NT4N39)
- System Utility card (NT4N48)
- Drive Carrier card (NTDU67)
- CS 1000E Core Call Server (NTDU63)

- Call Server chassis (NTDU30)
- Alarm/Fan module (NTDU64)
- Power Supply module (NTDU65) or air filter
- Main power cord
- Uninterruptible power supply (UPS)

Table 22 "Call Server fault indications" (page 76) shows common Call Server fault indicators.

Table 22
Call Server fault indications

Indicator	Possible indications
System messages	BSD080, 085, 086, 103 CCED messages CED messages CIOD messages HWR messages INI001, 002, 004, 005, 007 IOD006, 007, 060, 061, 291—297 NWS030, 102, 103, 142 SYS messages SRPT 181, Major failure
Visual indicators	Major alarm on attendant console Red LED lit on Call Server alarm/fan module. See "Alarm/fan module features" (page 29) for details.
Maintenance displays	The System Utility card liquid crystal display (LCD) provides system messages that indicate normal and fault conditions. Interpretations of the maintenance display codes are in the *Software Input/Output Reference – System Messages* NN43001-712.
User reports	Major alarm reported by attendant

Call Server fault indications and actions

Table 23 "Call Server faults" (page 77) lists Call Server fault indications and associated actions. See "Fault clearing process" (page 71) for a complete fault-clearing process. If you must replace equipment to clear a fault, see "Replacing equipment" (page 109) for instructions.

Table 23
Call Server faults

Condition	Possible cause	Action
Software Installation Tool does not load	Mismatch between the Security Device and keycode	Positively identify the eight digits engraved on the face of the Security Device beneath the Nortel logo (NT SDID) with the NT SDID on the keycode floppy disk label, and verify the NT SDIDs match.
	Incorrect Install Program disk	Verify that you are using the correct Install Program disk for your system.
Data dump error, or no access to overlays and OVL005 message is displayed	Manual initialize button pressed during a backup that uses the Customer Configuration Backup and Restore feature	Issue the **ENLT** command at the TTY.
System Utility card LED is red and no TTY output on Com 1 System constantly rebooting	Defective CP card	Unseat the CP card and reinstall it. Make sure all cables are securely connected. If the fault remains, continue with this step. Replace the cable to the Com 1 port. If the fault remains, replace the CP PIV card. If the CP card is replaced and the symptoms persist, replace the Call Server.
System Utility card LED is red and TTY output on Com 1	Defective System Utility card	Ensure the Enable/Disable switch is in the enabled position. If the LED remains red, test the card by entering **LD 135** **TEST SUTL C 15** C represents the affected Call Server, either 0 or 1. If the fault remains, replace the System Utility card.
Defective RMD	Defective CF card	Stat RMD in LD 135 to obtain partition status. Repartition if partition is corrupt or unreadable, or replace the CF card.
FMD not responding	Defective or unprogrammed CF card	Reinstall software or replace FMD.
Ethernet port LEDs are off	Bad cable or cable not connected	Test cable, replace cable if necessary, and make sure all equipment power is on.
Ethernet ports unable to communicate	Autonegotiation failed	Check configuration of LAN equipment (must be set to autonegotiate).

Table 23
Call Server faults (cont'd.)

Condition	Possible cause	Action
Drive Carrier card not operating	Defective Drive Carrier card	Unseat the Drive Carrier card and reinstall it. If the Drive Carrier card does not recover, continue with this procedure. Test the card by entering **LD 137** **STAT CMDU** **TEST CMDU** If the problem continues, a CIOD system message appears. If the fault remains, replace the Drive Carrier card.
CD-ROM drive not reading disk	CD-ROM is damaged	If you have another CD, insert it into a known operational Drive Carrier card, and load the Software Installation Tool from the correct Install Program diskette. In the Software Installation Tool, go to the Tools Menu and select **<j> -To check the customer-specific part of the CD-ROM** If the test suceeds, it is unlikely the CD is damaged. However, if the test indicates a failure to read all files on the CD, the CD is damaged and must be replaced.
CD-ROM drive not operating	Defective CD-ROM drive	Remove the CD from the CD-ROM drive, place it in the CD-ROM drive of the other Call Server, and test operation. If the CD is operational, replace the Drive Carrier card that contains the faulty CD-ROM drive.

Table 23
Call Server faults (cont'd.)

Condition	Possible cause	Action
Fan LED or temperature LED is red	High room temperature	Adjust room temperature as necessary. Allow the system to cool for a few minutes and then reset the system.
	Defective alarm/fan module	Verify that the fans in the alarm fan/module are operational. Unseat and reinstall alarm/fan module. If the fault continues, replace the alarm/fan module.
	Power supply air filter is obstructed	Check filter to ensure it is clean. If the filter is dirty or damaged, clean or replace the filter as described in Procedure 27 "Cleaning and replacing the power supply air filter" (page 141).
The power LED is red	Power fault or defective power supply module	Turn off the power switch at the rear of the Call Server and remove the power cord. Loosen the locking screw at the front of the module. Unseat and reseat the module firmly. Tighten the locking screw and replace the power cord. Turn on the power switch and observe if failure has cleared. If the fault continues, replace the power supply module.
Note: When in shutdown mode, the power supply continues to power the LEDs on the alarm/fan module that indicate a power supply failure.		
All LEDs in the Call Server are off	Power switch is off	Turn the power switch on.
	Disconnected power cable	Check the power cable connection to the power supply module. Ensure that it is firmly connected. If the cable is connected, check the power cable connection to the other Call Server. If all power cables are firmly connected, go to the next possible cause.
	Defective power cable	Replace power cable.

WARNING
The following tests are performed on a live power connection.

Table 23
Call Server faults (cont'd.)

Condition	Possible cause	Action
All LEDs in the Call Server are off	No power at outlet	With a meter or test lamp, test for AC power at the outlet. If no power is available at the outlet when AC power is supplied through a UPS unit, repair or replace the UPS following the manufacturer's instructions. If no power is available at the outlet when AC power is supplied through commercial service (not through a UPS), take the necessary steps to have the commercial power restored. If power is available at the outlet, go to the next possible cause.
	Defective power supply	Turn the power switch on the back of the power supply to OFF (down). Wait at least 60 seconds, and then turn the switch back to ON (up). Ensure power supply is well seated and the locking screw is tightened. If all LEDs remain off, or the power LED on the alarm/fan module is red, replace the power supply.
	Defective alarm/fan module	If the Nortel display remains lit and the alarm/fan LEDs are all off, ensure that the alarm/fan module is well seated and the locking screw is tightened. If it is still not operating properly, replace the alarm/fan module.
	Defective Call Server	If the power supply and alarm/fan module are replaced and the symptoms persist, replace the Call Server.

Clearing Signaling Server faults

The Signaling Server is an OEM or commercial-off-the-shelf (COTS) 1U server that provides signaling for the system. Signaling Servers have ELAN and TLAN network interfaces that are connected to an Ethernet switch through CAT5 cables. Signaling Servers have two serial ports and

visual indicators for maintenance. Signaling Servers have three push buttons, one each for power, reset, and INI (initialization). No support is available for the INI button, USB ports, keyboard port, and mouse port.

Table 24
Signaling Server Diagnosis

Condition	Possible Cause	Action
Signaling Server not running. All LEDs off	No power to system	Check power cable.
	Power supply failed	Replace Signaling Server.
Signaling Server running with no fan noise	Fan failed	Replace Signaling Server.
CD-ROM drive tries to access CD-ROM but stops	CD-ROM media is corrupted	Replace CD-ROM disk.
CD-ROM drive not accessing CD-ROM. No green light.	CD-ROM Drive failed	Replace Signaling Server.
100BT light not on	Auto Negotiate Failed	Provision Ethernet Switch to 100MB. Switch Auto Negotiate off.
ELAN or TLAN network interface Link light not active	Bad connection to Ethernet switch	Check power on Ethernet switch. Check CAT5 Ethernet cable. Check Ethernet switch port.
	Failed network interface	Replace Signaling Server.
Signaling Server unable to boot from hard drive	Hard drive not formatted	Install software. See *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).
	Hard drive with bad sectors	Install software and use disk check option. Replace Server if disk check fails.
	Hard drive failed	Replace Signaling Server
Signaling Server not responding through serial port.	Software failed	Reset Signaling Server
Signaling Server boots and then stops.	No software loaded	Load software. See *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

MG 1000E faults

Clearing ELAN network interface faults

On each MG 1000E, the MGC card connects to the ELAN subnet through the ELAN network interface. A CAT5 or 100BaseT Ethernet cable connects the ELAN network interface to a Layer 2 switch on the ELAN subnet. This provides speech path switching and transmit and receive signaling messages.

Faults related to the ELAN network interface can cause system initializations, disable conference capability, or disable all terminal connections (such as trunks and telephones) on a card. ELAN network interface faults can also make functional equipment appear faulty.

Table 25 "ELAN network interface fault indicators" (page 82) provides fault indicators for MG 1000E ELAN network interface faults.

Table 25
ELAN network interface fault indicators

Indicator	Possible indications
System messages	CNF messages
	ERR020, 120, 4060
	INI003, 008—012
	NWS101, 141, 201—204, 301, 401
	OVD021, 022, 023, 031
	SYS messages
	TDS messages
	XCT messages
	XMI messages
Visual indicators	Red LEDs lit or flashing on circuit cards

Isolating MG 1000E ELAN network interface faults

Troubleshooting MG 1000E ELAN network interface faults is required when there is no connection or the connection is dropped between the ELAN network interface and the IP network.

Use a Serial Data Interface (SDI) terminal to troubleshoot faults with the MG 1000E ELAN network interface. Follow the steps in Procedure 7 “Troubleshooting for MG 1000E ELAN network interface” (page 83).

Procedure 7
Troubleshooting for MG 1000E ELAN network interface

Step	Action
1	Verify that the green Link LED on the MGC is on (indicating that the physical connection is operational). If the Link LED is off, check the physical connection by verifying that the cables are properly installed.
2	Test the IP connectivity between the CS 1000E Core Call Server and the Layer 2 switch by pinging the IP address of the Layer 2 switch. Perform the same test between the MG 1000E and the Layer 2 switch. Consult the local IS department for the appropriate IP address.
3	Use the **PING <ip address of the MG 1000E>** command in LD 117 to verify network connection.
4	Reenable any disabled components. Verify the 100BaseT connection between the Call Server and the MG 1000E is operating by pinging the IP address of the MG 1000E(s) configured.

ATTENTION
The MG 1000E supports only Layer 2 and Layer 3 switches. Software-based routers are not recommended.

--End--

Clearing MG 1000E faults

The MG 1000E provides the interface between network switching and terminal equipment (such as trunks and telephones). MG 1000E faults can disable network and terminal equipment. See Table 26 "MG 1000E fault indicators" (page 84) for MG 1000E fault indicators.

An overload (OVD) message on an MG 1000E indicates a network loop is disabled and that all connections on the loop are disabled. The network loop number corresponds to a specific card number in the MG 1000E. System messages can also indicate that one or more cards is defective or disabled without producing an OVD message. In either case, look up all system messages in *Software Input/Output Reference – System Messages* NN43001-712 and follow the instructions given.

Manual continuity tests can also be used to isolate Network and Intelligent Peripheral Equipment (IPE) faults. See *Software Input/Output Reference – Maintenance* NN43001-711 for details on performing the tests.

If the fault does not clear, or when call processing has stopped on the MG 1000E, you may need to replace the following equipment:

- Media Gateway Controller card (NTDW60)
- Media Gateway Controller daughterboards (NTDW62, NTDW64, NTDW78)
- CAT 5 IP cables
- NTDU14 Media Gateway
- NTDU15 Media Gateway Expander
- NTDK95 Expander cables
- NTDU30 Call Server
- NTDW61 CP PM Signaling Server
- NTDU40 Media card

Table 26
MG 1000E fault indicators

Indicator	Possible indications
Sample system messages	ERR4062 NWS301, 401, 501 OVD001—010, 024 XMI messages
Visual indicators	Red LEDs lit on circuit cards

Table 27 "MG 1000E fault causes and actions" (page 84) provides additional instructions for isolating faults in an MG 1000E. See "Fault clearing process" (page 71) for complete fault clearing process.

ATTENTION
Call processing on the Media Gateway is interrupted when the MGC is unseated.

Table 27
MG 1000E fault causes and actions

Condition	Possible cause	Action
Red LED on CP PM Red LED on MGC		

Table 27
MG 1000E fault causes and actions (cont'd.)

Condition	Possible cause	Action
Red LED on circuit card and system message	Card circuitry latched	Disable the card. Unseat and reseat it and then reenable the card. If the fault persists, go to the next possible cause.
LED is red on circuit card Two or more units on a circuit card are disabled System message indicating the circuit card or units on it are disabled	Defective circuit card	Enable the circuit card by entering: **LD 32** **ENLC l s c u** (where l s c u represents the card number) If the fault persists, replace the affected circuit card.
Common visual indication and system messages on MG 1000E Expander	Defective NTDK95 Expander cable	Replace the NTDK95 cable connecting the MG 1000E to the MG 1000E Expander.
Degradation of quality, such as noise issues in the MG 1000E Expander	Incorrectly connected NTDK95 Expander cable	The NTDK95 cable is a uni-directional cable with a ferrite bead at one end that you must terminate on the expansion chassis end. The NTDK95 cable direction can be identified by the label on the cable. This label must be installed at the expansion chassis end. An incorrectly connected cable can cause site quality degradation, such as noise issues in the Expander.
Multiple cards exhibit problems	Defective Media Gateway	Replace the Media Gateway.
Nortel logo is not lit or fan is not running	Loss of AC power Defective Media Gateway	Restore AC power. Replace the Media Gateway.
MG 1000E constantly rebooting	Defective SSC card or Media Gateway or Expander	Replace the SSC card, Media Gateway, or Expander.

Table 27
MG 1000E fault causes and actions (cont'd.)

Condition	Possible cause	Action
Red LED on SSC card and system messages Media quality has deteriorated Intermittent trunk or line problems Multiple system messages about this MG 1000E	Defective IP Links	View the status of the IP links by entering: **LD 135** **STAT IPL x** (x is the number for the MG 1000E, 1 through 128) Enable the MG 1000E by entering: **LD 32** **ENLS l s** (where l s are the MG 1000E loop and shelf numbers) If the fault remains, go to the next possible cause.
	Defective NTDK83 IP daughterboard in MG 1000E	Disable the MG 1000E by entering: **LD 32** **DISS l s** (where l s are the MG 1000E loop and shelf number) Replace the IP daughterboard on the NTDK20 SSC circuit card. If the fault remains, replace the SSC card.

MG 1000E Problems with transferring, placing conference calls, or Music-on-Hold

If several users cannot transfer or place conference calls, or calls do not receive Music-on-Hold (MOH), a circuit card that provides conference capability may be disabled. Look up all system messages in the *Software Input/Output Reference – System Messages* NN43001-712 and follow the instructions.

Also, ensure that sufficient DSP resources are provisioned for Music, conference, and RAN (see *Communication Server 1000E Planning and Engineering* for details) NN43041-220.

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

If the fault does not clear, you may need to replace some of the following equipment:

- NTDW60BA MGC
- MGC DSP daughterboard

Table 28 "Conference channels causes and actions" (page 87) provides additional instructions for isolating conference channel faults in an MG 1000E.

ATTENTION
Call processing on the affected Media Gateway is interrupted when the MGC is unseated.

Table 28
Conference channels causes and actions

Condition	Possible cause	Action
Several users cannot place conference calls when links and phones are operational.	Defective IP links	View the status of the IP Links by entering: **LD 135** **STAT IPL x** (where x is the number for the MG 1000E 1 through 128) If the fault remains, check the IP daughterboard conference loops. If the fault remains, check the NTDK20 SSC conference loops.
System message indicates conference loop is defective.	Defective IP daughterboard on SSC card	If a fault is indicated on a conference loop, replace the daughterboard on the Media Gateway.
System message indicates conference loop is defective.	Defective SSC circuit card	If a fault is indicated on conference loop, replace the NTDK20 SSC circuit card. Reuse the daughterboards and security device installed on the original NTDK20 SSC circuit card.

Table 28
Conference channels causes and actions (cont'd.)

Condition	Possible cause	Action
Defective conference loop with no system message	Defective IP daughterboard or SSC circuit card	If there are no messages indicating a fault on any conference loop, test each conference loop in the system by entering: **LD 38** **CNFC loop** ("loop" represents the conference loop number) If the conference loop is disabled, try to enable it by entering: **LD 38** **ENLL loop** ("loop" represents the conference loop number)
	Defective NTDK20 SSC card	Install a new NTDK20 SSC circuit card. Reuse the daughterboards and security device attached to the original NTDK20 SSC circuit card. If the card tests "OK", the NTDK20 SSC circuit card was defective. If after a few minutes the problem reoccurs, replace the Media Gateway.

Clearing Core faults

The MGC card in the MG 1000T Core is the primary processor for the MG 1000T platform. It performs system control and switching for the MG 1000T Core and Expansions.

Faults on the MG 1000T Core can stop call processing on the MG 1000T. In addition, other equipment may not operate properly while there is an MG 1000T Core fault in the system.

Table 29 "MG 1000T Core fault indications" (page 89) lists common fault indications for the MG 1000T Core.

Table 29
MG 1000T Core fault indications

Indicator	Possible indications
System messages	CCED messages CED messages CIOD messages HWR messages INI001, 002, 004, 005, 007 IOD006, 007, 060, 061, 291—297 NWS030, 102, 103, 142 SYS messages
Visual indicators	

Fault indicated on the Core

Table 30 "Core fault causes and actions" (page 89) lists fault indications and associated actions for the MG 1000T Core. See "Fault clearing process" (page 71) for complete fault clearing process.

ATTENTION
Call processing on the Media Gateway is interrupted when the Core MGC card is unseated.

Table 30
Core fault causes and actions

Condition	Possible cause	Action
Software Installation Tool does not load	Mismatch between the Security Device and keycode	Positively identify the NT SDID on the MG 1000T Core (eight digits engraved on the face of the Security Device beneath the Nortel logo) with the NT SDID on the keycode floppy disk label. Verify the NT SDIDs match.
Data dump error	Corrupt data on software daughterboard	Perform an **EDD NBK** command in LD 43 to restore the data.
	Security failure during an upgrade	Reenter the keycodes. Up to three invalid keycodes can be entered. After the third invalid keycode is entered, all current changes are lost and the Setup Program returns to the main menu.
Data dump error, or no access to overlays while OVL005 message is displayed	Manual initialize button pressed when performing a backup using the Customer Configuration Backup and Restore feature	Issue the **ENLT** command at the TTY.

Table 30
Core fault causes and actions (cont'd.)

Condition	Possible cause	Action
Red LED is lit on SSC card	Card circuitry latched	Disable the SSC card. Unseat and reseat the card and then reenable it. If the fault persists, go to the next possible cause.
	Improperly installed NTTK25 software daughterboard	Power down the system and remove the NTDK20 SSC card. Unseat and reseat the software daughterboard. Reinsert the NTDK20 SSC circuit card. Power up the system.
Red LED is lit on SSC card	Defective NTTK25 software daughterboard	Unseat the NTDK20 SSC circuit card and replace the software daughterboard. Reinsert the NTDK20 SSC circuit card.
	Improperly installed NTDK 83 IP daughterboard	Power down the system and remove the NTDK20 SSC card. Unseat and reseat the IP daughterboard. Reinsert the NTDK20 SSC circuit card. Power up the system.
	Defective NTDK83 IP daughterboard	Unseat the NTDK20 SSC circuit card and replace the IP daughterboard. Reinsert the NTDK20 SSC circuit card.
	Defective NTDK20 SSC card	If the fault persists, replace the NTDK20 SSC card. Reuse all daughterboards and the security device installed on the original NTDK20 SSC circuit card. Enable and test the card by entering: **LD 30** **TEST** If the new card passes the test, the original NTDK20 SSC circuit card was defective. If after a few minutes the problem reoccurs, replace the Media Gateway.

Table 30
Core fault causes and actions (cont'd.)

Condition	Possible cause	Action
System constantly rebooting	Defective Media Gateway	Replace the Media Gateway.
Nortel logo is not lit or fan is not running	Loss of AC power Defective Media Gateway	Restore AC power. Replace the Media Gateway. Enable and test the cards by entering: **LD 30** **TEST**

Clearing MG 1000E Expansion faults

Table 31 "MG 1000E Expansion fault causes and actions" (page 91) provides additional instructions for isolating faults in an MG 1000E Expansion. Initial indicators can be red LEDs on the circuit cards or a system message indicating a circuit card or units on it are disabled. Look up all system messages in the *Software Input/Output Reference – System Messages* NN43001-712 and follow the instructions given.

Table 31
MG 1000E Expansion fault causes and actions

Condition	Possible cause	Action
Software does not load	Improper Security Device	Positively identify the NT SDID on the MG 1000T Expansion (eight digits engraved on the face of the Security Device beneath the Nortel logo). Verify that it matches the NT SDID on the MG 1000T Core Security Device.
Layer 7 LED is Red Link LED is off or flickering	Defective NTDU0606, NTTK34, or CAT5 IP cable	Inspect the cable connections visually and check them physically. Replace defective cables as required.
Red LED on SSC Intermittent trunk problems Multiple system messages about an MG 1000T Expansion	Defective NTDK20 SSC card in MG 1000T	Disable the MG 1000T Expansion by entering: **LD 32** **DISS x** (where x is the number for the MG 1000T Expansion, 1 through 4) Replace the SSC card. Enable the MG 1000T Expansion by entering: **LD 32** **ENLS x** (where x is the number for the MG 1000T Expansion, 1 through 4)

Table 31
MG 1000E Expansion fault causes and actions (cont'd.)

Condition	Possible cause	Action
		Perform a circuit card test by entering: **LD 30** **TEST** (this command ensures that all circuit cards are reenabled in the MG 1000T).
Red LED on SSC card	Improperly installed NTTK25 software daughterboard	Power down the MG 1000T and remove the NTDK20 SSC card. Unseat and reseat the software daughterboard. Reinsert the NTDK20 SSC circuit card. Power up the MG 1000T.
	Improperly installed NTD K99 IP daughterboard	Power down the MG 1000T and remove the NTDK20 SSC card. Unseat and reseat the daughterboard. Reinsert the NTDK20 SSC circuit card. Power up the MG 1000T.
	Defective NTDK99 IP daughterboard	Unseat the NTDK20 SSC circuit card and replace the daughterboard. Reinsert the NTDK20 SSC circuit card.
	Defective Media Gateway or Expander	Replace the defective Media Gateway or Expander.
Red LED on circuit card Two or more units on a circuit card are disabled	Defective circuit card	Enable the circuit card by entering: **LD 32** **ENLC c** (where c represents the card number)
System message indicating the circuit card or units on it are disabled		Test the card by entering: **LD 30** **UNTT c** (where c represents the card number). If the fault persists, replace the affected circuit card.
Common visual indication and system messages on MG 1000T Expander	Defective NTDK95 Expander cable	Replace the NTDK95 cable connecting the MG 1000T Expansion to the MG 1000T Expander.

Table 31
MG 1000E Expansion fault causes and actions (cont'd.)

Condition	Possible cause	Action
Degradation of quality, such as noise issues in the MG 1000T Expander	Incorrectly connected NTDK95 Expander cable	The NTDK95 cable is a uni-directional cable with a ferrite bead at one end that you must terminate on the expansion chassis end. The NTDK95 cable direction can be identified by the label on the cable. This label must be installed at the expansion chassis end. An incorrectly connected cable can cause site quality degradation, such as noise issues in the Expander.
Multiple cards exhibit problems	Defective Media Gateway	Replace the Media Gateway. Enable and test the cards by entering: **LD 30** **TEST**
Nortel logo is not lit or fan is not running	Defective Media Gateway	Replace the Media Gateway
Media quality has deteriorated	Defective IP links	To view the status of the IP links, enter: **LD 135** **STAT IPL x** (where x is the number for the MG 1000T Expansion, 1 through 4) Perform Local and Remote Loopback tests on the IP links by entering: **LD 135** **LLBK IPL x** (where x is the number for the MG 1000T Expansion, 1 through 4) Enable the MG 1000T by entering: **LD 32** **ENLS x** (where x is the number for the MG 1000T Expansion, 1 through 4) If the fault remains, go to the next possible cause.
	Defective NTDK99 IP daughterboard in MG 1000T	Disable the MG 1000T Expansion by entering: **LD 32** **DISS x** (where x is the number for the MG 1000T Expansion, 1 through 4) Replace the IP daughterboard on the NTDK20 SSC circuit card. If the fault remains, replace the SSC card.

Clearing MG 1000T Core-to-Expansion link faults

The Core-to-Expansion links in the MG 1000T are an integral part of the MG 1000T functionality. The link provides speech path switching and transmit and receive signaling messages between the SSC cards.

Core-to-Expansion link faults can cause system initializations, disable conference capability, or disable all trunk connections on a card. The Core-to-Expansion link faults can also make functional equipment appear faulty.

Table 32 "IP Network fault indicators" (page 94) provides fault indicators for MG 1000T Core-to-Expansion link faults.

Table 32
IP Network fault indicators

Indicator	Possible indications
System messages	CNF messages
	DTA, DTC, DTI messages
	ERR020, 120, 4060
	INI003, 008—012
	NWS101, 141, 201—204, 301, 401
	OVD021, 022, 023, 031
	SYS messages
	TDS messages
	XCT messages
	XMI messages
Visual indicators	Red LEDs lit or flashing on circuit cards

Troubleshooting Core-to-Expansion link connectivity faults

Troubleshooting the Core-to-Expansion 100BaseT link is required when there is no connection or the connection is dropped between the MG 1000T Core and an MG 1000T Expansion. Procedure 8 “Troubleshooting Layer 2 and Layer 3 LAN connections for MG 1000T” (page 95) provides troubleshooting procedures for Layer 2 and Layer 3 connections.

Use an SDI terminal to perform the following procedures using overlay commands.

Layer 2 and Layer 3 LAN connections

The MG 1000T platform supports only Layer 2 and Layer 3 switches. Software routers are not recommended. To troubleshoot for Layer 2 and Layer 3 LAN connection, follow the steps in Procedure 8 “Troubleshooting Layer 2 and Layer 3 LAN connections for MG 1000T” (page 95).

Procedure 8
Troubleshooting Layer 2 and Layer 3 LAN connections for MG 1000T

Step	Action
1	Verify that the green Link LED on the daughterboard in the MGCis on (this indicates that the physical connection is functioning). If the Link LED is off, check the physical connection by verifying that the daughterboard and cables are properly installed.
2	Test the LAN connectivity between the Call server and the Layer 2/3 switch by pinging the IP address of the Layer 2/3 switch. Perform the same test between the MG 1000E and the Layer 2/3 switch. Consult the local IS department for the appropriate IP address.
3	To disable the link for testing, in LD 32, enter **DISS <n>** (where n = IP daughterboard port#).
4	To test the signaling and voice path of the daughterboard, in LD 135, enter **LLBK <link #>**. If the card fails the LLBK test, replace the IP daughterboard.
5	In LD 117, enter **PING <ip address of the MG 1000T Expansion>** to verify the network connection.
6	Re-enable any disabled components. Verify that the 100BaseT connection between the MG 1000T Core and the MG 1000T Expansion is operating by pinging the IP address of the MG 1000T Expansion(s) configured.

--End--

Monitoring 100BaseT link voice Quality of Service

Behavioral characteristics of the network are dependent on factors like Round Trip Delay (RTD), queueing delay in the intermediate nodes, packet loss, and available bandwidth.

The service level of each IP link is measured and maintained on the Call Server for the operation of the MG 1000Es. Information for latency and packet loss is collected from the hardware and processed. Based on system-configured thresholds, the level of service is derived and reported automatically or when the technician requests a report with the **PRT QOS**

<cab#> command in LD 117. See *Software Input/Output Administration* NN43001-611 and *Software Input/Output Reference – Maintenance* NN43001-711.

Data Network Ratings (Excellent, Good, Fair, and Poor) are calculated along with the actual parameter values for the network delay. See Table 33 "Campus data network voice quality measurements" (page 96) for the Data Network Ratings parameters for specific values of Packet Delay Variation (PDV) and packet loss.

Table 33
Campus data network voice quality measurements

	PDV Max 7.8 ms	PDV Min 0.5 ms	Packet loss
Excellent	<5 ms	<12 ms	< 0.5%
Good	5 - 25 ms	12 - 32 ms	0.5 - 1%
Fair	25 - 45 ms	32 - 52 ms	1 - 1.5%
Poor	>45 ms	>52 ms	> 1.5%

The values presented in Table 33 "Campus data network voice quality measurements" (page 96) assume that there is no echo cancellation mechanism and no particular mechanism for recovering lost packets.

The command **PRT PDV <cab#>** in LD 117 displays both the current size of the PDV buffer and the number of PDV underflows.

In addition, a warning message is printed when a parameter threshold or a combination of thresholds is reached. You cannot configure the thresholds.

In LD 117, the command **CHG PDV <port#> <delay>** is used to configure a PDV buffer size for each link basis. The **<delay>** parameter can take values from 0.5 ms to 8 ms. This value should be initially tested at default settings. Increase the <delay> parameter value by 0.5 ms increments if an unacceptable level of voice quality is experienced ("pops and clicks"). Decrease this value if an echo is experienced. The goal is to operate with the smallest buffer possible.

The PDV buffer size for each IP connection is configured at the Call Server for the MG 1000Es.

ATTENTION
Systems must meet the minimum data networking requirements from *Converging the Data Network with VoIP Fundamentals* NN43001-260.

Clearing trunk faults

This section deals with trunk faults on either the MG 1000E or MG 1000T. Trunk circuit cards provide the interface between the system and Central Office (CO) trunks, or between PBXs. The maintenance telephone can be used to test trunks. Two types of trunk cards are considered:

- E&M Trunk: provides four trunk units, each of which can be connected to a trunk configured to operate as one of the following:
  - E&M signaling trunk
  - Two-wire Tie trunk
  - Four-wire Tie trunk
  - Paging trunk
- Universal Trunk: provides eight trunk units, each of which can be connected to a trunk configured to operate as one of the following:
  - CO trunk
  - Direct Inward Dialing (DID) trunk
  - Two-way Tie, Dial Repeating (2DR)
  - Two-way Tie, Outgoing Automatic Incoming Dial (OAID) trunk
  - Recorded Announcement (RAN) trunk
  - Music trunk
  - Paging trunk

Trunk faults can cause problems (such as noise) on outside calls and can keep calls from entering or leaving the system.

Fault clearing procedures using an SDI terminal

See Table 34 "Trunk fault indicators" (page 97) for trunk fault indicators.

Table 34
Trunk fault indicators

Indicator	Possible indications
System messages	ERR090, 220, 270 OVD001—010 TRK messages
Visual indicators	Red LED lit on trunk circuit card

Trunk cannot make or receive calls

A user cannot make or receive calls over a trunk. An OVD system message may be received, indicating that this trunk has been disabled. Look up all system messages in the *Software Input/Output Reference – System Messages* NN43001-712 and follow the instructions.

If the fault does not clear, manual continuity tests can be used to isolate faults to peripheral equipment, such as E&M or Universal Trunk circuit cards. See *Software Input/Output Reference – Maintenance*NN43001-711 for details on performing the tests in LD 30.

Trunk connections from the main frame to the trunk cards can be checked with a butt telephone or test telephone. Check the trunk wiring at the entry point for dial tone and progress toward the Media Gateway.

Constantly observe and look up system messages as you replace equipment.

You may need to replace:

- E&M Trunk circuit card: NT8D15
- Universal Trunk circuit card: NT8D14
- any other trunk circuit card
- NTAK03 TDS/DTR circuit card
- trunk equipment (such as music source or paging equipment)

Table 35 "Trunk cannot make or receive calls(OVD message may be received)" (page 98) provides additional instructions for isolating trunk faults in an MG 1000E.

Table 35
Trunk cannot make or receive calls
(OVD message may be received)

Possible cause	Action
Excessive traffic in the system	Additional trunk circuit cards may be required to handle the traffic in the system.
Defective trunk circuit card	If the indicated circuit card is an E&M or Universal Trunk circuit card, hardware-disable it and then reenable to initiate a self-test. If the test fails, replace the circuit card. If the test passes, disconnect the wiring between the circuit card and the cross-connect terminal.

Table 35
Trunk cannot make or receive calls(OVD message may be received) (cont'd.)

Possible cause	Action
	Enable the TN by entering the following: For MG 1000E: **LD 32** **ENLU l s c u** (where l s c u represent loop, shelf, card and unit numbers) Wait for an OVD message. If an OVD message appears, replace the circuit card. If there is no OVD message, reconnect the wiring and go to the next possible cause.
Disabled or defective TN	Test the TN by entering: **LD 30** **UNTT l s c u** : Where: l - loops s - shelf c - card u - unit numbers Test other TNs by entering: **TEST** If the test fails, replace the indicated item and test again. Otherwise, go to the next possible cause.
Defective wiring	At the main cross-connect terminal, disconnect the wiring to the CO or other trunk equipment (such as a music source or paging equipment). Enable the TN and wait for an OVD message. If an OVD message appears, repair or replace the wiring to the Media Gateway. If there is no OVD message, repair or replace the wiring from the cross-connect terminal to the telephone. If the trunk circuit card still does not enable or there is still a trunk problem, reconnect the wiring and go to the next possible cause.
Defective trunk equipment	Make sure the CO equipment or other trunk equipment is not defective. If there is no problem with this equipment, go to the next possible cause.

Clearing Terminal Server faults

One potential fault that can occur with the MRV Terminal Server is database corruption. When there is a database fault, all Terminal Server LEDs flash and the console port does not respond.

To correct this fault, configure all parameters to factory default as described in MRV procedures.

ATTENTION
To prevent database corruption in the MRV Terminal Server, never remove the Flash card or power down the Terminal Server while the Flash card LED is illuminated.

Clearing IP Phone faults

For IP Phone fault clearing procedures, see *IP Phones Fundamentals* NN43001-368 and *IP Line Fundamentals.*

Database management

Contents

This section contains the following topics:

Tools to backup and restore customer databases

Element Manager provides access to Call Server backup and restore functions. See “Call Server backup, data dump, and restore” (page 157).

LD 43 and LD 143 provide different methods to backup and restore customer data:

- LD 43: Equipment Data Dump (EDD)
  - CP PIV: backs up the customer database from internal memory to the internal drive on the SSC and to RMD (compact flash)
  - CP PM: backs up the customer database from internal memory to file (/u/ccbr/ccbr.gz) and to RMD (compact flash)
- LD 43: The BKO command copies EDD output to removable media.
- LD 143: The Archive Database Utilities program provides a way to copy EDD output to removable media in a format organized by the user.
- LD 143: Customer Configuration Backup and Restore (CCBR) backs up customer data to an external device over a direct serial connection.

Equipment Data Dump

Procedure 9
Performing a CP PIV or CP PM datadump:

Step	Action
1	Log on to the system.
2	Insert a CF card into the active Call Processor RMD slot to back up the database.
3	Load the Equipment Data Dump Program (LD 43). `LD 43` Load program `.` EDD
4	When "EDD000" appears on the terminal, enter: `EDD` Begin the data dump

CAUTION
Loss of Data
If the data dump is not successful, do not continue. Contact your technical support organization. You must correct a data dump problem before replacing circuit cards or upgrading the system.

5	When the data dump is successful, the following messages appear:
	`Internal backup complete`
	`All files backed up!`
	`DATADUMP COMPLETE`

6	`****` Exit program

--End--

Customer Configuration Backup and Restore

Communication Server 1000, Release 5.0 introduced the Customer Configuration Backup and Restore (CCBR) feature to the large system. With this feature you can perform the following tasks:

- Locally or remotely access the system.
- Backup the customer configuration database to a remote PC or external storage.

- Restore or update the customer configuration database when the system is operating.
- Restore or update the customer configuration database when the system is not operating.

Equipment requirements

CCBR requires the following equipment:

- a computer that supports Xmodem communications protocol

  Ensure that your communications package complies with the protocol specifications described in *Communication Server 1000E Installation and Commissioning* . Not all Xmodem protocols are identical. Some may not operate properly with the CCBR feature.

- modems for remote access

To remotely access the system, connect a modem to an SDI port on the MGC or on the CP PM card.

To locally access the system, connect a computer directly to an SDI port on the MGC or on the CP PM card.

Feature operations

Procedure 10
Backing up the customer configuration database

Step	Action
1	Log on to the system.
2	Perform a data dump using LD 43, as shown in “Equipment Data Dump” (page 102).
3	Type ******** to exit LD 43.
4	Type **LD 143**. The system responds with the following: `CCBR000` . **ATTENTION** Review Steps 5 through 7 before you proceed. If you do not perform these steps within approximately 5 minutes after you issue the **XBK** command, the system times out.

5	Type **XBK**.
	The system responds with the following:
	`INFO:`
	`total packets : xxx`

```
number of retries :  0
receive timeouts :  0
system errors :  0
unknown characters :  x
transfer cancelled :  0
packets received out of sequence :  0
packets with corrupted sequence :  0
packets failed checksum/crc check :  0
incomplete packets :  0
duplicate packets :  0
```

6 Enter a header name for the configuration data backup file and press **Enter**. Enter up to 128 characters of text, including spaces, carriage returns, and line feeds.

If you enter more than 128 characters, the system exits text entry mode and responds with `R>`. If you do not want to enter text, press **Enter**.

The system responds with `R>` , to indicate that it is ready to continue.

ATTENTION
You must complete the next step within 2 minutes or the system times out. If a timeout occurs, return to Step 5 and retype the **`XBK`** command.

7 To receive the configuration database file, use the Xmodem protocol. The file arrives in binary format.

For information about receiving files, see the manual supplied with your communications software package.

8 Wait for the file transfer operation to end. File transfer time depends on database size and baud rate. When the file transfer completes successfully, the system responds as follows:

```
total packets :  xxx
number of retries :  0
receive timeouts :  0
system errors :  0
unknown characters :  x
transfer cancelled :  0
packets received out of sequence :  0
packets with corrupted sequence :  0
packets failed checksum/crc check :  0
incomplete packets :  0
duplicate packets :  0
```

If the file transfer fails, the system responds as follows:

```
total packets :  0
number of retries :  0
```

```
receive timeouts :  x
system errors :  0
unknown characters :  xx
transfer cancelled :  0
packets received out of sequence :  0
packets with corrupted sequence :  0
packets failed checksum/crc check :  0
incomplete packets :  0
duplicate packets :  0
ERROR from sx
```

The configuration database backup procedure is complete. Type **** to exit the program.

--End--

Procedure 11
Restoring or updating the configuration database (system operating)

Step	Action
1	Type **LD 143**.
2	The system responds with the following: `CCBR`
3	Type **XRT** to begin the configuration database restore. The system prepares to receive the database file from the computer and restore it to the (CP PIV) or to the Call Processor (CP PM).

4	The system responds with the following:
	`WAIT - - 2 MINUTES`
	`R>`

WARNING
The receiving file is erased at the start of this step. If a problem occurs during the restore procedure, do not leave the system in this state. Repeat the restore procedure. If you encounter further problems, perform an EDD to dump the current data to the SSC (CP PII and CP PIV) or to the Call Processor file (CP PM).

5	Send the backed up database file to the system using the communications software and the XModem protocol on the computer. The system displays the character C every 3 seconds until the file transfer is complete. The file transfer must finish before the

character C appears 20 times (approximately 1 minute) to avoid a system timeout.

The system site ID, n the configuration database records being sent, is compared to the ID on the system. If the IDs do not match, the data is restored, but the following warning message appears:

BKP0011	The site ID in the restored data does not match that of the system. This response is normal when you use this procedure as part of an installation process. Corrective action: Ensure that the customer data file is correct and that you are not restoring the wrong file to the system. If the file is correct, contact Nortel technical support.

When the database restore succeeds, the system responds: OK.

6 If the database restore fails, the system sends one of the following messages:

BKP0003	The received file contains invalid data. Corrective action: Check the transmitted data file to ensure that it is the correct one. Repeat the restore procedure using the **XRT** command. If the procedure fails again, a corrupt data file is a probability.
BKP0008	Transmission error occurred due to a timeout or excessive line noise. Corrective action: Repeat the procedure.

7 Reboot or sysload the system.

ATTENTION
Using the STAD command
Effective in CS 1000, Release 5.0, only users that have SEC_ADMIN privileges can change the system time and date. For more information about security enhancements, see *Security Management Fundamentals* (NN43001-604).

8 Reset the correct time and date:

```
LD 2
STAD (day) (month) (year) (hour) (minute) (second)
```

9 Check the time and date entered:

```
TTAD
```

Customer configuration database restore is complete.
To exit LD 43, type ********.

--End--

Coresilient server Backup

Use the Nortel Linux Base **sysbackup** and **sysrestore** commands to backup the network configuration information. For information about these commands see, *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

OAM Backup

The maintenance events of OAM audit log captures all the upgrades, backups, restores and patching. After the upgrade of Linux Base, all the OAM log files and syslog.conf are restored.

Use the **sysbackup** command to backup the oam.log, security.log, and /etc/rsyslog.conf files.

Use the **sysrestore** command to restore all the OAM log files.

The upgrade time depends on the number of OAM log files. The maximum number of files that can be backed up and restored is 60.

Replacing equipment

Contents

This section contains the following topics:

ATTENTION
Back up customer database
Before you replace circuit cards, back up the customer database. See “Equipment Data Dump” (page 102).

Removing the MG 1000E cover

Procedure 12
Removing the MG 1000E cover

Step	Action
1	Simultaneously push in the spring-loaded latches at either side of the cover and pull forward.
2	Set the cover down on a stable surface.

--End--

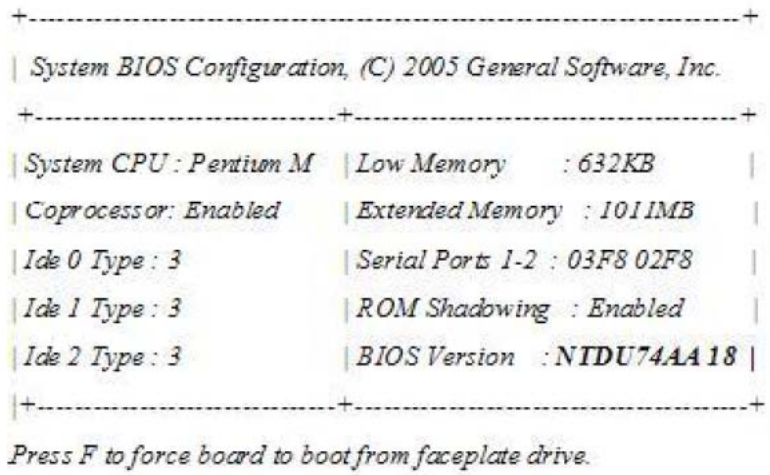
Replacing the NTDW61 CP PM Call Processor card

Note: If running a high availability (HA) system, both CP PM Call Processor cards must run the same BIOS Version. To Check the current BIOS version, see Procedure 13 “Upgrading the CP PM BIOS (vxWorks)” (page 110).
To upgrade the BIOS, see Procedure 14 “Upgrading the CP PM BIOS” (page 111).

Procedure 13
Upgrading the CP PM BIOS (vxWorks)

Step	Action
	Use this procedure for upgrading the BIOS for VxWorks CP PM systems. For Linux-based BIOS upgrade procedures, see NN43001-315.
1	Power up the CP PM hardware.
2	Observe the CP PM BIOS output from bootup screen, Figure 8 "System BIOS configuration" (page 111)

Figure 8
System BIOS configuration



3 If the BIOS version does not match with that of the other CP PM Call Server card, perform the Procedure 14 “Upgrading the CP PM BIOS” (page 111) procedure. If the BIOS version meets the requirements, proceed to installing your software.

--End--

Procedure 14
Upgrading the CP PM BIOS

Step	Action
1	Make a bootable Call Server Compact Flash (CF) RMD. To make a bootable Call Server CF RMD, follow these steps: **a** Select the correct software load zip file for your platform type (CPP4 or CP PM) from the software download site http://support.nortel.com/go/main.jsp. **b** Download the software load zip file. **c** Extract all the files to a temporary folder. You will see 6 folders under the root directory, as follows: • /backup • /install • /keycode • /licenses

- /swload
- /utilities

d Go to **utilities** directory and double click on **mkbootrmd.bat** file to make your RMD bootable.

ATTENTION

The Utility tool:

- works on all versions of Windows OS.
- does not validate whether the drive letter that the user enters is a valid RMD Compact Flash. So, make sure that you enter the correct RMD.
- has usually drive C: and D: as Windows hard disk partitions, so be careful when entering drive C or D.
- formats the drive, so by executing mkbootrmd.bat script you will lose the data on RMD Compact Flash or on any drive that you enter.

The mkbootrmd.bat script does the following:

- prompts the user to enter the RMD Compact Flash drive letter
- formats the RMD
- installs the VxWorks boot loader on to the boot sector of RMD.
- copies the fdrom.bin to RMD as bootrom.sys
- copies the nvram.sys to RMD.

2 Add a directory titled BIOS in the RMD root directory.

3 Download the CP PM BIOS software zip file from the software distribution site to your PC.

4 Extract the files to a temporary directory or create a folder you can easily locate. You will see two files in the directory:

- LMDU74AA_0018.ROM
- readmeCS.txt

5 Place the LMDU74AA_0018.ROM in the BIOS directory you created on the RMD.

6 Connect to serial port 0 on the CP PM.

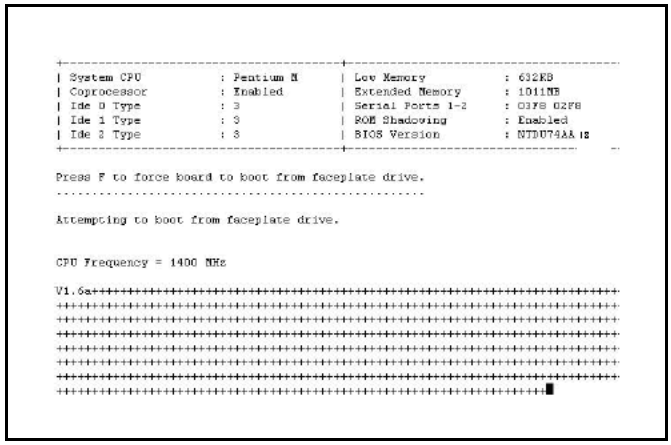
7 Insert the RMD into the faceplate Compact Flash slot.

8 Press the reset button.

Figure 9 "CP PM faceplate drive boot" (page 113) appears.

Press the **F** key to boot from the faceplate RMD.

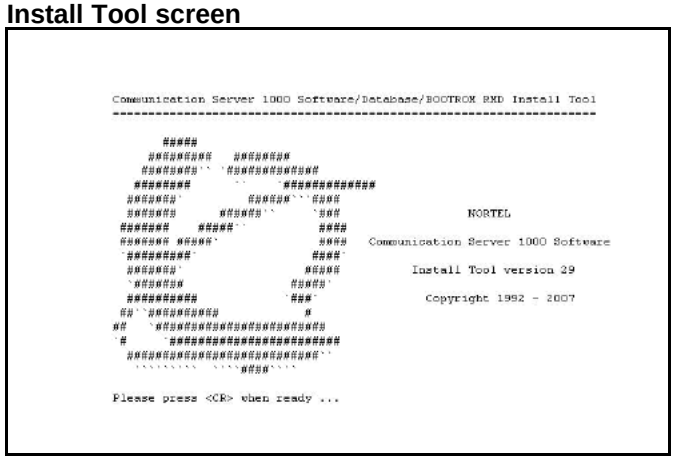
Figure 9
CP PM faceplate drive boot



9 Figure 10 "Install Tool screen " (page 113) appears.

Press **<CR>**.

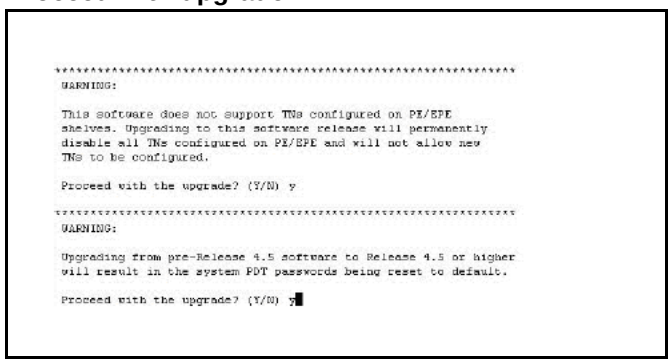
Figure 10
Install Tool screen



10 Figure 11 "Proceed with upgrade" (page 113) appears.

Press **y** twice to proceed with the upgrade.

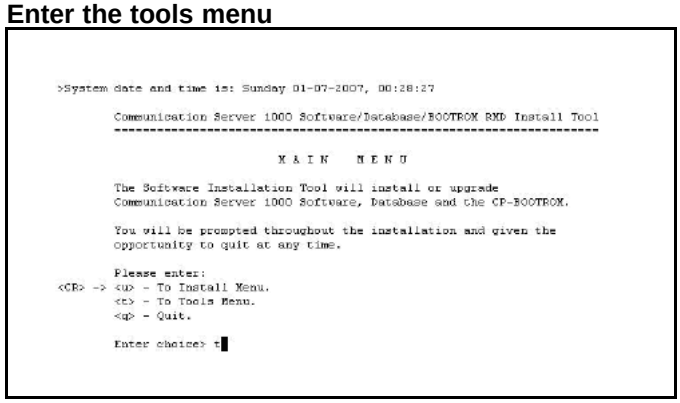
Figure 11
Proceed with upgrade



11 Figure 12 "Enter the tools menu" (page 114) appears.

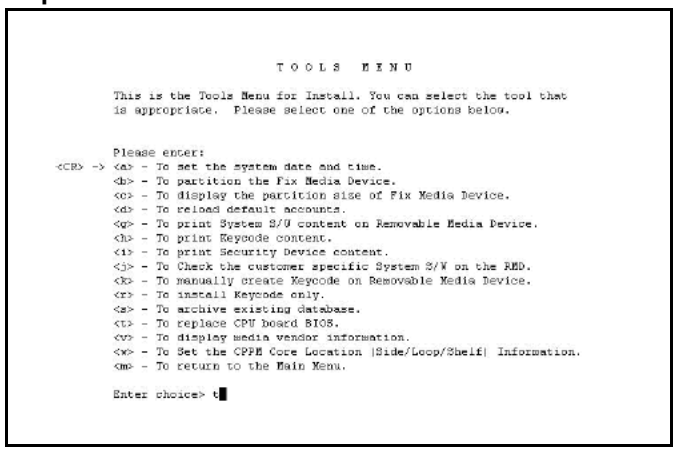
Press **t** to enter the tools menu.

Figure 12
Enter the tools menu



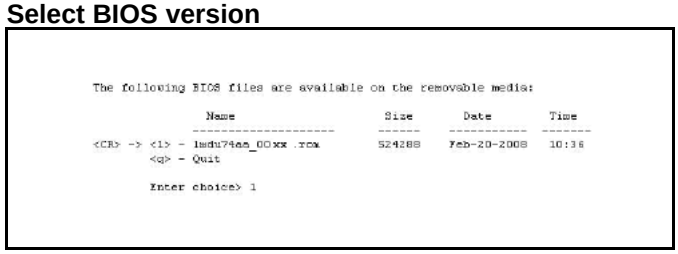
12 Figure 13 "Replace the CPU board BIOS" (page 114) appears. Press **t** to replace the CPU board BIOS.

Figure 13
Replace the CPU board BIOS



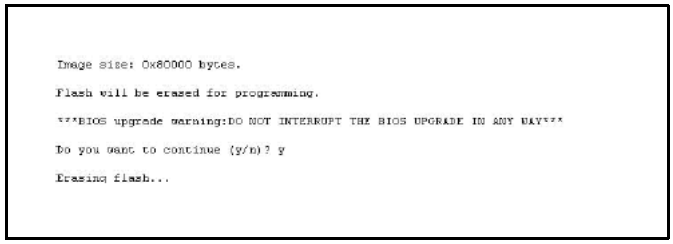
13 Figure 14 "Select BIOS version" (page 114) appears. Press **1** to select the BIOS rom.

Figure 14
Select BIOS version



14 Figure 15 "Erase flash and upgrade BIOS" (page 115) appears. Press **y** to erase the flash memory and start the BIOS upgrade.

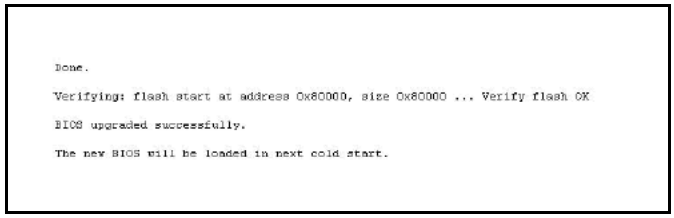
Figure 15
Erase flash and upgrade BIOS



CAUTION
Damage to Equipment Do not interrupt the BIOS upgrade process.

15 Figure 16 "Verify BIOS upgrade" (page 115) appears. Verify that the BIOS upgrade was successful.

Figure 16
Verify BIOS upgrade

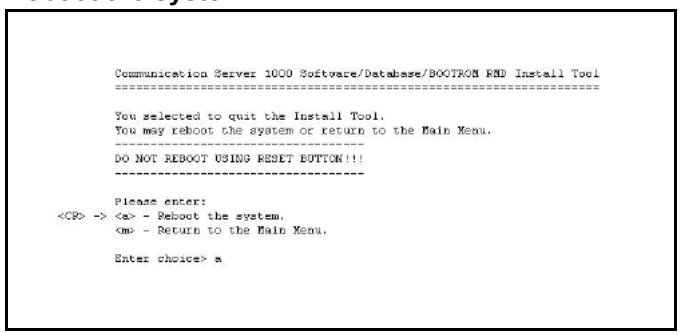


16 The tools menu appears. Press **m** to return to the main menu.

17 The main menu appears. Press **q** to quit and **y** to confirm.

18 Figure 17 "Reboot the system" (page 115) appears. Press **a** to reboot the system.

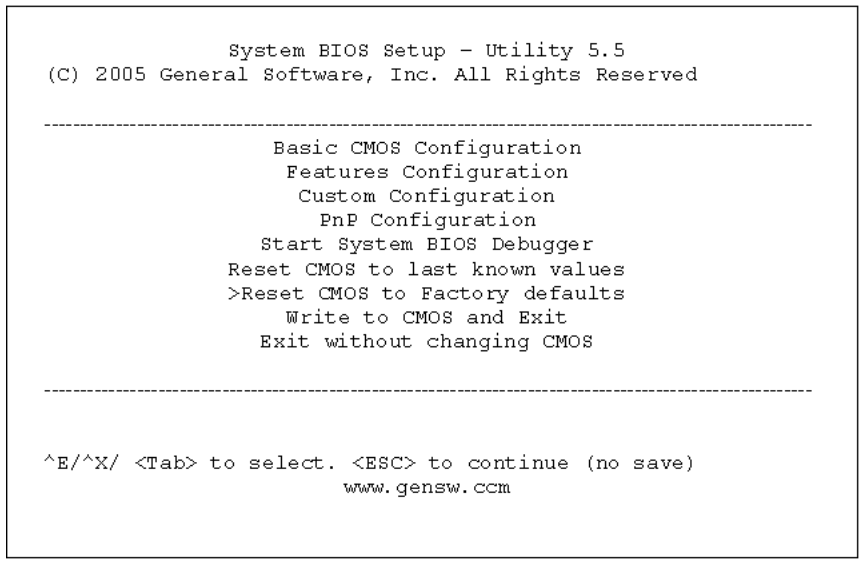
Figure 17
Reboot the system



19 During the reboot memory check, quickly press **CTRL+ C** to enter the CP PM BIOS.

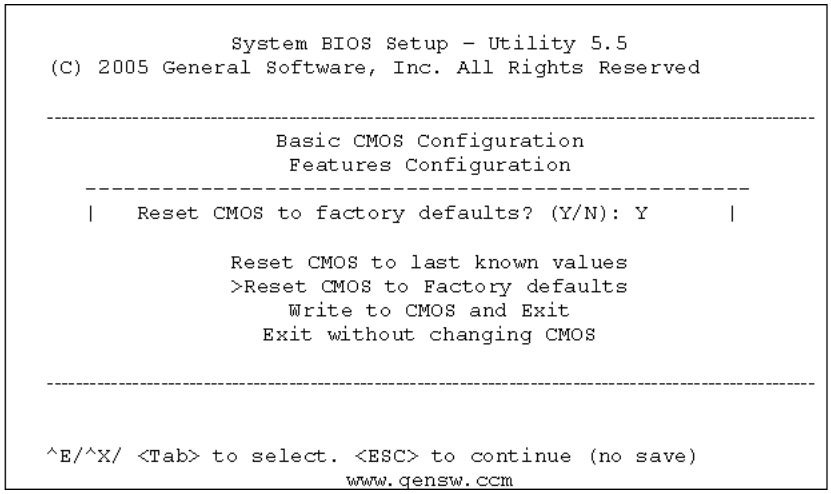
20 Figure 18 "CP PM BIOS setup" (page 116) appears. Select **Reset CMOS to factory defaults** from the menu.

Figure 18
CP PM BIOS setup



21 Figure 19 "CP PM BIOS reset" (page 116) appears. Press **y** to reset CMOS to factory defaults.

Figure 19
CP PM BIOS reset



22 The system reboots. Once the reboot is complete, the new BIOS version is displayed. Verify that the BIOS version is correct. You can now proceed with the Linux software installation.

ATTENTION
If you have reset the BIOS to factory defaults on an HA system, ensure that you re-define the 'CP PM Core Location |Side|Loop|Shelf| Information'. See Figure 13 "Replace the CPU board BIOS" (page 114).

--End--

Running a High Availability system

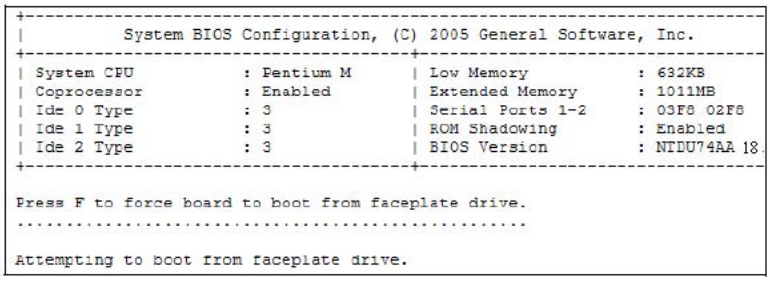
Step	Action
1	Check the card LED to verify that the Call Server card to be replaced is inactive.
2	If the card is active, switch Call Servers in LD 135: **a** In LD 135, load the program **b** Enter the SCPU command to switch call servers (if necessary)
3	In LD 135, split the CPU cores using the SPLIT command.

--End--

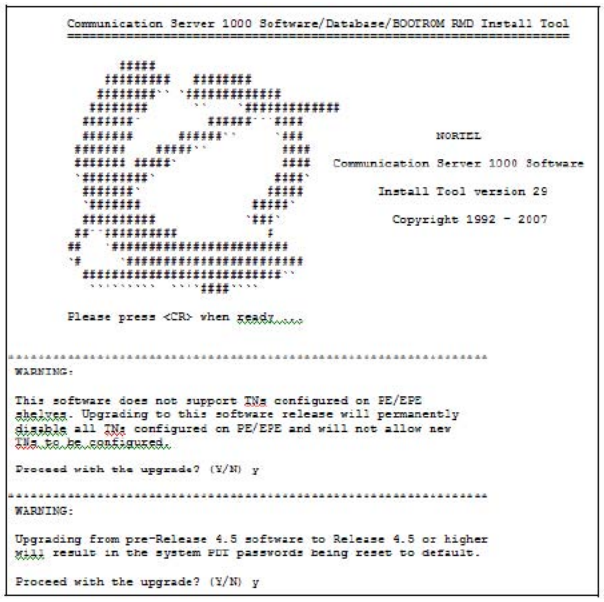
Procedure 15
Replacing the NTDW61 CP PM Call Processor card

Step	Action
1	If running a High Availability system
2	Perform an EDD on the active core to back up the customer configuration database.
3	Label and remove all cables.
4	Unlock faceplate latches and remove card.
5	Remove the security dongle and insert it on the replacement card.
6	Slide the CP PM Call processor into Slot 1 (or higher) of the chassis. Slot 1 provides for easiest cabling.
7	Lock in the card using the faceplate latches.
8	Reconnect all cables.
9	To install the software on the CP PM Call Processor:

1. Connect the terminal to port 0 with the NTAK19EC cable.
2. Insert the CF card into the Call Server faceplate.
3. Reboot the card by pressing the RST button on the faceplate of the Call Server. When prompted enter F to “force board to boot from faceplate drive” (prompt may appear twice).
   Figure 20
   Upgrade boot sequence



The Installation Tool banner screen appears:
Figure 21
Installation Tool banner



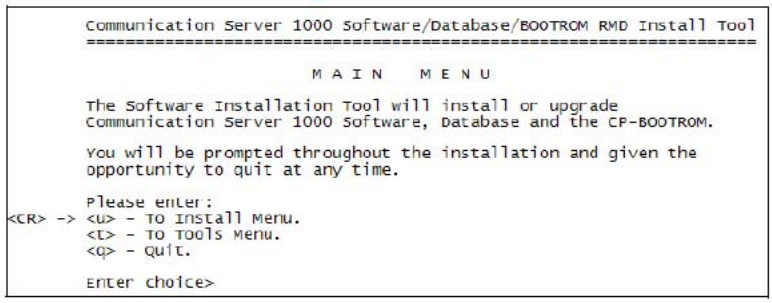
4. Enter y for both software warnings to proceed with the upgrade.

   Note: PE/EPE is not applicable for this upgrade as it only applies to large systems.

5. The Software Installation Tool Main Menu appears (see Figure 22 "Software Installation Tool Main Menu" (page 119)).

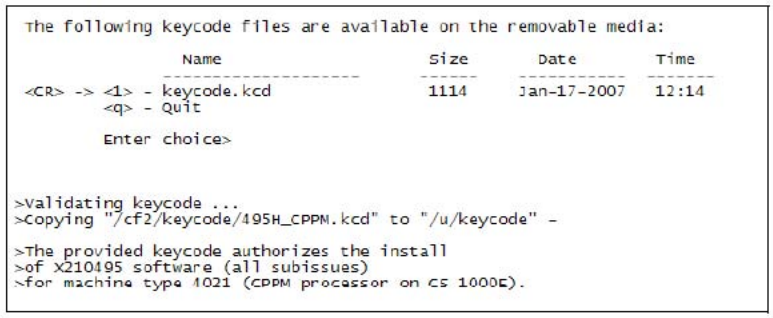
   Note: If the keycode files reside on a separate CF card, remove the software CF card and insert the CF card containing the keycode files. The keycode normally resides in the keycode folder of the OS CF card.

Figure 22
Software Installation Tool Main Menu



6. Enter **<CR>** or **u** to access the Install menu. The following screen appears (see Figure 23 "Keycode files" (page 119)).

Figure 23
Keycode files

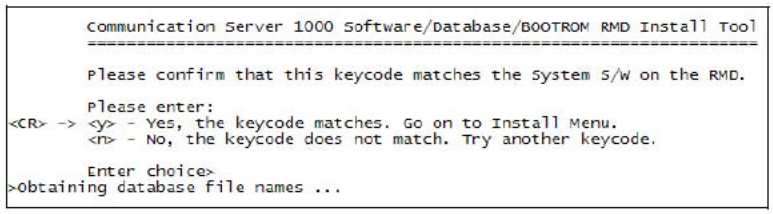


7. The keycode file appears in the list. Select the appropriate keycode file for this system and install the keycode.

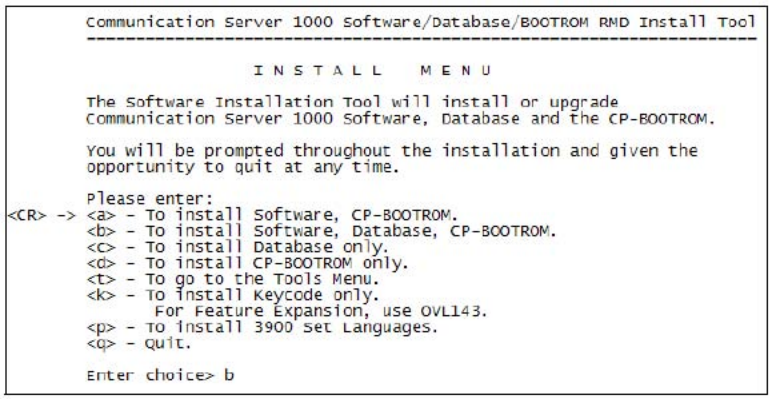
   Note: If the CF card was exchanged, insert the CF card containing CS 1000 Release 7.0.

8. Enter **CR** or **y** to confirm that the keycode matches the system software on the RMD (see Figure 24 "Keycode confirmation" (page 120)).

Figure 24
Keycode confirmation

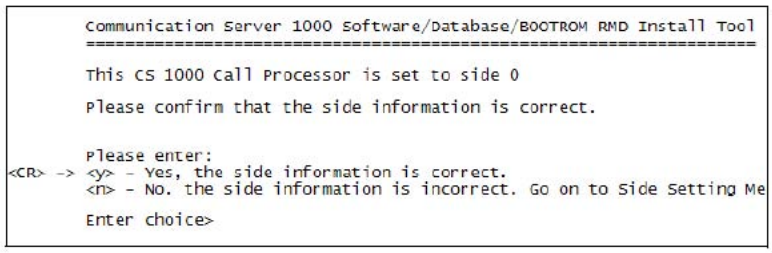


9. The Install Menu appears he Install Menu appears (see Figure 25 "Install Menu" (page 120)). Enter **b** to install the software, database, and CP-BOOTROM.
Figure 25
Install Menu



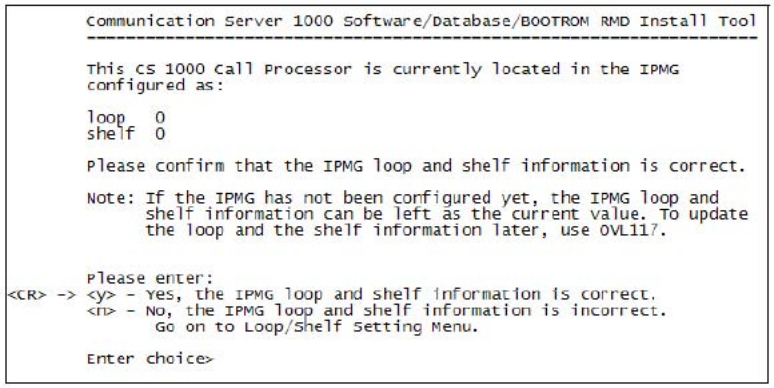
The following screen appears (see Figure 26 "Side information" (page 120)):

10. Enter **<CR>** or **y** to confirm that the call processor is set to side 0.
Figure 26
Side information



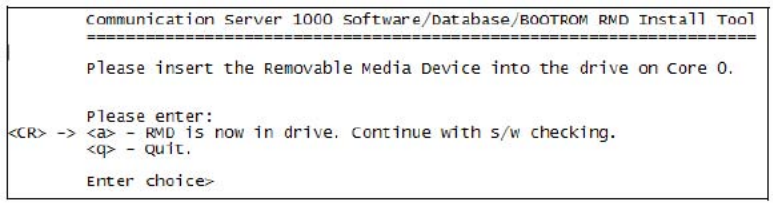
11. The location information screen appears (see Figure 27 "Call processor location" (page 121)), indicating that the call processor is located in loop 0 and shelf 0 of the IPMG. Enter **<CR>** or **y** to confirm their location.

Figure 27
Call processor location



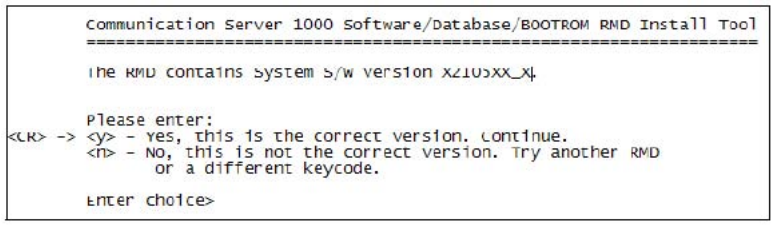
12. If not already present in the CF drive, insert the CF card containing CS 1000 Release 7.0 (see Figure 28 "Insert RMD" (page 121)).

Figure 28
Insert RMD

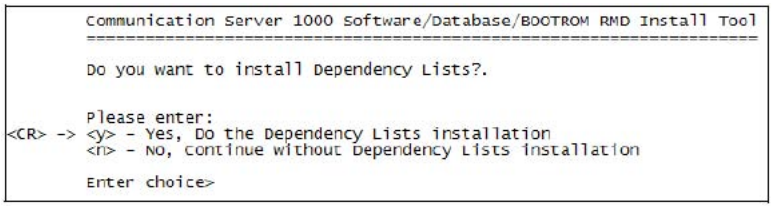


13. Enter **<CR>** or **y** to confirm that you have the correct software version (see Figure 29 "Confirm software version" (page 122)).

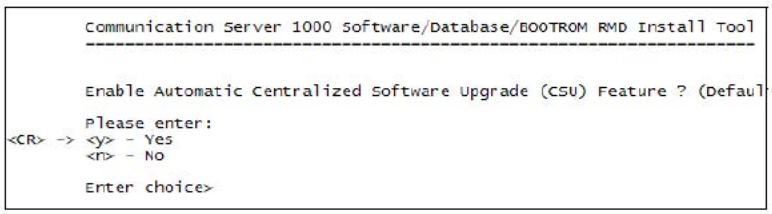
Figure 29
Confirm software version



14. Enter **<CR>** or **y** to install dependency lists and continue with the upgrade (see Figure 30 "Install Dependency Lists" (page 122)).
Figure 30
Install Dependency Lists

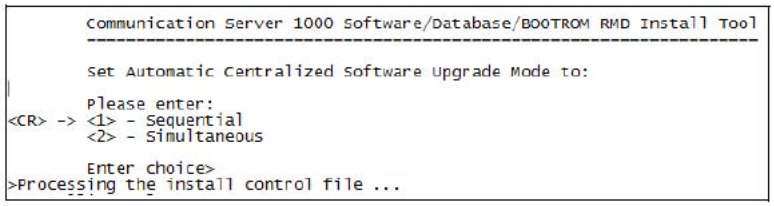


15. Enter **<CR>** or **y** (the default) to enable the Automatic Centralized Software Upgrade (CSU) feature (see Figure 31 "Centralized Software Upgrade" (page 122)).
Figure 31
Centralized Software Upgrade



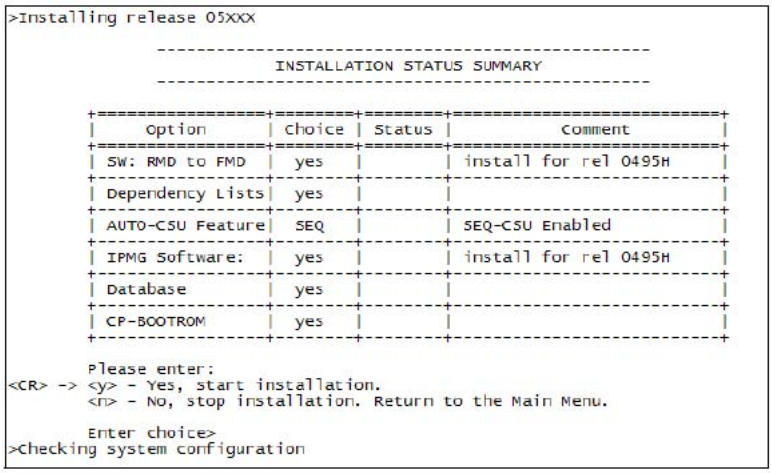
16. Set the CSU feature to Sequential by entering either <CR> or y (see Figure 32 "Automatic Centralized Software Upgrade Mode" (page 123))

Figure 32
Automatic Centralized Software Upgrade Mode



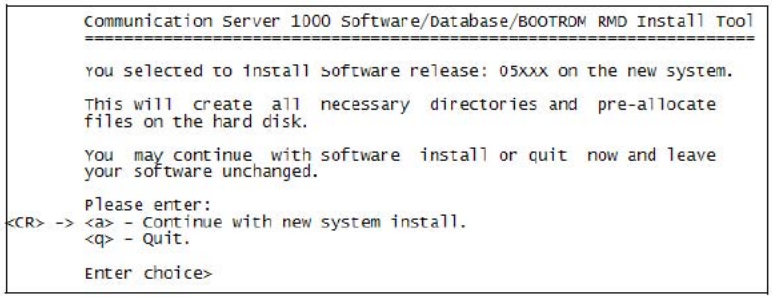
The Installation Status Summary screen appears (see Figure 33 "Installation Status Summary" (page 123)).

Figure 33
Installation Status Summary



17. Enter **<CR>** or **y** to begin the installation (see Figure 34 "Install Tool" (page 123)).

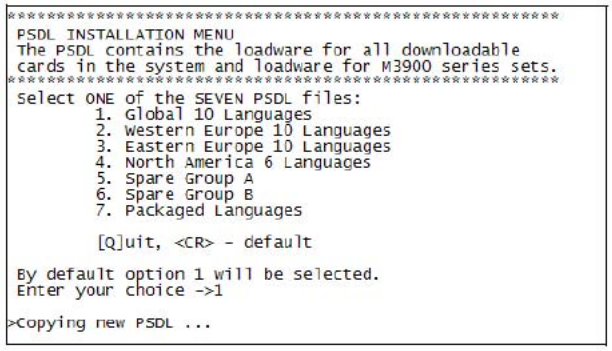
Figure 34
Install Tool



18. A prompt appears warning you that old system files will be deleted as a result of the installation. Enter **<CR>** or **y** to continue with the installation.

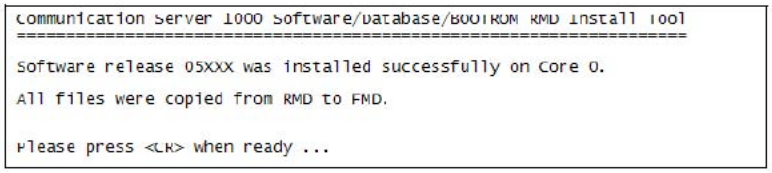
19. The PSDL Installation Menu appears (see Figure 35 "PSDL Installation Menu" (page 124)). Select the appropriate location based on your geographical location.

Figure 35
PSDL Installation Menu



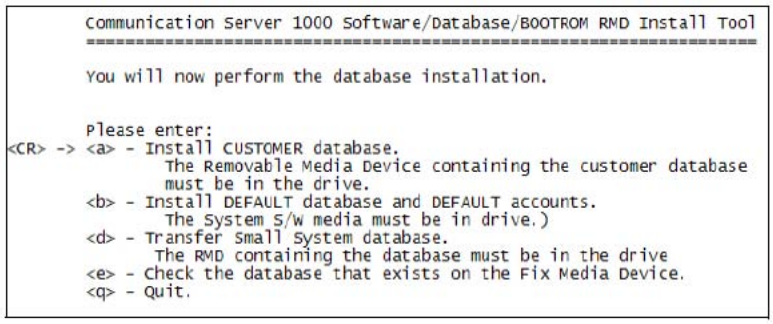
20. Enter **<CR>** to continue.
A message appears indicating that the installation on Core 0 was successful (see Figure 36 "Core 0 software installation complete" (page 124)).

Figure 36
Core 0 software installation complete



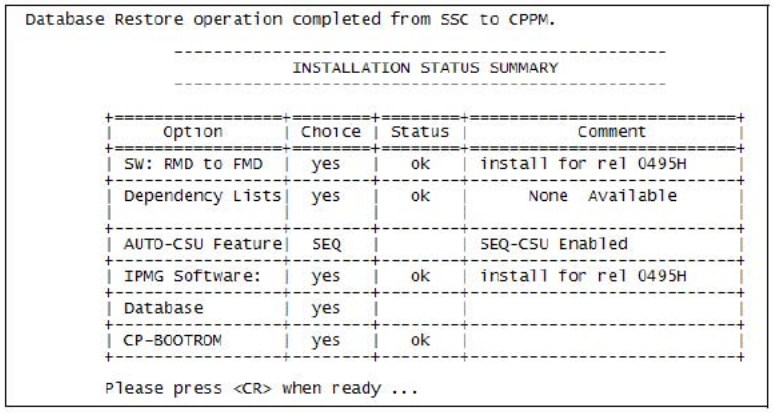
21. Enter <CR> to continue.
The following screen appears (see Figure 37 "Database installation" (page 125)).

Figure 37
Database installation



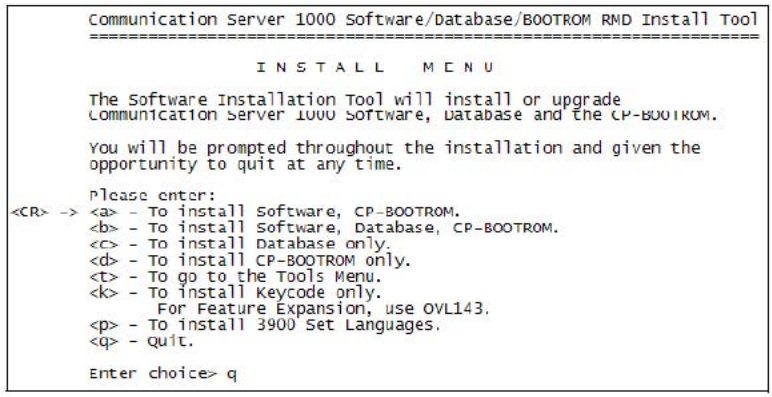
22. Enter **a**.
23. The Installation Status Summary screen appears, indicating that the installation was a success (see Figure 38 "Installation Status Summary" (page 125)). Enter **<CR>** to continue.

Figure 38
Installation Status Summary



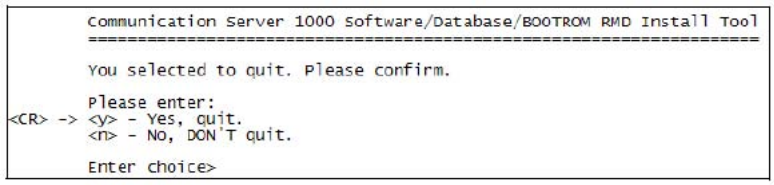
24. The Install Menu appears (see Figure 39 "Install Menu" (page 126)). Enter **q** to quit the Install Tool.

Figure 39
Install Menu



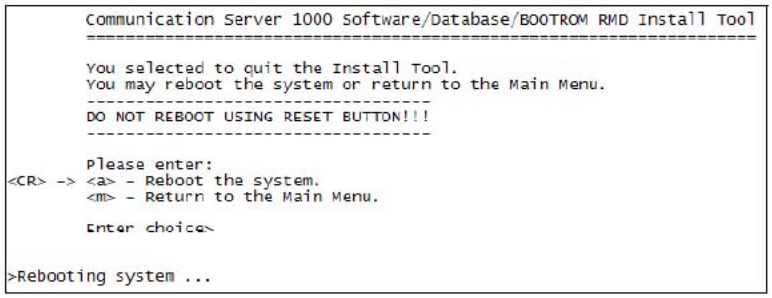
25. Enter **<CR>** or **y** to confirm selection (see Figure 40 "Quit Install Tool" (page 126)).

Figure 40
Quit Install Tool



26. Enter **<CR>** or **y** to reboot the system (see Figure 41 "System reboot" (page 127)). Once the system has completed its reboot, remove the CF from the faceplate.

Figure 41
System reboot



--End--

Replacing NTDW61 CP PM Signaling Server equipment

Replacing a defective Signaling Server

Replacing a defective Signaling Server requires that you perform a migration of the Signaling Server from one hardware platform to another.

For detailed instructions about how to replace a defective Signaling Server, see *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

Replacing the hard drive on a CP PM Signaling Server

For detailed instructions about how to replace the hard drive on a CP PM Signaling Server, see *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

CP PM Signaling Server card replacement

Before you replace a CP PM Signaling Server card, you must perform the following tasks:

- Use a Web browser to download the most recent version of the software from:

  www.nortel.com\support

- Create a bootable RMD with software on it.

  For more information, see “Create a bootable RMD with software” (page 128).

- Back up the NRS database.

  For more information, see “Back up the NRS database” (page 129).

Create a bootable RMD with software

CAUTION
Data Loss
The PC utility used in the following procedure (mkbootrmd.exe) does not validate whether the drive letter entered is a valid RMD CF card. You must enter the correct RMD drive letter when prompted or risk formatting the incorrect drive.

The installation RMD CF card must come preformatted and bootable from Nortel . Consumer CF cards are not bootable by default and must be made bootable. For more information, see Procedure 16 “Creating a bootable RMD with software” (page 128).

Procedure 16
Creating a bootable RMD with software

Step	Action
1	After downloading the software image file, unzip it to a directory on your PC.
2	Open the mkboot folder.
3	Double click the mkbootrmd.bat file. The mkbootrmd.exe utility is supported by all versions of Microsoft Windows.
4	After you see the prompt to do so, insert a blank 512 MByte CF card and press any key to continue.
5	At the prompt, enter the correct drive letter of the RMD and press Enter. The following prompt appears: Insert new disk for drive (drive letter:) and press ENTER when ready...
6	Press Enter. The disk is formatted and the boot sector files are created. After the boot sector files (bootrom.sys and nvram.sys) are successfully copied, the CF card is bootable A message appears stating the following: Check whether the following output shows "All the specified file(s) are contiguous" * * * Warning * * * IF THE FILES ARE NOT CONTIGUOUS, PLEASE RECREATE THE RMD * * * * * * * * * * Press any key to continue . . .

The following message is displayed:

All specified files are contiguous.
Press any key to continue . . .

See Figure 42 "mkbootrmd prompts " (page 129)

Figure 42
mkbootrmd prompts

7 Press any key.

8 Copy the files from the sub-folder they extract into, directly to the root of the RMD.

--End--

Back up the NRS database

Before replacing a CP PM Signaling Server card, back up the NRS database. For more information, see Procedure 17 “Backing up the NRS database” (page 129).

Procedure 17
Backing up the NRS database

Step	Action
1	Log into NRS.
2	Select the **Tools** tab from the top menu.
3	On the left navigation menu select **Database Backup**.
4	From the **Select backup action** drop down menu select **Manual Backup**.
5	Click **Submit**.
6	Ensure that the **manBackup** log does not indicate that there were any errors with the backup file creation.

7 Click the **Download the latest backup file** link to save the backup file to your local machine.

--End--

Replace a CP PM Signaling Server card

After you create a bootable RMD with software and complete the NRS backup, you can replace the CP PM Signaling Server card.

For information about installing Nortel Linux base on a CP PM, see *Linux Platform Base and Applications Installation and Commissioning* (NN4300-315).

Use the following procedure to restore a backed-up NRS database to your Signaling Server from your local PC.

Procedure 18
Restoring the NRS database

Step	Action
1	Log on to NRS Manager on the target Signaling Server (see).
2	Click the **Tools** navigation tab.
3	Click the **Database Restore** option on the navigation tree. The Database Restore web page appears.

Figure 43
Database Restore

4 Select the **Connected Signaling Server** option from the **Select restore source from** drop-down list and click **Submit** to restore the NRS database.

Data from the old StandBy database is replaced with data from the new NRS database.

Monitor the log messages that appear in the browser window. If additional log analysis is necessary, a generated XML file is accessible to the user.

Monitor these key logs:

- Logs indicating that some entries cannot be restored correctly:
  - The particular entry does not exist in the new database, so the user must check and provision it manually.
- Messages indicating corruption of the nrsback.tar file:
  - The nrsback.tar file is not properly formatted or the content is not recognizable to the Restoring tool. The user must check the tar file and possibly regenerate and upload it again.

ATTENTION
The new NRS database is loaded in standby DB view. You must activate the new NRS database to complete the migration process.

--End--

Replacing the NTDW60 Media Gateway Controller card

ATTENTION
Prior to starting this procedure, ensure that all of the latest MGC Loadware patches are applied to the PBX.

Procedure 19
Replacing the NTDW60 Media Gateway Controller card

Step	Action
1	Log into Element Manager.
2	Go to **System/IP Network** and click **Media Gateways**.
3	Select the Media Gateway Controller card (MGC card) that is to be replaced. Record the MGC card ELAN and TLAN IP information and the ELAN IP and hostname of the PBX.
4	Power down the chassis where the card is being replaced.

5 Label and remove all cables.

6 Unlock the faceplate latches.

7 Remove the NTDW60 MGC card from the Media Gateway and place the card on a clean, electrostatic discharge (ESD) surface.

8 Place the new NTDW60 MGC card on a clean, electrostatic discharge surface.

9 Remove the daughterboards from the defective MGC card. Be certain to note the card position (position 1 or position 2) the cards are removed from.

10 Reinstall the DSP daughterboards in the same position (position 1 or position 2) on the replacement MGC card. For more information, see"Replacing the NTDW62 or NTDW64 DSP daughterboard" (page 133).

11 Insert the MGC card into Slot 0 of the chassis.

12 Reconnect all cables.

13 Connect a terminal (9600-N-8-1) to port 0 of the Serial cable connected to the MGC card and boot the card.

14 Enter the following information from the old card for each of the following fields:

```
Hostname:  (optional)
ELAN IP: 0.0.0.0
ELAN subnet mask:  0.0.0.0
ELAN gateway IP:
TLAN IP: 0.0.0.0
TLAN subnet mask:  0.0.0.0
TLAN gateway IP :
Primary CS Hostname:  (optional)
Primary CS IP:
Leading Secondary CS Hostname:<enter>
Leading Secondary CS IP: 0.0.0.0
Secondary CS Hostname:<enter>
Secondary CS IP: 0.0.0.0
```

15 Reboot the MGC card.

16 Go to **Element Manager** and navigate to **IP Telephony/Media Gateway**.

17 Select the gateway you just replaced.

18 Verify the first screen information is correct and click **Next**.

19 Validate (and populate, if needed) any required information and click **Submit Changes**.

> ***Note:*** You must submit the MGC card information to transmit the full MCG configuration information to all MGC devices in the system. The MGC card reboots twice before coming into service. MGC Loadware should also be downloaded from the Call Server to get it in sync with the other MGCs.

To configure the MGC and install MGC software, see *Communication Server 1000E Installation and Commissioning* (NN43041-310).

20 Use commands such as **`LD 143 UPGMGSETUP PRT, UPGMG STAT, UPGMG <supl shelf>`** to check the upgrade settings, status and to initiate an MGC Upgrade.

For more information about MGC upgrade commands, see *Software Input Output Reference — Maintenance* (NN43001-711).

--End--

Replacing the NTDW62 or NTDW64 DSP daughterboard

To access the DSP daughterboards on the Media Gateway Controller, see "Replacing the NTDW60 Media Gateway Controller card" (page 131).

Procedure 20
Replacing the NTDW62 or NTDW64 daughterboard

Step	Action
1	Remove the NTDW60 Media Gateway Controller card from the Media Gateway and place the card on a clean, electrostatic discharge (ESD) surface.
2	Remove the defective DSP daughterboard.
3	Place the new DSP daughterboard in the position from which you removed the defective daughterboard: position 1 or position 2.
4	Using the supplied screws, securely attach the daughterboard to the MGC.
5	Reinsert the NTDW60 MGC card in slot 0 of the Media Gateway.

--End--

Replacing the NTDW65 Voice Gateway Media Card

Procedure 21
Replacing the NTDW65 Voice Gateway Media Card

Step	Action
1	In Element Manager, select **System > Maintenance** from the navigator. The **Maintenance** Web page appears. You can select an overlay or a function to perform maintenance. The default is overlay.
2	Select **Select by Functionality**. A list of available diagnostics appears.
3	Select **Network & Peripheral Equipment Diagnostics**. The **Network & Peripheral Diagnostics** page appears.
4	Select **DISC – Disable specified card** from the **Card Commands** list.
5	Enter the card number in the corresponding **Command Parameter** text box.
6	Click **Submit** to the right of the text box. The output from this command is shown in the text box in the lower half of the web page.
7	Remove the card: **a** Label and remove all cables. **b** Unhook the locking devices.
8	Install the replacement card: **a** Pull the top and bottom locking devices away from the card faceplate. **b** Hook the locking devices.

--End--

Replacing the NT4N39AA CP PIV Call Processor card

Procedure 22
Replacing the NT4N39AA CP PIV Call Processor card

Step	Action
1	Check the System Utility card maintenance display to verify that the Call Processor containing the CP PIV card to be replaced is inactive.

If the Call Processor containing the CP PIV card is active, switch Call Processors in LD 135:

`LD 135`	Load the program.
`SCPU`	Switch Call Processors (if necessary).

2 In LD 135, split the CPU cores:

```
SPLIT
```

3 Remove all cables connected to the CPU being replaced.

4 Use a small-bladed screwdriver to loosen the screws on each latch of the CP PIV card.

5 To remove the card, pull the faceplate latches outward and gently pull it out of the slot.

6 To install the replacement card, hold the card by the faceplate latches and gently push it into the slot until the connectors make contact with the backplane.

7 Gently push the latches forward to set the card and lock it in place.

CAUTION
Damage to Equipment
Never force the card into the slot. It the card gets stuck, remove it and try again.

8 Use a small-bladed screwdriver to replace the screws on the card.

9 Replace all cables on the replaced CP PIV card.

ATTENTION
Before continuing with this procedure, you must reinstall the software from Compact Flash. See Installing the software on the CP PM Call Server.

10 After the inactive Call Server reloads, check status in LD 135:

```
STAT CPU
```

11 In LD 135, on the active Call Server, rejoin the two CP PIV cards:

```
JOIN
```

12 After the disk sync and memory sync complete, enter the following in LD 135:

`STAT CPU`	To check for normal system operation.

13 In LD 135, verify that the replaced CP PIV card can control call processing:

`SCPU`	To check replaced CP PIV.

14 Switch Call Server back, if necessary.

--End--

Replacing the NT4N48 System Utility card

ATTENTION
On a CS 1000E, the System Utility card minimum vintage is NT4N48BA.

Procedure 23
Replacing the NT4N48 System Utility card

Step	Action
1	Check the System Utility card maintenance display to verify that the Call Server containing the CP PII card to be replaced is inactive.
	a If the Call Server containing the System Utility card is active, switch Call Servers in LD 135:
	`LD 135` To load the program.
	`SCPU` Switch Core (if necessary).
2	In LD 135, split the Call Servers:
	`SPLIT`
3	In LD 135, on the inactive Call Server, software-disable the System Utility card:
	`DIS SUTL c 15` Disable the System Utility card, where: c = Call Server number (0 or 1)
4	Hardware-disable the System Utility card: configure the faceplate switch to DIS.
5	Use a small-bladed screwdriver to remove the screws from the System Utility card.
6	To remove the card, hold the card by the faceplate latches and gently pull it out of the slot.
7	Before you install the new System Utility card, hardware-disable it: configure the faceplate switch to Dis.
8	Ensure the security device is installed on the card.
9	Ensure the switch setting for core side is configured appropriately (for Call Server 0 or Call Server 1).

10 To install the replacement card, hold the card by the faceplate latches and gently push it into the slot until the connectors make contact with the backplane.

11 Gently push the latches forward to set the card and lock it in place.

CAUTION
Damage to Equipment
Never force the card into the slot. It the card gets stuck, remove it and try again.

12 Use a small-bladed screwdriver to tighten the screws on the card.

13 Hardware-enable the System Utility card: configure the faceplate switch to ENB.

14 In LD 135, software-enable the System Utility card:

`ENL SUTL c 15`	Enable the System Utility card, where: c = Call Server number (0 or 1)

15 In LD 135, check status:

`STAT SUTL c 15`	Check the System Utility card status, where: c = Call Server number (0 or 1)

16 In LD 135, on the active Call Server, rejoin the two Call Servers:

```
JOIN
```

--End--

Replacing the NTDU67 Drive Carrier card (CP PII only)

See *Software Input/Output Administration* NN43001-611 for a description of all maintenance commands, and *Software Input/Output Reference – System Messages* NN43001-712 for interpreting system messages.

CAUTION
Service Interruption
At some point in this procedure, the system warm starts, causing a momentary interruption in call processing.

Procedure 24
Replacing the NTDU67 Drive Carrier card

Step	Action
1	Check the Drive Carrier card maintenance display to verify that the Call Server containing the Drive Carrier card to be replaced is inactive. **a** If the Call Server containing the Drive Carrier card is active, switch cores in LD 135: `LD 135` To load the program. `SCPU` Switch Core (if necessary).
2	In LD 135, split the CPU Cores: `SPLIT`
3	Power down the Call Server using the power switch at the right rear of the Call Server.
4	Use a small-bladed screwdriver to loosen the four screws on the Drive Carrier card.
5	Unhook the locking devices and remove the Drive Carrier card.
6	Put the Drive Carrier card being replaced into a static bag and box.
7	Insert the new Drive Carrier card into the Call Server slot.
8	Lock the locking devices by pushing them gently towards the faceplate.
9	Use a small-bladed screwdriver to tighten the screws on the Drive Carrier card.
10	Press the Reset button on the CP PII Call Processor card. When the keycode is validated against the Security Device, the Install menu is displayed.
11	Choose **<b> - To Install Software, Database, CP-BOOTROM** from the Install Menu.
12	Install the Operating Software from the Install Disk. See *Communication Server 1000E Software Upgrades* NN43041-458.
13	Install the Customer Database.
14	In LD 135, check status: `STAT CMDU` This checks the Drive Carrier card status
15	In LD 135, on the active Call Server, rejoin the two Call Servers:

```
JOIN
```

--End--

Replacing the NTDU64 alarm/fan module

Procedure 25
Replacing the NTDU64 alarm/fan module

Step	Action

Note: *The alarm/fan module can be replaced without powering down the Call Server.*

1 Use a Phillips screw driver to loosen the alarm/fan module locking screw.

2 Pull the alarm/fan module out of the Call Server. (See Figure 44 "Alarm/fan module" (page 139)).

Figure 44
Alarm/fan module

3 Insert the replacement alarm/fan module into the vacated slot and use a Phillips screw driver to tighten the locking screw.

--End--

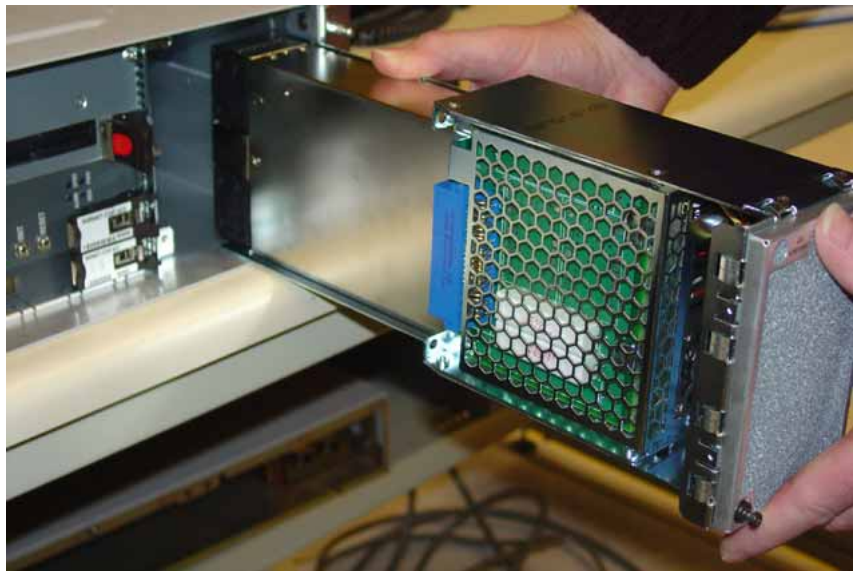
Replacing the NTDU65 power supply module

Procedure 26
Replacing the NTDU65 power supply module

Step	Action
1	Unplug the power cord at the rear of the Call Server.
2	Loosen the locking screw on the front of power supply.
3	Unseat the power supply module by pulling on the module handle.

4 Pull the power supply out of the Call Server. (See Figure 45 "Power supply module" (page 140))

Figure 45
Power supply module



5 Insert the replacement power supply into the vacated slot and ensure it is well-seated.

6 Use a Phillips screwdriver to tighten the locking screw on the power supply.

7 Reattach the power cord at the rear of Call Server and reconnect to the power source.

8 Tag defective equipment with a description of the problem, and package it for return to a repair center.

--End--

Figure 46 "CS 1000Epower supply air filter" (page 141) shows the Call Server power module air filter (P06094950). It consists of one aluminium frame and foam insert. The air filter foam kit (N0003712) contains ten replacement foam inserts.

Figure 46
CS 1000Epower supply air filter

Procedure 32 “Removing the NTAK20 and NTAK93/NTBK51 from the NTBK50 card” (page 146) describes how to clean and replace the air filter.

Procedure 27
Cleaning and replacing the power supply air filter

Step	Action
	Note: *The power supply can remain powered on during this procedure.*
1	To remove the power supply air filter, gently unsnap the filter from the front of the power supply module. If the aluminium frame is damaged, replace the filter.
2	Pull the foam insert loose from the frame. If the foam is damaged, replace the foam insert.
3	To clean the foam insert, rinse it with clean water under a tap or carefully vacuum it. After rinsing, allow the foam to dry thoroughly before reinstalling in the frame.
4	To reinstall the air filter, replace the foam insert into the aluminium frame and gently snap the aluminium frame back into the small slots on the front of the power supply module.

--End--

Accessing Media Gateway internal components

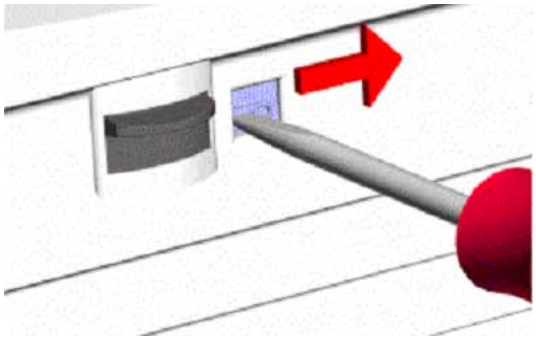
This procedure describes how to access components in the Media Gateway and Expander. To remove the front cover for access to terminal components, follow the steps in Procedure 28 “Removing the front cover for access to internal components” (page 142).

CAUTION
CAUTION WITH ESDS DEVICES
To avoid card damage from static discharge, wear a properly connected antistatic wrist strap.

Procedure 28
Removing the front cover for access to internal components

Step	Action
1	If the front cover lock latches are in their locked position, use a flat screwdriver to slide the icon away from the latch. See Figure 47 "Inserting screwdriver in slot" (page 142).
2	Simultaneously slide both spring-loaded latches toward the bottom of the cabinet and pull forward. Lift the cover upward to remove it from the cabinet. See Figure 48 "Depressing latches and pulling back on front cover" (page 143).

Figure 47
Inserting screwdriver in slot



ATTENTION
The bottom of the front cover is supported by but is not secured to the cabinet. Be careful not to drop the cover.

Figure 48
Depressing latches and pulling back on front cover

--End--

Replacing the NTAK02 SDI/DCH circuit card

The NTAK02 SDI/DCH circuit card can be installed only on the MG 1000T platform.

Procedure 29
Replacing the NTAK02 SDI/DCH circuit card

Step	Action
1	If the following circuit cards are configured, disable them in the following overlays: SDI `LD 48` DCHI `LD 96` The system may initialize if you do not perform this step.
2	Hold the SDI/DCH circuit card by the lock latches, unlock the latches, and slide the circuit card out of the Media Gateway.
3	Verify the settings of the switches and jumper plugs on the replacement circuit card and correct any settings that need to be changed. Ensure the settings are the same as the existing circuit card. For information about settings see the *Communication Server 1000E Installation and Commissioning* NN43041-310.
4	Hold the SDI/DCH circuit card by the lock latches and slide it into its assigned slot until it connects with the backplane.
5	Secure the lock latches on the circuit card.

6 If the following circuit cards were previously disabled, enable them in the following overlays:

SDI	`LD 48`
DCHI	`LD 96`

--End--

Replacing the NTAK03 TDS/DTR circuit card

Procedure 30
Replacing the NTAK03 TDS/DTR circuit card

Step	Action
1	Disable the SDI ports in LD 48.
2	Disable the TDS channels and Digitone Receivers in LD 34.
3	Hold the TDS/DTR circuit card by the lock latches, unlock the latches, and slide the circuit card out of the Media Gateway.
4	Hold the replacement TDS/DTR circuit card by the lock latches and slide it into its assigned slot until it connects with the backplane.
5	Secure the lock latches on the circuit card.
6	Enable the SDI ports, TDS channels, and Digitone Receivers in their respective overlays.

--End--

Replacing the NTAK79 or NTBK50 2.0 Mb PRI card

NTAK79 and NTBK50 2.0 Mb PRI cards can be installed only on the MG 1000T platform.

Procedure 31
Replacing the NTAK79 or NTBK50 2.0 Mb PRI card

Step	Action
1	If the card is an NTAK79, or is an NTBK50 with the NTAK93 DCHI daughterboard attached, disable the associated D-channel using the following overlay and commands: `LD 96 DIS DCH X` If the card is an NTBK50 with the NTBK51 DDCH daughterboard attached, disable the associated downloadable D-channel using the following overlay and commands:

```
LD 96              DIS DCH X


LD 96              DIS MSDL X
```

2 Disable the Clock Controller using these commands:

```
LD 60              DIS CC 0
```

3 Disable the PRI pack using these commands:

```
LD 60              DISL X
```

The LEDs on the front of the card change from green (enabled) to red (disabled.) For this to happen, the **DIS MSDL** command must be used, as in step 1.

4 Hold the circuit card by the lock latches, unlock the latches, and slide the circuit card out of the Media Gateway. If required, remove any daughterboards that may be attached. See Procedure 32 “Removing the NTAK20 and NTAK93/NTBK51 from the NTBK50 card” (page 146).

5 On the replacement PRI circuit card, configure any switches and install any daughterboards as required. Hold the card by the lock latches and slide it into its assigned slot until it connects with the backplane.

6 Secure the lock latches on the circuit card.

7 Enable the Clock Controller and the PRI in their corresponding overlays:

```
LD 60              ENL CC 0

LD 60              ENLL X
```

The associated DCHI/DDCH is automatically enabled.

8 Check the tracking of the Clock Controller with the following overlay:

```
LD 60              SCK 0
```

If it is not tracking or is not locked, use the following commands to track:

```
LD 60              TRCK PCK/SCLK
```

--End--

Removing daughterboards from the NTBK50 card

Because of the physical layout of the motherboards and daughterboards, remove the NTAK20 before the NTAK93/NTBK51.

Procedure 32
Removing the NTAK20 and NTAK93/NTBK51 from the NTBK50 card

Step	Action
1	Starting at the two corners opposite the connector, gently lift each corner out of the locking groove of the standoff.
2	At the two corners adjacent to the connector, gently lift the entire side until the mounting holes are clear of the locking groove of the standoff.
3	To remove the connector pins, grasp the edge of the board adjacent to the connector and lift gently.

--End--

If more than one NTBK50 card is installed, the additional cards may not carry daughterboards, depending on the system configuration. At least one NTAK20 for each system is required.

Mounting the daughterboards

Work on a flat, static-free surface when mounting or removing daughterboards. To install the NTAK93 and NTBK51 daughterboard before the NTAK20 daughterboard, follow the steps in Procedure 33 “Installing the NTAK93/NTBK51 daughterboard before the NTAK20 daughterboard” (page 146).

Procedure 33
Installing the NTAK93/NTBK51 daughterboard before the NTAK20 daughterboard

Step	Action
1	Visually inspect the connector pins on the underside of the daughterboard. Realigned bent pins prior to mounting.
2	Place the NTBK50 flat on an antistatic pad.
3	From an overhead view, with the daughterboard parallel above the NTBK50 and the connector pins aligned over the connector sockets, line up the mounting holes on the daughterboard with the tops of the standoffs on the NTBK50.
4	Lower the daughterboard onto the NTBK50, keeping the standoffs in line with all four holes, until the holes rest on the tops of the four standoffs.
5	If more than a very slight amount of pressure is required at this point, the connector pins may not be aligned with the connector socket. If so, lift the daughterboard off the NTBK50 and return to Step 2.

6 Apply pressure along the edge of the board where the connector is located until the standoffs at the two corners adjacent to the connector snap into a locked position.

7 Press down on the two corners opposite until they lock into place.

--End--

Replacing the NTAK09 1.5 Mb DTI/PRI card (PRI applications)

Procedure 34
Replacing the NTAK09 1.5 Mb DTI/PRI card when it is configured as PRI

Step	Action

1	If the NTAK93 DCHI daughterboard is attached to the card, disable the associated D-channel using the following overlay commands:
	`LD 96 DIS DCH X`
	If the NTBK51 DDCH daughterboard is attached to the card, disable the associated downloadable D-channel using the following overlay commands:
	`LD 96 DIS DCH X`
	`LD 96 DIS MSDL X`

2	To disable the Clock Controller (if on PRI), use the following command: `LD 60 DIS CC 0`
3	To disable the PRI pack, use the following command: `LD 60 DIS L X` The LEDs on the front of the card change from green (enabled) to red (disabled.) For this to happen, the **`DIS MSDL`** command must be used, as in Step 1.
4	Hold the circuit card by the lock latches, unlock the latches, and slide the circuit card out of the Media Gateway. If required, remove any attached daughterboards . Because of the physical layout of the motherboards and daughterboards, remove the NTAK20 before the NTAK93. To remove the NTAK20 and NTAK93 from the NTAK09 card, follow the steps in Procedure 32 “Removing the NTAK20 and NTAK93/NTBK51 from the NTBK50 card” (page 146). To reinstall the daughterboards, see Procedure 33 “Installing the NTAK93/NTBK51 daughterboard before the NTAK20 daughterboard” (page 146).

5 On the replacement PRI circuit card, configure switches and install daughterboards as required. Hold the card by the lock latches and slide it into the assigned slot until it connects with the backplane.

6 Secure the lock latches on the circuit card.

7 Enable the Clock Controller and the PRI in their corresponding overlays:

```
LD 60              ENL CC 0


LD 60              ENLL X
```

The associated DCHI is automatically enabled.

8 Check the tracking of the Clock Controller with the following command:

```
LD 60              SCK 0
```

If the clock is not tracking or is not locked, use the following command to track:

```
LD 60              TRCK PCK/SCLK
```

--End--

Replacing the NTAK09, NTAK10, or NTRB21 circuit cards (DTI applications)

To replace any card that is configured as a Digital Trunk Interface (DTI), use the following procedure.

Procedure 35
Replacing the NTAK09, NTAK10, or NTRB21 when configured as a DTI

Step	Action
1	Disable the Clock Controller by using the command: `LD 60 DIS CC 0`
2	Disable the DTI pack by using the command: `LD 60 DISL X`
3	Hold the circuit card by the lock latches, unlock the latches, and slide the circuit card out of the Media Gateway. If required, remove any daughterboards attached to the card.
4	On the replacement DTI circuit card, configure any switches and install any daughterboards as required. Hold the replacement

DTI circuit card by the lock latches and slide it into the assigned slot until it connects with the backplane.

5 Enable the Clock Controller (if on the DTI) and the DTI in their corresponding overlays:

```
LD 60              ENL CC 0


LD 60              ENLL X
```

6 Secure the lock latches on the circuit card.

7 Check the tracking of the Clock Controller with the following overlay:

```
LD 60              SSCK 0
```

If the clock is not tracking or is not locked, use the following commands to start tracking.

```
LD 60              TRCK PCK/SCLK
```

--End--

Replacing equipment cards

Follow the steps in Procedure 36 “Replacing equipment cards” (page 149) to replace Intelligent Peripheral Equipment (IPE) cards, including the following:

- NT8D02 Digital Line Card
- NT8D03 Analog Line Card
- NT8D09 Analog Message Waiting Line Card
- NT8D14 Universal Trunk Card
- NT8D15 E&M Trunk Card

See *Software Input/Output Reference – Maintenance* NN43001-711 and *Software Input/Output Reference – System Messages* NN43001-712 for a description of all maintenance commands and system messages.

Procedure 36
Replacing equipment cards

Step	Action
1	Software-disable the card with the following command: `LD 32  DISC l s c`

2 Unhook the locking devices on the card. Pull it out of the card cage.

3 On the replacement card, configure option switches or jumper plugs to the same settings as those on the card you removed.

4 Insert the replacement card into the vacated slot and hook the locking devices.

When cards are installed, the red LED on the faceplate flashes as a self-test runs. If the self-test is completed successfully, the card is automatically enabled (if it is configured in software) and the LED goes out. If the self-test fails, the LED lights steadily and remains lit.

5 Software-enable the card by entering: **ENLC l s c**

When the process is complete, a system response appears.

6 To end the program, enter four asterisks (********).

--End--

Replacing the NT5K21 equipment card

Procedure 37
Replacing the NT5K21 XMFC/MFE equipment card

Step	Action
1	Software-disable the card with the following command: `LD 54 DISC l s c`
2	Unhook the locking devices on the card. Pull it out of the card cage.
3	Insert the replacement card into the vacant slot and hook the locking devices. After you install cards, the red LED on the faceplate flashes as a self-test runs. If the self-test succeeds, the card is automatically enabled (if it is configured in software) and the LED turns off. If the self-test fails, the LED lights steadily and remains lit.
4	Software-enable the card by entering: **ENLC l s c** When the process is complete, a system response appears.

5	To end the program, enter four asterisks (****).

--End--

Replacing the NTAG26 equipment card

Procedure 38
Replacing the NTAG26 equipment card

Step	Action
1	Software-disable the card with the following command: `LD 34 DISC l s c`
2	Unhook the locking devices on the card. Pull it out of the card cage.
3	Insert the replacement card into the vacant slot and hook the locking devices. After you install cards, the red LED on the faceplate flashes as a self-test runs. If the self-test succeeds, the card is automatically enabled (if it is configured in software) and the LED turns off. If the self-test fails, the LED lights steadily and remains lit.
4	Software-enable the card by entering: **`ENLC l s c`** When the process is complete, a system response appears.
5	To end the program, enter four asterisks (****).

--End--

Replacing the NTAK92 off-premises protection module

A lightening strike can cause failure of the NTAK92 protection assembly. The first indication of such a failure is an out-of-service telephone. To check for and replace failed protectors, follow the steps in Procedure 39 “Testing for loop closure” (page 151) or Procedure 40 “Testing continuity” (page 152).

Procedure 39
Testing for loop closure

Step	Action
1	To test for a dial tone across cable pairs on J1 and J2, use standard loop closure test equipment (for example, butt-in). If

a protector failed, go to Step 2. If not, go to the appropriate chapter in this guide.

2 Remove the protection module cover plate.

3 Remove the faulty protector.

4 Install a new protector in the same position as the faulty protector.

5 Replace the cover plate.

6 Test the set for proper operation.

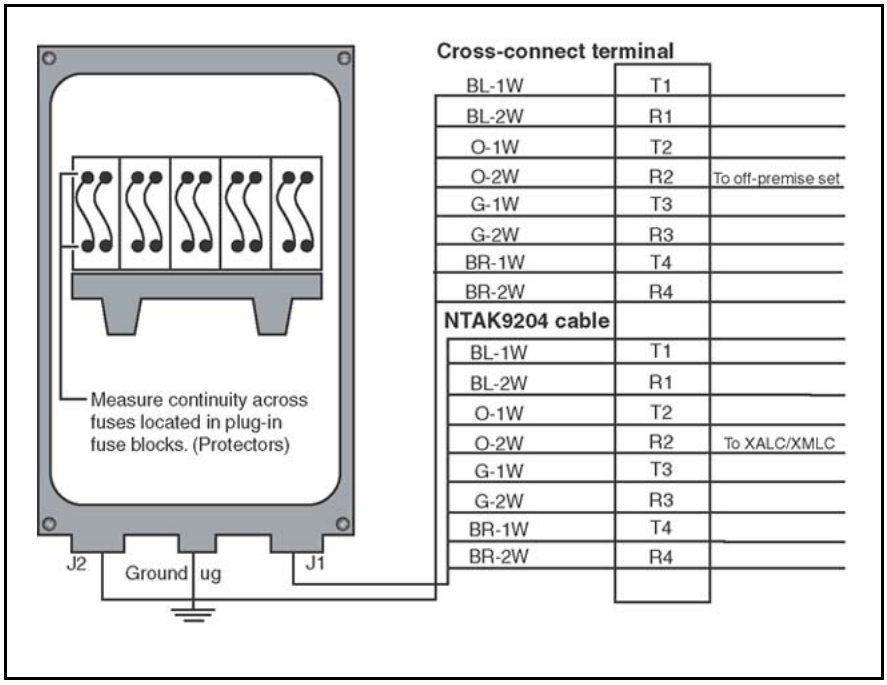
--End--

Procedure 40
Testing continuity

Step	Action
1	Remove the cover plate from the protection module.
2	Use an ohmmeter to measure continuity across the protectors. See Figure 49 "Wiring diagram for NTAK92 off-premises protection module" (page 153). If a protector failed, go to Step 3. If not, go to the appropriate chapter in this guide.
3	Remove the faulty protector.
4	Install a new protector in the same position as the faulty protector.
5	Replace the cover plate.
6	Test the set for proper operation.

--End--

Figure 49
Wiring diagram for NTAK92 off-premises protection module



Replacing IP daughterboards

Procedure 41
Replacing the NTDK83 or NTDK99 IP daughterboard

Step	Action
1	Turn the power supply and reserve power off.
2	Unplug the IP cable from the Media Gateway bulkhead.
3	Unplug and remove the NTDK20 SSC from the Media Gateway and place on a clean flat surface.
4	Disconnect the cable from the IP daughterboard and the LED connector if used.
5	Detach the IP daughterboard.
6	Position the replacement IP daughterboard.
7	Seat the replacement IP daughterboard into the same slot you removed the defective IP daughterboard from on the NTDK20 SSC card.
8	Reconnect the IP cable. Ensure that the cable is fully inserted into the connector. A click should be heard when the cable is fully engaged.

9 Reconnect the LED connector that was disconnected in step 4 if necessary.

10 Record the MAC address of the new IP daughterboard installed on the SSC in the Media Gateway. When necessary use LD 117 to configure the new MAC address for the Media Gateway. See *Communication Server 1000E Installation and Commissioning (NN43041-310).*

11 Reinstall the NTDK20 SSC circuit card in slot 0 of the Media Gateway.

12 Reconnect the IP cable to the Media Gateway bulkhead.

13 Power up the system.

--End--

Element Manager

Contents

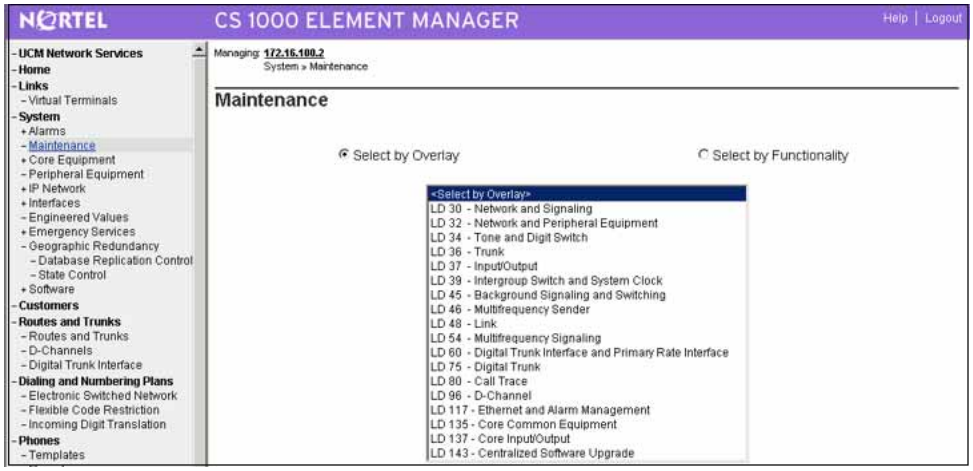
This section contains the following topics:

Call Server maintenance

To perform maintenance on the Call Server, you can access a subset of overlay functions in Element Manager.

Search for maintenance functions by LD number or by functionality on the system maintenance page, as shown in Figure 50 "Element Manager Call Server maintenance" (page 156).

Figure 50
Element Manager Call Server maintenance



You can perform some of the following maintenance functions using Element Manager.

- LD 36 – Trunk Diagnostics
  - card commands
  - unit commands
  - customer route commands
  - miscellaneous commands, such as CMIN, CMIN ALL, and CDSP
- LD 60 – Digital Trunk Interface (DTI) and Primary Rate Interface (PRI) Diagnostics
  - digital trunk diagnostic commands
  - clock controller commands
- LD 96 – D-channel Diagnostics
  - D-channel commands
  - MSDL commands
  - TMDI commands
- LD 32 – Network and Peripheral Equipment Diagnostics
  - loop, shelf, card, and unit commands
  - M39xx unit commands
  - DSL commands
  - BRIL, BRIE, and BRIT applications commands

You can use the rlogin command to the Call Server/H.323 gateway if you have a configured Pseudo TTY (PTY) and if an rlogin client is available on the administrative PC or workstation.

Use three asterisks (***) to rlogin directly to any SSC. The administrative workstation must be on the ELAN network and must have an rlogin client application. Otherwise, if administration is on the TLAN network or customer LAN, you must use a telnet client to connect to a primary SSC, and you must then rlogin to the Call Server.

- LD 117 – Ethernet and Alarm Management
  - — Zone diagnostic commands
  - — Ethernet diagnostic commands
  - — Ethernet Quality of Service diagnostic commands
  - — Emergency Services diagnostics, such as ERL, ELIN, and subnet commands
- Equipment Data Dump (EDD)

  As of Release 5.0, support no longer exists for LD 43 on Element Manager. EDD is now part of the Call Server backup procedure. See "Call Server data dump (EDD)" (page 158).
- installation, activation, and deactivation of patches

For a complete list and explanation of LD commands, see *Element Manager System Reference – Administration*(NN43001-632).

Call Server backup, data dump, and restore

The Backup and Restore link of the Tools branch of the Element Manager navigator provides access to Call Server Backup and Restore functions.

Call Server backup

Procedure 42
Backing up the Call Server in Element Manager

Step	Action
1	Click **Tools > Backup and Restore > Call Server**. The Call Server Backup and Restore page appears.
2	Click **Backup**. The Call Server Backup Web page appears.
3	Select **Backup** from the **Action** list, and click **Submit**. The Call Server Backup Waiting page opens to indicate that the backup is in progress. An Equipment Data Dump (EDD) is also in progress. See "Call Server data dump (EDD)" (page 158).

--End--

Call Server data dump (EDD)

The Backup function invokes a data dump and writes the Call Server data to the primary and internal backup drives.

The Backup function performs the same task as the **EDD** CLI command traditionally configured in LD 43.

When the backup finishes, a dialog box appears to indicate that the Equipment Data Dump (EDD) is complete.
Click **OK**.

A summary of the results of the EDD appears at the bottom of the Call Server Backup web page.

Call Server restore

The Call Server Restore function restores the backed-up files from the internal backup device to the primary device. The Restore function performs the same task as the CLI **RIB** command traditionally configured in LD 43.

WARNING
The process to restore data using the Element Manager interface is immediate. No warning or detailed information is provided on the specifics of the data to be restored. You must cold start the system before the restored data is in effect.

Procedure 43
Restoring Call Server data in Element Manager

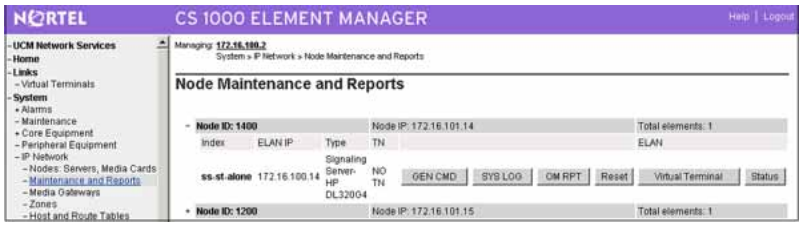
Step	Action
1	Click **Tools > Backup and Restore > Call Server**. The Call Server Backup and Restore page appears.
2	On the Call Server Backup and Restore page, click **Restore**. The Call Server Restore page appears.
3	Select **Restore from Backup Data (RES)** in the **Action** list, and click **Submit**.

--End--

Signaling Server maintenance

To access Signaling Server maintenance functions in Element Manager, as shown in Figure 51 "Element Manager Signaling Server maintenance" (page 159), select **IP Network > Maintenance and Reports**.

Figure 51
Element Manager Signaling Server maintenance



You can perform the following Signaling Server maintenance functions using Element Manager:

- reset
- access the maintenance window
- download new firmware
- upload new firmware
- telnet
- increase virtual trunk capacity and perform configuration tasks on virtual trunks
- turn the gatekeeper on or off
- view report log and trace files
- view Operational Measurement (OM) files
- upload log, trace, or OM files
- perform CLI commands
- access Help
- configure and manage the Web-based services for Personal Directory, Redial List, and Callers List

Media Card maintenance

To access Media Card maintenance functions in Element Manager, select **IP Network > Maintenance and Reports**.

You can perform the following Media Card maintenance functions using Element Manager:

- reset Voice Gateway Media Card
- enable or disable Voice Gateway Media Card
- telnet to the Media Card maintenance window

- download loadware and firmware for upgrades
- view individual DSPs
- view or upload Operational Measurement (OM) data
- access Help
- install and uninstall patches

You can reinstall Media Card software by using Deployment Manager. For information about Deployment Manager, see *Linux Platform Base and Applications Installation and Commissioning* NN43001-315.

LD 36 analog trunk card status

The STAT command in LD 36 provides status for all analog trunk cards within the system. The card number prints before the list of units.

Sample output of LD 36 with the STAT command:

```
CARD 1
UNIT 00 = DSBL (TRK)(TIE LDR IMM/IMM)
UNIT 01 = UNEQ
UNIT 02 = DSBL (TRK)(TIE LDR IMM/IMM)
UNIT 03 = UNEQ
UNIT 04 = UNEQ
UNIT 05 = DSBL (TRK)(DID LDR IMM/IMM)
UNIT 06 = UNEQ
UNIT 07 = DSBL (TRK)(TIE LDR IMM/IMM)
```

Media Card maintenance

Contents

This section contains the following topics:

Introduction

This chapter provides information about the maintenance functions of the Media Card.

Check the Nortel web site for information about the latest software, firmware and application releases. See *IP Line Fundamentals* for verification steps.

Faceplate maintenance display codes

The Media Card maintenance display provides the diagnostic status of the card during power-up, its operational state when in service, and error information on the functional state of the card.

During power-up, the card performs multiple self-tests, including:

- internal RAM test
- ALU test
- address mode test

- Boot ROM test, timer test
- external RAM test

If any of these tests fail, the card enters a maintenance loop, and no further processing is possible. A failure message is printed on the display to indicate which test failed. For more information and a list of the maintenance display codes, see *Signaling Server IP Line Applications Fundamentals* (NN43001-125).

If the maintenance display shows a persistent T:20, indicating a software failure, and this occurs after the card is reset during a software download procedure, call the Nortel technical support for assistance in downloading new software onto the card.

If a test fails on the Media Card, F:XX appears on the Hex display for three seconds after the T:13 (Testing SEEPROM) message. For example, if the 8051 coprocessor test failed, F:05 is displayed on the Media Card faceplate. If more than one test fails, the message indicates the first failure.

Table 36 "Media Card faceplate maintenance display codes" (page 162) provides a list of related normal and fault display codes for the Media Card.

Table 36
Media Card faceplate maintenance display codes

Normal code	Corresponding Fault code	Message
T:00	F:00	Initialization
T:01	F:01	Testing Internal RAM
T:02	F:02	Testing ALU
T:03	F:03	Testing address modes
T:04	F:04	Testing watchdog
T:05	F:05	Testing 8051 coprocessor
T:06	F:06	Testing timers
T:07	F:07	Testing external RAM
T:08	F:08	Testing security device
T:09	F:09	Programming timeswitch FPGA
T:10	F:10	Programming ISPDI FPGA
T:11	F:11	Testing host dual port RAM
T:12	F:12	Testing DS-30 dual port RAM

Table 36
Media Card faceplate maintenance display codes (cont'd.)

Normal code	Corresponding Fault code	Message
T:13	F:13	Testing SEEPROM
T:14	F:14	Booting Host processor, waiting for response with self-test information
T:15	F:15	Not used at present
T:16	F:16	Not used at present
T:17	F:17	Not used at present
T:18	F:18	Not used at present
T:19	F:19	Not used at present
T:20	F:20	Waiting for application startup message from Host processor
T:21	F:21	CardLAN enabled, waiting for request configuration message
T:22	F:22	CardLAN operational, A07 enabled, display now under host control

If the IXP encounters any failures during its initialization, an H:XX error code is displayed. Table 37 "List of error codes for the Media Card" (page 163) shows the list of error codes:

Table 37
List of error codes for the Media Card

Code	Description
H:00	Host Processor not booting
H:01	SDRAM test failure
H:02	SRAM test failure
H:04	PC Card device failure
H:08	Network interface failure
H:10	CS 1000E interface failure
H:20	DSP interface failure
H:40	NVRAM/EEPROM interface failure
H:80	PCM connector failure

Media Card error messages

When an error or specific event occurs, SNMP sends an alarm trap to any SNMP manager that is configured in the SNMP Manager's list in the ITG Card properties. It also puts the system error message into the error log file containing error messages.

You can view the log file in any text browser after uploading it to an FTP host using the LogFilePut command.

Error messages with a severity category of "Critical" are displayed on the maintenance faceplate in the form: "Gxxx" or "Sxxx", where xxx is the last three digits of the ITG or ITS message. Table 38 "Critical ITG Error messages" (page 164) lists the critical ITG messages and Table 39 "Critical ITS Error messages" (page 166) lists the critical ITS messages.

For a complete listing of other error messages, see *Software Input/Output Reference – System Messages* NN43001-712.

Table 38
Critical ITG Error messages

Maintenance Display	Corresponding Critical Error Message	Description
G000	ITG1000	Card (re)booted.
G001	ITG1001	Task spawn failure <name>.
G002	ITG1002	Memory allocation failure.
G003	ITG1003	File IO error <operation> <object> <errno> <errtext>.
G004	ITG1004	Network IO error <operation> <object> <errno> <errtext>.
G005	ITG1005	Message queue error <operation> <object> <errno> <errtext>.
G006	ITG1006	Unexpected state encountered <file> <line> <state>.
G007	ITG1007	Unexpected message type <file> <line> <msg>.
G008	ITG1008	Null pointer encountered <file> <line> Name of pointer.
G009	ITG1009	Invalid block <file> <line> Type of block.
G010	ITG1010	Unable to locate data block <file> <line> Type of block.
G011	ITG1011	File transfer error: <operation> <file> <host>.
G012	ITG1012	Module initialization failure: <moduleName>.
G013	ITG1013	Ethernet receiver buffer unavailable, packet(s) discarded.
G014	ITG1014	Ethernet carrier: <ifName> <state>.
G015	ITG1015	Ethernet device failure: <ifName>.
G016	ITG1016	Unused alarm value: 16.
G017	ITG1017	Invalid or unknown SSD message: <ssdType> <TN> <msg>.

Table 38
Critical ITG Error messages (cont'd.)

Maintenance Display	Corresponding Critical Error Message	Description
G018	ITG1018	Unused alarm value: 18.
G019	ITG1019	DSP channel open failure <channel>.
G020	ITG1020	Configuration error <param> <value> <reason>.
G021	ITG1021	DSP successfully reset <dsp>.
G022	ITG1022	DSP channel not responding, channel disabled <channel>.
G023	ITG1023	DSP device failure: <dsp> <errnum> <errtext>.
G024	ITG1024	Unused alarm value: 24.
G025	ITG1025	DSP download: <dsp> <reason>.
G026	ITG1026	Unused alarm value: 26.
G027	ITG1027	DSP memory test: <dsp> <reason>.
G028	ITG1028	Voice packet loss: <channel> <%packetLoss> <direction> <dstAddr>.
G029	ITG1029	Error in DSP task <file> <line> <errno> <errtext>.
G030	ITG1030	Allocation failure in DSP memory pool.
G031	ITG1031	Invalid codec number: <codec>.
G032	ITG1032	Attempt to open a DSP that is already open: <channel>.
G033	ITG1033	Failed to send data to DSP channel: <channel>.
G034	ITG1034	DSP channel unexpectedly closed: <channel>.
G035	ITG1035	Encountered and unexpected open DSP channel, closed it: <channel>.
G036	ITG1036	Call Server communication link.
G037	ITG1037	Wrong image downloaded. Binary was created for <cardType> card.
G038	ITG1038	IPLlogin protection (login available/locked).
G039	ITG1038	Bad DSP channel <channel id>.
G040	ITG1040	Last reset reason for card: <reasonString> where the reason String can be: Reboot command issued; Watchdog Timer Expired; Manual reset; Internal XA problem; or Unknown.

Table 39
Critical ITS Error messages

Maintenance Display	Corresponding Critical Error Message	Description
S000	ITS1000	VTI function call timeout.
S001	ITS1001	User terminal registration failed. <ip> <hwid> <errno> <errtext>.
S002	ITS1002	Connect service activation error <reason>.
S003	ITS1003	Duplicate master <node> <ip1> <ip2>.
S004	ITS1004	Invalid node ID <ip> <hwid>.
S005	ITS1005	Corrupted node ID/TN field <ip> <hwid>.
S006	ITS1006	Received corrupted UNIStim message <message dump>.
S007	ITS1007	Received unknown UNIStim message <message dump>.
S008	ITS1008	Terminal connection status: <ip> <status>.
S009	ITS1009	Call Server communication link:<state>.
S010	ITS1010	Terminal doesn't support Codec:<ip><codec>.
S011	ITS1011	<IP Address>: Last reset reason for phone: <reasonID> (<reasonString>).

Replacing a Media Card

Replace the Media Card when the following conditions occur:

- After a reboot, the Media Card displays a fault code of the form F:xx on the faceplate LED display and the card cannot register with the CS 1000E. This indicates an unrecoverable hardware failure.
  If the Media Card displays the F:08 code, this can merely indicate that the Security Device is missing from the card.
- The management Ethernet interface or the voice Ethernet interface on the Media Card fails. The failure is originating in the Media Card if its associated hub port and TLAN network interface cable are operational. The failure can be indicated as follows:
  - — No link pulse on the Media Card voice IP interface status LED and on the associated hub.
  - — The maintenance terminal continuously prints **InIsa0 Carrier Failure** messages.
- A voice channel on the Media Card has a consistent voice quality fault, such as persistent noise or lack of voice path, even after resetting the card and retransmitting the card properties.

To replace a Media Card, see *IP Line Fundamentals*

Verify Media Card software and firmware

To verify the Media Card software and firmware, see *IP Line Fundamentals*

IP Line and IP Phone maintenance and diagnostics

For Nortel IP Phones, there are two kinds of Terminal Numbers (TNs) to consider:

- A physical TN, which represents a physical unit of the Media Card.
- A virtual TN, which is configured on a virtual superloop and represents an IP Phone.

The physical TNs are seen as trunk units and are managed using existing LD 32 commands. These commands do not apply to virtual TNs. Use Element Manager for virtual TN maintenance. See *Element Manager System Reference – Administration*NN43001-632 for details.

LD 32 supports STAT, DISU, ENLU, and IDU commands on an IP Phone virtual TN. All other commands generate an NPR047 message.

The IDU command provides the usual information, such as:

- TN
- TNID
- NT code
- color code
- release code
- serial number
- IP address of the IP Phone
- IP address of the Media Card that acts as the terminal proxy

The serial number is the last three bytes of the IP Phone’s MAC address, printed in ASCII hex format.

Because the system must obtain the requested information from the IP Phone, IDU is effectively a "ping" command. Consequently, it can be used to test the end-to-end IP connectivity of the IP Phone.

If the IP Phone is not registered with the CS 1000E, an NPR0048 message is generated. If the IP Phone is registered but idle, the system prints the IP Phone IP address and Media Card IP address and generates an NPR0053 message.

For additional information on the output format of the IDU command in LD 32 and the maintenance commands in LD 32 for the IP Phone, see *IP Line Fundamentals*.

Lamp Audit

The Lamp Audit function provides a continuous source of heartbeat messages to ensure the IP Phone is powered and the IP connection is active. Because there is a reliable UDP connection from the Call Server to the IP Phones, any failure in the IP Phones, or the IP connections is detected. In addition to Lamp Audit, Network Signaling Diagnostics can be run as part of the midnight routines.

IP line shell commands

The IP Line shell commands are designed to supplement overlay commands and to manage features specific to the IP Line platform.

The IP Line shell commands are accessed by connecting a TTY to the MAINT port on the Media Card faceplate.

Commands are grouped into six categories:

- General purpose commands
- File transfer commands
- IP configuration commands
- Reset commands
- DSP commands

To view a list of the ITG shell commands applicable to the Media Card see *IP Line Fundamentals.*

Warm rebooting the Media Card

To warm reboot an out-of-service Media Card, use the following IP Line shell command:

`cardReset`

Media Card DSP tests

At the IP Line shell, you can perform the following DSP tests:

- To run a self-test on the DSP daughterboard, type
  `DSPselfTest`
  If the self-test fails, replace the Media Card.
- To run or stop a PCM loopback test, type
  `DSPPcmLpbkTestOn` or **`DSPPcmLpbkTestOff`**

- To run or stop a Send loopback test, type:
  DSPSndLpbkTestOn or **DSPSndLpbkTestOff**
- To run or stop a Receive loopback test, type
  DSPRcvLpbkTestOn or **DSPRcvLpbkTestOff**

Invoking alarm and log files

Alarm and log file output is turned on using the IP Line shell. The following commands are entered at the IP Line shell prompt:

- To turn on/off the error log file, type: **logFileOn** or **logFileOff**.
- To display the modes of all log files/alarms, type: **logFileShow**.

Media Card 32S and DSP daughterboard DSP tests

Media Card 32S and DSP daughterboards have new commands that can be accessed with the OAM and PDT2 shells.

At the OAM shell, you can perform the following DSP tests:

- To run a basic hardware DSP self-test, type
  dsphwcheck
  If the self-test fails, reseat or replace the Media Card or DSP daughterboard.
- To run a DSP loopback test, type
  dsplooptest [channel1 channel2]
- To list the state of each channel on the DSP, type
  dspchanstateshow
- To display the number of channels for each DSP, type
  dspnumshow

At the PDT2 shell, you can perform the following PCM tests

- To start a PCM capture for a specific channel, streaming the output to the supplied destination IP address, type
  pcmcapturestart [channel IP address]
- To stop a PCM capture, type
  pcmcapturestop

Proactive Voice Quality Management

Contents

This section contains the following topics:

Introduction

CS 1000E systems, that are equipped with Voice Gateway Media Cards running IP Line 4.0 or later, support Proactive Voice Quality Management (PVQM). PVQM includes the following capabilities for UNIStim IP Phones.

ATTENTION
These capabilities are not applicable to SIP sets.

- Monitoring of voice quality metrics (latency, jitter, packet loss, and R-Value) for IP Phones and gateway endpoints.
  R-Value monitoring is available on Phase 2 IP Phones only.
- Two levels of voice quality alarms (Warning and Unacceptable). Alarm thresholds, configured in LD 117, are used to classify system performance as good, poor, and unacceptable.
  This is available on Phase 2 IP Phones only.
- SNMP alarm generation when voice quality metric thresholds are violated based on a call or bandwidth zone.
- Controlling the number of voice-quality-related SNMP alarms. This is performed zone-by-zone by configuring zone alarm notification in LD 117. Alarm control assists in isolating voice quality problems and reducing network traffic.
- Recording of voice quality metric threshold violations, accessible in IP Phone Zone Traffic Report 16 (LD 2) and SNMP MIB.
  IP Phone Zone Traffic Report 16 (TFS016) includes peg counts for both alarm levels (Warning and Unacceptable) when recording threshold violations for latency, jitter, and packet loss. R-Value is limited to one peg count: Unacceptable.
- R-Value information, available in Operational Measurement (OM) reports. OM reports contain hourly summary of voice quality metrics and endpoint registration activity.
- Network diagnostic utilities to identify, isolate, and report network problems affecting voice quality. The diagnostic utilities are available by using the Command Line Interface (CLI) or IP Phones with Phase 2 software.

  Network diagnostic utilities includes the following:

  — Ping
  — Traceroute
  — Ethernet statistics
  — IP Network statistics
  — UNIStim/Reliable User Data Protocol (RUDP) statistics
  — Real-Time Control Protocol (RTCP) statistics
  — Dynamic Host Control Protocol (DHCP) data

How voice quality monitoring works

PVQM monitors voice quality by polling IP endpoints during and at the end of a call to sample the following voice-quality metrics:

- **Latency** - length of time, in seconds, for information to travel through the network
- **Jitter** - the variability in latency, in seconds
- **Packet Loss** - number of packets lost during transmission, in percentage
- **R-Value** - measurement of listening R-Value using ITU E-Model. R-Value maps to Mean Opinion Score (MOS).

The sampled metrics are compared to user-configured thresholds to determine system performance. When sampled metrics exceed configured thresholds, the system generates statistics.

For details about configuring metric thresholds, see “LD 117 Configure voice-quality metric thresholds” (page 175).

The Signaling Server collect statistics for each metric to create a Quality Detail Report (QDR). The QDR summarizes metric threshold violations into one of the following categories:

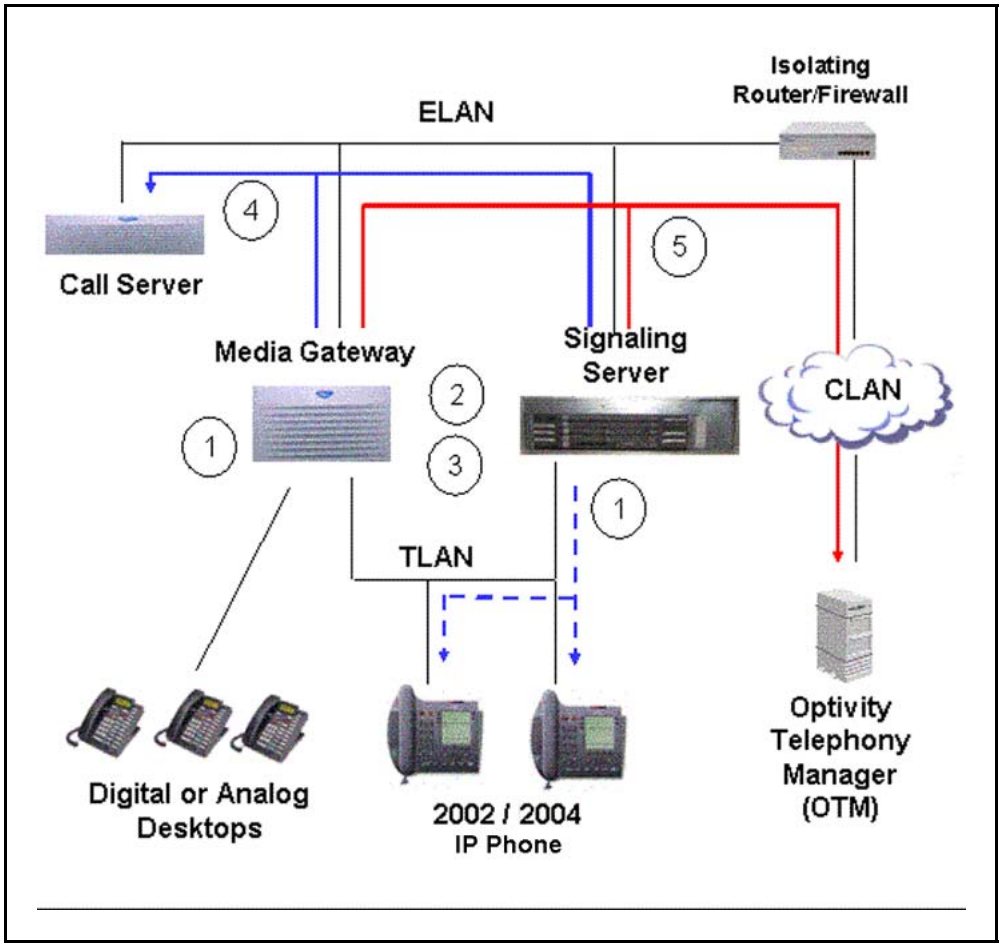
- Warning
- Unacceptable

Each summarized QDR record is added to the IP Phone Zone Traffic Report 16 (TFS016). The TFS016 report summarizes by zone the voice quality over the reporting period to allow the administrator to view the overall voice quality. For more information about TFS016, see *Traffic Measurement: Formats and Outputs Reference* .

An SNMP alarm is generated when a voice quality metric threshold exceeds Warning or Unacceptable status. For details about controlling the number of SNMP alarms generated, see “LD 117 Configure zone alarm-notification levels” (page 177).

Figure 52 "Voice quality monitoring flow diagram" (page 174) illustrates PVQM within the Voice over IP (VoIP) system.

Figure 52
Voice quality monitoring flow diagram



Legend

1. IP Phones and endpoints are polled during a call and at the end of a call to extract voice-quality statistics.
2. Statistics for each metric are collected on the Signaling Server or Voice Gateway Media Card.
3. Voice-quality statistics are compared to threshold settings and a QDR is created.
4. The QDR is forwarded to the Call Server for reporting purposes.
5. An SNMP alarm is generated when a voice-quality metric exceeds the Warning or Unacceptable threshold.

Feature packaging

To monitor the R-Value audio-quality metric, the Proactive Voice Quality Management (PVQM) package 401 is required. Monitoring of all other voice-quality metrics is available with base CS 1000 Release 7.0 software.

Supported system types

CS 1000E systems, that are equipped with Voice Gateway Media Cards running IP Line 4.0, support PVQM.

Feature implementation

To implement this feature, you must install the PVQM_401 software package.

Task summary list

Following is a summary of tasks in this section:

LD 117 Print zone QoS IP statistics

Display QoS IP statistics for zones, ordered by attribute or by zone, in LD 117. Traffic Report 16 contains similar information and a list of attributes. For more details about traffic reports, see *Traffic Measurement: Formats and Outputs Reference* .

Table 40
LD 117 Print zone QoS IP statistics

Command	Description
AQOS <attribute> <zone>	Print QoS IP statistics by attribute for a specific zone.
AQOS <attribute> ALL	Print QoS IP statistics by attribute for all zones.
ZQOS <zone> <attribute>	Print QoS IP statistics by zone for a specific attribute.
ZQOS <zone> ALL	Print QoS IP statistics by zone for all attributes.

LD 117 Configure voice-quality metric thresholds

To configure voice-quality metric thresholds based on a call or zone in LD 117, see Table 41 "LD 117 Configure voice-quality metric thresholds" (page 176).

Table 41
LD 117 Configure voice-quality metric thresholds

Command	Description
CHG CQWTH <WarnJitter><WarnLatency><WarnPacketLoss><WarnRFactor>	Change voice-quality Warning thresholds on a per-call basis Where: <WarnJitter> = 5-(20)-200 msec <WarnLatency> = 5-(40)-100 msec <WarnPacketLoss> = 5-(20)-100 in units [1/10 of a percent] For example, 10 means 1% <WarnRFactor> = 20-(65)-94
CHG CQUTH <UnacceptJitter><UnacceptLatency><UnacceptPacketLoss><UnacceptRFactor>	Change voice-quality Unacceptable thresholds on a per-call basis Where: <UnacpJitter> = 5-(40)-500 msec <UnacpLatency> = 5-(100)-500 msec <UnacpPacketLoss> = 5-(70)-250 in units [1/10 of a percent] For example, 10 means 1% <UnacpRFactor> = 20-(60)-94
CHG ZQWTH <WarnJitter><WarnLatency><WarnPacketLoss><WarnRFactor>	Change voice-quality Warning thresholds on a zone basis Where: <WarnJitter> = 0-(20)-100% <WarnLatency> = 0-(20)-100% <WarnPacketLoss> = 0-(20)-100% <WarnRFactor> = 0-(20)-100%
CHG ZQUTH <UnacceptJitter><UnacceptLatency><UnacceptPacketLoss><UnacceptRFactor>	Change voice-quality Unacceptable thresholds on a zone basis Where: <UnacpJitter> = 0-(2)-100% <UnacpLatency> = 0-(2)-100% <UnacpPacketLoss> = 0-(2)-100% <UnacpRFactor> = 0-(2)-100%

To configure voice-quality metric thresholds using Element Manager, select **IP Network > QoS Thresholds** from the System menu of the Element Manager navigator bar.

ATTENTION
Changes to threshold values do not propagate to the Signaling Server until you perform a datadump.

LD 117 Print voice-quality metric thresholds

Table 42
LD 117 Print voice-quality metric thresholds

Command	Description
PRT QSTHS	Print all voice-quality thresholds

LD 117 Configure voice-quality sampling (polling)

To configure the sampling (polling) period, zone alarm-rate collection window, and the minimum number of samples to collect during the window, see Table 43 "LD 117 Configure voice-quality sampling (polling)" (page 177).

To configure voice-quality sampling using Element Manager, select **IP Network > QoS Thresholds** from the System menu of the Element Manager navigator bar.

Table 43
LD 117 Configure voice-quality sampling (polling)

Command	Description
CHG SQOS <SamplePeriod><SampleRateWindow><MinSampleCnt>	Change voice-quality sampling parameters Where: <SamplePeriod> = 5-(30)-60 <SampleRateWindow> = 60-(300)-3600 seconds <MinSampleCnt> = 50-(100)-1000

LD 117 Configure zone alarm-notification levels

Systems that process a large number of calls potentially generate a significant number of SNMP alarms. Controlling the number of alarms by configuring zone alarm-notification levels helps isolate voice-quality problems and reduce network traffic.

Voice-quality threshold alarms are examined for their severity relative to the alarm-notification level settings. If the voice-quality threshold alarm severity exceeds the configured notification level, it generates an SNMP alarm. Otherwise it is suppressed.

You can configure Voice-quality threshold alarm-notification levels by zone so that some bandwidth zones can be monitored for all alarms and other zones report only serious voice-quality problems. Alarm-notification levels are defined in Table 44 "Voice-quality threshold alarm-notification levels" (page 178).

Table 44
Voice-quality threshold alarm-notification levels

Level	Description	Alarms
0	All voice-quality alarms are suppressed	None
1	Allow zone-based Unacceptable alarms	QOS0017 QOS0018 QOS0019 QOS0020 QOS0021
2	Allow all of the preceding plus zone-based Warning alarms	All preceding plus QOS0012 QOS0013 QOS0014 QOS0015 QOS0016
3	Allow all preceding plus per-call Unacceptable alarms	All preceding plus QOS0007 QOS0008 QOS0009 QOS0010 QOS0011 QOS0021 QOS0032 QOS0033 QOS0036 QOS0037
4	Allow all preceding plus per-call Warning alarms	All preceding plus QOS0001 QOS0002 QOS0003 QOS0005 QOS0006 QOS0018 QOS0019 QOS0022 QOS0023 QOS0024 QOS0025 QOS0026 QOS0027

To control the number of alarms generated by the system, see Table 45 "LD 117 Configure zone alarm-notification levels" (page 179).

To configure zone alarm-notification levels using Element Manager, select **IP Network > QoS Thresholds** from the System menu of the Element Manager navigator bar.

Table 45
LD 117 Configure zone alarm-notification levels

Command	Description
CHG ZQNL <ZoneNumber> <level>	Change the notification level for the specified zone Where: <ZoneNumber> = 0–8000 <level> = 0-(2)-4

LD 117 Print zone alarm-notification levels

Table 46
LD 117 Print zone alarm-notification levels

Command	Description
PRT ZQNL <ZoneNumber>	Print the notification level for the specified zone Where: <ZoneNumber> = 0–8000

Diagnosing and isolating voice-quality problems

To isolate voice-quality problems, access network diagnostic utilities on an IP Phone. You can run directly the utilities from the IP Phone itself or remotely through a CLI. Diagnostic utilities include the following:

- **Ping** and **Traceroute**

  Run the Ping or Traceroute command from a specific endpoint with any destination, typically another endpoint or Signaling Server.

- **IP Networking statistics**

  View information on the packets sent, packets received, broadcast packets received, multicast packets received, incoming packets discarded, and outgoing packets discarded.

- **Ethernet statistics**

  For an IP Phone on a particular endpoint, view Ethernet statistics, such as number of collisions, VLAN ID, speed, and duplex. The exact statistics depend on what is available from the IP Phone for the specific endpoint.

- **UNISTIM/RUDP statistics**

  View RUDP statistics for IP Phones, such as number of messages sent or received, retries, resets, and uptime.

- **UNIStim Security with DTLS**

View UNIStim (Lexicon) Security with DTLS statistics for UNIStim IP Phones based on the industry standard DTLS protocol (RFC4347).

- **Real time Transport Protocol statistics**

  While a call is in progress, view RTP/RTCP QoS metrics, such as packet loss and jitter.

- **DHCP**

  View DHCP settings, such as IP address; and S1, S2, and S4 addresses for each IP Phone.

For detailed information about network diagnostic utilities, see *IP Phones Fundamentals* NN43001-368.

SNMP interface

Simple Network Management Protocol (SNMP) interfaces with the traffic-reporting system so that any third-party system, can have a simple, standards-based interface into the system traffic reports.

For details about the SNMP interface, see *Communication Server 1000 Fault Management – SNMP* NN43001-719.

Heterogeneous environments

In a heterogeneous environment, with a mixture of Nortel equipment and third-party equipment, voice-quality monitoring, detection, and alarming are performed only on IP endpoints that have voice-quality monitoring capabilities.

For information about IP endpoints and their voice-quality capabilities in the system, see Table 47 "IP endpoint and voice-quality capabilities" (page 180).

Table 47
IP endpoint and voice-quality capabilities

Endpoint type	Voice-quality monitoring operation
Phase 0 and Phase I IP Phones	Detect jitter, packet loss, and latency (when the far end is RTCP-compliant) threshold violations. Polling detects threshold violations. .
Phase 2 IP Phones without PVQM package	Detect jitter, packet loss, and latency (when the far end is RTCP-compliant) threshold violations. The IP Phone asynchronously detects threshold violations.
Phase 2 IP Phones with PVQM package	Detect jitter, packet loss, and latency (when the far end is RTCP-compliant) and R-Value threshold violations. Threshold violations are detected asynchronously by the IP Phone.

Endpoint type	Voice-quality monitoring operation
IP Softphone 2050	Detect jitter, packet loss, and latency (when the far end is RTCP-compliant) threshold violations. Polling detects threshold violations.
CS 1000E systems with Voice Gateway Media Cards running IP Line 4.0	Detect jitter and packet loss threshold violations. Polling detects threshold violations.
Third-party Media Gateway	Not supported.

pbxLink connection

Contents

This section contains the following topics:

Introduction

pbxLink Connection Failure Detection and status reporting provide the following functionality:

- The pbxLink Connection Failure Detection feature provides a way to detect the link status of Signaling Servers and Voice Gateway Media Cards. An alarm is generated if the pbxLink is not detected after a warm or cold start of the Call Server.
- The STAT SERV command in LD 117 displays the link status of the Signaling Server and Voice Gateway Media Cards that are configured to connect to the system. The display also provides information about the applications that run on the Signaling Server and Voice Gateway Media Cards.

pbxLink connection failure detection

The Call Server, which maintains a list of all known registered elements (Signaling Servers and Voice Gateway Media Cards), monitors the pbxLink. When booted, a Call Server has a 5-minute delay to enable these known elements to reestablish contact with the Call Server.

If a known element fails to register with the Call Server, an ELAN0028 alarm is generated.

If an unknown Signaling Server registers with the Call Server, an ELAN0029 alarm is generated.

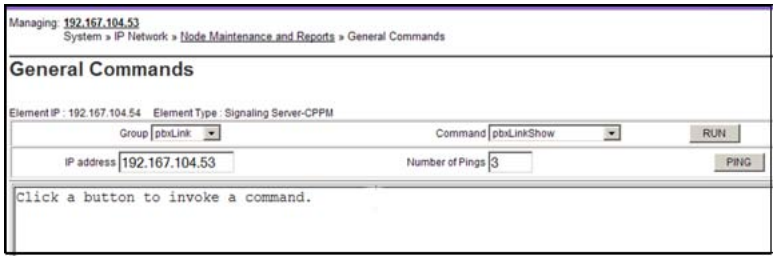
Displaying pbxLink information

Element Manager (EM)

To display pbxLink information in Element Manager, use the **pbxLinkShow** command, as shown in Figure 53 "Displaying pbxLink information in Element Manager" (page 184).

To access the pbxLinkShow command in EM, dfollow the steps in Procedure 44 “Displaying pbxLink information in Element Manager” (page 184).

Figure 53
Displaying pbxLink information in Element Manager



Procedure 44
Displaying pbxLink information in Element Manager

Step	Action
1	In the EM navigator System menu, select **IP Network > Maintenance and Reports** . The **Node Maintenance and Reports** page appears.
2	Click **GEN CMD** to the right of the Call Server information line.
3	Select **pbxLink** from the **Group** list.
4	Select **pbxLinkShow** from the **Command** list.
5	Click **Run**.

--End--

CLI

To display the pbxLink information for a CS 1000E system, use the LD 117 STAT SERV command at the Command Line Interface (CLI) of the Call Server.

LD 117 STAT SERV enhancement

To display link-status information for Voice Gateway Media Cards that are registered to a Call Server you can use the suite of Statistic Services (STAT SERV) commands.

STAT SERV provides consolidated link-status information by application type, IP address, host name, and IP Telephony Node ID.

STAT SERV status information includes the following:

- node ID
- host name
- ELAN IP address
- element role
- platform type
- connection ID
- enabled applications
- registered and unregistered endpoints, such as IP Phones and Voice Gateway Media Cards
- information about the pbxLink and enabled applications
- the Signaling Server resource count

pbxLink information

The STAT SERV command provides the following pbxLink information:

- the time the pbxLink was last established
- the time the pbxLink was lost, if previously established
- the time the pbxLink last attempted to establish a connection, if the pbxLink failed to establish
- the Signaling Server resource count, which helps to determine the number of virtual trunks that you can configure.

Application information

If an active link to an element is established, the Call Server obtains information about the applications that run on the element. Table 48 "Queried information in STAT SERV" (page 186) lists the applications and describes the information provided by those applications.

Table 48
Queried information in STAT SERV

Application/element	Information provided
LTPS application	number of registered IP Phones number of busy IP Phones
VTRK application	number of registered VTRKs number of busy VTRKs
Voice Gateway Media Cards	number of registered Voice Gateway Media Cards number of busy Voice Gateway Media Cards
Signaling Servers and Voice Gateway Media Cards	time that the element established a link with the Call Server elements that failed to register or lost a link

Figure 54 "Sample LD 117 STAT SERV output" (page 186) shows an example of LD 117 STAT SERV output.

Figure 54
Sample LD 117 STAT SERV output

Commands

STAT SERV	IP	xx.xx.xx.xx
		xx.xx.xx
		xx.xx
		xx
	TYPE	SRV
	APP	APPS
	NAME	HOSTNAME
	NODE	NODE_ID

Response

```
NODE ID  HOSTNAME          ELANIP          LDR  SRV   APPS   PBXLINK STATE  PBXLINK DATE  PBXLINK TIME  CONNECTID
909      vxTarget          47.11.216.126   YES  SMC   LTPS   LINK UP        5/06/2003     22:51:06      0x200a2128

         sets: [reg - 0002] [busy - 0000]      vgws: [reg - 0020] [busy - 0002]

999      IPService         47.11.216.141   N/A  SS    LTPS   LINK UP        5/06/2003     22:51:06      0x200a2128
                                                    VTRK

         Sets: [reg - 0302] [busy - 0056]
         VTRK: [reg - 0050] [busy - 0015]

999      IPService         47.11.216.141   YES  SS    LTPS   LINK UP        5/06/2003     22:51:06      0x200a2128
                                                    VTRK

         Sets: [reg - 0302] [busy - 0056]       VTRK: [reg - 0050] [busy - 0015]

999      vxTarget          47.11.216.143   NO   ITGP  LTPS   INV CONN       5/06/2003     23:18:08      0x0

999      vxTarget          47.11.216.144   NO   ITGP  LTPS   FAILED         5/06/2003     22:51:06      0x0
```

Table 49 "STAT SERV response fields and description" (page 187) lists field descriptions in the STAT SERV response.

Table 49
STAT SERV response fields and description

STAT SERV response field	Description
NODE ID	The related node. Value is a number from 0 – 9999.
HOSTNAME	The alias that the system assigned to the host. Value is a string.
ELANIP	The element IP connection to the Call Server. Value is an IP address.
LDR	Specifies if the element is the Leader for the related node. Value is YES or NO.
SRV	The element type. Values are • SMC – Media Card 32-port card • ITGP – ITG-P 24-port card • SS – Signaling Server
APPS	The application running on the element. Values are • LTPS • VTRK
PBXLINK STATE	Tthe element current pbxLink state. Values are • LINK UP • LOST • FAILED • INV CONN (element is connected, but its configuration was not found on the Call Server, which indicates that this element might be connected to the wrong Call Server)
PBXLINK DATE/TIME	When the element pbxLink state last changed.
CONNECTED	The element connection ID.
Sets	Values are • reg – the number of IP Phones registered to the element • busy – the number of IP Phones that are currently busy
VGWs	Values are • reg – the number of voice gateways (DSP resources) are configured on the element • busy – the number of voice gateways (DSP resources) are active/busy on the element

STAT SERV response field	Description
VTRK	Values are • reg – the number of VTRK channels are configured on the element • busy – the number of VTRK channels are active/busy on the element
SSRC	Signaling Server capacity

Technical Assistance service

Contents

This section contains information on the following topics:

Nortel Technical Assistance Centers

To help customers obtain maximum benefit, reliability, and satisfaction from their CS 1000E system s, Nortel provides technical assistance in resolving system problems. Table 50 "Customer Technical Services (CTS)" (page 189) lists the centers that provide this service.

Table 50
Customer Technical Services (CTS)

Location	Contact
Nortel Global Enterprise Technical Support (GETS) PO Box 833858 2370 Performance Drive Richardson, TX 75083 USA	North America Telephone: 1 800 4NORTEL
Nortel Corp. P.O. Box 4000 250 Sydney Street Belleville, Ontario K8N 5B7 Canada	North America Telephone: 1 800 4NORTEL

Table 50
Customer Technical Services (CTS) (cont'd.)

Location	Contact
Nortel Service Center - EMEA	EMEA Telephone: 00 800 8008 9009 or +44 (0)870 907 9009 E-mail: emeahelp@nortel.com
Nortel 1500 Concord Terrace Sunrise, Florida 33323 USA	Brazil Telephone: 5519 3705 7600 E-mail: entcts@nortel.com English Caribbean Telephone: 1 800 4NORTEL Spanish Caribbean Telephone: 1 954 858 7777 Latin America Telephone: 5255 5480 2170
Network Technical Support (NTS)	Asia Pacific Telephone: +61 28 870 8800 Australia Telephone:1800NORTEL (1800 667835) or +61 2 8870 8800 E-mail: asia_support@nortel.com People's Republic of China Telephone: 800 810 5000 E-mail: chinatsc@nortel.com Japan Telephone: 010 6510 7770 E-mail: supportj@nortel.com Hong Kong Telephone: 800 96 4199 E-mail: chinatsc@nortel.com Taiwan Telephone: 0800 810 500 E-mail: chinatsc@nortel.com

Table 50
Customer Technical Services (CTS) (cont'd.)

Location	Contact
	Indonesia Telephone: 0018 036 1004 Malaysia Telephone: 1 800 805 380 New Zealand Telephone: 0 800 449 716 Philippines Telephone: 1 800 1611 0063 or 632 917 4420 Singapore Telephone: 800 616 2004 South Korea Telephone: 0079 8611 2001 Thailand: Telephone: 001 800 611 3007

Services available

Services available through the Technical Assistance Centers include:

- diagnosing and resolving software problems not covered by support documentation
- diagnosing and resolving hardware problems not covered by support documentation
- assisting in diagnosing and resolving problems caused by local conditions

There are several classes of service available. Emergency requests (Class E1 and E2) receive an immediate response. Service for emergency requests is continuous until normal system operation is restored. Non-emergency requests (Class S1, S2, and NS) are serviced during normal working hours. Table 51 "Technical service emergency classifications" (page 192) and Table 52 "Technical services non-emergency classifications" (page 192) describe the service classifications.

Table 51
Technical service emergency classifications

Class	Degree of failure	Symptoms
E1	Major failure causing system degradation or outage	System out-of-service with complete loss of call-processing capability. Loss of total attendant console capability. Loss of incoming or outgoing call capability. Loss of auxiliary Call Detail Reporting (CDR) in resale application. Call processing degraded for reasons such as trunk group out-of-service: • 10% or more lines out-of-service • frequent initializations (seven per day or more) • inability to recover from initialization or SYSLOAD • consistently slow dial tone (eight seconds or more delay)
E2	Major failure causing potential system degradation or outage	Standby CPU out-of-service. Frequent initializations (one per day or more). Disk drive failure. Two sets of disks inoperative.

Table 52
Technical services non-emergency classifications

Class	Degree of failure	Symptoms
S1	Failure that affects service	Software or hardware trouble directly and continuously affecting user's service or customer's ability to collect revenue. Problem that seriously affects service at in-service or cut-over date.

Table 52
Technical services non-emergency classifications (cont'd.)

Class	Degree of failure	Symptoms
S2	Intermittent failure that affects service	Software or hardware faults that intermittently affect service. System-related documentation errors that directly result in or lead to impaired service.
NS	Failure that does not affect service	Documentation errors. Software inconsistencies that do not affect service. Hardware diagnostic failures (not previously defined) that cannot be corrected by resident skills. Test equipment failures for which a backup or manual alternative can be used. Any questions concerning products.

Except as excluded by the provisions of warranty or other agreements with Nortel, a fee for technical assistance may be charged, at rates established by Nortel. Information on rates and conditions for services are available through Nortel sales representatives.

Requesting assistance

Collect the information listed in Table 53 "Checklist for service requests" (page 193) before you call for service.

Table 53
Checklist for service requests

Name of person requesting service	_____
Company represented	_____
Telephone number	_____
System number/identification	_____
Installed software generic and issue (located on data disk)	_____
Modem telephone number and password (if applicable)	_____

Table 53
Checklist for service requests (cont'd.)

Seriousness of request (see Table 51 "Technical service emergency classifications" (page 192) and Table 52 "Technical services non-emergency classifications" (page 192)) _____
Description of assistance required _____
_____
_____

Index

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

Nortel Communication Server 1000

Communication Server 1000E Maintenance

Release: 7.0
Publication: NN43041-700
Document revision: 04.01
Document release date: 4 June 2010

To provide feedback or to report a problem in this document, go to www.nortel.com/documentfeedback.

www.nortel.com