
Nortel Communication Server 1000

Nortel Communication Server 1000 Release 4.5

Communication Server 1000S

Maintenance

Document Number: 553-3031-500

Document Release: Standard 3.00

Date: August 2005

Copyright © Nortel Networks Limited 2005

All Rights Reserved

Produced in Canada

Information is subject to change without notice. Nortel reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant.

Nortel, Nortel (Logo), the Globemark, This is the Way, This is Nortel (Design mark), SL-1, Meridian 1, and Succession are trademarks of Nortel Networks.

Revision history

August 2005

Standard 3.00. This document is up-issued for Communication Server 1000 Release 4.5.

September 2004

Standard 2.00. This document is up-issued for Communication Server 1000 Release 4.0.

October 2003

Standard 1.00. This document is a new NTP for Succession 3.0. It was created to support a restructuring of the Documentation Library. This document contains information previously contained in the following legacy document, now retired: Maintenance (553-3023-510).

Contents

List of procedures	11
About this document	15
Subject	15
Applicable systems	15
Intended audience	16
Conventions	16
Related information	16
Precautions	19
Contents	19
General precautions	19
Circuit cards	20
Communicating with the system	21
Contents	21
Introduction	21
Optivity Telephony Manager	22
Serial Data Interface terminal local and remote access	25
Connecting to the Media Card's RS-232 maintenance port	29
Accessing the system	29

Hardware maintenance tools	35
Contents	35
Introduction	35
Circuit card features	35
Signaling Server LEDs	37
Call Server alarms	53
Line transfer	54
 Software maintenance tools	 57
Contents	57
Introduction	57
Maintenance applications	58
Diagnostic programs	60
OTM alarm management	65
Interactive diagnostics	67
 Clearing faults	 69
Contents	69
Fault clearing process	70
Fault indicators	72
Clearing Call Server faults	75
Clearing Signaling Server faults	81
Clearing CS-MG Link faults	83
Clearing MG 1000S faults	95
Clearing trunk faults	101
Clearing IP Phone faults	108
 Replacing equipment	 109
Contents	109
Access to internal components	110
Replacing the NTAK02 SDI/DCH circuit card	112

Replacing the NTAK03 TDS/DTR circuit card	113
Replacing the NTAK09 1.5 Mb DTI/PRI card (PRI applications)	114
Replacing the NTBK50 2.0 Mb PRI card	117
Replacing the NTAK10, NTAK09, or NTRB21 circuit cards (DTI applications)	120
Replacing equipment cards	121
Replacing the NT5K21 equipment card	122
Replacing the NTAG26 equipment card	123
Replacing the NTAK92 Off-premise protection module	124
Replacing the NTDK20 SSC card	125
Replacing the NTKK25 Software Daughterboards	126
Replacing IP Daughterboards	129
Element Manager maintenance	131
Contents	131
Maintenance functions	132
Signaling Server	136
Media Card maintenance	149
Contents	149
Introduction	149
Faceplate maintenance display codes	150
Replacing a Media Card	157
Verify Media Card software and firmware	157
IP line and IP Phone maintenance and diagnostics	157
IP line shell commands	159
Warm rebooting the Media Card	159
Tests for the Media Card DSPs	160
Invoking alarm and log files	160

Simple Network Management Protocol	161
Contents	161
Introduction	162
Configuration	164
Supported MIBs	166
Configuration of system group MIB parameters	167
Traffic MIB	171
Community name strings	172
Test Alarm utility	174
EDT and EPT	176
Backup and restore	177
More information	178
 Proactive Voice quality Management	 179
Contents	179
Introduction	180
How voice quality monitoring works	181
Feature packaging	183
Supported system types	183
Feature implementation	183
New voice-quality alarms	192
Diagnosing and isolating voice-quality problems	193
SNMP interface	194
Heterogeneous environments	194
 pbxLink connection failure detection and status reporting enhancement	 197
Contents	197
Introduction	197
pbxLink connection failure detection	198
LD 117 STAT SERV enhancement	198

Technical Assistance service 205

 Contents 205

 Nortel Technical Assistance Centers 205

 Services available 208

 Requesting assistance 211

Appendix A: Establishing a PPP connection 213

 Contents 213

 Establishing a PPP connection 213

Index 239

List of procedures

Procedure 1	
Accessing the system from an SDI system terminal . .	30
Procedure 2	
Accessing the maintenance telephone	32
Procedure 3	
Clearing a fault in the CS 1000S	70
Procedure 4	
Verifying operation	71
Procedure 5	
Troubleshooting for a Point-to-Point connection	85
Procedure 6	
Troubleshooting for Layer 2 and Layer 3 LAN connection	86
Procedure 7	
Removing the front cover for access to internal components	110
Procedure 8	
Replacing the NTAK02 SDI/DCH circuit card	112
Procedure 9	
Replacing the NTAK03 TDS/DTR circuit card	113

Procedure 10 Replacing the NTA09 1.5 Mb DTI/PRI card when configured as a PRI	114
Procedure 11 Removing the NTA20 and NTA93 from the NTA09 card.	115
Procedure 12 Installing the NTA93 daughterboard before the NTA20 daughterboard	116
Procedure 13 Replacing the NTB50 2.0 Mb PRI card	117
Procedure 14 Removing the NTA20 and NTA93/NTB51 from the NTB50 card	118
Procedure 15 Installing the NTA93/NTB51 daughterboard before the NTA20 daughterboard	119
Procedure 16 Replacing the NTA10, NTA09 and NTRB21 when configured as a DTI	120
Procedure 17 Replacing equipment cards	121
Procedure 18 Replacing the NT5K21 XMFC/MFE equipment card ...	122
Procedure 19 Replacing the NTA26 XMFR equipment card	123
Procedure 20 Testing for loop-closure	124

Procedure 21	
Testing continuity	124
Procedure 22	
Replacing the NTDK20 SSC card	125
Procedure 23	
Replacing the Software Daughterboard	126
Procedure 24	
Replacing a failed Software Daughterboard	127
Procedure 25	
Replacing a NTDK83 or NTDK99 IP daughterboard ...	129
Procedure 26	
Backing up the Call Server	139
Procedure 27	
Backing up Gatekeeper from the web interface	143
Procedure 28	
Restoring the Gatekeeper from a floppy disk	143
Procedure 29	
Backing up the Gatekeeper to a floppy disk	144
Procedure 30	
Setting the modem serial-port speed for the Signaling Server	217
Procedure 31	
Using the AT command set	219
Procedure 32	
Configuring a Dial-up Networking PPP client for remote access to the Signaling Server	220
Procedure 33	
Configuring the Call Server route	231

Procedure 34
Configuring the Media Card ELAN route231

Procedure 35
Using Remote Single Point of Access232

About this document

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

Subject

This document describes Communication Server 1000S system maintenance, with sections on hardware and software maintenance tools; technical assistance; clearing faults on CS 1000S Call Server, Signaling Server, CS-MG Link, Media Gateway 1000S (MG 1000S), Trunk, and Telephone; replacing equipment; Element Manager and Media Card maintenance; establishing a PPP connection.

Note on legacy products and releases

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

www.nortel.com/

Applicable systems

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

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

Intended audience

This document is intended for individuals responsible for configuring, maintaining and troubleshooting CS 1000S systems.

Conventions

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

Related information

This section lists information sources that relate to this document.

NTPs

The following NTPs are referenced in this document:

- *Converging the Data Network with VoIP* (553-3001-160)
- *Circuit Card: Description and Installation* (553-3001-211)
- <Retag>OBSOLETE: Replace or remove
- *Software Input/Output: Administration* (553-3001-311)
- *Optivity Telephony Manager: System Administration* (553-3001-330)
- *Element Manager: System Administration* (553-3001-332)
- *IP Line: Description, Installation, and Operation* (553-3001-365)
- *Software Input/Output: System Messages* (553-3001-411)
- *Software Input/Output: Maintenance* (553-3001-511)
- *Communication Server 1000S: Installation and Configuration* (553-3031-210)

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 customer representative.

Precautions

Contents

This section contains information on the following topics:

General precautions	19
Circuit cards	20

General precautions

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

DANGER OF ELECTRIC SHOCK

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

In the CS 1000S power supply, there are no user-serviceable parts. Do not disassemble a power supply under any circumstances, because there is a risk of electric shock. If a power supply fails, the MG 1000S must be replaced.

Wear the antistatic wrist strap, provided with the CS 1000S equipment, when handling circuit cards to prevent damage caused by static electricity.

For the CS 1000S, the power supply is internal to the MG 1000S, and not field serviceable. In addition, there is no battery backup supported in the

CS 1000S. A battery backup can be provided by using a Uninterruptible Power Supply (UPS).

Circuit cards

Handle the circuit cards as follows:

- Wear the 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:

- Insert the cards into compatible slots only.
- Turn off the power switch located on the rear panel of the Call Server or on the inside front panel of the MG 1000S (the power status LED will then turn off).
- The software disables the cards, if applicable, before they are removed or inserted.
- The hardware disables the cards, whenever there is an enable/disable switch, before they are removed or inserted.
- 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 information on the following topics:

Introduction	21
Optivity Telephony Manager	22
Serial Data Interface terminal local and remote access.	25
Connecting to the Media Card's RS-232 maintenance port	29
Accessing the system	29

Introduction

You can 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
- RS-232-C compatible printer as an output only device
- Maintenance telephone set as an input only device
- Optivity Telephony Manager
- Element Manager

Refer to *Communication Server 1000S: Installation and Configuration* (553-3031-210) for information on how to connect these devices and management tools.

Optivity Telephony Manager

The Optivity Telephony Manager (OTM) is a management server. It collects and processes alarms from the CS 1000S, collects call accounting and traffic data from CS 1000S systems, and acts as a terminal server for multiple devices. One OTM Windows NT® Server replaces multiple buffer boxes, access modems, and terminal servers.

See *Optivity Telephony Manager: System Administration* (553-3001-330) for details on how to use the OTM graphics-based user interface that incorporates icons, pull-down menus, and a mouse for maintenance functions.

OTM applications

OTM provides:

- Alarm Management
- Maintenance Applications

Alarm Management

The OTM alarm management provides an alarm collection and a processing center for multiple systems and devices. The OTM receives SNMP traps from the CS 1000S systems, and stores them in a circular log file on the OTM Server. The OTM Alarm Notification application monitors incoming traps and notifies the appropriate users of important events and alarms.

The OTM alarm management has the following components:

- A web-based alarm browser server to view alarms from multiple systems and devices. HTML Help is provided for individual alarms.
- A Microsoft® Windows® alarm browser (Event Monitor) to view CS 1000S system specific alarms. Windows help is provided for individual alarms.

- An Alarm Notification application provides a scripting language to generate notifications on selected incoming traps. Notification types include pagers, e-mail, and the forwarding of SNMP traps to an upstream processor (such as Optivity NMS). The notification is triggered by trap data such as alarm severity, device type, and time of day. A Script Wizard application simplifies the creation of Alarm Notification scripts.
- A PC Event Log and Viewer to view events and alarms generated on the OTM Server and its Windows clients. This Windows application can also generate SNMP traps based on event severity level.

Maintenance applications

CS 1000S systems have over 600 overlay-based maintenance commands that support powerful capabilities. Prior to OTM, looking up the appropriate commands and syntax was time-consuming.

The OTM Maintenance Windows groups 37 Maintenance Overlays into hardware-related windows, enabling users to perform all the maintenance tasks without having to remember or look up any overlay-based commands. The new interface provides a comprehensive view of the CS 1000S system hardware configuration with the following benefits allowing users to:

- See quickly the equipped hardware. The hardware list works like a spreadsheet data view – users can scroll through the list, sort the list, and select items for changing.
- Select an item from the list and apply a Maintenance command from the right-mouse button pop-up menu.
- Print the list or copy it to a spreadsheet.
- Select a TN or DN and print the TN/DN block.
- See Enabled/Disabled status in real time.

OTM System Terminal

The System Terminal helps users to perform overlay-based tasks directly through the TTY interface. System Terminal provides online, context sensitive help for overlays, prompts, and error messages. The System Terminal also provides a terminal emulation capability.

In the web environment, the Terminal Client provides the same functionality as the System Terminal.

There are two versions of System Terminal to support two different connection types – Ethernet or PPP and Serial – as follows:

- The Overlay Passthru is available on the OTM using Ethernet or PPP. The Overlay Passthru only supports access to the overlays.
- The VT220 provides similar functions using serial connections, as well as terminal emulation for all application modules.

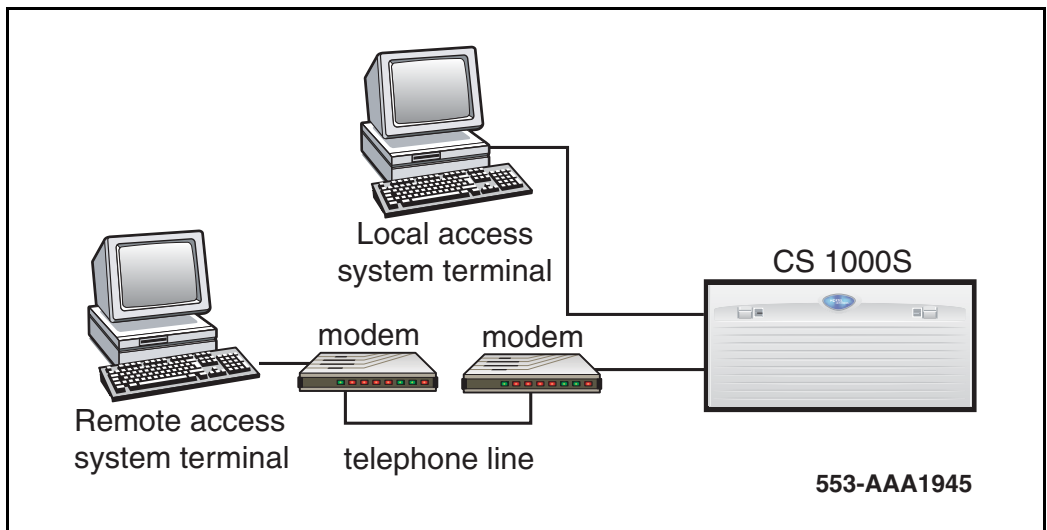
Users can access overlays through the System Terminal and application modules through VT220.

Serial Data Interface terminal local and remote access

Many devices can be installed at the local and remote locations.

When a terminal is installed locally, it is connected directly to a Serial Data Interface (SDI) port, located within the Call Server or MG 1000S. When a system terminal is installed at a remote location, modems and a telephone line are required between the terminal and the SDI port. Figure 1 shows a typical system terminal configuration to the Call Server.

Figure 1
CS 1000S local and remote access system terminals



With the CS 1000S, a system terminal can connect at the Call Server, Signaling Server, Media Cards, and MG 1000S.

Note: The MG 1000S must be connected to the Call Server with a 100BaseT cable.

When a system terminal is installed at the Call Server, it connects to a SDI port within the Call Server. Media Cards are also connected to their own SDI ports.

When a system terminal connects to an MG 1000S, it connects to a SDI port, which is part of the Small System Controller (SSC) card in the MG 1000S.

When a system terminal is installed at a remote location that does not have an MG 1000S, modems and a telephone line are required between the terminal and the SDI port.

When a system terminal is installed on the Signaling Server, it connects to a SDI port on the server.

When a system terminal is installed on the Media Cards, it connects to the Media port on the Call Server. See the Media Card installation in *Communication Server 1000S: Installation and Configuration* (553-3031-210).

An alternate connection option for either or remote access is to use the OTM 10BaseT Ethernet port on the Call Server. Figure 2 on page 27 shows a typical system terminal configuration.

Remote TTY

The three SDI ports available on the SSC card of an MG 1000S can be used as additional system TTYs. All applications on SDI ports of the SSC in the Call Server, with the exception of LSL, are supported on the SDI ports of the MG 1000S SSC.

The purpose of a remote TTY is to access the Call Server from an MG 1000S. However, TTYs configured on the Call Server cannot access the MG 1000S.

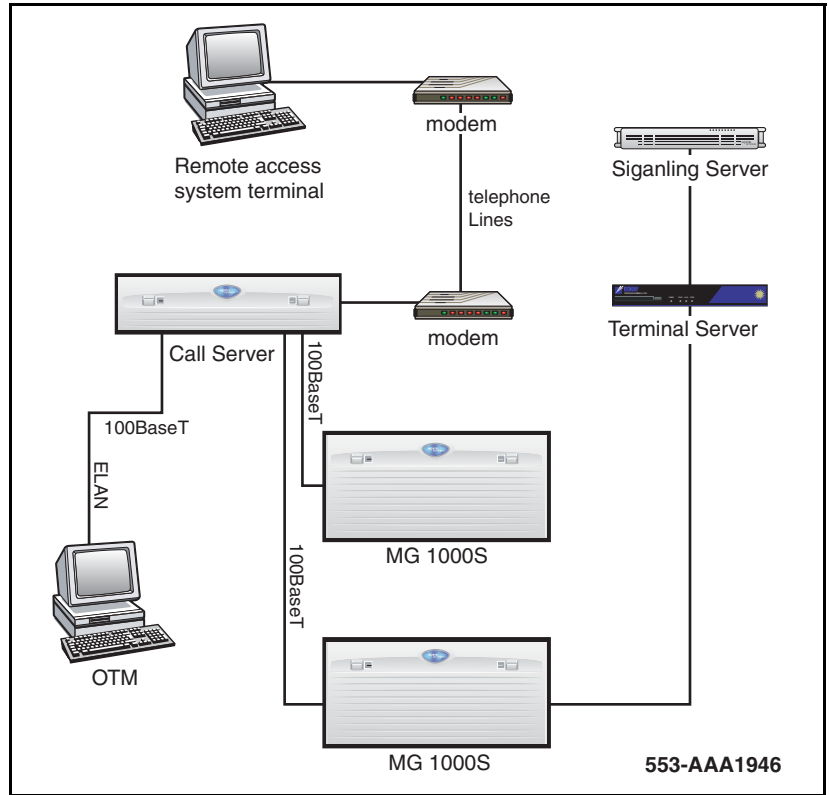
If the MG 1000S is configured to be survivable, the SDI ports of the MG 1000S SSC can be used during survival mode, and function exactly like a TTY connected to a stand-alone CS 1000S. However, the TTY has no access to either LD 43 or LD 143. In survival mode, the SDI ports of the MG 1000S cannot be used to access the Call Server. Either port on the Signaling Server can be used as a remote access.

Additional Serial Ports

The maximum number of serial ports used for maintenance, administration, CDR, and traffic will depend upon the number of MG 1000S units equipped.

There are three serial ports on the Call Server and another three for each equipped MG 1000S.

Figure 2
CS 1000S local and remote access system terminals



Note: A Terminal Server connects serial devices to the LAN.

MG 1000S 10BaseT port

The MG 1000S SSC 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 1000S 10BaseT Ethernet port can run in the Normal or Survival mode. In Normal mode, the MG 1000S does not provide access to maintenance or alarm management.

MG 1000S/Expander card slot assignment

The MG 1000S and MG 1000S Expander contain physical card slots numbered 1 to 10. When configuring the CS 1000S system, the physical card slot numbers must be transposed to “logical” card slot numbers. For example, to configure a card physically located in slot 2 of the first MG 1000S, use logical slot 12. To configure a card physically located in slot 2 of the second MG 1000S, use logical slot 22. See Table 1.

Table 1
MG 1000S and MG 1000S Expander slot assignments

	MG 1000S/MG 1000S Expander							
	First		Second		Third		Fourth	
	Physical card slot	Logical card slot	Physical card slot	Logical card slot	Physical card slot	Logical card slot	Physical card slot	Logical card slot
MG 1000S	1	11	1	21	1	31	1	41
	2	12	2	22	2	32	2	42
	3	13	3	23	3	33	3	43
	4	14	4	24	4	34	4	44
	5	*	5	*	5	*	5	*
	6	*	6	*	6	*	6	*
MG 1000S Expander	7	17	7	27	7	37	7	47
	8	18	8	28	8	38	8	48
	9	19	9	29	9	39	9	49
	10	20	10	30	10	40	10	50
Legend * Not supported.								

Connecting to the Media Card's RS-232 maintenance port

Connect a serial cable either to the P2 connector on the backplane breakout box or to the faceplate connector - but not both at once. The card's hardware cannot support two devices connected at once.

The terminal device should be set to 9600, 8, N, 1. Set the flow control to "None" or a similar setting. If the hardware flow control is enabled, users will see information from the card but the card will not respond to any keystrokes. The condition eventually deteriorates until there is no response. If this happens, ensure the flow control is set to "None", close the session, and reopen it. The card should then respond.

Accessing the system

When replacing equipment, send the maintenance commands to the system software to disable faulty equipment and to software enable and test newly installed equipment.

To perform system maintenance on the CS 1000S, use the following:

- OTM Server or OTM Client PC using a graphics-based user interface that incorporates icons, pull-down menus and a mouse.
- OTM System Terminal Overlay Passthru/VT220 or an SDI system terminal using command line inputs in an area on screen that accepts typed-in commands.
- Element Manager using a web browser. For details on Element Manager using a web browser, refer to *Element Manager: System Administration* (553-3001-332).
- Maintenance Telephone

Access through an OTM Server

See *Optivity Telephony Manager: System Administration* (553-3001-330) for details on how to access the system with OTM.

Access through an SDI system terminal or OTM System Terminal Overlay Passthru/VT220

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

When the user accesses the system through a system terminal, a login procedure is required. All system passwords are initially set as 0000, but the user can change passwords through the Configuration Record (LD 17).

If a sysload (system reload) occurs before the new password is saved in a data dump, the last active password remains valid.

Each system has two levels of passwords: level 1 is for general use, and level 2 is for administrative use. Either password is accepted in the login procedure.

Accessing the system from an SDI system terminal

Note: See *Optivity Telephony Manager: System Administration* (553-3001-330) for details on using OTM System Terminal Overlay Passthru/VT220.

To access the system from an SDI system terminal, follow the steps in Procedure 1.

Procedure 1

Accessing the system from an SDI system terminal

- 1 Press the return key.

Decision Point. If the response is OVL111 nn IDLE or OVL111 nn BKGD, the user is ready to log into the system. Go to step 2. If the response is **OVL000 >**, the user is already logged into the system. Go to step 4.

Responses vary with different Background Terminal packages.

- 2 Enter **LOGI ADMIN1**, then press the return key.
The normal response is **'PASS?'**. If there is any other response, see the *Software Input/Output: Maintenance* (553-3001-511).
- 3 Enter either the level 1 or level 2 password and press the return key. If the password is correct, the system responds with the prompt **">"**.

- 4 Enter 'LD xx', Where "xx" represents the number of the program.
- 5 Perform tasks.
- 6 End the program by entering **** (star symbols).
- 7 End the login session with **LOGO**.

End of Procedure

Access through the maintenance telephone

A telephone functions as a maintenance telephone when the class-of-service is defined as MTA (maintenance telephone allowed) in LD 11.

A maintenance telephone enables the user to send a subset of commands. The maintenance telephone takes priority over a system terminal and will log 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 Internet Telephone operating as a maintenance telephone: 30, 32, 33, 34, 36, 37, 38, 41, 42, 43, 45, 46, 60, and 62.

Note: The above maintenance overlay operations are supported on Internet Telephones 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 (defined in the customer data block) is entered followed by "91". To enter commands, press the keys that correspond to the letters and numbers of the command (for example, to enter *LD 42 return*, key in

53#42##). Table 2 on page 32 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	R	S	7	7
T	U	V	8	8
W	X	Y	9	9
			0	0
		Space or # (pound symbol)		#
		Return		##
Note: Q = 7 and Z = 9 on the dial pad.				

Accessing the maintenance telephone

To access the maintenance telephone, follow the steps in Procedure 2.

Procedure 2

Accessing the maintenance telephone

- 1 Press the prime DN key.
- 2 Place the telephone in maintenance mode by entering **xxxx91** ("xxxx" represents the customer SPRE code. It is defined in the Customer Data Block and can be printed in LD 21. The SPRE code is typically "1" (which means the user would enter 191).

- 3 Check for busy tone by entering **** (star symbols)**
 - 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 ****** (star symbols)**
- 4 Load a program by entering **53#xx##** ("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 of Procedure

Note: Nortel RM-356 Modem Router equipment is recommended to enable remote dial-in to the ELAN subnet.

Hardware maintenance tools

Contents

This section contains information on the following topics:

Introduction	35
Circuit card features	35
Signaling Server LEDs	37
Call Server alarms	53
Line transfer	54

Introduction

There are fault indicators and hardware features which help perform maintenance tasks (particularly identifying and clearing faults). These maintenance tools include:

- Circuit card features which perform self-tests, indicate status, and minimize adverse affects on call processing.
- Alarm Notification generates notifications on pagers and e-mails of selected incoming traps.

Circuit card features

Circuit card features include:

- self-tests

- LED indicators Card faceplate hexadecimal displays
- enable/disable switches

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.

Faceplate LEDs

Media Card LEDs

Status LED

The NTVQ01xx 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 NTVQ01xx Media Card faceplate contains Ethernet activity LEDs for each network. The faceplate contains six Ethernet activity LEDs. Three for the ELAN network and three for the TLAN network. The LEDs indicate the following links on the ELAN network and TLAN network (in order from the top):

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

Maintenance hex display

This is a four-digit LED-based hexadecimal display that provides the status of the NTVQ01xx 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. Refer to Table 32 on [page 150](#) for a description of the hex display codes.

It also indicates the progress of the internal self-test in the form of T:xx.

ITG Trunk LED display

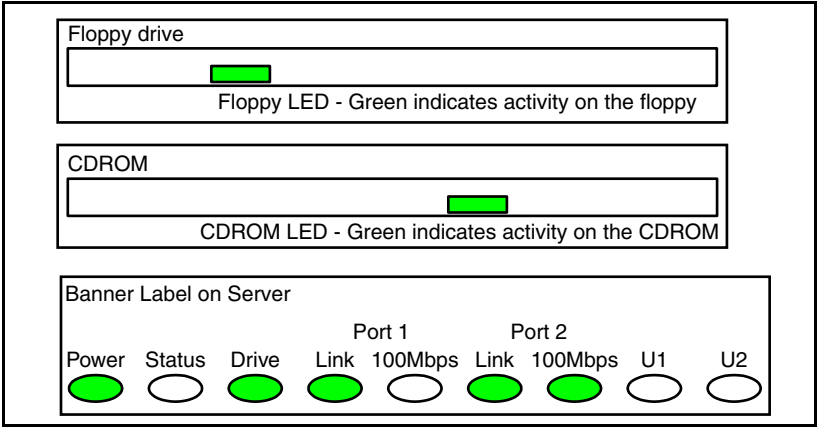
The LED display on the ITG Trunk Card faceplate reflects only the functional state of the card. It does not reflect the operational state of the ITG card. Error messages with a severity category of "Critical" are displayed on the maintenance faceplate in the form: "Gxxx" or "Sxxx", where xxx is the last three digits of the ITG or ITS message. Table 34 on [page 153](#) lists the critical ITG messages and Table 35 on [page 156](#) lists the critical ITS messages.

Signaling Server LEDs

Refer to Figure 3 and the following for the status of the Signaling Server LEDs:

- Power – LED Green power is on, LED OFF power is off
Note: When the power is turned off on a Signaling Server that is operational the two Link leds for Port 0 and Port 1 will continue to flash.
- Status – LED off indicates CPU is running. RED LED indicates CPU has halted
- Drive – Flashing Green means Hard drive or CDROM is active
- Link – Green LED indicates an active Link for either ethernet Port 1 or Port 2
- 100Mbps – Green LED indicates the ethernet port 0 or Port 1 is running at 100Mbps. Off indicates 10Mbps.
- U1 and U2 are not used

Figure 3
Signaling Server LEDs



ITG-P LED (Card Status)

The red status faceplate LED indicates the enabled/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 card is enabled by the system. If the LED remains on, the self-test failed, the card is disabled, or the card rebooted.

NTAK09 Faceplate LEDs

The NTAK09 1.5 Mb DTI/PRI circuit card has a total of seven faceplate LEDs. Five of the LEDs are directly associated with the operation of the NTAK09 circuit card. The remaining two LEDs are associated with the optional daughterboards. The first of these LEDs is used to indicate the status of the NTAK20 Clock Controller daughterboard. The second LED indicates the status of the NTAK93 D-channel interface daughterboard.

The LEDs found on the NTAK09 DTI/PRI circuit card are described in Table 3.

Table 3
NTAK09 LEDs (Part 1 of 2)

Affected circuit card	LED	State	Definition
NTAK09	DIS	On (Red)	The NTAK09 circuit card is disabled.
		Off	The NTAK09 is not in disabled state.
	ACT	On (Green)	The NTAK09 circuit card is in active state. No alarm states exist, the card is not disabled, nor is it in a loopback state.
NTAK09	ACT	Off	An alarm state or loopback state exists, or the card has been disabled. See other faceplate LEDs for more 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 NTAK09 is in loopback mode.
		Off	The NTAK09 is not in loopback mode.

Table 3
NTAK09 LEDs (Part 2 of 2)

Affected circuit card	LED	State	Definition
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, then this state is acceptable, and the flashing is identifying jitter on the reference.
		Off	The NTAK20 is not equipped.
NTAK93/ 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.

Note: Only one of the five NTAK09 related LEDs should be on at any one time.

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 2 Mb DTI circuit card. The remaining LED is associated with the on-board clock controller.

The LEDs on the NTAK10 are described in Table 4.

Table 4
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, then this state is acceptable, and the flashing is identifying jitter on the reference.
	Off	The clock controller is switched off.

NTAK79 Faceplate LEDs

The NTA79 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 on-board Clock Controller and the on-board D-channel interface (DCHI).

The NTA79 faceplate LEDs are described in Table 5.

Table 5
NTAK79 LEDs (Part 1 of 2)

LED	State	Definition
OOS	On (Red)	The NTA79 2 Mb PRI circuit card is either disabled or out-of-service state.
	Off	The NTA79 2 Mb PRI is not in disabled state.
ACT	On (Green)	The NTA79 2 Mb PRI circuit card is in active state.
	Off	NTA79 2 Mb PRI is not in disabled state. The OOS LED will be 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.

Table 5
NTAK79 LEDs (Part 2 of 2)

LED	State	Definition
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, then this state is acceptable, and the flashing is identifying 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 NTB50 2 Mb PRI circuit card LEDs are described in Table 6.

Table 6
NTBK50 faceplate LEDs (Part 1 of 2)

LED	State	Definition
OOS	On (Red)	The NTB50 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 NTB50 2 Mb PRI is not in disabled state.
ACT	On (Green)	The NTB50 2 Mb PRI circuit card is in active state.
	Off	The NTB50 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 NTB50 2 Mb PRI is in loopback mode.
	Off	The NTB50 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.

Table 6
NTBK50 faceplate LEDs (Part 2 of 2)

LED	State	Definition
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, then this state is acceptable, and the flashing is identifying 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.

NTDK20 SSC card Faceplate LEDs

The NTDK20 SSC card has either three or five faceplate LEDs, depending on the version of the card.

The SSC/PC card LED indicates the following, if the LED is:

- Off, the SSC is in normal operation
- Yellow, the SSC is disabled
- Red, the SSC is running self-test
- Red and flashes three times, the self-test passed
- Green steady or flashing, the PC card is accessed

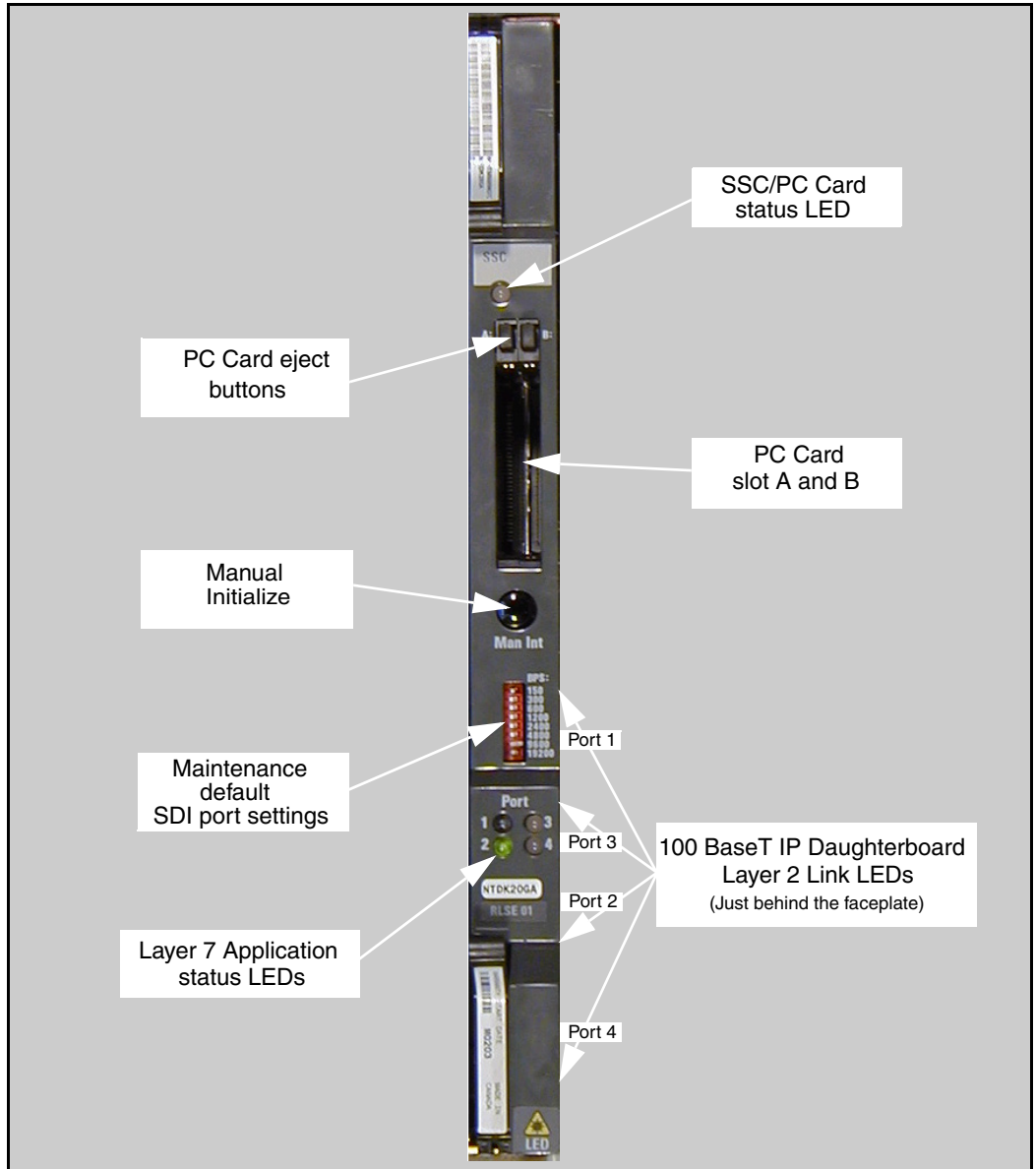
The Layer 7 Port LEDs indicate the following, if the Port LEDs are:

- Red, the link is disabled and voice is disabled
- Amber, the link is established and voice is disabled
- Green, the link and voice are established

The IP Daughterboard port Layer 2 Link LEDs indicate the following, if the Link LEDs are:

- Green, the link is established
- Red (receive) and yellow (transmit) flashing, show network activity

Figure 4
Call Server SSC card faceplate



NTDK83 and NTDK99 card circuit board LEDs

There are three LEDs for each port on these daughterboards as shown in Figure 5. They provide the status of the Layer2 network link on all the MG 1000S IP daughterboards. See Figure 6 on page 49 for Call Server IP DaughterBoard locations and See Figure 7 on page 49 for MG 1000S IP DaughterBoard location.

Figure 5
NTDK83 and NTDK99 card circuit board LEDs

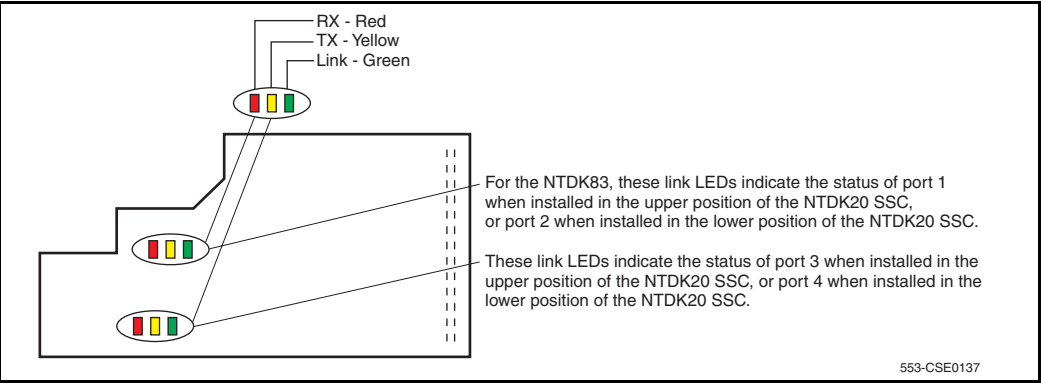


Table 7
NTDK83 and NTDK99 daughterboards LEDs

LED	State	Definition
Receive	Red	The information/data is being received.
	Off	No information/data is being received.
Transmit	Yellow	Information/data is being transmitted.
	Off	No information/data is being transmitted.
Link	Green	A physical connection with link pulses exists between the card and the customer's data equipment.
	Off	No connection exists.

Figure 6
Call Server IP DaughterBoard LEDs

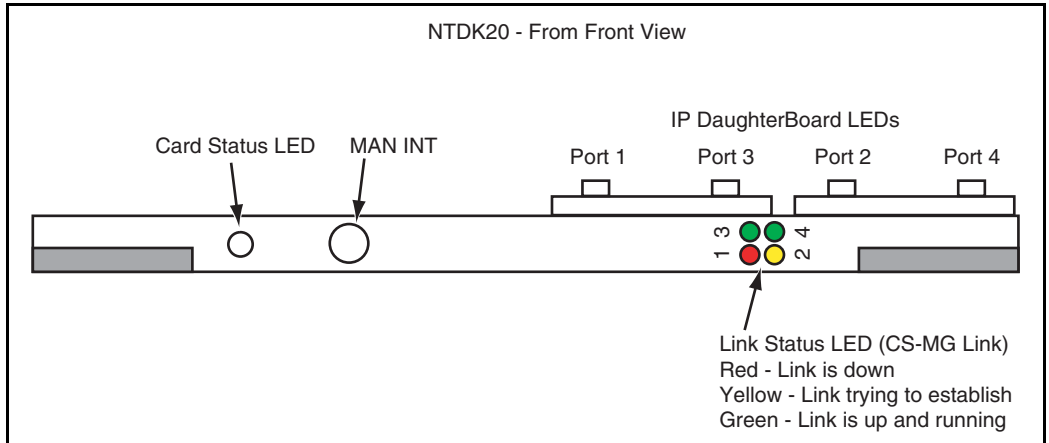


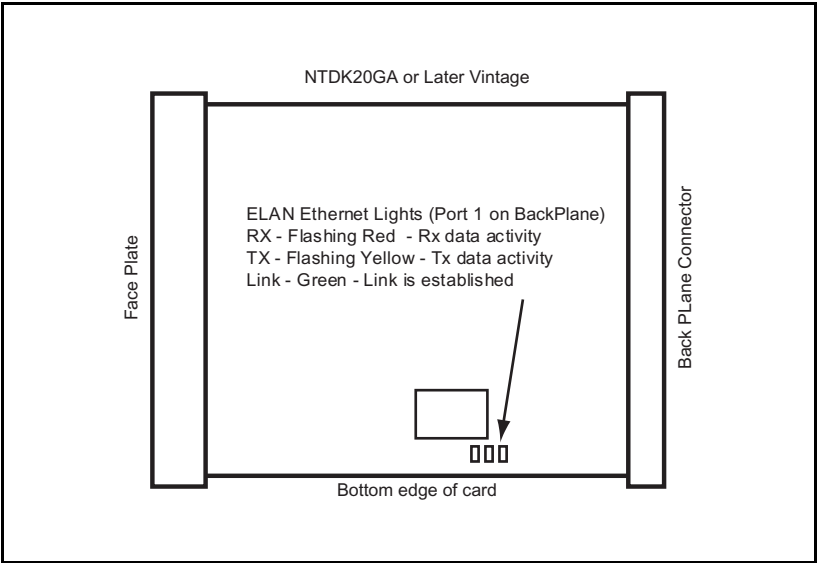
Figure 7
MG 1000S SSC IP daughterboard link LED



ELAN Ethernet LEDs

The NTDK20GA or later SSC card has three LEDs to indicate the status of the ELAN network. See Figure 8 for location and description of the LEDs.

Figure 8
ELAN Ethernet LEDs on SSC



NTRB21 Faceplate LEDs

The NTRB21 1.5 Mb DTI/PRI/DCH circuit card has a total of seven faceplate LEDs. Five of the LEDs are directly associated with the operation of the NTRB21 circuit card. The remaining two LEDs are associated with the optional daughterboards. The first of these LEDs is used to indicate the status of the NTAK20 Clock Controller daughterboard. The second LED indicates the status of the D-channel interface.

The LEDs found on the NTRB21 DTI/PRI/DCH circuit card are described in Table 8. Only one of the five NTRB21 related LEDs should be on at any one time.

Table 8
NTRB21 LEDs (Part 1 of 2)

Affected circuit card	LED	State	Definition
NTRB21	DIS	On (Red)	The NTRB21 circuit card is disabled.
		Off	The NTRB21 is not in disabled state.
	ACT	On (Green)	The NTRB21 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 has been disabled. See other faceplate LEDs for more 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 NTRB21 is in loopback mode.
		Off	The NTRB21 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.

Table 8
NTRB21 LEDs (Part 2 of 2)

Affected circuit card	LED	State	Definition
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, then this state is acceptable, and the flashing is identifying jitter on the reference.
		Off	The NTAK20 is not equipped.

Monitor jacks

The NTAK09, NTAK10, NTAK79, NTBK50, and NTRB21 have two bantam jacks (RCV and XMT) located 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.

Initialize button

Press the manual initialize button, designated MAN INIT on the faceplate of the NTDK20 SSC to start the Initialize program. The Initialize program clears Core Equipment faults, rebuilds call-dependent data, and generates system messages indicating the status of the system. This process is called an initialization (or INI). Call processing is briefly interrupted during an initialization.

Call Server alarms

Major and Minor Alarms can be displayed on the Attendant Console when connected to the system.

Major alarms

A major alarm indicates a fault which seriously interferes with call processing. The causes of major alarms are listed in Table 9 on page 54.

When an MG 1000S 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 9.

A minor alarm displays an alarm 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 9
Causes of major and minor alarms

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

External alarms

A remote alarm, in the context of general maintenance, is an extension of a major alarm on the CS 1000S to another location or to an audible or visual indicator. The system generates a signal indicating it has a major alarm condition and sends it to a remote location, such as a monitoring center or a test center, or to an indicator, such as a light or bell.

Line transfer

As an option, connect one or more PFTUs to the system. 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 CPU failure
- if there is a loss of power to the MG 1000S
- if there is a loss of power to the PFTU
- if a line transfer switch on the PFTU is turned on

Power supply failure

The CS 1000S only supports an AC power source. The power indicator is the Nortel logo.

These are the only replaceable components:

- NTDU30 – Call Server shelf assembly
- NTDU14 – MG 1000S shelf assembly
- NTDU15 – MG 1000S Expander shelf assembly
- NTDU27 – Signaling Server

Software maintenance tools

Contents

This section contains information on the following topics:

Introduction	57
Maintenance applications	58
Diagnostic programs	60
OTM alarm management	65
Interactive diagnostics.	67

Introduction

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

- Diagnostic programs monitor a variety of operations, detect faults, and initiate a corrective action during normal call processing.
- Interactive diagnostics test hardware, isolate faults, and verify fault clearing.
- Element Manager provides status and allows you to issue a variety of commands.
- OTM alarm management has the following components:
 - a web-based alarm browser
 - a Microsoft ® Windows ® alarm browser (Event Monitor)

- an Alarm Notification
- a PC Event Log and Viewer
- OTM maintenance applications

Maintenance applications

CS 1000S systems have over 600 overlay-based maintenance commands that support their powerful capabilities. To maintain a CS 1000S system using SDI terminals, the user has to remember (or look up) which overlay has the appropriate commands and the syntax of each command.

Element Manager enables a certain subset of the overlay functions to be performed for maintenance of the Call Server, Signaling Server and Media Cards.

Note: There are two versions of the OTM Maintenance applications: Maintenance Windows (windows based) and Maintenance Pages (web based). Both provide the same functionality.

With OTM Maintenance Windows, there are 37 Maintenance Overlays grouped into hardware-related windows to allow users to perform all the maintenance tasks without having to remember or look up any overlay-based commands. The OTM interface provides a comprehensive view of the CS 1000S system hardware configuration with the following benefits:

- See the equipped hardware quickly. The hardware list works like a spreadsheet data view. Users can scroll through the list, sort the list, and select items for changing.
- Select an item from the list and apply a Maintenance command from the right-mouse button pop-up menu.
- Print the list or copy it to a spreadsheet.
- Select a TN or DN and print the TN/DN block.
- See enabled/disabled status in real time.

Maintenance Windows applications

The OTM Maintenance Windows includes the following applications:

SSC

The SSC window displays the status of the Call Server and MG 1000S SSC cards on the CS 1000S system. Perform actions and tasks on the SSC cards in the CS 1000S system's Call Server and MG 1000S from the SSC window.

I/O Ports

The I/O (Input/Output) Ports window displays the status of all I/O ports on the CS 1000S system, and allows users to execute actions and tasks on a selected port.

Network Loops

The Network Loops window lists all the network loops on the CS 1000S system. It allows users to execute actions and tasks on a selected loop by choosing commands from the Maintenance menu.

Intelligent Peripheral Equipment (IPE) Cards

The IPE Cards window displays the status of all IPE type cards associated with each MG 1000S on a system, and allows users to execute actions and tasks on a selected card.

IPE Units

The IPE Units window displays information for all IPE units and Directory Numbers on the CS 1000S system, and allows users to execute actions and tasks on a selected unit.

B- and D-channels

The PRI/PRI2 B- and D-channels window displays the B- and D-channels on the selected digital trunk (for example, PRI loop), and allows users to execute actions and tasks on a selected channel.

For detailed information on each Maintenance Windows function, see the Maintenance Applications chapter in *Optivity Telephony Manager: System Administration* (553-3001-330).

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

See the *Software Input/Output: Maintenance* (553-3001-511) and *Software Input/Output: System Messages* (553-3001-411) for detailed information on all diagnostic programs.

Overlays

Non-resident 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).

Error Monitor

The Error Monitor is a resident program which 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 as 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. This process is called an initialization (or INI).

Activate an initialization by pressing the manual initialize (Man Int) button on the NTDK20 SSC 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 non-resident software programs which will 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 users log on to check the status of a circuit card) or the Midnight Routine runs.

Include the programs listed in Table 10 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 10
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
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	Multi-frequency 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 non-resident 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. Once 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 Overlay.

Maintenance commands for 10BaseT connectivity

The 10BaseT Link (ELAN network) is the signaling connection between the Call Server and other system components, such as the Signaling Server and MG 1000S. Troubleshooting the 10BaseT Link is required when there is no connection or the connection is dropped between the Call Server and MG 1000S. The following maintenance commands in LD 135 are used to troubleshoot 10BaseT Links:

- STAT IPL <link #>
- LLBK IP <media gateway #>

Note: See *Software Input/Output: Maintenance* (553-3001-511) for details.

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 MG 1000S operation. 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 request a report with the **PRT QOS <cab#>** command in LD 117. See *Software Input/Output: Administration* (553-3001-311) and *Software Input/Output: Maintenance* (553-3001-511).

Data Network Ratings (Excellent, Good, Fair, and Poor) are calculated along with the actual parameter values for the network delay. See Table 11 for the Data Network Ratings parameters.

Table 11
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 11 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. The user cannot configure the thresholds.

In LD 117, the command **CHG PDV <port#> <delay>** is used to set a Packet Delay Variation (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 and is automatically downloaded to the MG 1000S.

Note: Systems must meet the minimum data networking requirements from *Converging the Data Network with VoIP* (553-3001-160).

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 how many days it has been 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 have been loaded and all checks performed, the System Loader is erased from system memory, the Initialize Program runs, and the 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.

OTM alarm management

Web-based alarm browser

The web-based alarm management provides a list of alarms and events from multiple systems and devices. The Alarm Browser page is used to retrieve, view, sort, and view help on alarms received by the OTM server.

Microsoft ® Windows ® alarm browser (Event Monitor)

The alarm management consists of a number of components that improve handling of system-generated alarms and events. The alarm management is

only available for systems configured with the alarm management package (296).

The CS 1000S alarm management components are:

- Text Handler
- Alarm Banner dialog box

PC Event Log and viewer

The Events Monitor window displays the CS 1000S system's Event Log, showing all recent system alarms and events previously stored in the CS 1000S system's history file.

The Events Monitor window displays active events in a way that lets users quickly view the most important events. System events with a severity of critical, major, or minor are considered alarms. These alarms are events which can require some corrective action. System events with a severity of Info are for informational purposes only and are not considered alarms.

Alarm Notification

The Alarm Notification application receives SNMP events from designated network equipment over an Ethernet network and sends out alarm notifications when specified event conditions are detected. Received events are compared to a set of rules which can activate notifications of different types. These notifications include:

- SNMP traps or events transmitted to predefined destinations
- text notification over a modem
- pager notification to alpha or numeric pagers
- e-mail using Simple Mail Transfer Protocol (SMTP)
- log

For detailed information on Alarm Management, see *Optivity Telephony Manager: System Administration* (553-3001-330).

Interactive diagnostics

Load non-resident software programs into the memory through the OTM System Terminal or an SDI terminal. These programs, also called overlays or loads, are identified by a title and a number which 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 10 on page 62.

Non-resident 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 then performs the task and sends system messages indicating status or errors back to the user.

With interactive diagnostics the user 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: Maintenance* (553-3001-511) and in *Software Input/Output: System Messages* (553-3001-411).

Enhanced Maintenance feature

The system software sometimes requires modifications, called patches 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 there is a patch in service.

The Enhanced Maintenance feature:

- Enables patches to automatically survive a sysload.
- Enables patches on non-resident programs.
- Records all patches in the system.
- Enables data cartridges to be shipped with pre-loaded patches.

If there is a problem with a patch, the CPU sends system messages, with the mnemonic EHM, to the system terminal or the History File.

This enhancement allows a technician to upgrade a site using the same software generic by new or replacement patches preloaded on disk. Also, specified patches can be selectively dumped from core memory to disk. The Dump Patch facility is used for these purposes.

A maximum of 50 dummy globals are allowed for patches, instead of the normal five. Usage of these globals is tracked, and a warning message is given if an attempt is made to use them for another patch.

Clearing faults

Contents

This section contains information on the following topics:

Fault clearing process	70
Fault indicators	72
Clearing Call Server faults	75
Clearing Signaling Server faults	81
Clearing CS-MG Link faults	83
Clearing MG 1000S faults	95
Clearing trunk faults	101
Clearing IP Phone faults	108

Fault clearing process

To clear a fault in the CS 1000S, follow the steps in Procedure 3.

Procedure 3

Clearing a fault in the CS 1000S

- 1 Observe and record all fault indicators.
- 2 System messages, visual fault indicators and user reports identify many problems. If the indicators are not current or seem incomplete, review previous messages, initialize the system for information on the current status, or both.
- 3 Look up all system messages in *Software Input/Output: System Messages* (553-3001-411).

The interpretation of the message can identify faulty equipment and tell the user what action to take to clear the problem. If the user cannot clear the fault using a Maintenance Application or through information in the *Software Input/Output: Maintenance* (553-3001-511), follow the process in this chapter to isolate and clear the fault.

- 4 Try to enable or test disabled equipment.

CAUTION WITH ESDS DEVICES

Wear the antistatic wrist strap, provided with the equipment, when handling circuit cards to prevent damage caused by static discharge.

- 5 Hardware re-enable circuit cards by unseating then reinstalling them. Software re-enable cards by disabling then re-enabling them. When the cause of a fault is not clearly evident, a software test can help identify the problem.
- 6 Replace equipment as necessary.

End of Procedure

Verification

To verify that the CS 1000S is operating properly and there are no remaining faults, follow the steps in Procedure 4.

Procedure 4

Verifying operation

- 1 Make sure all circuit cards that could have been removed are reinserted in their assigned location and enabled.
- 2 Make sure all wiring and connectors that could have been disconnected are reconnected.
- 3 Set 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

**** (star symbols)

LOGO (the midnight routine will now run)

- 4 Check system messages produced when the midnight routine runs. Clear any faults indicated.
- 5 If there was a sysload (reload) 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:

**** (star symbols)

LOGO

- 6 Replace any covers that were removed.
- 7 Tag defective equipment with a description of the fault and return it to a repair center.

End of Procedure

Fault indicators

When there is a fault in the system, the user can be notified 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. The number identifies the specific message. Use system messages with other indicators, such as visual indicators, to identify and clear faults.

Table 12 on [page 73](#) lists the most common fault indicating messages and the type of fault they indicate. For a complete list and interpretation of system messages, see the *Software Input/Output: System Messages* (553-3001-411). View system messages in the OTM PC Event Log. Right-clicking on the system message in the Event Log list shows a description and a maintenance action for system messages.

Each type of fault indicator is described in Table 12.

Table 12
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	Core Equipment
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	Network
ERR4062 NWS301, 401, 501 OVD001—010, 024 XMI messages	Peripheral Equipment
ERR090, 220, 270 OVD001—010 TRK messages	Trunk
ERR500 MWL500 NWS501 OVD001—010	Telephone

Visual fault indicators

Users can identify faults by using the following visual indicators:

- A major alarm display indicates a possible power, Call Server, or SSC fault.
- Circuit card Light Emitting Diodes (LEDs): indicates a card or a unit on a circuit card is disabled.

Table 13 on page 74 lists visual indicators and the type of fault they indicate for CS 1000S systems.

Table 13
Visual fault indicators and related fault types for CS 1000S

Indicator	Type of fault
NT logo on the MG 1000S	Power
Red LED lit on associated card	Peripheral Equipment
Red LED lit on trunk card	Trunk
Red LED lit on associated cards	Telephone
Green LED off, on 100BaseT daughterboards	Cable connection

For Signaling Server and MG 1000S card, refer to “Faceplate LEDs” on [page 36](#).

Clearing Call Server faults

Call server components

The Call Server performs system control and switching. The NTDU08 Call Server components are:

- NTDK20 SSC card
 - NTKK25 Software daughterboard
 - NTDK83 or NTDK99 100BaseT IP daughterboard
- NTDU30 Call Server chassis

The Call Server NTDK20 SSC card can include:

- a CPU comprised of two processors:
 - The main processor handles call processing, serial ports, and network traffic.
 - The auxiliary processor handles card polling, power monitoring, tone generation, and control of a Digital Signal Processor (DSP) for tone detection.
- Ethernet controller provides one port between the CPU and a Local Area Network (LAN).
- Serial Data Interface provides three ports between the CPU and external devices.
- Personal Computer Memory Card Industry Association (PC Card) interface provides access for one Type III or two Type II PC Card drives to allow software delivery or customer data storage.
- Tone and Digit Switch provides 30 channels of tone generation.
- Digitone Receiver provides eight DTR/XTD units with an additional user selectable eight DTR/XTD units or four MFC, MFE, MFK5, MFK6, or MFR units.
- 32 conference channels:

- 16 with each Single-Port IP Daughterboard equipped
- 32 with each Dual-Port IP Daughterboard equipped
- IP Daughterboard provides 16 additional conference channels for each MG 1000S and access to the MG 1000S hardware.
- Software Daughterboard provides storage for system software.

Call Server faults

Call Server faults can disable the CPU and stop call processing. In addition, other peripheral equipment may not operate properly while there is a Call Server fault in the system. Refer to Table 14 for Call Server fault indicators.

When call processing has stopped on the Call Server you may need to replace the following equipment:

- NTDK20 SSC card
 - NTKK25 Software daughterboard
 - NTDK83 or NTDK99 100BaseT IP daughterboard
- NTDU30 Call Server Chassis

Table 14
Call Server 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	Red LED lit on NTDK20 SSC circuit card

Fault indicated on the SSC card, or Memory fault indicated

If the red LED is lit on the SSC card, or a memory fault is indicated, refer to Table 15 for possible causes and actions to perform.

Table 15
SSC or memory fault causes and actions (Part 1 of 2)

Condition	Possible cause	Action
Red LED is lit or memory fault indicated.	Improperly installed NTKK25 Software Daughterboard	Power down the system, remove the NTKK20 SSC card. Unseat the Software Daughterboard and then reseat it. Reinsert the NTKK20 SSC circuit card. Power up the system.
	Improperly installed NTKK83, NTKK99, Daughterboard	Power down the system, remove the NTKK20 SSC card. Unseat the daughterboard and then reseat it. Reinsert the NTKK20 SSC circuit card. Power up the system.

Table 15
SSC or memory fault causes and actions (Part 2 of 2)

Condition	Possible cause	Action
Red LED is lit or memory fault indicated.	Defective NTDK20 SSC card	<p>Replace the NTDK20 SSC circuit card with the original daughterboards installed on it.</p> <p>Reuse all daughterboards installed on the original NTDK20 SSC circuit card.</p> <p>Note: Call processing on the entire system will be interrupted while the NTDK20 SSC circuit card is being replaced.</p> <p>If the system does not recover, go to the next possible cause.</p>
	Defective NTDK83, NTDK99 Daughterboard	<p>Unseat the NTDK20 SSC circuit card and replace the daughterboard.</p> <p>Note: Call processing on the entire system will be interrupted while the NTDK20 SSC circuit card is unseated.</p> <p>Reinsert the NTDK20 SSC circuit card.</p> <p>If the system will not reload, go to the next possible cause.</p>

Fault indicated when trying to perform a data dump

A data dump is done using LD 43 on an SDI terminal. The EDD command is only supported on the Call Server. The user is able to log onto the system but will get an error message when trying to perform a data dump. Refer to Table 16 for possible causes and actions to perform.

Table 16
Data dump error causes and actions

Condition	Possible cause	Action
Data dump error	Data on Software Daughterboard	Perform an EDD NBK command in LD 43 to restore the data.
	Manual initialize button pressed when performing a backup using the Customer Configuration Backup and Restore feature	While still in remote backup mode, issue an ENLT command.
	Security failure during an upgrade	Re-enter the keycodes. Note: Up to three invalid keycodes can be entered. After the third invalid keycode, all changes are lost and the Setup Program returns to the main menu.

OVL005 message displayed and no access to overlays

This fault will occur if the user presses the manual initialize button on the System Controller card when performing a data backup, restore, or verification using the Customer Configuration Backup and Restore (CCBR) feature.

When logging back onto the system after completing the remote backup activity, the user is unable to access overlays and an OVL005 message is displayed.

Table 17
OVL0005 message displayed and no access to overlays

Condition	Possible cause	Action
OVL0005 and no access to overlays	Manual initialize button pressed when using the CCBR feature	After logging onto the system, issue the ENLT command at the TTY.

Call Server problems

Major problems with the system may be caused by the Call Server.

Table 18
Call Server problems

Condition	Possible cause	Action
System constantly rebooting	Defective SSC or MG 1000S	Replace the SSC or MG 1000S. Enable and test the cards by entering: LD 30 TEST
Logo LED is off or fan is not running	Loss of AC power Defective MG 1000S	Restore AC power Replace the MG 1000S Enable and test the cards by entering: LD 30 TEST

Clearing Signaling Server faults

The Signaling Server is an OEM server that meets the CS 1000S environmental requirements. It has ELAN and TLAN Ethernet ports which are connected to an Ethernet switch through CAT 5 cables. It has two serial ports and visual indicators for maintenance. It has three push buttons, one for power, reset and INI. The INI button, USB ports, keyboard port and mouse port are not supported.

The Signaling Server has no serviceable parts inside. It is serviced as a unit. If the system cover is removed, the warranty is void.

Table 19
Signaling Server Diagnosis (Part 1 of 2)

Condition	Possible Cause	Action
System not working. All LED's off.	No Power to system	Check power cable
	Power supply failed	Replace Server
System on with no fan noise	Fan failed	Replace Server
Floppy drive tries accessing floppy but fails	Floppy media is corrupted	Replace floppy
	Floppy not formatted	Format floppy
Floppy drive not accessing floppy & green light not coming on.	Floppy drive failed	Replace Server
CDROM drive tries to access CDROM but stops.	CDROM media is corrupted	Replace CDROM
CDROM drive not accessing CDROM. No green light.	CDROM Drive failed	Replace Server
100BT Light not on	Auto Negotiate Failed	Provision Ethernet Switch to 100MB. Auto Negotiate off.

Table 19
Signaling Server Diagnosis (Part 2 of 2)

Condition	Possible Cause	Action
ELAN or TLAN Link Light not active	Bad Connection to Ethernet Switch	Check power on Ethernet Switch. Check Ethernet cable Check Ethernet Switch port
	Failed Ethernet port	Replace Server
System unable to boot from Hard Drive	Hard Drive not formatted	Install software. Refer to <i>Communication Server 1000S: Installation and Configuration</i> (553-3031-210).
	Hard Drive with Bad Sectors	Install software and use disk check option. Replace Server if fails.
	Hard Drive Failed	Replace Server
Signaling Server not responding through serial port.	Software failed	Reset Server
Signaling Server boots then stops.	No Software loaded	Load Software. Refer to <i>Communication Server 1000S: Installation and Configuration</i> (553-3031-210).

Clearing CS-MG Link faults

Call Server to MG 1000S Link faults

The Call Server to MG 1000S (CS-MG) Link functions in the CS 1000S are an integral part of the NTDK20 SSC cards. The CS-MG link specifically refers to the connectivity between two SSC cards and the two 100BaseT connections between them. The cards provides speech path switching, and transmit and receive signaling messages between the CPUs. The CS-MG link functions include:

- Conference/Tone and Digit Switch combines the functionality of Conference by providing 32 channels of conferencing and 60 channels of tone generation. Each daughterboard connected to the SSC provides an additional 16 Conference channels per port (16 channels with each single-port daughterboard and 32 channels with each dual-port daughterboard).
- SSC circuit cards provides the digital switching and conferencing for the system.
- Tone Digit Switch/Digitone Receiver provides 60 channels of tone generation for the system and eight DTR/XTD units with an additional user selectable eight DTR/XTD units or four MFC, MFE, MFK5, MFK6, or MFR units that convert multi-frequency dialing signals.
- Serial Data Interface provides the interface for up to three Input/Output device ports from the SSC card.
- Ethernet controller provides one port between the CPU and the network.

The CS-MG link faults can cause system initializations, disable conference capability or disable all terminal connections (such as trunks and telephones) on a card. The CS-MG link faults can make functional peripheral equipment appear faulty.

Fault clearing procedures

To clear CS-MG Link faults, see fault indicators in Table 20.

Table 20
 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

Isolating CS-MG Link connectivity faults

The CS-MG Link is the physical connection between the Call Server and MG 1000S. Troubleshooting this 100BaseT Link is required when there is no connection or the connection is dropped between the Call Server and MG 1000S. Troubleshooting procedures are provided for Point-to-Point, Layer 2 and Layer 3 connections.

Note: Use a SDI terminal to perform the following procedures using overlay commands.

Point-to-Point connection

To troubleshoot for a Point-to-Point connection, follow the steps in Procedure 5.

Procedure 5

Troubleshooting for a Point-to-Point connection

- 1 Verify that the green Link LED on the daughterboard in the Call Server is on (physical connection is good). If Link LED is off, check the physical connection by verifying that the daughterboard and cables are properly installed.

Note: See *Communication Server 1000S: Installation and Configuration* (553-3031-210) for details.

- 2 Use the LD 32 command DISS <n> (n = IP daughterboard port#) to disable the link for testing. Use the LLBK <link #> to test the signaling and voice path of the daughterboard. If the card fails the LLBK test, replace the IP daughterboard.
- 3 Verify that the MAC address of the MG 1000S is correctly configured on the Call Server. Use the PRT IPR command in LD 117 to access the MAC data.
- 4 Use the **PING <ip address of the MG 1000S>** command in LD 117 to verify network connection.
- 5 Re-enable any disabled components. Verify the 100BaseT connection between the Call Server and the MG 1000S is operating by pinging the IP address of the MG 1000S(s) configured.

Note: Any MG 1000S using a Point-to-Point connection cannot be pinged from other data network nodes. However, the Call Server can ping a MG 1000S, and the MG 1000S can ping the Call Server.

End of Procedure

Layer 2 and Layer 3 LAN connections

To troubleshoot for Layer 2 and Layer 3 LAN connection, follow the steps in Procedure 6.

Procedure 6

Troubleshooting for Layer 2 and Layer 3 LAN connection

- 1 Verify that the green Link LED on the daughterboard in the Call Server is on (physical connection is good). 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 1000S and the Layer 2/3 switch. Consult the local IS department for the appropriate IP address.
- 3 Use the LD 32 command DISS <n> (n = IP daughterboard port#) to disable the link for testing. Use the LLBK <link #> to test the signaling and voice path of the daughterboard. If the card fails the LLBK test, replace the IP daughterboard.
- 4 Verify that the MAC address of the MG 1000S is correctly configured on the Call Server. Use the PRT IPR command in LD 117 to access the MAC data.
- 5 Use the **PING <ip address of the MG 1000S>** command in LD 117 to verify network connection.
- 6 Re-enable any disabled components. Verify the 100BaseT connection between the Call Server and the MG 1000S is operating by pinging the IP address of the MG 1000S(s) configured.

Note: The CS 1000S only supports Layer 2 and Layer 3 switches. Software based routers are not recommended.

End of Procedure

Fault clearing procedures using an SDI terminal

Follow these procedures to clear faults using an SDI terminal as indicated in the following error messages.

Disabled card indicated by OVD message

An overload (OVD) message indicates a network (loop) is disabled. The network (loop) number in the CS 1000S system corresponds to the slot number in the MG 1000S Expander. All terminal connections on the loop are disabled.

Test the card with LD 30. Enter the following command:

TEST

If the card tests OK, the problem has cleared. If an overload message appears after a few minutes, you may need to replace some of the following equipment:

- For CS 1000S:
 - NTDK95 - MG 1000S Expansion cables
 - NTDU30 - Call Server
 - NTDU14 MG 1000S
 - NTDU15 MG 1000S Expander
 - NTDU0606 100BaseT used to connect the NTDK83/99 to the bulk head connectors
 - NTTK34 UTP 100BaseT CAT 5 Cross-over cable (2 m)
 - NTDK20 SSC card
 - NTTK25 Software Daughterboard. The NTTK13 is still supported.
 - NTDK99 Single-port 100BaseT IP Daughterboard
 - NTDK83 Dual-port 100BaseT IP Daughterboard
 - NTDU27 Signaling Server
 - NTDU40 - Media Card

Look up all system messages in *Software Input/Output: System Messages* (553-3001-411) and follow the instructions given. If the fault does not clear, continue with the Manual Continuity Tests.

Manual Continuity Tests can be used to isolate Network and Peripheral Equipment faults. See LD 30 in *Software Input/Output: Maintenance* (553-3001-511) for details on performing the tests.

Constantly observe and look up system messages as you perform the actions in Table 21.

Table 21
CS-MG Link causes and actions (Part 1 of 2)

Condition	Possible cause	Action
Visual indicators on NTDK20 (Red or Amber) and system messages	Defective NTDK83 in Call Server or NTDK99 in MG 1000S	<p>Replace the Daughterboard on the NTDK20 SSC circuit card.</p> <p>Note: Call processing on the system will be interrupted while the NTDK20 SSC circuit card is unseated.</p> <p>If the fault remains, replace and test the cable.</p>
	Defective IP Links	<p>View the status of the IP Links by entering:</p> <p>LD 135 STAT IPL x (where x is the number for the MG 1000S 1 through 4)</p> <p>If the fault remains replace the daughterboard and dongle in the MG 1000S.</p> <p>If the fault remains, replace the NTDK20 SSC circuit card.</p>
	Defective NTDU0606, NTTK34	<p>Replace the cable or coupler between the Call Server and MG 1000S.</p> <p>Note: Call processing for the MG 1000S will be interrupted while the cable is replaced.</p> <p>Enable and test the card by entering:</p> <p>LD 30 TEST</p> <p>If the fault persists, go to the next possible cause.</p>

Table 21
CS-MG Link causes and actions (Part 2 of 2)

Condition	Possible cause	Action
Red LED on SSC or no visual link indicators	Defective NTDK20 SSC card	<p>Install a new NTDK20 SSC card. Reuse the daughterboards and the dongle attached to the original NTDK20 SSC circuit card.</p> <p>Note: Call processing on the system will be interrupted while the NTDK20 SSC circuit card is being replaced.</p> <p>Enable and test the card by entering: LD 30 TEST Wait for an overlay message.</p> <p>If the card tests "OK", the NTDK20 SSC circuit card was defective.</p> <p>If after a few minutes the problem reoccurs, replace the Call Server chassis.</p>

Card disabled without overlay message

When a system message indicates one or more cards are defective or disabled, but there is no overload (overlay) message indicating disabled equipment. Look up all system messages in the *Software Input/Output: System Messages* (553-3001-411) and follow the instructions given. If the fault does not clear, users may need to replace some system components as listed in section Fault

clearing procedures using an SDI terminal on page 86. Refer to Table 22 on page 90 for system causes and actions.

Table 22
All systems causes and actions

Condition	Possible cause	Action
Visual indication (Red LED) that card is disabled and system message	Card circuitry latched	Disable card, reseal card and enable the card. If the fault persists, go to the next possible cause.
	Defective circuit card	Replace the circuit card. Enable and test the card by entering: LD 30 TEST If the fault persists, replace the circuit card.

Voice media problems

The Call Server clock is synchronized to the MG 1000S via the IP packets. When the CS-MG Link is point-to-point, it is recommended that the ZeroBandwidth parameter be set to “No”. When the MG 1000S has a T1 or

E1 clock controller, it is recommend, that the ZeroBandwidth parameter be set to No.

Table 23
Voice media problems

Condition	Possible cause	Action
Perceived one way speech path, broken speech or static on the line	Call Server has lost synchronization with it clock reference in the MG 1000S	<p>Ensure that Zerobandwidth parameter is set to "NO"</p> <p>LD 117 PRT IPR <port></p> <p>LD 117 CHG IPR <port> <MAC address> [<IP address> <subnet mask> <zero bandwidth>]</p>

CAUTION — Service Interruption

If you are running the Call Server and MG 1000S in point to point, zero bandwidth must be NO.

If a Clock controller (T1 or E1) is in the MG 1000S, zero bandwidth must be NO for that link.

Setting the zero bandwidth to NO, allows the Call Server to have a clock reference.

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

Several users cannot transfer or place conference calls, or calls do not receive Music-on-Hold (MOH). A circuit card that provides conference capability can be disabled. Look up all system messages in the *Software Input/Output: System Messages* (553-3001-411) and follow the instructions. If the fault does not clear, users may need to replace some of the following equipment:

- NTDK20 SSC card
- NTDK99 IP Daughterboard
- NTDK83 IP Daughterboard

Note: In addition to the conference channels on the SSC the NTDK83 and the NTDK99 IP Daughterboards each provide an additional 32 conference channels when installed on the Call Server SSC.

Table 24
Conference channels causes and actions (Part 1 of 3)

Condition	Possible cause	Action
Several users cannot place conference calls when links are fine, sets are fine.	Defective CS-MG links	<p>View the status of the IP Links by entering: LD 135 STAT IPL x (where x is the number for the MG 1000S 1 through 4)</p> <p>If the fault remains, check the IP Daughterboard conference loops.</p> <p>If the fault remains, check the NTDK20 SSC conference loops.</p>
System message indicates conference loop 31, 62, 94 or 95 is defective.	Defective Call Server IP Daughterboard	<p>If a fault is indicated on conference loop 31, replace the Daughterboard for MG 1000S 1.</p> <p>If a fault is indicated on conference loop 62, replace the Daughterboard for MG 1000S 2.</p> <p>If a fault is indicated on conference loop 94, replace the Daughterboard for MG 1000S 3.</p> <p>If a fault is indicated on conference loop 95, replace the Daughterboard for MG 1000S 4.</p> <p>Call processing on the System will be interrupted while the NTDK20 SSC circuit card is unseated.</p>

Table 24
Conference channels causes and actions (Part 2 of 3)

Condition	Possible cause	Action
System message indicates conference loop 29 or 30 is defective.	Defective SSC circuit card.	<p>If a fault is indicated on conference loop 29 or 30, replace the NTDK20 SSC circuit card.</p> <p>Reuse the daughterboards and dongle installed on the original NTDK20 SSC circuit card.</p> <p>Note: Call processing on the entire system will be interrupted while the NTDK20 SSC circuit card is being replaced.</p>
Defective conference loop with no system message	Defective IP Daughterboard or SSC circuit card.	<p>If there are no messages indicating a fault on any conference loop, test each conference loop in the system by entering:</p> <p>LD 38 CNFC loop ("loop" represents the conference loop number 29, 30, 31, 62, 94 or 95)</p> <p>If the conference loop is disabled, try to enable it by entering:</p> <p>LD 38 ENLL loop ("loop" represents the conference loop number 29, 30, 31, 62, 94 or 95)</p> <p>If a fault is indicated on conference loop 31,62, 94 or 95 replace the associated IP Daughterboard.</p> <p>If a fault is indicated on conference loop 29 or 30, go to the next possible cause.</p>

Table 24
Conference channels causes and actions (Part 3 of 3)

Condition	Possible cause	Action
	Defective NTDK20 SSC card	<p>Install a new NTDK20 SSC card.</p> <p>Reuse the Daughterboards and dongle attached to the original NTDK20 SSC circuit card.</p> <p>Note: Call processing on the system will be interrupted while the NTDK20 SSC circuit card is being replaced.</p> <p>Enable and test the card by entering: LD 30 TEST</p> <p>If the card tests "OK", the NTDK20 SSC circuit card was defective.</p> <p>If after a few minutes the problem reoccurs, replace the Call Server chassis.</p>

Clearing MG 1000S faults

The MG 1000S provides the interface between network switching and terminal equipment (such as trunks and telephones). MG 1000S faults can disable network and terminal equipment. Refer to Table 25 on page 95 for MG 1000S fault indicators.

When call processing has stopped on the MG 1000S you may need to replace the following equipment:

- NTDK20 SSC card
 - NTKK25 Software daughterboard
 - NTDK99 100BaseT IP daughterboard
- NTDU14 MG 1000Ss

Table 25
MG 1000S 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

Fault clearing procedures using an SDI terminal

Follow these procedures to clear faults using an SDI terminal.

Disabled circuit card in MG 1000S

The following tables are provided to assign in isolating faults in a MG 1000S or MG 1000S Expander. 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: System Messages* (553-3001-411) and follow the instructions given. If the fault does not clear, you may need to replace some of the following equipment:

- NTTK34 or NTDU0606 IP MG 1000S cables
- NTDK95 MG 1000S Expansion cables
- NTDK20 SSC card
- NTDK99 Single-port 100BaseT Daughterboard

Table 26
Defective components causes and actions (Part 1 of 2)

Condition	Possible cause	Action
<p>Red LED on card</p> <p>Two or more units on a circuit card are disabled</p> <p>System message indicating the circuit card or units on it are disabled</p>	Defective circuit card	<p>Enable the circuit card by entering: LD 32 ENLC c ("c" represents the card number)</p> <p>Test the card by entering: LD 30 UNTT c ("c" represents the card number).</p> <p>Replace the affected circuit card.</p>
<p>Layer 7 LED is Red</p> <p>Link LED is Off or Flickering</p>	Defective NTDU0606, NTTK34 or IP cable to switch.	<p>Do a visual and physical check of the cable connections. Replace if necessary.</p> <p>Disable the MG 1000S by entering: LD 32 DISS x (x is the number for the MG 1000S 1 through 4)</p> <p>Enable the MG 1000S by entering: LD 32 ENLS x (x is the number for the MG 1000S 1 through 4)</p> <p>Test the circuit card by entering: LD 30 TEST (the TEST command ensures that all circuit cards are re-enabled in the MG 1000S).</p>

Table 26
Defective components causes and actions (Part 2 of 2)

Condition	Possible cause	Action
Common visual indication and system messages on MG 1000S Expansion	Defective NTDK95 MG 1000S Expansion cable	<p>Note: Call processing for the MG 1000S will be interrupted while the MG 1000S cable or coupler is being replaced.</p> <p>If the affected cards are in the MG 1000S Expansion, replace the NTDK95 cable connecting to the MG 1000S.</p>

Table 27
NTDK20 causes and actions (Part 1 of 2)

Condition	Possible cause	Action
CS-MG Link Red visual indication on affected MG 1000S (yellow LED on Call Server)	Defective NTDK99 card in MG 1000S	<p>Disable the MG 1000S by entering: LD 32</p> <p>DISS x (x is the number for the MG 1000S 1 through 4)</p> <p>Replace the card.</p>
Media quality has deteriorated		<p>View the status of the IP links by entering: LD 135</p> <p>STAT IPL x (x is the number for the MG 1000S 1 through 4)</p> <p>Perform Local and Remote Loop-back tests on the IP links by entering: LD 135</p> <p>LLBK IPL x (x is the number for the MG 1000S 1 through 4)</p> <p>Enable the MG 1000S by entering: LD 32</p> <p>ENLS x (x is the number for the MG 1000S 1 through 4)</p>

Table 27
NTDK20 causes and actions (Part 2 of 2)

Condition	Possible cause	Action
Red LED on SSC Media quality has deteriorated Intermittent trunk or line problems Multiple system messages about this MG 1000S	Defective NTDK20 SSC card in MG 1000S	<p>Replace the NTDK20 SSC card.</p> <p>Note: Call processing for the entire system will be interrupted while the NTDK20 SSC circuit card is being replaced.</p> <p>Reuse the Software Daughterboard, if equipped, attached to the original NTDK20 SSC circuit card.</p> <p>Test the circuit card by entering: LD 30 UNTT c (c represents the card number.)</p>

More than one disabled circuit card MG 1000S

More than one circuit card in an MG 1000S, or two or more units on different circuit cards, are disabled in the same MG 1000S. There is a system message indicating the circuit cards or units on the circuit cards are disabled. Look up all system messages in the *Software Input/Output: System Messages* (553-3001-411) and follow the instructions given. If the fault does not clear, use this procedure.

Manual Continuity Tests can be used to isolate Intelligent MG 1000S faults. See “Overlay 30” in the *Software Input/Output: Maintenance* (553-3001-511) for details on performing the tests.

Constantly observe and look up system messages as you perform this procedure.

You may need to replace:

- NTDK20 SSC card
- NTDK83 or NTDK99 IP Daughterboard

Table 28
NTDK20 MG 1000S causes and actions

Condition	Possible cause	Action
Red LED on SSC Media quality has deteriorated Intermittent trunk or line problems Multiple system messages about this MG 1000S	Defective NTDK20 SSC card in MG 1000S	<p>Disable the MG 1000S by entering: LD 32</p> <p>DISS x (x is the number for the MG 1000S 1 through 4)</p> <p>Replace the NTDK20.</p> <p>Enable the MG 1000S by entering: LD 32</p> <p>ENLS x (x is the number for the MG 1000S 1 through 4)</p> <p>Test the circuit cards by entering: LD 30</p> <p>TEST (the TEST command ensures that all circuit cards are re-enabled in the MG 1000S)</p> <p>Note: Call processing for the MG 1000S will be interrupted while the cable is being replaced.</p>
Multiple cards exhibit problems	Defective MG 1000S	<p>Replace the MG 1000S.</p> <p>Enable and test the cards by entering: LD 30</p> <p>TEST</p>
Logo LED is off or fan is not running	Defective MG 1000S	Replace the MG 1000S

Clearing trunk faults

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:
 - Central Office 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 CS 1000S system.

Fault clearing procedures using an SDI terminal

Refer to Table 29 for Trunk fault indicators.

Table 29
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 (OVD message received)

A user cannot make or receive calls over a trunk and an overload (OVD) system message is received. The message indicates only this trunk has been disabled. Look up all system messages in the *Software Input/Output: System Messages* (553-3001-411) and follow the instructions. If the fault does not clear, use manual continuity tests.

Manual continuity tests can be used to isolate faults to peripheral equipment, such as E&M or Universal Trunk circuit cards. See “Overlay 30” in the *Software Input/Output: Maintenance* (553-3001-511) for details on performing the tests.

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
- NTDK20 SSC card
- Trunk equipment (such as music source or paging equipment)

Table 30
Trunk cannot make or receive calls (OVD message received) (Part 1 of 3)

Condition	Possible cause	Action
Trunk cannot make or receive calls (OVD message received).	Defective trunk circuit card.	<p>If the indicated circuit card is an E&M or Universal Trunk circuit card, hardware disable then re-enable the circuit card to initiate a self-test. If the test fails, replace the circuit card. If the test passes, follow the procedure below.</p> <p>Disconnect the wiring between the circuit card and the cross-connect terminal.</p> <p>Enable the TN by entering: LD 32 ENLU c u ("c u" represents card and unit numbers)</p> <p>Wait for an OVD message.</p> <p>If an OVD message appears, replace the circuit card.</p> <p>If there is no OVD message, reconnect the wiring and go to the next possible cause.</p>

Table 30

Trunk cannot make or receive calls (OVD message received) (Part 2 of 3)

Condition	Possible cause	Action
	Defective wiring	<p>At the main cross-connect terminal, disconnect the wiring to the CO or other trunk equipment (such as a music source or paging equipment).</p> <p>Enable the TN and wait for an OVD message. If an OVD message appears, repair or replace the wiring to the IPE shelf.</p> <p>If there is no OVD message, repair or replace the wiring from the cross-connect terminal to the telephone.</p> <p>If the trunk circuit card still will not enable or there is still a trunk problem, reconnect the wiring and go to the next possible cause.</p> <p>Enable the TN by entering: LD 32 ENLU c u ("c u" represents card and unit numbers)</p> <p>Wait for an OVD message.</p> <p>If an OVD message appears, replace the circuit card.</p> <p>If there is no OVD message, reconnect the wiring and go to the next possible cause.</p>

Table 30

Trunk cannot make or receive calls (OVD message received) (Part 3 of 3)

Condition	Possible cause	Action
	Defective trunk equipment	<p>Make sure the CO equipment or other trunk equipment is not defective.</p> <p>If there is no problem with this equipment, go to the next possible cause.</p>
	Defective DTR, TDS, MFS or SSC card	<p>Seize trunks and audibly test for dial tone and outpulsing, or use a maintenance telephone and enter:</p> <p>LD 36</p> <p>TRK c u (“c u” represents card and unit numbers)</p> <p>Note: See the <i>Software Input/Output: Maintenance</i> (553-3001-511) for information on using this test.</p> <p>If there is no outpulsing sound, the Digitone Receiver, Tone and Digit Switch, or Multi-Frequency Sender may not be sending or receiving digits and the fault will affect more than one trunk. See the procedures for clearing faults on this equipment.</p>

Trunk cannot make or receive calls (no OVD message)

A user cannot make or receive calls over a trunk, but there is no overload (OVD) or other system message showing the TN for this trunk is defective or has been disabled. Look up all system messages in the *Software Input/Output: System Messages* (553-3001-411) and follow the instructions given. If the fault does not clear, use this procedure.

Manual continuity can be used to isolate faults to equipment, such as E&M and Universal Trunk circuit cards. See “Overlay 30” in the *Software Input/Output: Maintenance* (553-3001-511) for details on performing the tests.

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

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
- NTDK20 SSC (Small System Controller) card
- Trunk equipment (such as music source or paging equipment)

Table 31
Trunk cannot make or receive calls (no OVD message) (Part 1 of 3)

Condition	Possible cause	Action
Trunk cannot make or receive calls (no OVD message)	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.
	Disabled or defective TN	Test the TN by entering: LD 30 UNTT c u ("c u" represents card and unit numbers) Test other TNs by entering: TEST If the test fails, replace the indicated item and test again, go to the next possible cause.

Table 31**Trunk cannot make or receive calls (no OVD message) (Part 2 of 3)**

Condition	Possible cause	Action
	Defective trunk circuit card	<p>If the circuit card is an E&M or Universal Trunk circuit card, hardware disable the circuit card and then re-enable it to initiate a self-test.</p> <p>If the test fails, replace the circuit card.</p> <p>If the test passes, go to the next possible cause.</p>
	Defective wiring	<p>At the main cross-connect terminal, disconnect the wiring to the CO or other trunk equipment.</p> <p>Enable the TN and wait for an OVD message. If an OVD message appears, repair or replace the wiring to the IPE shelf.</p> <p>If there is no OVD message, repair or replace the wiring from the cross-connect terminal to the telephone.</p> <p>If the trunk circuit card still will not enable or there is still a trunk problem, reconnect the wiring and go to the next possible cause.</p>
	Defective DTR, TDS, MFS or System Core circuit card	<p>Use the attendant console Barge-in feature to seize trunks and audibly test for dial tone and outpulsing, or use a maintenance telephone and enter:</p> <p>LD 36</p> <p>TRK c u ("c u" represents card and unit numbers)</p> <p>Note: See the <i>Software Input/Output: Maintenance</i> (553-3001-511) for information on using this test.</p>

Table 31
Trunk cannot make or receive calls (no OVD message) (Part 3 of 3)

Condition	Possible cause	Action
		<p>If there is no outpulsing sound, the Digitone Receiver, Tone and Digit Switch, or Multi-Frequency Sender may not be sending or receiving digits and the fault will affect more than one trunk. See the procedures for clearing faults on this equipment.</p> <p>If there is no problem with this equipment, go to the next possible cause.</p>
	Excessive traffic in the system	Additional trunk circuit cards may be required to handle the traffic in the system.

Clearing IP Phone faults

For fault clearing procedures, refer to *IP Line: Description, Installation, and Operation* (553-3001-365).

Replacing equipment

Contents

This section contains information on the following topics:

Access to internal components	110
Replacing the NTAK02 SDI/DCH circuit card.	112
Replacing the NTAK03 TDS/DTR circuit card	113
Replacing the NTAK09 1.5 Mb DTI/PRI card (PRI applications). . . .	114
Replacing the NTBK50 2.0 Mb PRI card	117
Replacing the NTAK10, NTAK09, or NTRB21 circuit cards (DTI applications)	120
Replacing equipment cards	121
Replacing the NT5K21 equipment card	122
Replacing the NTAG26 equipment card.	123
Replacing the NTAK92 Off-premise protection module	124
Replacing the NTDK20 SSC card.	125
Replacing the NTTK25 Software Daughterboards	126
Software Daughterboard compatibility	126
Replacing IP Daughterboards	129

Access to internal components

This procedure describes how to access components in the Call Server, MG 1000S and MG 1000S Expander. To remove the front cover for access to terminal components, follow the steps in Procedure 7.

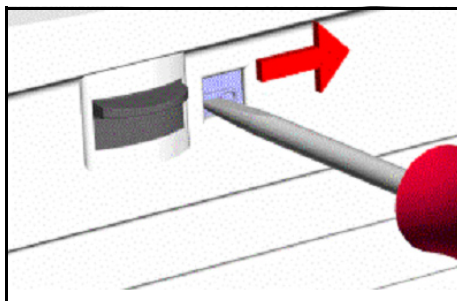
Procedure 7

Removing the front cover for access to internal components

- 1 If the front cover lock latches are in their locked position, use a flat screwdriver to slide the icon away from the latch. Refer to Table 9.

Figure 9

Inserting screwdriver in slot



- 2 Simultaneously slide both spring loaded latches toward the bottom of the cabinet and pull forward. Then lift the cover upward to remove it from the cabinet. Refer to Figure 10.

Note: The bottom of the front cover is supported but not secured to the cabinet. Be careful not to drop it.

Figure 10
Depressing latches and pulling back on front cover



End of Procedure

Replacing the NTA02 SDI/DCH circuit card

To replace the NTA02 SDI/DCH circuit card, follow the steps in Procedure 8.

Procedure 8

Replacing the NTA02 SDI/DCH circuit card

- 1 If the following circuit cards are configured, disable them in the following overlays:

SDI LD 48

DCH LD 96

The system can initialize if users 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 MG 1000S.
- 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 refer to the *Communication Server 1000S: Installation and Configuration* (553-3031-210).

- 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 have been previously disabled, enable them in the following overlays:

SDI LD 48

DCH LD 96

End of Procedure

Replacing the NTA03 TDS/DTR circuit card

To replace the NTA03 TDS/DTR circuit card, follow the steps in Procedure 9.

Procedure 9

Replacing the NTA03 TDS/DTR circuit card

- 1 Disable the SDI ports, and the DTR and TDS capabilities in the following overlays.

SDI ports **LD 48**

TDS and DTR **LD 34**

The system can initialize if users do not perform this step.

- 2 Hold the TDS/DTR circuit card by the lock latches, unlock the latches, and slide the circuit card out of the MG 1000S.
- 3 Hold the replacement TDS/DTR circuit card by the lock latches and slide it into its assigned slot until it connects with the backplane.
- 4 Secure the lock latches on the circuit card.
- 5 Enable the SDI ports, TDS channels, and Digitone Receivers in their corresponding overlays:

SDI **LD 48**

TDS and DTR **LD 34**

End of Procedure

Replacing the NTA09 1.5 Mb DTI/PRI card (PRI applications)

To replace the NTA09 1.5Mb DTI/PRI card when configured as a PRI, follow the steps in Procedure 10.

Procedure 10

Replacing the NTA09 1.5 Mb DTI/PRI card when configured as a PRI

- 1 If the NTA93 DCHI daughterboard is attached to the card, disable the associated D-channel using the following overlay and commands:

LD 96 DISDCHX

If the NTB51 DDCH daughterboard is attached to the card, disable the associated downloadable D-channel using the following overlay and commands:

LD 96 DISDCHX

LD 96 DISMSDLX

- 2 Disable the Clock Controller (if on PRI) by using the command:

LD 60 DISCC 0

- 3 Disable the PRI pack by using the command:

LD 60 DISLX

Note: The LEDs on the front of the NTA09 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 MG 1000S. If required, remove any daughterboards which can be attached. See Procedure 11.
- 5 On the replacement PRI circuit card, set 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 Enable the Clock Controller (if on the PRI) and the PRI in their corresponding overlays.

LD 60 ENLCC0

LD 60 ENLLX

The associated DCHI will automatically enable.

- 7 Check the tracking of the Clock Controller with the following overlay.

LD 60 SSCK0

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

LD 60 SSCK0

LD 60 TRCKPCK/SCLK

End of Procedure

Removing the daughterboards

Because of the physical layout of the motherboards and daughterboards, the NTAK20 should be removed before the NTAK93.

To remove the NTAK20 and NTAK93 from the NTAK09 card, follow the steps in Procedure 11.

Procedure 11

Removing the NTAK20 and NTAK93 from the NTAK09 card.

- 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 of Procedure

If more than one NTAK09 card is installed, the additional cards may not carry daughterboards, depending on system configuration. At least one NTAK20 for each system is required.

Mounting the daughterboards

Install the NTAk93 daughterboard before the NTAk20 daughterboard. Work on a flat surface when mounting or removing daughterboards. To install the NTAk93 daughterboard before the NTAk20 daughterboard, follow the steps in Procedure 12.

Procedure 12

Installing the NTAk93 daughterboard before the NTAk20 daughterboard

- 1 Visually inspect the connector pins on the underside of the daughterboard. Any pins that are bent should be realigned prior to mounting.
- 2 Place the NTAk09 down flat on an antistatic pad.
- 3 From an overhead view, with the daughterboard parallel above the NTAk09 and the connector pins aligned over the connector sockets, align the mounting holes on the daughterboard with the tops of the standoffs on the NTAk09.
- 4 Slowly lower the daughterboard toward the NTAk09, keeping the standoffs in line with all four holes, until the holes rest on top of the four standoffs.

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 NTAk09 and return to step 2.

- 5 Gently 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. Press down the two corners on the opposite side until they lock into place.

End of Procedure

Replacing the NTB50 2.0 Mb PRI card

To replace the NTB50 2.0 Mb PRI card, follow the steps in Procedure 13.

Procedure 13

Replacing the NTB50 2.0 Mb PRI card

- 1 If the NTAK93 DCHI daughterboard is attached to the card, disable the associated D-channel using the following overlay and commands:

LD 96 DISDCHX

If the NTB51 DDCH daughterboard is attached to the card, disable the associated downloadable D-channel using the following overlay and commands:

LD 96 DISDCHX

LD 96 DISMSDLX

- 2 Disable the Clock Controller using these commands:

LD 60 DISCC0

- 3 Disable the PRI pack using these commands:

LD 60 DISLX

Note: The LEDs on the front of the NTB50 change from green (enabled) to red (disabled.) In order for this to happen, the DISMSDL command has to 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 MG 1000S. If required, remove any daughterboards which can be attached. See Procedure 14.

- 5 On the replacement PRI circuit card, set 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 Enable the Clock Controller and the PRI in their corresponding overlays:

LD 60 ENLCC0

LD 60 ENLL X

The associated DCHI/DDCH will automatically enable.

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

LD 60 SCK0

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

LD 60 TRCKPCK/SCLK

End of Procedure

Removing the daughterboards

Because of the physical layout of the motherboards and daughterboards, remove the NTAK20 before the NTAK93/NTBK51. To remove the NTAK20 and NTAK93/NTBK51 from the NTBK50 card, follow the steps in Procedure 14.

Procedure 14

Removing the NTAK20 and NTAK93/NTBK51 from the NTBK50 card

- 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 of Procedure

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 surface when mounting or removing daughterboards. To install the NTAK93 and NTB51 daughterboard before the NTAK20 daughterboard, follow the steps in Procedure 15.

Procedure 15

Installing the NTAK93/NTBK51 daughterboard before the NTAK20 daughterboard

- 1** Visually inspect the connector pins on the underside of the daughterboard. Realign bent pins prior to mounting.
- 2** Place the NTB50 down flat on an antistatic pad.
- 3** From an overhead view, with the daughterboard parallel above the NTB50 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 NTB50.
- 4** Lower the daughterboard onto the NTB50, 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 NTB50 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. Then press down on the two corners on the opposite until they lock into place.

End of Procedure

Replacing the NTAk10, NTAk09, or NTRB21 circuit cards (DTI applications)

To replace the NTAk10, NTAk09 and NTRB21 when configured as a DTI, follow the steps in Procedure 16.

Procedure 16

Replacing the NTAk10, NTAk09 and NTRB21 when configured as a DTI

- 1 Disable the Clock Controller by using the command:

LD 60 DISCC0

- 2 Disable the DTI pack by using the command:

LD 60 DISLX

- 3 Hold the circuit card by the lock latches, unlock the latches, and slide the circuit card out of the MG 1000S. If required, remove any daughterboards attached to the NTAk09.

- 4 On the replacement DTI circuit card, set any switches and install any daughterboards as required. Hold the replacement DTI circuit card by the lock latches and slide it into its 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 ENLCC0

LD 60 ENLLX

- 6 Check the tracking of the Clock Controller with the following overlay:

LD 60 SSSCK0

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

LD 60 TRCKPCK/SCLK

End of Procedure

Replacing equipment cards

Use Procedure 17 to replace the following equipment cards:

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

See the *Software Input/Output: Maintenance* (553-3001-511) and the *Software Input/Output: System Messages* (553-3001-411) for a description of all maintenance commands and system messages.

To replace equipment cards, follow the steps in Procedure 17.

Procedure 17 Replacing equipment cards

- 1 Software disable the card by using these commands:

LD 32

DISC c ("c" is the card number)

- 2 Unhook the locking devices on the card; pull it out of the card cage.
- 3 Set option switches or jumper plugs on the following replacement cards the same as on the card you removed:

NT8D14 Universal Trunk Card

NT8D15 E&M Trunk Card

- 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 completes 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 c
When the process is complete, a system response will appear.
End the session:
****** (star symbols)**

End of Procedure

Replacing the NT5K21 equipment card

See the *Software Input/Output: Maintenance* (553-3001-511) and the *Software Input/Output: System Messages* (553-3001-411) for a description of all maintenance commands and system messages.

To replace the NT5K21 XMFC/MFE equipment card, follow the steps in Procedure 18.

Procedure 18

Replacing the NT5K21 XMFC/MFE equipment card

- 1 Software disable the card by using the command:
LD 54
DISC c ("c" is the card number)
- 2 Unhook the locking devices on the card; pull it out of the card cage.
- 3 Insert the replacement card into the vacated slot and hook the locking devices.
- 4 When cards are installed, the red LED on the faceplate flashes as a self-test runs. If the self-test completes 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 remains lit.
- 5 Software enable the card by entering:
ENLC c
- 6 When the process is complete, a system response will appear.
End the session:
****** (star symbols)**

End of Procedure

Replacing the NTAG26 equipment card

See the *Software Input/Output: Maintenance* (553-3001-511) and the *Software Input/Output: System Messages* (553-3001-411) for a description of all maintenance commands and system messages.

To replace the NTAG26 XMFR equipment card, follow the steps in Procedure 19.

Procedure 19

Replacing the NTAG26 XMFR equipment card

- 1 Software disable the card by using the command:

LD 34

DISC c ("c" is the card number)

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

- 4 Software enable the card by entering: **ENLC c**
- 5 When the process is complete, a system response will appear.
End the session:
****** (star symbols)**

End of Procedure

Replacing the NTA92 Off-premise protection module

A lightning strike can cause failure of the NTA92. The first indication of such failure is an out-of-service telephone. To check for and replace failed protectors, follow the steps in Procedure 20 or Procedure 21.

Procedure 20

Testing for loop-closure

- 1 Test for dial tone across cable pairs on J1 and J2, using standard loop closure test equipment (for example, butt-in). If a protector has 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 of Procedure

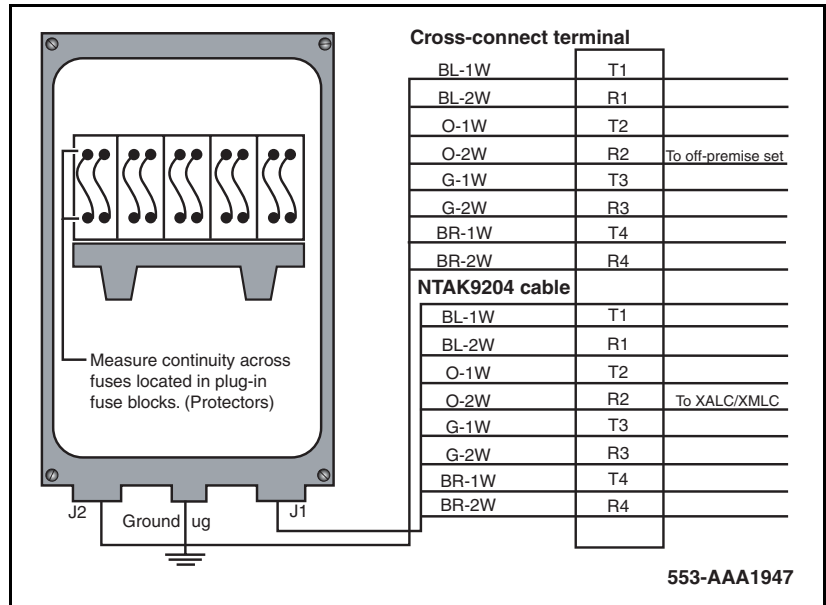
Procedure 21

Testing continuity

- 1 Remove the cover plate from the protection module.
- 2 Using an ohmmeter, measure continuity across the protectors (see Figure 11 on page 125). If a protector has 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 of Procedure

Figure 11
Wiring diagram for NTAK92 Off-premises protection module



Replacing the NTDK20 SSC card

To replace the NTDK20 SSC card, minimum vintage FA, follow the steps in Procedure 22.

Note: The system still supports the NTTK13 card. However, an NTDK20 SSC card will be provided.

Procedure 22 Replacing the NTDK20 SSC card

- 1 Perform an **EDD** backup in **LD 43**.
- 2 Turn the MG 1000S power supply off.
- 3 Hold the NTDK20 SSC circuit card by the lock latches, unlock the latches, and slide the circuit card out of the MG 1000S.
- 4 Remove the Software Daughterboard. Install the Software Daughterboard and the dongle on the replacement NTDK20 SSC card.

Refer to “Replacing the NTTK25 Software Daughterboards” on [page 126](#).

- 5 Transfer any IP daughterboards used to the replacement NTDK20 SSC:
 - NTDK83
 - NTDK99

Refer to “Replacing IP Daughterboards” on [page 129](#).

- 6 Hold the NTDK20 SSC circuit card by the lock latches and slide it into the Call Server or slot 0 of the MG 1000S until it connects with the backplane.
- 7 Secure the lock latches on the circuit card.
- 8 Set the breaker on the MG 1000S power supply to the on position.

End of Procedure

Replacing the NTTK25 Software Daughterboards

This procedure is equivalent to a new system installation. It requires a PC card or an external PC card drive to back up the configuration files, the current keycodes, feature set, License parameters and a Software Delivery Card with the current version of software.

Software Daughterboard compatibility

There are two types of Software Daughterboards:

- NTTK25 - provided with the system
- NTTK13 - still supported

Replacement of a Software Daughterboard

To replace the Software Daughterboard, follow the steps in Procedure 23.

Procedure 23

Replacing the Software Daughterboard

- 1 Log in and back up the configuration files.
- 2 If required, update the Boot Code on the SSC card.
- 3 Power down the system.

- 4 Remove the NTDK20 SSC card from the MG 1000S.
- 5 Lift the daughterboard up, and away from the NTDK20 SSC card until it is clear of the connector assembly.
- 6 Position the replacement Software Daughterboard.
- 7 Seat the Software Daughterboard on the NTDK20 SSC card.
- 8 Reinstall the NTDK20 SSC card in the Call Server or slot 0 of the MG 1000S.
- 9 Power up the system.
- 10 Complete the steps required to perform a “New System Installation”.
- 11 Restore the backup configuration files.

End of Procedure

Unscheduled replacement of a Software Daughterboard

To replace a failed Software Daughterboard, follow the steps in Procedure 24.

Note: Configuration files will only be as current as the last Data Dump (EDD).

Procedure 24**Replacing a failed Software Daughterboard**

- 1 **Decision Point.** If the system is down, go to step 6.
If the system is operating, go to step 2.
- 2 If users back up to a PC, use the XBK command in LD 143.
- 3 Perform a Data dump.
 - Use LD 143.
 - Enter command EDD.
- 4 Disable all DCH using LD 60.
- 5 Disable all AML links using LD 48.

- 6 To change the Software Daughterboard:
 - a. Power down the system.
 - b. Remove the SSC from the MG 1000S.
 - c. Remove the Software Daughterboard from the SSC card and replace with a replacement Software Daughterboard of the same family.
Example: The NTSK11AF, providing the vintage is the same.

OR

If the new card is not the same vintage but the same base board, use a Software Delivery Card to install the software daughterboard.
Proceed to step 7 after system power up.

- 7 If the new software daughterboard is the same vintage as the old one, a Software Delivery Card is not needed for the install. After power up, the card will come up in the main menu. From the Install menu, select item 1 "New System Installation - From Software Daughterboard". Proceed to step 10.
- 8 If an NTKK25 or a programmed daughterboard of a different vintage is being used, insert a Software Delivery card with the same release and issue of software as is being replaced into slot A of the SSC card. The user can then log into the system.
- 9 From the main menu, select item 4 "New System Installation - From Software Delivery Card".
- 10 Proceed with the Installation Menu choices as described in *Communication Server 1000S: Installation and Configuration* (553-3031-210). When prompted for the choice of database, select item 2 "Basic Configuration".

Note: It is important to choose "Basic Configuration", otherwise the system can invoke an EDD after loading the new software which can overwrite the customer data stored on the CPU.

- 11** Once the software is installed and the system is rebooted, the customers' backup configuration files must be restored:
- If you use a PC to restore, use the RBK command in LD 143.
 - Login and load LD 143.
 - Need to perform an upgrade.
 - From the Main Menu, select item 3 "Utilities".
 - Select item 1 "Restore".
 - Select item 1 "Backup Flash Drive".
 - Confirm Restore database from the Backup Flash drive.
 - Reboot system by setting the power supply off, and then on.

End of Procedure

Replacing IP Daughterboards

To replace a NTDK83 or NTDK99 IP Daughterboard, follow the steps in Procedure 25.

Procedure 25

Replacing a NTDK83 or NTDK99 IP daughterboard

- 1** Turn the power supply and reserve power off.
- 2** Unplug the IP cable from the Call Server or MG 1000S bulkhead.
- 3** Unplug and remove the NTDK20 SSC from the system 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 MG 1000S. When necessary use LD 117 to configure the new MAC address for the MG 1000S. See *Communication Server 1000S: Installation and Configuration* (553-3031-210).
- 11** Reinstall the NTDK20 SSC circuit card in the Call Server or in slot 0 of the MG 1000S.
- 12** Reconnect the IP cable to the Call Server or MG 1000S bulkhead.
- 13** Power up the system.

End of Procedure

Element Manager maintenance

Contents

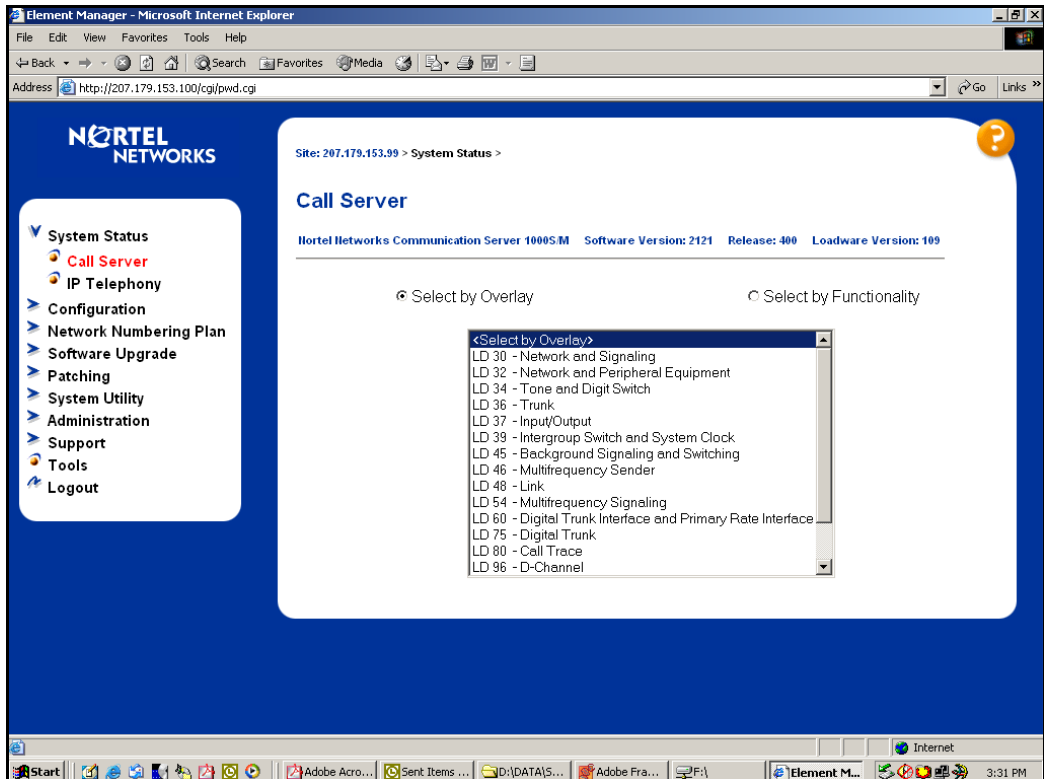
This section contains information on the following topics:

Maintenance functions	132
Signaling Server	136
Media Card	138
Signaling Server software	139
Call Server back up	139
Gatekeeper back up	143
Remote upgrade	144
Overlay 36	146

Maintenance functions

Element Manager enables a certain subset of the overlay functions to be performed for maintenance of the Call Server MG 1000S. Refer to Figure 12 for a sample page.

Figure 12
Call Server maintenance



The following is the list of the maintenance functions which can be performed (and their associated overlay function):

1 LD 36 – trunk Diagnostic

Trunk card and trunk unit diagnostic commands are supported. The following is a list of prompts and responses available through the web interface:

LD 36
DISC <card>
DISI <card>
DISU <tn>
ENLC <card>
LDIC <card> <unit>
RSET <card> <unit>
STAT <card>
STAT <tn>

2 LD 60 – Digital Trunk Interface and Primary Rate Interface Diagnostic

DTI, PRI and clock controller (CC) diagnostic commands are supported. The following is a list of prompts and responses available through the web interface:

DTI/PRI commands
DISL <card>
DSCH <card> <ch>
DISI <card>
ENCH <card> <ch>
ENLL <card>
STAT
STAT <card>
STAT <card> <ch>
CC commands
DIS CC <n>
ENL CC <n>
SSCK <n>

3 LD 43 – Equipment Data dump

The ability to perform a data dump or a data restore from internal database will be supported. The following is the list of prompts and responses available through the web interface:

LD 43
EDD
RIB

4 LD 96 – D-channel diagnostic

The following lists the prompts and responses available through the web interface:

LD 96
DIS DCH <n>
ENL DCH <n>
EST DCH <n>
DIS TMDI <card>
ENL TMDI <card>
RLS CDCH <n>
STAT DCH <n>
STAT TMDI <card>

5 LD 32 – Network and Peripheral Equipment Diagnostic

Most of the card maintenance commands for trunks are covered in LD 36, therefore only one command from LD 32 is required. The following lists the prompts and responses available through the web interface:

LD 32
IDC <card>
DISC <card>
DISI <card>
DISU <tn>
ELNLC <card>
ENLU <tn>
STAT <card>
STAT <tn>
STAT

The command rlogin to the Call Server/H.323 Gateway is supported assuming the administrator has configured a Pseudo TTY on the platform and a rlogin client application exists on the administrator's PC or workstation.

Use *** (star symbols) to rlogin to any SSC directly. The administration workstation must be on the ELAN network and must have a rlogin client application. Otherwise, if the administration is on the TLAN network (or regular customer LAN), a telnet client application must be used to connect to a primary SSC, and the technician must then rlogin to the CS (for example, relay).

The installation, activation and deactivation of patches are also supported through the web.

6 LD 117 – Zone Diagnostics:

PRT ZONE <number>
PRT ZBW <number> (Zone Bandwidth Properties)
PRT ZACB <number> (Zone Access Code Behavior)
PRT ZESA <number> (Zone ESA Properties)
PRT ZTP <number> (Zone Time Properties)
PRT ZDESC <number> (Zone Description)

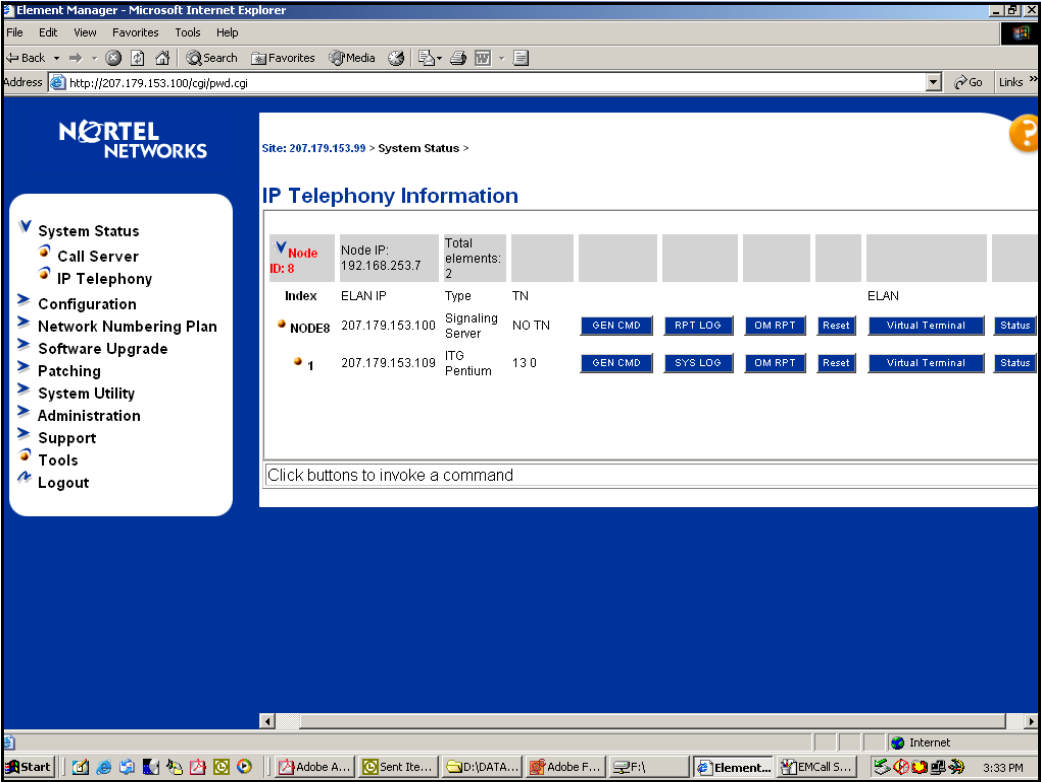
ENL ZONE <number>
DIS ZONE <number>
STAT ZONE <number>

ENL ZBR [ESA LOC TIM]
DIS ZBR [ESA LOC TIM]
STAT ZBR <number>

Signaling Server

Element Manager enables maintenance to be performed on all of the Signaling Servers within the system. Refer to Figure 13 on page 136 for a sample page.

Figure 13
IP Telephony Information



The following is the list of the maintenance functions which can be performed from the web interface:

1 Reset the Signaling Server.

Note 1: The technician is notified that the Gatekeeper application should be disabled first (if it is running), but is still allowed to proceed if they so choose.

Note 2: Since the web server runs on a Signaling Server, the reset function causes the web client to be disconnected from the Signaling Server for five to ten minutes. The configuration of other elements can also stop if the elements are configured through the web server running on the Signaling Server.

2 Enable/Disable Signaling Server.

Note: This is an ungraceful Signaling Server disable.

3 Telnet to Signaling Server (maintenance window).

4 Signaling Server software is delivered by a CD installed in the Signaling Server CD-ROM drive.

5 Configure/Remove the various software components (this should be performed gracefully from the applications point of view).

a Set TPS (On/Off)

b Vtrunk TPS (On/Off)

6 Gatekeeper (On/Off).

7 View log/trace/OM files on web client.

8 Upload log/trace/OM files to client workstation/PC.

9 Help – similar help as to what is provided through OTM for Media Card.

10 Provide a web interface for other CLI commands available for Signaling Server.

Media Card

Element Manager enables the maintenance to be performed on the Media Cards within the system. The following is a list of maintenance functions available through the web interface:

- 1 Reset of the Media Card.
- 2 Enable/Disable Media Card.

Note: The disable command uses LD 32 DISI (disable when idle) command for all channels on the card.
- 3 Telnet to the Media Card (maintenance window).
- 4 Patching (if available on the platform) of the Media Card delivered by a CD in the Signaling Server CD-ROM drive or by a web mechanism (for example, download from management client).
- 5 View individual DSPs:
 - a DSP SW version visible
 - b DSP reset/self-test option.
- 6 Application SW version visible on each card (could be viewed as part of startup card information screen - which should include card processor type).
- 7 View log/trace/OM files on web client.
- 8 Upload log/trace/OM files to client workstation/PC.
- 9 Help – similar help as to what is provided through OTM for DSP parameters.
- 10 Provide web interface for other CLI commands available for Media Cards.

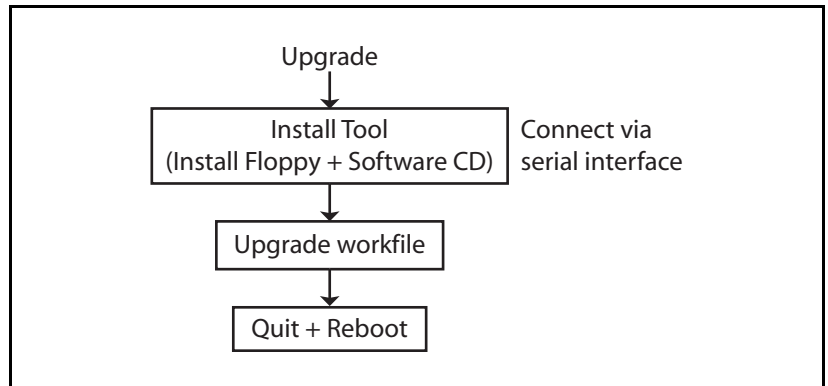
The maintenance of Media Cards running IP Line software are similar to the maintenance provided for Media Cards or Signaling Servers.

The Media Card software can be reinstalled following a procedure similar to a new install (using a PC Card). Every Media Card must be manually upgraded. Remote software upgrade procedures for IP Line are similar for SSC, Media Card and ITGL.

Signaling Server software

Signaling Server software can be upgraded through the Install Tool, following a similar procedure as a new install. The disadvantage of this method is that every SSC must be manually upgraded by a technician: a software media must be present at the element (for example, software CD) and the Install Tool can only be accessed through the serial interface.

Figure 14
Signaling Server upgrade flow with Install Tool



Call Server back up

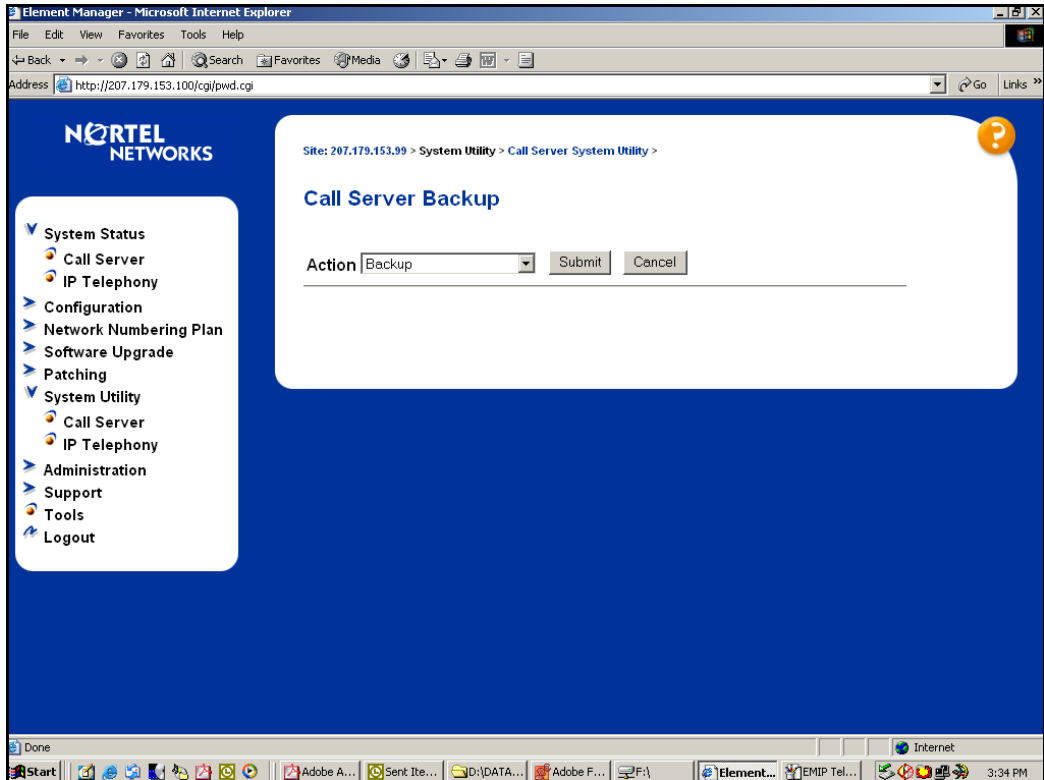
This procedure is to back up the Call Server just like when EDD is entered in LD 43.

To back up the Call Server, follow the steps in Procedure 26.

Procedure 26 **Backing up the Call Server**

- 1 Click on **System Utility** and then **Back Up** in the menu selection.
- 2 Click **Submit**. See Figure 15 on page 140.

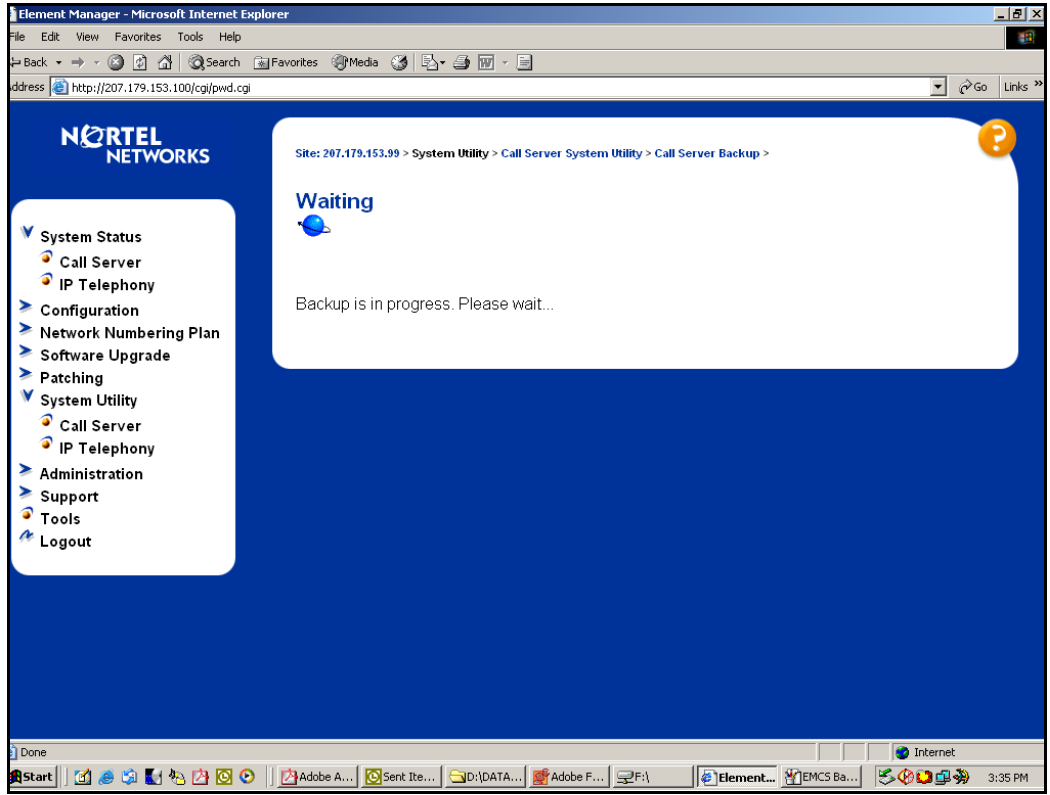
Figure 15
Call Server backup



- 3 When the Call Server is doing the EDD, a screen will appear. See Figure 16 on page 141. The time depends on the size of the Call Server database. This steps takes approximately 90 to 120 seconds.

Note: During this time, all other overlay transactions will be stopped. "Transaction server busy" message could appear on the users' screen.

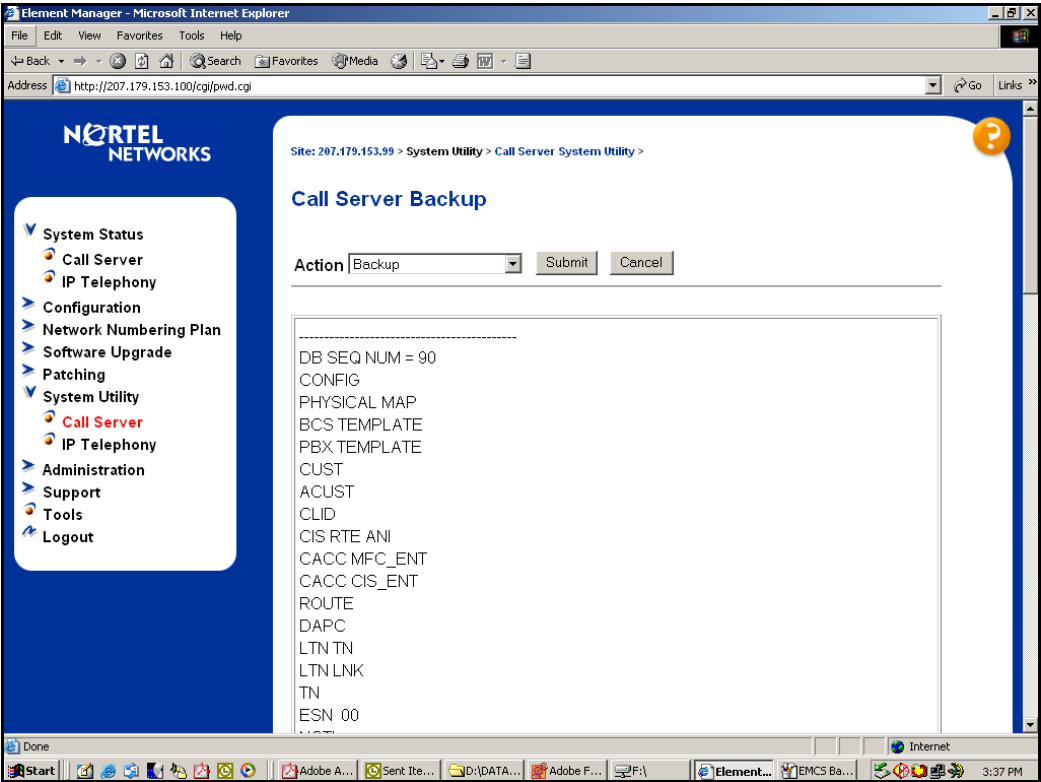
Figure 16
Call Server Back Up screen waiting message



- 4 After the EDD is done, results will appear on the user's screen. See Figure 17 on page 142.

End of Procedure

Figure 17
Call Server Back Up results



Gatekeeper back up

To back up the Gatekeeper to a floppy disk from the web interface, follow the steps in Procedure 27.

Procedure 27

Backing up Gatekeeper from the web interface

- 1 Get a 1.44 Mb floppy disk and label it with the following information:

GATEKEEPER BACKUP

IP ADDRESS: 47.11.249.86

DATE: June 1, 2002

TIME: 10:15 AM

- 2 Make sure the disk is not write protected.
- 3 Insert the labeled floppy disk into the floppy disk drive of the Gatekeeper.
- 4 Log into the Gatekeeper web interface as Administrator.
- 5 From the navigation tree, select "Database Backup/Restore", click on "Database Backup", and then click on "Backup".
- 6 Wait to receive confirmation message.
- 7 Remove the floppy disk from the drive.

End of Procedure

To restore the Gatekeeper from a floppy disk, follow the steps in Procedure 28.

Procedure 28

Restoring the Gatekeeper from a floppy disk

- 1 Get the correct floppy disk according to the label on it.
- 2 Insert the floppy disk in the floppy disk drive of the Gatekeeper.
- 3 Log into the Gatekeeper web interface as Administrator.
- 4 From the navigation tree, select "Database Backup/Restore", click on "Database Restore", and then click on "Restore".
- 5 Click on one of these three options:

- a. Restore both the database and configuration parameters
 - b. Restore only the database
 - c. Restore only the configuration parameters
- 6 Wait to receive a confirmation message.
- 7 Remove the floppy disk from the drive.

End of Procedure

To back up the Gatekeeper automatically to a floppy disk, follow the steps in Procedure 29.

Procedure 29

Backing up the Gatekeeper to a floppy disk

- 1 Get a 1.44 Mb floppy disk and label it with the following information:

**GATEKEEPER
AUTOMATIC BACKUP**

IP ADDRESS: 47.11.249.86

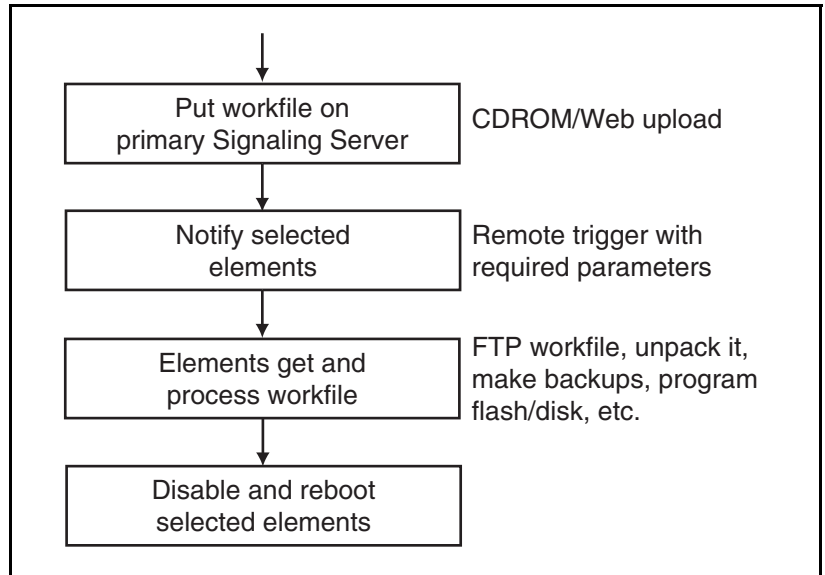
- 2 Make sure the floppy disk is not write protected.
- 3 Insert and leave the labeled floppy disk into the floppy disk drive of the Gatekeeper.
- 4 The Gatekeeper will automatically back up the database and configuration files to the floppy disk on a daily basis at a certain hour at night.

End of Procedure

Remote upgrade

The normal method of upgrading Signaling Servers/Media Cards and Voice Gateway Media Cards is to remotely deliver new software and have the elements upgrade themselves, similarly to the way that an ITGL is upgraded through the OTM.

Figure 18
Element remote upgrade flow



New software is distributed as single, packed and compressed workfiles that are named to uniquely identify their type (SSC or Media Card) and version.

Workfiles are placed in a directory on a node's primary SSC. Workfiles can be delivered directly on a CD-ROM drive on the Signaling Server using CLI or web maintenance menus. Workfiles can also be delivered through the network on a web interface (for example, workfiles come from the web browser workstation).

Workfiles for SSCs and Media Cards can be on the primary SSC, but each node is managed separately. If the primary SSC on which the workfiles were originally placed becomes unavailable, then the workfiles must now be placed on the new primary SSC. The technician is responsible for validating the version of a workfile before initiating a remote upgrade.

The elements are notified individually to download and process a new workfile. To limit service interruption, an element must be disabled before it is upgraded. Software upgrades are typically timed to minimize the impact.

The web user interface allows the selection of multiple elements to disable and upgrade. However, the CLI will only allow the selection of one element at a time. Note that the primary SSC should be upgraded separately from the other elements since the upgrade procedure includes a disable and a reboot. A reboot interrupts web service and may interrupt other elements' upgrades.

The element upgrade “trigger” mechanism delivers appropriate parameters to the elements to perform the upgrade, including:

- software server address
- login and password
- workfile path and filename.

With this generic approach, the software server (primary SSC) can be accessible through its ELAN or TLAN interface, depending on the IP address specified. The path to a workfile is also not fixed.

The trigger function returns as soon as an element is notified. Pacing of the downloads (to minimize network and server resource impact) is accomplished by notifying the elements serially: the next element is not notified until the current element has completed its workfile download.

The element retrieves and processes the workfile when triggered. Processing can include, for example:

- Unpacking the workfile.
- Making a backup copy of the original software.
- Programming flash memory.
- Copying disk files.

The technician must refresh the software management web pages to view the elements status, including the software version. The selected elements must be rebooted to use the new software when the upgrade process is complete.

Overlay 36

The STAT command in LD 36 provides status for all analog trunk cards within the system. Prior to printing a list of units, the card number is printed.

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)

CARD 2

UNIT 00 = DSBL (TRK)(TIE LDR IMM/IMM)

UNIT 01 = UNEQ

UNIT 02 = UNEQ

UNIT 03 = UNEQ

UNIT 04 = UNEQ

UNIT 05 = UNEQ

UNIT 06 = UNEQ

UNIT 07 = UNEQ

Media Card maintenance

Contents

This section contains information on the following topics:

Introduction	149
Faceplate maintenance display codes	150
Replacing a Media Card	157
Verify Media Card software and firmware	157
IP line and IP Phone maintenance and diagnostics	157
IP line shell commands	159
Warm rebooting the Media Card.	159
Tests for the Media Card DSPs	160
Invoking alarm and log files	160

Introduction

This chapter provides information on the maintenance functions of the Media Card. Where reference is made to Optivity Telephone Management (OTM), the latest version, OTM 2.0 (or later), is assumed.

Note: Check the CS 1000S ESD web site for information on the latest software, firmware and application releases. Refer to *IP Line: Description, Installation, and Operation* (553-3001-365) 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 *IP Line: Description, Installation, and Operation* (553-3001-365).

If the maintenance display shows a persistent T:20, indicating a software failure, and if 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 co-processor test failed, F:05 is displayed on the Media Card faceplate. If more that one test fails, the message indicates the first failure.

Table 32
Media Card faceplate maintenance display codes (Part 1 of 3)

Normal code	Fault code	Message
T:00	F:00	Initialization
T:01	F:01	Testing Internal RAM

Table 32
Media Card faceplate maintenance display codes (Part 2 of 3)

Normal code	Fault code	Message
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 co-processor
T:06	F:06	Testing timers
T:07	F:07	Testing external RAM
T:08	F:08	Testing dongle
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
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 start-up message from Host processor

Table 32
Media Card faceplate maintenance display codes (Part 3 of 3)

Normal code	Fault code	Message
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 33 shows the list of error codes:

Table 33
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	PCMCIA device failure
H:08	Network interface failure
H:10	CS 1000S interface failure
H:20	DSP interface failure
H:40	NVRAM/EEPROM interface failure
H:80	PCM connector failure

ITG System error messages

When an error or specific event occurs, SNMP sends an alarm trap to OTM or 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 error log in OTM IP Line 3.0 application by clicking the **Open Log File** button on the **Maintenance** tab of the **ITG Card Properties**. You can also 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 34 lists the critical ITG messages and Table 35 on page 156 lists the critical ITS messages.

For a complete listing of other error messages, see *Software Input/Output: System Messages* (553-3001-411).

Table 34
Critical ITG Error messages (Part 1 of 3)

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.

Table 34
Critical ITG Error messages (Part 2 of 3)

Maintenance Display	Corresponding Critical Error Message	Description
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>.
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>.

Table 34
Critical ITG Error messages (Part 3 of 3)

Maintenance Display	Corresponding Critical Error Message	Description
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 Unkown.

Table 35
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 or the card is removed for other reasons:

- After a reboot, if the Media Card displays a code of the form F:xx on the faceplate LED display, this indicates an unrecoverable hardware failure and the card cannot register with the CS 1000S. The exception is the F:10 code, which can indicate that the Security Device is missing from the card.
- If the management Ethernet interface or the voice Ethernet interface on the Media Card fails. The failure can be indicated by not showing a link pulse on the voice IP interface status LED, or on the hub, or if the maintenance port continuously prints “InIsa0 Carrier Failure” messages, after proving that the hub port and TLAN cable are good.
- If 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, refer to *IP Line: Description, Installation, and Operation* (553-3001-365).

Verify Media Card software and firmware

To verify the Media Card software and firmware, refer to *IP Line: Description, Installation, and Operation* (553-3001-365).

IP line and IP Phone maintenance and diagnostics

For Nortel IP Phones, there are two kinds of 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, that are seen as trunk units, are managed using existing LD 32 commands. These commands due not apply to virtual TNs. Use Element Manager for virtual TN maintenance.

LD 32 supports STAT, DISU, ENLU, and IDU commands on an IP Phone virtual TN. All other commands lead to the 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 CS 1000S must request the information from the IP Phone, the IDU is effectively a "ping" command and 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 1000S, 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.

Additional information on the output format of the IDU command in LD 32 and the maintenance commands in LD 32 for the IP Phone, refer to *IP Line: Description, Installation, and Operation* (553-3001-365).

Lamp Audit and Keep Alive

The Lamp Audit function provides a continuous source of heartbeat messages to ensure the IP Phone is powered and the IP connection is active. Since there

is a reliable UDP connection from the Call Server through to the IP Phones, any failure in the IP Phones, the IP Line card, or the IP connections is detected. In addition to Lamp Audit, Network Signaling Diagnostics can be run as part of the midnight routines:

- When the IP Line card detects the set is disconnected, the IP Line card logs the event and sends an unregistered message to the Call Server for that set.
- When the Call Server detects a loss of connection with the IP Line card, it logs a message and unregisters all of the sets and gateway channels associated with that IP Line card.

IP line shell commands

The IP Line shell commands are designed to supplement overlay commands, and to introduce new 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. Alternatively, the OTM ITG “Telnet” command can be used to access the IP Line shell.

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 refer to *IP Line: Description, Installation, and Operation* (553-3001-365).

Warm rebooting the Media Card

The following IP Line shell command performs a warm reboot of an out-of-service Media Card: **cardReset**

Tests for the Media Card DSPs

At the IP Line shell, the following two tests can be performed on the DSPs:

- To run a self-test on the DSP daughterboard: **DSPselfTest**.
Note: If the DSP self-test fails, the Media Card must be replaced.
- To run a PCM loopback test, a Send loopback test, or a Receive loopback test on the DSP daughterboard, respectively:
 - **DSPPCmLpbkTestOn** (“DSPPCmLpbkTestOff” to stop the test)
 - **DSPSndLpbkTestOn** (“DSPSndLpbkTestOff” to stop the test)
 - **DSPRcvLpbkTestOn** (“DSPRcvLpbkTestOff” to stop the test)

Note: The DSPs and all associated ports must be disabled before performing these tests.

Invoking alarm and log files

Alarm and log file output is turned on via the IP Line shell. The following commands may be performed 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**

Simple Network Management Protocol

Contents

This section contains information on the following topics:

Introduction	162
MIBs	162
SNMP Overview	163
Configuration	164
Supported MIBs	166
MIB security	167
Configuration of system group MIB parameters.	167
Print commands	171
Config.ini file	171
Traffic MIB	171
Community name strings	172
Test Alarm utility	174
EDT and EPT	176
Backup and restore	177
LD 43	177
LD 143	178

Introduction

MIBs

In typical IP network devices, the operator requires a large amount of management information to properly run the device. This information is kept on the system and can be made available to network management systems through Simple Network Management Protocol (SNMP). The information itself is kept on the device (conceptually) in a database, referred to as a Management Information Base (MIB). The network management system can query the MIB through SNMP query commands (called **gets**), and in some cases can write into the MIB through SNMP **set** commands.

For the Network Management System (NMS) to communicate with the agent on a managed device, the NMS must have a description of all manageable objects the agent knows about. Therefore, each type of agent has an associated document, called a MIB Module, which contains these descriptions. MIB Module files are loaded into the NMS. MIB Modules are frequently referred to as “MIBs”. The primary purpose of the MIB module is to provide a name, structure and a description for each of the manageable objects a particular agent knows about.

The NMS uses two kinds of MIB modules:

- a generic MIB Module that describes the structure of the data that can be retrieved by the NMS
- a trap MIB Module that describes the structure of the data sent by the device agent as an SNMP trap

MIB data is arranged in a tree structure. Each object (each item of data) on the tree has an identifier, called an Object ID (OID), which uniquely identifies the variable. To prevent naming conflicts and provide organization, all major device vendors, as well as certain organizations, are assigned a branch of this tree structure (referred to as the “MIB Tree”). The MIB Tree is managed by the Internet Assigned Numbers Authority (IANA). Each object on the MIB Tree has a number and a name, and the complete path from the top of the tree down to the point of interest forms the name.

An SNMP MIB must be written in Abstract Notation One (ASN.1) format to conform with the SNMP standards.

SNMP Overview

CS 1000 Release 4.5 software introduces the following Simple Network Management Protocol (SNMP) features:

- Support of standard MIBs on the Call Server. See “Supported MIBs” on [page 166](#).
- Support of the Entity MIB on the Call Server. See “Supported MIBs” on [page 166](#).
- Configurable system group MIB values for the Call Server and synchronization of those values to the Signaling Servers and Media Cards when a data dump is performed. See “Configuration of system group MIB parameters” on [page 167](#).
- Accessibility of Quality of Service (QoS) data through an SNMP MIB. See “Traffic MIB” on [page 171](#).
- Configurable community name strings on the Call Server which are synchronized to the Signaling Servers and Media Cards when a data dump is performed. See “Community name strings” on [page 172](#).
- An alarm test utility, providing the ability to manually send out a test SNMP trap from the Call Server to confirm the SNMP configuration is correct. See “Test Alarm utility” on [page 174](#).
- The ability to import/export the EPT from the Call Server to removable media, and from the removable media back to the Call Server. See “EDT and EPT” on [page 176](#).

CS 1000 Release 4.5 also provides enhancements to the following SNMP features:

- An increase in the number of entries allowed in the Event Preference Table (EPT) from 200 to 500. See “EDT and EPT” on [page 176](#).
- The ability to reload the EPT from disk using an overlay command. See “EDT and EPT” on [page 176](#).

- New LD 117 commands to print the Event Default Table (EDT) or EPT entries, based on the severity of the system message. See “EDT and EPT” on [page 176](#).
- Removal of community name strings from the config.ini file. See “Config.ini file” on [page 171](#).
- Modifications to LD 143 and LD 43 for the backup/restore of the Call Server’s SNMP configuration files. See “Backup and restore” on [page 177](#).

Configuration

Different tools, such as the Command Line Interface (CLI), Element Manager, and Optivity Telephony Manager (OTM) are used to configure SNMP elements for a system, depending on the system platform (CS 1000E, CS 1000S, CS 1000M, or Meridian 1) and the network device. See Table 36.

Table 36
SNMP elements and where they are configured (Part 1 of 2)

SNMP configuration of.....	CLI	Element Manager	OTM
Call Server			
Community name strings (Note 1)	Yes	Yes	Yes
Trap destinations	Yes	No	No
sysgroup MIB info	Yes	Yes	Yes
EDT/EPT edits	Yes	No	Yes
Signaling Server			
Community name strings	See Note 1.	See Note 1.	See Note 1.
Trap destinations	No	Yes	No

Table 36
SNMP elements and where they are configured (Part 2 of 2)

SNMP configuration of.....	CLI	Element Manager	OTM
sysgroup MIB info	No	Yes	No
Media Cards			
Community name strings	See Note 1.	See Note 1.	See Note 1.
Trap destinations	No	Yes	See Note 2.
sysgroup MIB info	No	Yes	See Note 2. See Note 3.
<p>Note 1: Propagated to the Signaling Server and Media Cards on EDD.</p> <p>Note 2: On a Meridian 1 (no Signaling Server), OTM is used to provision the Media Cards and other ITG devices.</p> <p>Note 3: For the Meridian 1 (no Signaling Server), OTM can use the same values as for the Call Server.</p>			

Supported MIBs

Table 37 lists the standard and enterprise-specific MIBs supported in CS 1000 Release 4.5 for each device.

Table 37
 Supported MIBs (Part 1 of 2)

Component	Standard MIB	Enterprise-specific MIB
Call Server	<ul style="list-style-type: none"> System group (RFC 1213) Interface group (RFC 2863) IP group (RFC 2011) UDP group (RFC 2013) TCP group (RFC 2012) ICMP group (RFC 2011) SNMP group (RFC 3418) Entity group (RFC 2737) (only the following two sub-groups) <ul style="list-style-type: none"> Physical General 	<ul style="list-style-type: none"> Trap group – Rel 4_0 Call Server trap.mib

Table 37
Supported MIBs (Part 2 of 2)

Component	Standard MIB	Enterprise-specific MIB
Signaling Server	<ul style="list-style-type: none"> • System group (RFC 1213) • Interface group (RFC 2863) • IP group (RFC 2011) • UDP group (RFC 2013) • TCP group (RFC 2012) • ICMP group (RFC 2011) • SNMP group (RFC 3418) 	<ul style="list-style-type: none"> • Trap group – Rel 4_0 Sig Server trap.mib • Zonetrafficrpt group – zonetrafficrpt.mib
Media Card	<ul style="list-style-type: none"> • System group (RFC 1213) • Interface group (RFC 2863) • IP group (RFC 2011) • UDP group (RFC 2013) • TCP group (RFC 2012) • ICMP group (RFC 2011) • SNMP group (RFC 3418) 	<ul style="list-style-type: none"> • Trap group – Rel 4_0 IP Line trap.mib

MIB security

For security purposes, read and write community name strings are used to control access to all MIB data.

Configuration of system group MIB parameters

Commands have been added to LD 117 to modify the parameters for MIB groups. This includes the parameters needed for the system group MIB (1.3.6.1.2.1.1). The system group provides the basic information about the identity of the system such as system name, system location, and system contact. By default, a set of variables are defined for the system group MIB,

but they are also configurable in LD 117 using the commands listed in Table 38.

Both the standard MIB read-only community name string and the enterprise-specific MIB community name strings (public, admingroup2, and admingroup3) are defined by default. However, they can also be configured in LD 117.

The system group MIB parameters and the community name strings are configured on the Call Server and synchronized to the Signaling Server and the Media Cards when a data dump is performed. As well, they are synchronized when a link is established between a Signaling Server or Media Card and the Call Server.

Table 38
LD 117 - Configure system group MIB parameters (Part 1 of 3)

=> Command	Description
CHG NAV_SITE aa... a	<div>Change the navigation site name (for example, MyCity) where:</div> <ul style="list-style-type: none">aa...a = a string with maximum length of 32 charactersdefault = Navigation Site Name <div>Note: Use a single X to clear the field.</div>
CHG NAV_SYSTEM aa... a	<div>Change the navigation site name (for example, Station Switch) where:</div> <ul style="list-style-type: none">aa...a = a string with a maximum length of 32 charactersdefault = Navigation Site Name <div>Note: Use a single X to clear the field.</div>

Table 38
LD 117 - Configure system group MIB parameters (Part 2 of 3)

=> Command	Description
CHG SNMP_SYSCONTACT aa... a	<p>Change the contact person name for this machine where:</p> <ul style="list-style-type: none"> aa...a = a string with a maximum length of 100 characters default = System Contact <p>Use a single X to clear the field.</p>
CHG SNMP_SYSLOC aa...a	<p>Change the defined physical location for this machine where:</p> <ul style="list-style-type: none"> aa...a = a string with a maximum length of 100 characters default = System Location <p>Use a single X to clear the field.</p>
CHG SNMP_SYSNAME aa...a	<p>Change the name assigned to this machine where:</p> <ul style="list-style-type: none"> aa...a = a string with a maximum length of 100 characters <p>Default = Navigation Site Name: Navigation System Name : Hostname</p> <p>Use a single X to clear the field.</p>
CHG SNMP_SYSNAME NAV	<p>Revert the name assigned to this machine to the default name. The default name is comprised of the currently configured <NAV_SITE> : <NAV_SYSTEM> : <HOSTNAME>.</p>

Table 38
LD 117 - Configure system group MIB parameters (Part 3 of 3)

=> Command	Description
CHG ADMIN_COMM n aa...a	<p>Change the admin groups community name string, where:</p> <ul style="list-style-type: none"> • n = a number from 1 to 32 • aa...a = a string with a maximum length of 32 characters <p>Default(1) = public</p> <p>Default(2) = admingroup2</p> <p>Default(3) = admingroup3</p> <p>These communities are used for accessing different SNMP objects on the Call Server, Signaling Servers, and Media Cards.</p>
CHG SYSMGMT_RD_COMM aa...a	<p>Change the system management read-only community name string where:</p> <p>aa...a = a string with a maximum length of 32 characters</p>
CHG SYSMGMT_WR_COMM aa...a	<p>Change the system management read/write community name string where:</p> <p>aa...a = a string with a maximum length of 32 characters</p>

IMPORTANT!

Changes made to the NAV_SITE, NAV_SYSTEM, and HOSTNAME are not automatically propagated to the SNMP_SYSNAME. The CHG SNMP_SYSNAME NAV command **must** be used.

Note: The data dump (EDD) command saves the configurable system group MIB parameters and community name strings to a file called syscfg.db, which is saved at c:/u/db (Small Systems) or /u/db (Large Systems).

Print commands

Printing the system group MIB parameters and community name strings is done through LD 117. See Table 39.

Table 39

LD 117 - Print system group MIB parameters and community name strings

=> Command	Description
PRT NAV_SITE	Print the navigation site name.
PRT NAV_SYSTEM	Print the navigation system name.
PRT SNMP_SYSGRP	Print all parameters of the MIB system group.
PRT ADMIN_COMM	Print the administration group read-only community name strings.
PRT SYSMGMT_COMM	Print the system management community name strings

Config.ini file

Since the community name strings are synchronized when a link is established between a Signaling Server/Media Card and the Call Server, the IP Telephony devices no longer read the config.ini file to retrieve the community strings. Therefore the community name strings have been removed from the config.ini file.

Traffic MIB

The Zonetrafficrpt MIB on the Signaling Server handles traffic report parameters generated on the Call Server. The SNMP manager sends an SNMP query to the Signaling Server to retrieve the Zonetrafficrpt

parameters. The Signaling Server communicates with the Call Server to retrieve the information from the traffic report and respond to the SNMP query. The SNMP agent on the Signaling Server incorporates the Zonetrafficrpt MIB and handles SNMP queries to the Zonetrafficrpt MIB. The Zonetrafficrpt parameter values from the Call Server are transferred to the Signaling Server. On the Call Server, the Zonetrafficrpt parameters are accessed through LD 2 and LD 117.

The Zonetrafficrpt MIB consists of traffic parameters for a zone provisioned on the Call Server. The two sets of parameters are intra-zone parameters and inter-zone parameters. Each parameter is assigned an object ID in the MIB. For further information about the Zonetrafficrpt traffic parameters that are available, refer to *Simple Network Management Protocol: Description and Maintenance* (553-3001-519).

Community name strings

Read-only and read/write community name strings control access to all MIB data. A community name string is defined by default to access standard MIBs. A set of administrator community name strings is supported with read-only privileges, with the default strings of “public”, “admingroup2”, and “admingroup3”. The first and third community name strings provide access to system group MIB variables, while the second community name string provides access to all MIBs.

New commands are created in LD 117 to configure MIB community name strings for read-only access to Call Server MIBs (system group MIB objects) and for read/write access to Signaling Server/Media Card MIBs. Table 40 on [page 173](#) lists the Call Server community name strings. Table 41 on [page 174](#) lists the Signaling Server/Media Card community name strings.

Table 40
Call Server community name strings

Community Name (User group)	Access privileges	Interface	View	Where configured
ADMIN_COMM(1) (public)	read	ELAN network	system group MIB	LD 117
ADMIN_COMM(2) (admingroup2)	read	ELAN network	All MIBs	LD 117
ADMIN_COMM(3) (admingroup3)	read	ELAN network	system group MIB	LD 117
SYSMGMT_RD_COMM (otm123)	read	ELAN network	All MIBs	LD 117
SYSMGMT_WR_COMM (otm321)	read/write	ELAN network	CorpDir MIB	LD 117

Table 41
Signaling Server/Media Cards community name strings

Community Name (User group)	Access privileges	Interface	View	Where configured
ADMIN_COMM(1) (public)	read	ELAN network	system group MIB	LD 117
ADMIN_COMM(2) (admingroup2)	read	ELAN network	All MIBs	LD 117
ADMIN_COMM(3) (admingroup3)	read	ELAN network	Zonetrafficrpt MIB (Signaling Server only) system group MIB (Media Cards only)	LD 117

The community name strings used by the Signaling Server and Media Cards are synchronized from the Call Server to the Signaling Server and Media Cards when a data dump is performed. As well, they are synchronized when a link is established between a Signaling Server or Media Card and the Call Server.

Test Alarm utility

A diagnostic utility has been added to the Call Server to be used for alarm testing by entering a command in LD 117. The Test Alarm utility simulates an alarm to verify that the alarms are generated correctly and sent to their configured destinations. The alarm is sent to the trap destination list configured on the system, using LD 117 and the Open Alarm feature.

The TEST ALARM command creates and sends an open_alarm (trap type 10) to the trap destination list and displays a message on the console. The alarm test utility sends a trap for any parameter specified.

The flow of the message travels through the following:

- Event Default Table (EDT) to assign correct severity if system message is valid; otherwise, system message is assigned a severity of **Info**
- Event Preference table (EPT) to modify severity or suppress system message based on threshold

If the Test Alarm utility uses a valid system message and correctly sends a trap to the trap destination, the same system message, if it occurs on the system, is not guaranteed to be sent as a trap. Some system messages currently do not generate a trap. The LD 117 TEST ALARM command is described in Table 42.

Table 42
LD 117 - Test alarm command

=> Command	Description
TEST ALARM aaaa nnnn	<p>Generate an alarm where:</p> <p>aaaa = any character sequence. However, to test how an existing system message category (for example, BUG, ERR, INI) would appear in an alarm browser, use an existing system message.</p> <p>nnnnn = any numeric sequence (for example, 3458) and is optional, defaulting to 0000</p> <p>The actual output on the TTY is the system message passed as the parameter; for example:</p> <p>BUG1234</p> <p>The actual trap sent to the trap destination list is trap type 10 with the following details:</p> <p>operator description = 'This is a test'</p> <p>operator data = 'This is a test'</p> <p>error code = aaaannnn</p> <p>The rest of the binding variables are NULL.</p>

EDT and EPT

The Event Default Table (EDT) and Event Preference Table (EPT) are repositories on the Call Server for storing system event information.

The EDT contains a list of system events that are generated on the system. Each event contains an event code, a description, and severity information. The EPT is used to override the severity of an event assigned in the EDT. The EPT can also be used to set escalation thresholds and suppression thresholds for certain event severities.

The number of entries allowed in the EPT has been increased from 200 to 500.

Additional commands are added to LD 117 to import and export an EPT file from/to removable media, to load an updated EPT file into memory, and to print the entries in the EDT and EPT. See Table 43.

Table 43
LD 117 - EDT and EPT commands

=> Command	Description
EXPORT EPT	The EPT file stored on the hard disk (/u/db/ smpserv.db) is copied to the floppy / PC Card drive (a:/smpserv.db).
IMPORT EPT	The EPT file stored on the floppy / PC Card (a:/smpserv.db) drive is copied to the hard drive (/u/db/smpserv.db).
RELOAD EPT	The new/modified EPT file is loaded into memory from disk (/u/db/smpserv.db).
PRTS EPT severity <eventID> <eventID>	The entries in the EPT can be listed based on the severity field for all entries or the specified range of entries.
PRTS EDT severity <eventID> <eventID>	The entries in the EDT can be listed based on the severity field for all entries or the specified range of entries.

Error messages are issued if the import or export of the EPT file was not successful.

Backup and restore

LD 43

The LD 43 commands listed in Table 44 have been modified to enable a backup and restore of the Call Server system group MIB variables, System Navigation variables, and community name strings.

Table 44
LD 43 - Backup and restore commands

Command	Description
EDD	The Call Server system group MIB variables, System Navigation variables, and community name strings are dumped to disk as a file when this command is executed. As well, this file is backed up to the A: drive floppy (Large Systems) or to the internal Z: drive (Small Systems).
BKO	The new file created to store the system group MIB variables, System Navigation variables, and community name strings is copied from the primary device to the backup (external storage) device.
RES	The new file created to store the system group MIB variables, System Navigation variables, and community name strings is restored from the backup (external storage) device to the primary device.
RIB (Small Systems only)	The new file created to store the system group MIB variables, System Navigation variables, and community name strings is restored from the internal backup device to the primary device.

LD 143

Small systems

The commands listed in Table 45 are part of the LD 143 Small System Upgrade Utilities menu. Select Option 2 to archive (backup) the system group MIB variables, System Navigation variables, and community name strings file to a PC Card.

Table 45
Small System backup and restore commands using a PC Card

Menu choices	Description
2. Archive Customer-defined databases.	The new file created to store the system group MIB variables, System Navigation variables, and community name strings is archived on the PC Card.
3. Install Archived database.	The new file created to store the system group MIB variables, System Navigation variables, and community name strings is installed from an archive on the PC Card.

More information

For more detailed information on SNMP, refer to *Simple Network Management Protocol: Description and Maintenance* (553-3001-519).

Proactive Voice quality Management

Contents

This section contains information on the following topics:

Introduction	180
How voice quality monitoring works	181
Feature packaging	183
Feature implementation.	183
Task summary list.	183
LD 117 - Configure voice-quality metric thresholds	184
LD 117 - Print voice-quality metric thresholds	186
LD 117 - Configure voice-quality sampling (polling)	186
LD 117 - Configure zone alarm-notification levels	187
LD 117 - Print zone alarm-notification levels	192
New voice-quality alarms	192
Diagnosing and isolating voice-quality problems.	193
SNMP interface.	194
Heterogeneous environments	194

Introduction

Proactive Voice quality Management (PVQM) includes the following enhancements for CS 1000 Release 4.5:

- Monitoring of voice-quality metrics (for example, latency, jitter, packet loss, and R-Value) for the IP Phone and voice MG 1000S endpoints.
- Threshold configuration (for example, Warning and Unacceptable) of voice-quality metrics in Overlay 117. Thresholds are used to classify system performance as good, poor, and unacceptable.
- SNMP alarm generation when voice-quality metric thresholds are violated on a per-call or bandwidth zone basis.
- Voice quality related SNMP alarm control, on a zone basis, by configuring Alarm Notification Levels in Overlay 117. Alarm control assists in isolating voice-quality problems and reducing network traffic.
- Recording of voice-quality metric threshold violations in Traffic Report 16. Traffic Report 16 is now accessible in Overlay 2 and SNMP MIB.
- Retrieval of Operational Measurement (OM) reports containing hourly summations of the voice-quality metrics and endpoint registration activity. R-Value information is now available in OM reports.
- Network diagnostic utilities to identify, isolate, and report network problems affecting voice quality. The diagnostic utilities are available by using the CLI or IP Phones with Phase 2 software. The utilities include Traceroute, Ping, Ethernet statistics, IP Network statistics, UNISim/Reliable User Data Protocol (RUDP) statistics, Real-Time Control Protocol (RTCP) statistics, and Dynamic Host Control Protocol (DHCP) data.

These enhancements assist network administrators and craft persons to:

- Make informed decisions for capacity planning and Quality of Service (QoS) network engineering.
- Monitor the performance of their systems.
- Diagnose, isolate, and correct networking problems that cause deterioration in voice quality.

How voice quality monitoring works

The PVQM feature monitors voice quality by polling IP endpoints during a call, and at the end of a call, to sample the following voice-quality metrics:

- **Latency** - the length of time needed for information to travel through the network, value expressed in seconds
- **Jitter** - the variability in latency, value expressed in seconds
- **Packet Loss** - the number of packets lost during transmission, value expressed in percentage
- **R-Value** - measurement of audio quality using ITU E-Model

The sampled metrics are compared to user-configured thresholds in order to determine system performance. When sampled metrics exceed configured thresholds, statistics are generated on the system.

Note: For details on configuring metric thresholds, refer to “LD 117 - Configure voice-quality metric thresholds” on [page 184](#).

Statistics for each metric are collected on the Signaling Server or Voice Gateway Media Card to create a Quality Detail Report (QDR). The QDR summarizes metric threshold violations into one of the following categories:

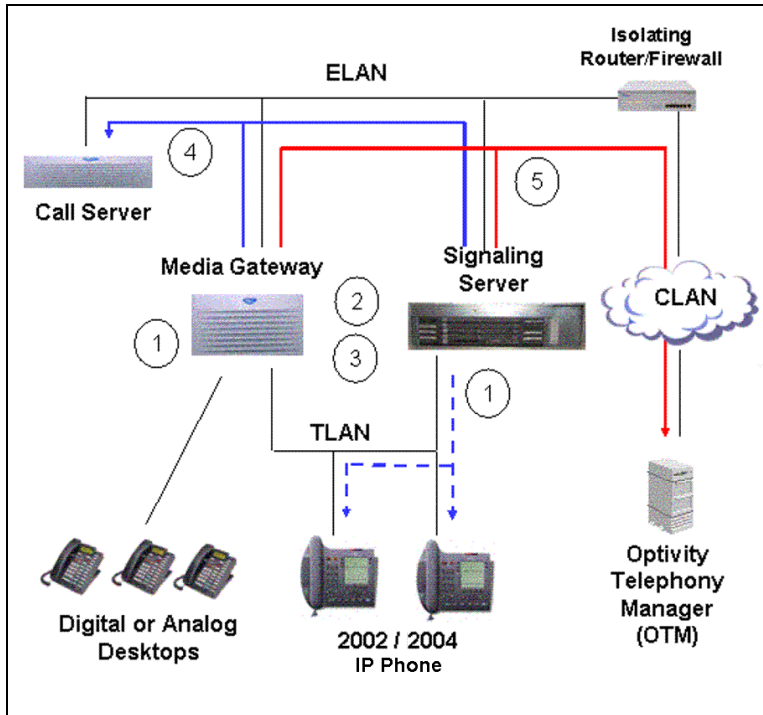
- Warning
- Unacceptable

Each summarized QDR record is added to the IP Phone Zone Traffic Report 16. The enhanced traffic report summarizes the voice quality over the reporting period on a zone-by-zone basis to allow the administrator to view the overall voice quality.

An SNMP alarm is generated when a voice-quality metric threshold exceeds Warning or Unacceptable status. For details on controlling the number of SNMP alarms generated, refer to “LD 117 - Configure zone alarm-notification levels” on [page 187](#).

Figure 19 on [page 182](#) illustrates PVQM within the Voice over IP (VoIP) system.

Figure 19
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 voice-quality metric exceeds the Warning or Unacceptable threshold.

Feature packaging

Monitoring of all other voice-quality metrics is available with base CS 1000 Release 4.5 software. To enable monitoring of the R-Value audio quality metric, the Proactive Voice quality Management (PVQM) package 401 is required.

Supported system types

PVQM is supported by CS 1000 Release 4.5 and Meridian 1 systems equipped with Voice Gateway Media Cards running IP Line 4.0.

Feature implementation

The system implements this feature during an installation or upgrade to the PVQM_401 software package, available from Feature Service Level 2 - Enhanced Business Services.

Task summary list

The following is a summary of the tasks in this section:

- 1** LD 117 - Configure voice-quality metric thresholds.
- 2** LD 117 - Print voice-quality metric thresholds.
- 3** LD 117 - Configure voice-quality sampling (polling).
- 4** LD 117 - Configure zone alarm-notification levels.
- 5** LD 117 - Print zone alarm-notification levels.

LD 117 - Configure voice-quality metric thresholds

New commands have been added to LD 117 to configure voice-quality metric thresholds on a per-call or zone basis. See Table 46.

To configure voice-quality metric thresholds using Element Manager, select:
Configuration > IP Telephony > Quality of Service

Table 46

LD 117 - Configure voice-quality metric thresholds (Part 1 of 2)

=> Command	Description
CHG CQWTH <WarnJitter> <WarnLatency> <WarnPacketLoss> <WarnRFactor>	<p>Change voice-quality Warning thresholds on a per-call basis</p> <p>Where:</p> <p><WarnJitter> = 5-(20)-200 msec <WarnLatency> = 5-(20)-200 msec <WarnPacketLoss> = 0-(1)-10% <WarnRFactor> = 1-(3)-5</p> <p>Note: Changes to threshold values are not propagated to the Signaling Server or the Voice Gateway Media card until a data dump is performed.</p>
CHG CQUTH <UnacpJitter> <UnacpLatency> <UnacpPacketLoss> <UnacpRFactor>	<p>Change voice-quality Unacceptable thresholds on a per-call basis</p> <p>Where:</p> <p><UnacpJitter> = 5-(40)-500 msec <UnacpLatency> = 5-(40)-500 msec <UnacpPacketLoss> = 0-(3)-25% <UnacpRFactor> = 1-(3)-5</p> <p>Note: Changes to threshold values are not propagated to the Signaling Server or the Voice Gateway Media card until a data dump is performed.</p>

Table 46
LD 117 - Configure voice-quality metric thresholds (Part 2 of 2)

=> Command	Description
CHG ZQWTH <WarnJitter> <WarnLatency> <WarnPacketLoss> <WarnRFactor>	<p>Change voice-quality Warning thresholds on a zone basis</p> <p>Where:</p> <p><WarnJitter> = 0-(20)-100%</p> <p><WarnLatency> = 0-(20)-100%</p> <p><WarnPacketLoss> = 0-(20)-100%</p> <p><WarnRFactor> = 0-(20)-100%</p> <p>Note: Changes to threshold values are not propagated to the Signaling Server or the Voice Gateway Media card until a data dump is performed.</p>
CHG ZQUTH <UnacpJitter> <UnacpLatency> <UnacpPacketLoss> <UnacpRFactor>	<p>Change voice-quality Unacceptable thresholds on a zone basis</p> <p>Where:</p> <p><UnacpJitter> = 0-(2)-100%</p> <p><UnacpLatency> = 0-(2)-100%</p> <p><UnacpPacketLoss> = 0-(2)-100%</p> <p><UnacpRFactor> = 0-(2)-100%</p> <p>Note: Changes to threshold values are not propagated to the Signaling Server or the Voice Gateway Media card until a data dump is performed.</p>

LD 117 - Print voice-quality metric thresholds

A new command has been added to LD 117 to print voice-quality metric thresholds. See Table 47.

Table 47

LD 117 - Print voice-quality metric thresholds

=> Command	Description
PRT QSTHS	Print all voice-quality thresholds

LD 117 - Configure voice-quality sampling (polling)

The following command has been added to LD 117 to configure the sampling (polling) period, zone alarm-rate collection window, and the minimum number of samples to collect during the window.

To configure voice-quality sampling using Element Manager, select:
Configuration > IP Telephony > Quality of Service

Table 48

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 assists in isolating voice-quality problems and reducing 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.

Voice-quality threshold alarm notification levels can be set on a zone-by-zone basis 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 49: “Voice-quality threshold alarm notification levels” on [page 187](#).

Table 49
Voice-quality threshold alarm notification levels (Part 1 of 4)

Level	Description	Alarms
0	All voice-quality alarms are suppressed	None
1	Allow zone-based Unacceptable alarms	QOS0017 QOS0018 QOS0019 QOS0020 QOS0021

Table 49
Voice-quality threshold alarm notification levels (Part 2 of 4)

Level	Description	Alarms
2	Allow all of the above PLUS zone-based Warning alarms	All of the above PLUS QOS0012 QOS0013 QOS0014 QOS0015 QOS0016

Table 49
Voice-quality threshold alarm notification levels (Part 3 of 4)

Level	Description	Alarms
3	Allow all of the above PLUS per-call Unacceptable alarms	All of the above PLUS QOS0007 QOS0008 QOS0009 QOS0010 QOS0011 QOS0021 QOS0032 QOS0033 QOS0036 QOS0037

Table 49
Voice-quality threshold alarm notification levels (Part 4 of 4)

Level	Description	Alarms
4	Allow all of the above PLUS per-call Warning alarms	All of the above PLUS QOS0001 QOS0002 QOS0003 QOS0005 QOS0006 QOS0018 QOS0019 QOS0022 QOS0023 QOS0024 QOS0025 QOS0026 QOS0027

The craft person controls the number of alarms generated by the system using the following new alarm notification level configuration command in LD 117. See Table 50.

To configure zone alarm-notification levels using Element Manager, select:
System Status > Call Server > IP Telephony Quality of Service Diagnostic

Table 50
LD 117 - Configure zone alarm-notification levels

=> Command	Description
CHG ZQNL <ZoneNumber> <level>	Change the Notification Level for the specified zone Where: <ZoneNumber> = 0-255 <level> = 0-(2)-4

LD 117 - Print zone alarm-notification levels

The following command has been added to LD 117 to print zone alarm-notification levels. See Table 50.

Table 51
LD 117 - Print zone alarm-notification levels

=> Command	Description
PRT ZQNL <ZoneNumber>	Print the Notification Level for the specified zone Where: <ZoneNumber> = 0-255

New voice-quality alarms

This feature introduces new Warning and Unacceptable voice-quality alarms. The alarms are defined on a per-call basis or zone basis. For detailed information on QoS alarms, see *What’s New for Communication Server 1000 Release 4.5* (553-3001-015).

Diagnosing and isolating voice-quality problems

New network diagnostic utilities are accessible on IP Phones to isolate voice-quality problems. The diagnostic utilities can be run directly from the IP Phone itself, or remotely through a CLI.

Ping and Traceroute

The administrator can execute the Ping or Traceroute command from a specific endpoint with any arbitrary destination, typically another endpoint or Signaling Server.

IP Networking statistics

The administrator can view information on the packets sent, packets received, broadcast packets received, multicast packets received, incoming packets discarded, and outgoing packets discarded.

Ethernet statistics

The administrator can view ethernet statistics (for example, number of collisions, VLAN ID, speed and duplex) for the IP Phone on a particular endpoint. The exact statistics will depend on what is available from the IP Phone for the specific endpoint.

UNISTIM/RUDP statistics

The administrator can view RUDP statistics (for example, number of messages sent, received, retries, resets, and uptime) for the IP Phones.

Real time Transport Protocol statistics

The administrator can view RTP/RTCP QoS metrics (for example, packet loss, jitter, and so on) while a call is in progress.

DHCP

The administrator can view DHCP settings (for example, IP address, S1, S2, and S4 addresses) for each IP Phone.

For detailed information on network diagnostic utilities, refer to *IP Phones: Description, Installation, and Operation* (553-3001-368)

SNMP interface

A new SNMP interface has been added to the traffic reporting system so that OTM, or any third-party system, can have a simple, standards-based interface into the system traffic reports.

For details on the new SNMP interface, refer to *Simple Network Management Protocol: Description and Maintenance* (553-3001-519).

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 on IP endpoints and their voice-quality capabilities in the system, refer to Table 52.

Table 52
IP Endpoint and voice-quality capabilities (Part 1 of 2)

Endpoint type	Voice-quality monitoring operation
Phase 0/1 IP Phones	Detects jitter, packet loss, and latency (when the far end is RTCP-compliant) threshold violations. Threshold violations are detected by polling.
Phase 2 IP Phones without PVQM package	Detects jitter, packet loss, and latency (when the far end is RTCP-compliant) threshold violations. Threshold violations are detected asynchronously by the IP Phone.

Table 52
IP Endpoint and voice-quality capabilities (Part 2 of 2)

Endpoint type	Voice-quality monitoring operation
Phase 2 IP Phones with PVQM package	Detects 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.
IP Softphone 2050	Detects jitter, packet loss, and latency (when the far end is RTCP-Compliant) threshold violations. Threshold violations are detected by polling.
CS 1000 and Meridian 1 systems with Voice Gateway Media Cards running IP Line 4.0	Detects jitter and packet loss threshold violations. Threshold violations are detected by polling.
Third-party Media Gateway	Not supported

pbxLink connection failure detection and status reporting enhancement

Contents

This section contains information on the following topics:

Introduction	197
pbxLink connection failure detection	198
Displaying pbxLink information	198
LD 117 STAT SERV enhancement	198
pbxLink information	199
Application information	199

Introduction

The pbxLink connection failure detection and status reporting enhancement provides the following functionality:

- The pbxLink connection failure detection provides a means of detecting 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 status reporting enhancement applies to the STAT SERV command in LD 117. This command has been enhanced to display the link status of the Signaling Server and Voice Gateway Media Cards that were configured to connect to the system. As well, the display provides information about the applications running on the Signaling Server and Voice Gateway Media Cards.

pbxLink connection failure detection

The Call Server monitors the pbxLink.

The Call Server maintains a list of all known registered elements (Signaling Servers and Voice Gateway Media Cards). When a Call Server is booted, it has a 5-minute delay to enable these known elements to re-establish 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 or Voice Gateway Media Card registers with the Call Server, an ELAN0029 alarm is generated.

Displaying pbxLink information

Element Manager

For a CS 1000S And CS 1000M, use the Element Manager **System Status > Call Server > IP Telephony Services Management** page to display the pbxLink information.

CLI

For a Meridian 1 system, use the LD 117 STAT SERV command at the CLI of the Call Server to display the pbxLink information.

LD 117 STAT SERV enhancement

The suite of STAT SERV (Stat Services) commands enables a technician to display link status information for elements that are registered to a Call Server.

STAT SERV can provide consolidated link status information by application type, IP address, host name, and IP Telephony node ID.

Prior to CS 1000 Release 4.5, STAT SERV status information included the following:

- node ID
- host name
- IP address
- element role
- platform type
- enabled applications
- registered/unregistered endpoints, such as IP Phones and Voice Gateway Media Cards

In CS 1000 Release 4.5, the STAT SERV command has been enhanced to provide information about the pbxLink and enabled applications.

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

Application information

If an active link to an element is established, the Call Server obtains information about the applications running on the element.

Table 53 lists the applications and describes the information obtained about those applications.

Table 53
Queried information in STAT SERV

Application/element	Information provided
LTPS application	number of registered IP Phone 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 its link with the Call Server elements that failed to register or lost their link

Figure 20 on [page 201](#) shows an example of LD 117 STAT SERV output.

Figure 20
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 VTRK	LINK UP	5/06/2003	22:51:06	0x200a2128
	Sets: [reg - 0302] [busy - 0056] VTRK: [reg - 0050] [busy - 0015]								
999	IPService	47.11.216.141	YES	SS	LTPS VTRK	LINK UP	5/06/2003	22:51:06	0x200a2128
	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 54 lists the descriptions for the fields in the STAT SERV response.

Table 54
STAT SERV response fields and description (Part 1 of 3)

STAT SERV response field	Description
NODE ID	Identifies the related node. Value is a number from 0 – 9999.
HOSTNAME	Identifies the alias that the host has been given by the system. Value is a string.
ELANIP	Identifies the element's 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	Specifies the element type. Values are: <ul style="list-style-type: none"> • SMC – Media Card 32-port card • ITGP – ITG-P 24-port card • SS – Signaling Server
APPS	Specifies the application running on the element. Values are: <ul style="list-style-type: none"> • LTPS • VTRK

Table 54
STAT SERV response fields and description (Part 2 of 3)

STAT SERV response field	Description
PBXLINK STATE	Specifies the element's current pbxLink state. Values are: <ul style="list-style-type: none">• LINK UP• LOST• FAILED• INV CONN (element is connected, but its configuration was not found on the Call Server, indicating that this element might be connected to the wrong Call Server)
PBXLINK DATE/TIME	Specifies when the element's pbxLink state last changed.
CONNECTED	Specifies the element's connection ID.
sets	Values are: <ul style="list-style-type: none">• reg – the number of IP Phones registered to the element• busy – the number of IP Phones that are currently busy

Table 54
STAT SERV response fields and description (Part 3 of 3)

STAT SERV response field	Description
vgws	Values are: <ul style="list-style-type: none">• reg – how many DSP resources are configured on the element• busy – how many DSP resources are active/busy on the element
VTRK	Values are: <ul style="list-style-type: none">• reg – how many VTRK channels are configured on the element• busy – how many VTRK channels are active/busy on the element

Technical Assistance service

Contents

This section contains information on the following topics:

Nortel Technical Assistance Centers.	205
Services available	208
Requesting assistance	211

Nortel Technical Assistance Centers

To help customers obtain maximum benefit, reliability, and satisfaction from their CS 1000E systems, Nortel provides technical assistance in resolving system problems. Table 55 lists the centers that provide this service.

Table 55
Customer Technical Services (Part 1 of 3)

Location	Contact
Nortel Global Enterprise Technical Support (GETS) PO Box 833858 2370 Performance Drive Richardson, TX 75083 USA	North America Telephone: 1 800 4NORTEL

Table 55
Customer Technical Services (Part 2 of 3)

Location	Contact
Nortel Corp. P.O. Box 4000 250 Sydney Street Belleville, Ontario K8N 5B7 Canada	North America Telephone: 1 800 4NORTEL
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

Table 55
Customer Technical Services (Part 3 of 3)

Location	Contact
Network Technical Support (NTS)	<p>Asia Pacific Telephone: +61 28 870 8800</p> <p>Australia Telephone: 1800NORTEL (1800 667835) or +61 2 8870 8800 E-mail: asia_support@nortel.com</p> <p>People's Republic of China Telephone: 800 810 5000 E-mail: chinatsc@nortel.com</p> <p>Japan Telephone: 010 6510 7770 E-mail: supportj@nortel.com</p> <p>Hong Kong Telephone: 800 96 4199 E-mail: chinatsc@nortel.com</p> <p>Taiwan Telephone: 0800 810 500 E-mail: chinatsc@nortel.com</p> <p>Indonesia Telephone: 0018 036 1004</p> <p>Malaysia Telephone: 1 800 805 380</p> <p>New Zealand Telephone: 0 800 449 716</p> <p>Philippines Telephone: 1 800 1611 0063 or 632 917 4420</p> <p>Singapore Telephone: 800 616 2004</p> <p>South Korea Telephone: 0079 8611 2001</p> <p>Thailand: Telephone: 001 800 611 3007</p>

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.
Tables 56 and 57 describe the service classifications.

Table 56
Technical service emergency classifications

Class	Degree of failure	Symptoms
E1	Major failure causing system degradation or outage	<p>System out-of-service with complete loss of call-processing capability.</p> <p>Loss of total attendant console capability.</p> <p>Loss of incoming or outgoing call capability.</p> <p>Loss of auxiliary Call Detail Reporting (CDR) in resale application.</p> <p>Call processing degraded for reasons such as trunk group out-of-service:</p> <ul style="list-style-type: none"> • 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	<p>Standby CPU out-of-service.</p> <p>Frequent initializations (one per day or more).</p> <p>Disk drive failure.</p> <p>Two sets of disks inoperative.</p>

Table 57
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 will seriously affect service at in-service or cut-over date.
S2	Intermittent failure that affects service	Software or hardware faults that only 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 defined above) 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 58 before you call for service.

Table 58
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)	_____
Seriousness of request (see Tables 56 and 57)	_____
Description of assistance required	_____

Appendix A: Establishing a PPP connection

Contents

This section contains information on the following topics:

Establishing a PPP connection	213
Using a PPP link to the Signaling Server for remote, single point of access	214
Modem and serial COM port configuration for	
using PPPLink to the Signaling Server	215
Modem Configuration Example: US Robotics Sportster Faxmodem 56K...	217
Configuring a Dial-up Networking PPP Client	
for remote access to the Signaling Server	220
Configure the Call Server route	231
Configure Voice Gateway Media Card ELAN route	231
Using Remote Single Point of Access to CS 1000S via	
Signaling Server PPP link	232
Benchmarking.	236

Establishing a PPP connection

The following are requirements and procedures for establishing a PPP connection.

Using a PPP link to the Signaling Server for remote, single point of access

PPP over a dialup modem connection to COM1 on the rear of the Signaling Server Leader is the preferred method of remote, single point of access to the CS 1000S system. For example, a PPP link is used for:

- 1** Web browser access to Element Manager on the Signaling Server (for example, configuration changes, installation of patches)
- 2** FTP to transfer files to and from the Signaling Server (for example, binary loadware files for Media Cards)
- 3** Telnet/rlogin sessions to access system elements on the ELAN network using the Signaling Server (for example, Call Server, Media Cards)

Modem and serial COM port configuration for using PPPlink to the Signaling Server

For the best performance of the IP-based management clients (such as the Element Manager Web browser, Telnet, rlogin, and FTP) over the PPP link to the Signaling Server, use a V.34bis, V.90, or V.92 modem at both ends of the dialup connection. Ensure that both modems are configured to enable:

- hardware flow control

Note: For hardware flow control, you must use a straight-through (not a null modem) RS232 cable with full RS232 modem control signals, including Clear to Send (CS or CTS) and Request to Send (RS or RTS). The Signaling Server COM1 and COM2 serial ports are equipped with DB-9 male connectors operating as RS232 Data Terminal Equipment (DTE).

- modem error control (ARQ)
- modem data compression.

Different operating systems use different names for the serial ports. Table 59 shows the name of serial ports on the Signaling Server.

Table 59
Serial port name by operating system

Serial Port	Windows	Linux	Solaris	VxWorks
rear	COM1	/dev/ttyS0	/dev/ttya	/tyC0/0
front	COM2	/dev/ttyS1	/dev/ttyb	/tyC0/1

Note: The MS Windows nomenclature is used in this section.

Table 60 shows the maximum bidirectional modem connect speed over a high-quality dialup telephone connection for the V.34bis, V.90, and V.92 modems.

Table 60
Maximum bidirectional connect speed of modem types

Modem type	Maximum bidirectional connect speed
V.34bis modem	33.6 kbps
V.90 modem	33.6 kbps
V.92 modem (operating in V.PCM mode)	48.0 kbps

Modem serial port speeds

The serial port speeds for the remote PC and the Signaling Server must be correctly set.

Modem serial port speed for the Signaling Server

The modem must be installed on the Signaling Server's COM1 (rear) serial port. This allows you to observe the startup messages that are displayed when the Signaling Server performs a cold or warm reboot.

The modem serial-port speed for the Signaling Server's COM1 port must be set to exactly 38400 bps (not higher) using the Signaling Server's TTY command from the oam> CLI on Signaling Server COM1 (rear) or COM2 (front).

- Using the STTY command from either the COM1 or COM2 serial port changes the speed of both Signaling Server COM ports.
- Using the STTY command from a Telnet terminal connected to the Signaling Server does not change the speed of COM1 and COM2.

Procedure 30**Setting the modem serial-port speed for the Signaling Server**

- 5 Log in to the oam shell.
- 6 Issue the STTY command and set the serial port speed of COM1 to 38400 bps.

```
oam> stty 38400
```

End of Procedure

Modem serial-port speed for the remote PC

The modem serial-port speed for the remote PC running the Dialup Networking client must be configured to 38400 bps or higher. Use the Dialup Networking Client to set the speed. Refer to the General tab of the Dialup Networking Client properties; see Figure 22 on [page 222](#) in Procedure 32 starting on [page 220](#)).

**Modem Configuration Example:
US Robotics Sportster Faxmodem 56K**

This example refers to US Robotics Product ID 00568603. Read and follow the steps in the technical reference for the modem that you are installing.

The modem must be configured to:

- Send Data hardware flow control only.
- Ignore Request To Send (RTS).

For normal operation of the modem that is connected to COM1 on the Signaling Server, the modem DIP switch settings are ALL UP (OFF) except for DIP switch 1 and 4 DOWN (ON). See Table 61 on [page 218](#).

Table 61
DIP switch settings

DIP Switch	Position	Description
DIP Switch 1	Down (ON)	Modem ignores Data Terminal Ready
DIP Switch 2	Up (OFF)	Modem displays verbal result codes
DIP Switch 3	Up (OFF)	Modem suppresses display of result codes
DIP Switch 4	Down (ON)	Modem suppresses display of result codes
DIP Switch 5	Up (OFF)	Modem answers if S0 = 1 or greater
DIP Switch 6	Up (OFF)	Modem sends Carrier Detect signal on serial port when carrier is present
DIP Switch 7	Up (OFF)	Modem loads the previously modified and stored NVRAM configuration profile (Y0 or Y1), or the read-only factory configuration profile (Y2, Y3, or Y4) selected by the Y parameter. You must use the modem AT command AT Y0 to select NVRAM stored configuration profile 0 which has been configured to enable Send Data hardware flow control only.
DIP Switch 8	Up (OFF)	Modem ignores AT commands (Dumb Mode)

DIP switch settings are read and applied when:

- the modem is powered on
- the modem is reset by using the ATZn command

AT command set

To temporarily use the AT command set on the modem that you will connect to Signaling Server's COM1 port, you must:

- 1** Connect a terminal directly to the modem
- 2** Set DIP switch 8 DOWN (ON)
- 3** Power the modem OFF/ON.

The modem will now respond to the AT command set, however, type carefully as the modem still suppresses local echo of AT commands entered from the terminal and also suppresses display of result code "OK". DIP switches 3 and 4 can be adjusted, but typing carefully will work.

Procedure 31

Using the AT command set

- 1 Type **AT Z4** and press Enter to reset default S registers and load factory configuration profile 1 which is the hardware flow-control template.

Factory profile 1 enables hardware flow control for both Send Data and Receive Data.

Note: You must disable Receive Data hardware flow control to operate the modem on the Signaling Server COM port.

- 2 Type **AT &R1** and press Enter to configure the modem to ignore Request To Send (RTS).

This disables Receive Data hardware flow control and allows you to log into the Signaling Server COM port.

- 3 Type **AT &W0** and press Enter to store the modified hardware flow control configuration in NVRAM stored profile 0.

- 4 Type **AT Y0** and press Enter to set Y0.

If DIP switch 7 is UP (OFF) upon resetting, the modem loads NVRAM stored configuration profile 0 which enables Send Data hardware flow control only.

- 5 Type **ATZ** and press Enter to reset the modem and load the Y0 Send Data hardware flow control configuration according to DIP switch 7 UP (OFF).

- 6 Type **at i4** and press Enter to display the current modem configuration and verify the settings Y0, H1, and R1.

If the settings are not correct repeat step 1 to step 6. Read and follow the technical reference for the modem you are installing to configure it for Send Data hardware flow control only.

End of Procedure

Configuring a Dial-up Networking PPP Client for remote access to the Signaling Server

Use Procedure 32 to configure a Dialup Networking PPP Client on the remote PC running MS Windows 2000 or other MS Windows operating system with MS Internet Explorer version 5.5 or later.

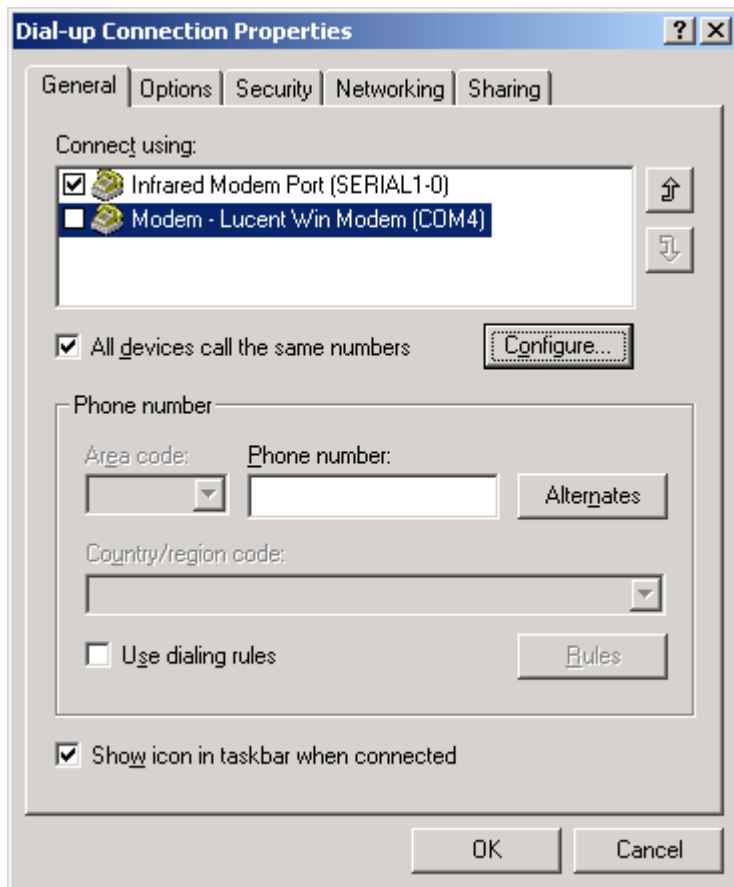
Note: Enable or disable properties as recommended; leave other properties with the default settings (that is, do not change them).

Procedure 32 Configuring a Dial-up Networking PPP client for remote access to the Signaling Server

- 1 Select **Start | Settings | Control Panel**.
- 2 Double-click **Network and Dial-up Connections**.
- 3 Double-click **Make New Connection**.
The Network Connection Wizard window opens. Click **Next**.
- 4 Select the Network Connection Type.
- 5 Right-click the connection and selection **Properties**.

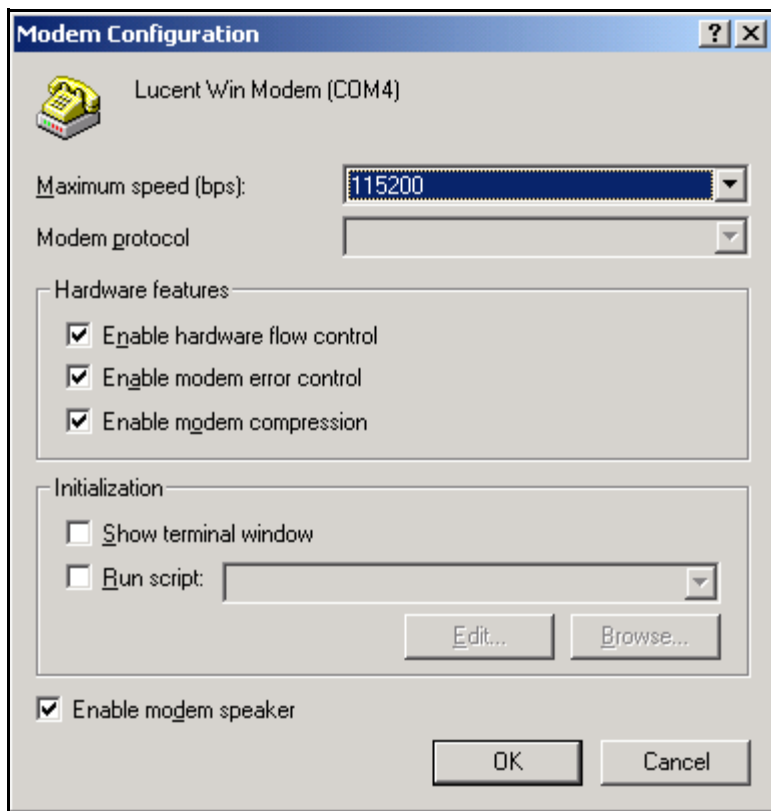
The properties window for the newly created dial-up connection appears. The Properties window has five tabs (see Figure 21 on [page 221](#)). Configure the properties as outlined in the following steps.

Figure 21
Dial-up connection - General tab



- 6** On the **General** tab, click the **Configure** button.
The **Modem Configuration** window opens (see Figure 22 on [page 222](#)).

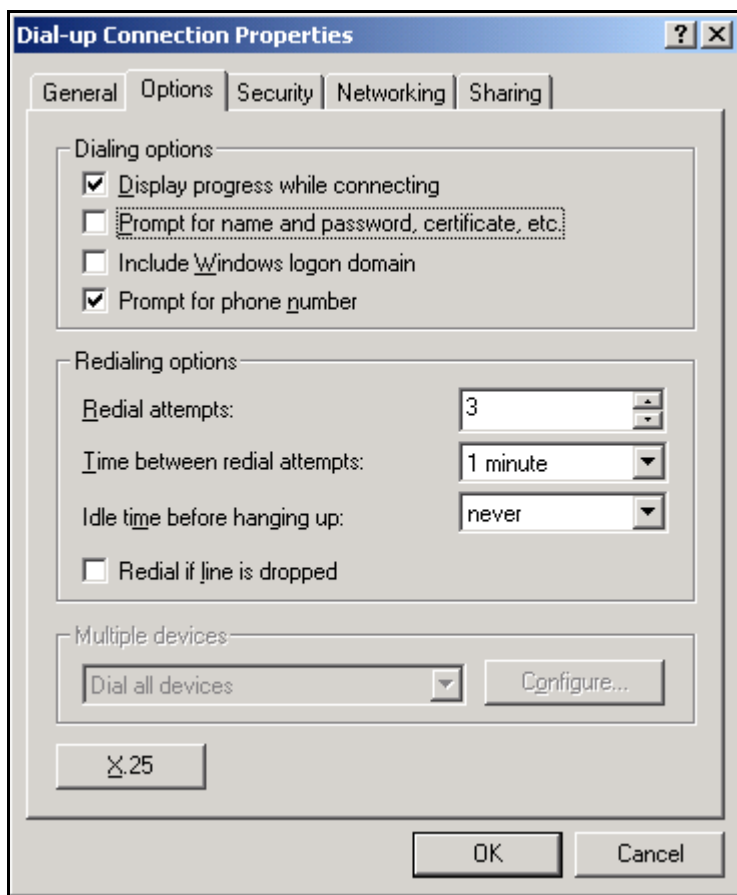
Figure 22
Modem Configuration



- 7 Set the following:
 - a. Set **Maximum speed (bps)** to 38400, 57600, or 115200.
 - b. Check **Enable hardware flow control**.
 - c. Check **Enable modem error control**.
 - d. Check **Enable modem data compression**.
 - e. Uncheck **Show terminal window**.
 - f. Uncheck **Run script**

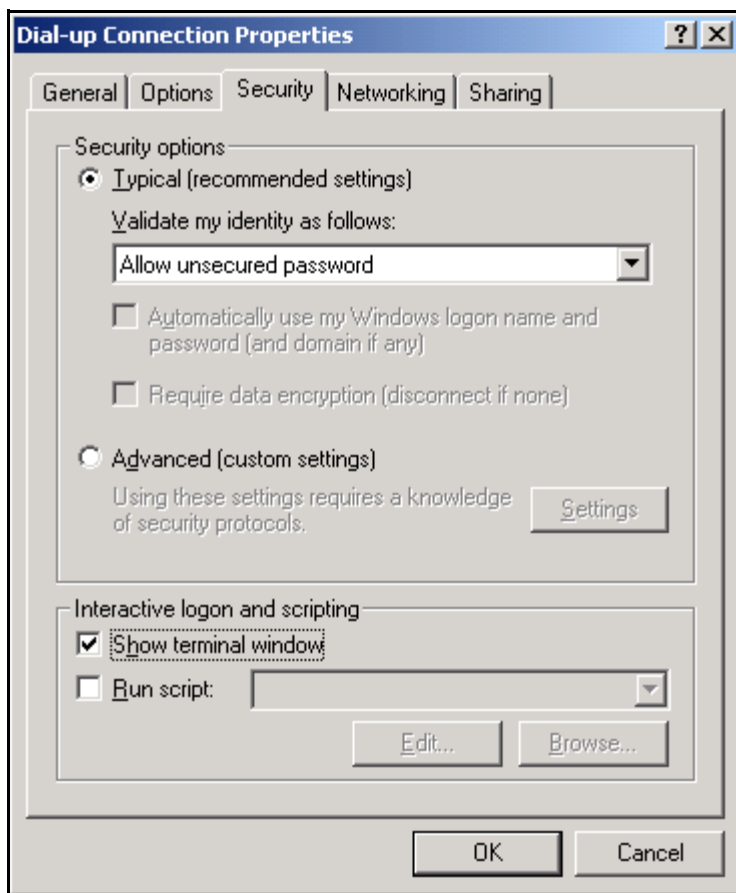
- g. Check **Enable modem speaker**.
- h. Click **OK**. The Dial-up Connection window reappears.

Figure 23
Dial-up connection - Options tab



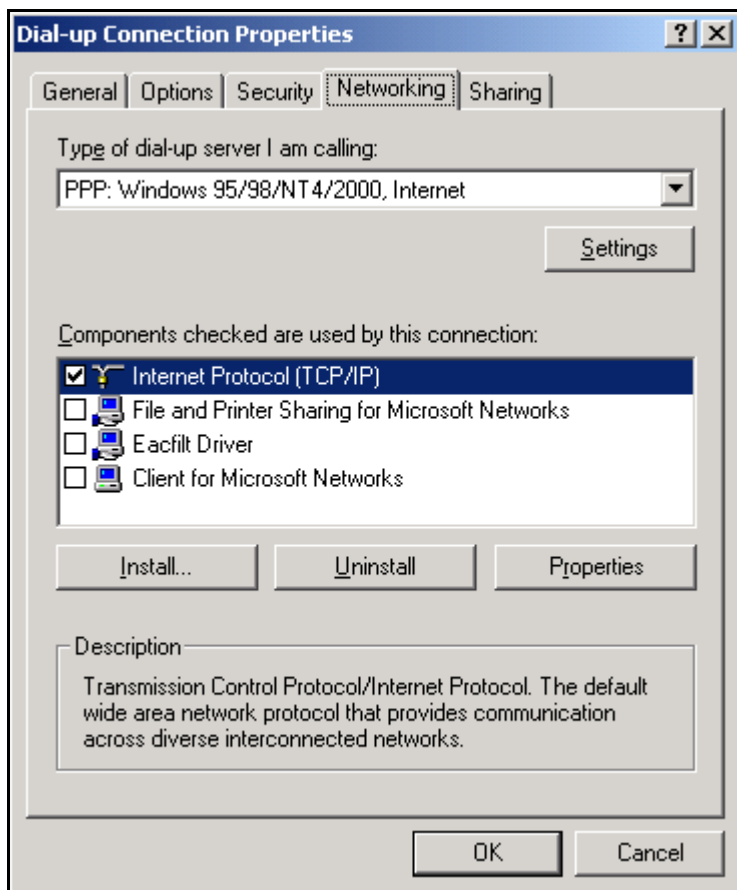
- 8 Select the **Options** tab (see Figure 23 on [page 223](#)).
 - a. Enable **Display progress while connecting**.
 - b. Disable **Prompt for name and password**.
 - c. Disable **Include Windows logon domain**.
 - d. Enable **Prompt for phone number**
 - e. Leave all the other properties with the default settings.

Figure 24
Dial-up connection - Security tab



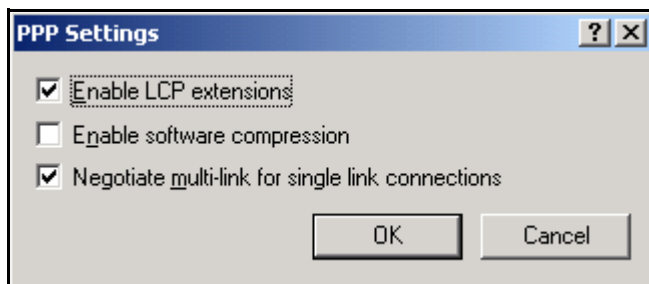
- 9 Select the **Security** tab (see Figure 24 on [page 224](#)).
 - a. Under **Security options**, select **Typical (recommended settings)** radio button.
 - b. Under **Interactive logon and scripting**:
 - i. Enable **Show terminal window**.
 - ii. Ensure that **Run script** is not checked.

Figure 25
Dial-up connection - Networking tab



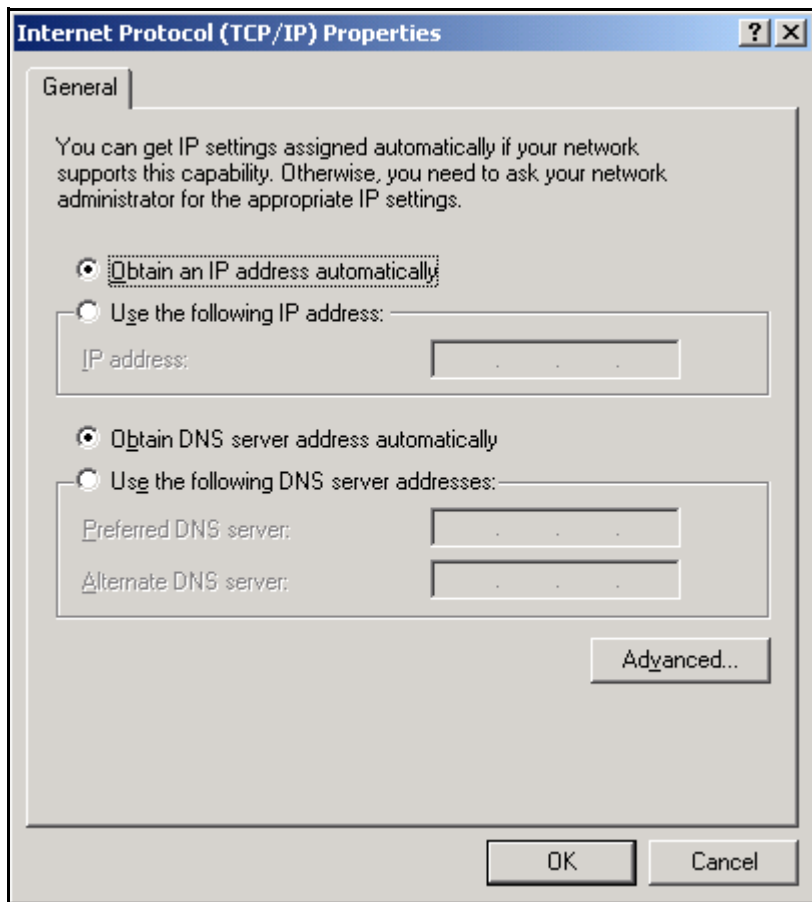
- 10 Select the **Networking** tab (see Figure 25 on [page 225](#)).
 - a. Under **Type of dialup server I am calling:**, select PPP, Windows 95/98/NT4/2000, Internet.
 - b. Click the **Settings** button. The PPP Setting window opens (see Figure 26 on [page 226](#)).
 - i. Uncheck the **Enable software compression** checkbox.
 - ii. Click **OK** to close the PPP Settings window.

Figure 26
PPP Settings



- c. Under **Components used by this connection:**
 - i. Enable **Internet Protocol (TCP/IP)**.
 - ii. Disable **File and Printer Sharing for Microsoft Networks**.
 - iii. Disable **Client for Microsoft Networks**.
 - iv. Disable any other components.
 - d. Highlight Internet Protocol (TCP/IP) and click the **Properties** button.
 - i. The Internet Protocol (TCP/IP) Properties window opens (see Figure 27 on [page 227](#)). Select the **Obtain IP address automatically** radio button.
 - ii. Select the **Obtain DNS server address automatically** radio button.

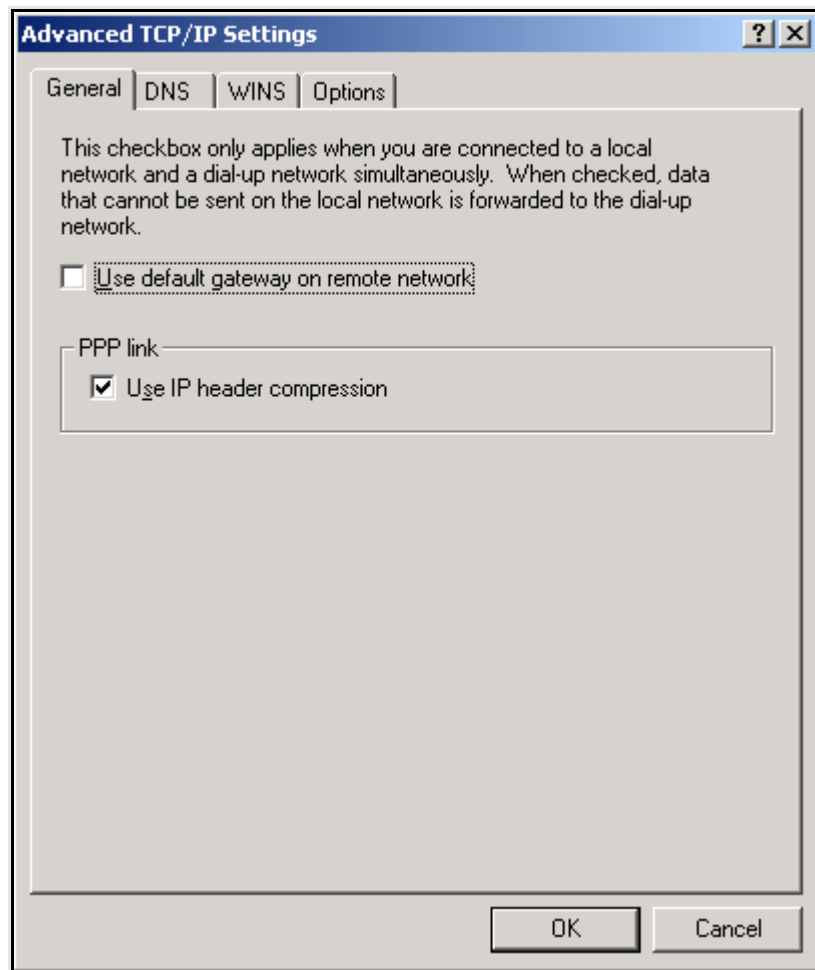
Figure 27
Internet Protocol (TCP/IP) Properties



- e. Click the **Advanced** button.

The **Advanced TCP/IP Properties** window opens (see Figure 28 on [page 228](#)).

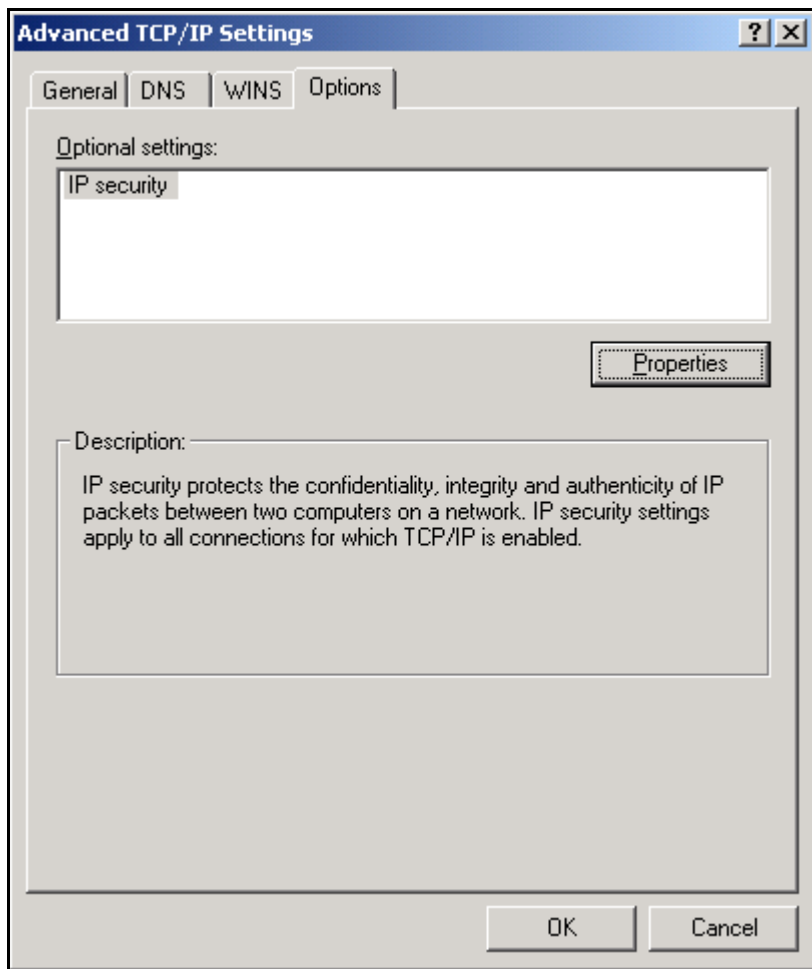
Figure 28
Advanced TCP/IP Properties - General tab



- f. On the **General** tab:
 - i. Disable **Use default gateway on remote network**.
 - ii. Enable **Use IP header compression**.

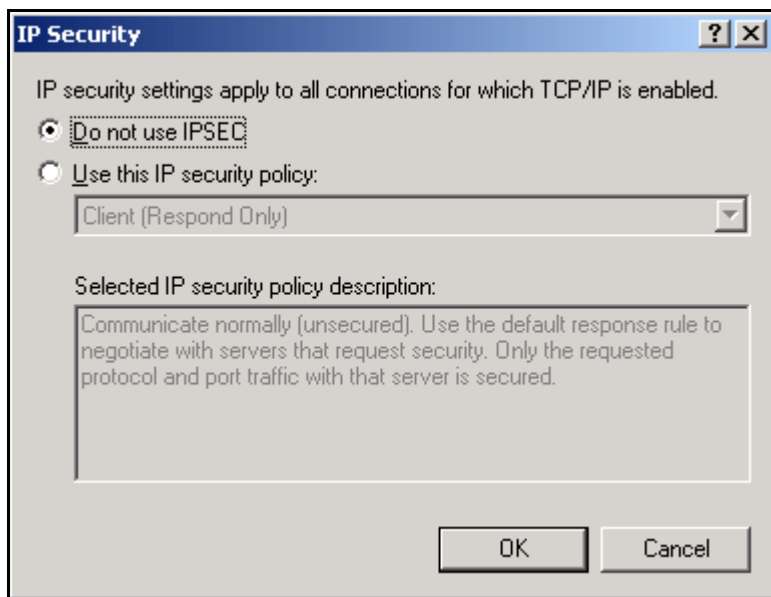
- g. Select the **Options** tab (see Figure 29).

Figure 29
Advanced TCP/IP Settings - Options Tab



- h. Click the **Properties** button. The **IP Security** window opens (see Figure 30).

Figure 30
IP Security



- i. Check the **Do not use IPSEC** radio button.
- j. Click **OK** to save the settings and close the IP Security window.
- k. Click **OK** to save the settings and close the Advanced TC/IP Settings window.
- l. Click **OK** to save the settings and close the Internet Protocol TCP/IP Properties window.
- m. Click **OK** to save the settings and close your dial-up connection window.

End of Procedure

Configure the Call Server route

Use Procedure 33 to configure the Call Server route for remote single point of access using the Signaling Server PPP link.

Procedure 33 **Configuring the Call Server route**

- 1 Log in to LD 117.
- 2 Issue the following command:

NEW ROUTE <Signaling Server's ELAN network IP Address>
- 3 Issue the following command:

PRT ROUTE
- 4 Issue the following command:

ENL ROUTE n
- 5 Issue the following command:

STAT ROUTE
- 6 Verify presence of route to destination xxx.xxx.xxx.xxx by Gateway <Signaling Server's ELAN IP Address>.

End of Procedure

Configure Voice Gateway Media Card ELAN route

Configure Media Card ELAN route for remote single point of access using the Signaling Server PPP link.

Procedure 34 **Configuring the Media Card ELAN route**

- 1 Connect to each Voice Gateway Media Card and login to VxWorks shell.
- 2 Issue the following command to go to the root directory:

cd "/C:"
- 3 Create a new directory called **etc** by issuing the following command:

mkdir "etc"

- 4 Use the change directory command to go to the etc directory.
 `cd "etc"`
- 5 Issue the following command:
 `copy 0,"startup"`
- 6 Issue the following command:
 `routeAdd "137.135.3.2","<Signaling Server's ELAN IP Address>"`
- 7 Press Ctrl-D.
- 8 Issue the following command:
 `copy "startup"`
- 9 Verify correct contents of /C:/etc/startup script file.
- 10 Issue the **cardReset** command.
- 11 Verify the successful execution of startup script (immediately following the VxWorks startup banner.)
- 12 Login to IPL> shell and enter the **routeShow** command. Verify presence of HOST ROUTE to Destination 137.135.3.2 by Gateway <SS ELAN IP Address>.

End of Procedure

Using Remote Single Point of Access to CS 1000S via Signaling Server PPP link

Use Procedure 35 to apply Remote Single Point of Access to CS 1000S via the Signaling Server PPP link.

Procedure 35 **Using Remote Single Point of Access**

- 1 Once the Dialup Networking Client connects to the modem on the Signaling Server:
 - a. Use the interactive login terminal window to log in to oam> shell
 - b. Enter the **ppp** command without parameters.
 `oam> ppp`

Table 62 shows the result of entering the ppp command.

Table 62
Result of entering ppp command without parameters

If you are connected to the...	Entering ppp without parameter gets...
rear COM port (/tyCo/0) on the Signaling Server	<ul style="list-style-type: none">• the default Local IP address 137.135.3.1 for the Signaling Server ppp3 interface• the default Remote IP address 137.135.3.2 for your remote PC PPP interface
front COM port (/tyCo/1) on the Signaling Server	<ul style="list-style-type: none">• the default Local IP address 137.135.5.1 for the Signaling Server ppp5 interface• the default Remote IP address 137.135.5.2 for your remote PC PPP interface

- c. Click the **Done** or **Continue** button on PPP Client Interactive Login Terminal window.

WARNING

After entering the ppp command you will see the ASCII display of the binary PPP protocol.

Once you have entered the ppp command, there is a window of *approximately 50 seconds* for you to click the Done or Continue button, and for the PPP service on the Signaling Server and the PPP dialup client on the remote PC to establish the PPP link.

If you allow the window to time out, you must cancel and try again.

- 2 From the remote PC, start a primary Telnet connection to IP address 137.135.3.1 on the Signaling Server.

From within a primary Telnet session on the Signaling Server you can establish:

- a secondary, nested rlogin session to the Call Server, or
- a secondary, nested Telnet or rlogin session to another Signaling Server or to any Media Card using the ELAN network.

When you “exit” the secondary rlogin or Telnet session, you will revert to the primary Telnet session on the Signaling Server.

Note: You can have multiple logins to the oam> and PDT> shells on a single Signaling Server, but only one login at a time to the VxWorks shell on the Signaling Server.

- 3 Log in to the oam> shell of the Signaling Server using Telnet to the Signaling Server ppp3 local IP address.
- 4 Use the **IPInfoShow** command to get the ELAN network ID and subnet mask of the Signaling Server:

```
oam> IPInfoShow
```

The ELAN network id is the Destination of the NET ROUTE entry that shows the Signaling Server ELAN IP address as the Gateway.

- 5 Write down the Signaling Server ELAN network ID and subnet mask.
- 6 Open a command window on the remote PC.
- 7 Enter the following command to add an IP route to the ELAN network ID by the Gateway of the PPP interface IP address of the remote PC (that is, the Signaling Server ppp3 Remote IP address).

```
oam> route add <Signaling Server ELAN network ID> mask <Signaling  
Server ELAN subnet mask> 137.135.3.2
```

Note: This IP route must be added on the remote PC every time a new dialup PPP connection to the Signaling Server is established. The route to the SS ELAN network by the PPP interface is automatically removed from the remote PC's IP route table whenever the PPP link is disconnected.

- 8 Open a web browser on the remote PC and enter the URL of the Element Manager web server on the Signaling Server on the PPP IP address 137.135.3.1/.

9 If there is a Primary or Alternate Gatekeeper on the same Signaling Server, you can point the web browser to the Gatekeeper web pages in the Element Manager web server on the PPP IP address 137.135.3.1/gk.

10 Once you have:

- created HOST ROUTE entries to Destination 137.135.3.2 by the Signaling Server ELAN IP address Gateway on each of the system elements, and
- added the route to the Signaling Server ELAN Destination by the GATeway of the PPP interface IP address 137.135.3.2 on the remote PC

Use Element Manager to establish a direct Telnet session from the remote PC to the Media Card or other Signaling Servers on the Signaling Server ELAN network.

To do this, click **Status | IP Telephony | Node** and then click the **Telnet via ELAN** button.

11 Establish a direct rlogin connection from the remote PC to the Call Server using the Signaling Server ELAN network.

If you use an rlogin client such as VanDyke Software CRT 4.0 on the remote PC, you can configure the rlogin connection with the Username: CPSID. This rlogin username, CPSID, bypasses the PDT login on the Call Server and goes straight to the Overlay login.

12 Once logged in to Call Server SL1 Overlay command line, use the:

- **LON** command to turn on Line Editing mode
- **LOF** command to turn off Line Editing mode

Note: The Call Server CLI becomes easier to use when SL1 Overlay Line Editing mode is turned on. In Line Edit mode, you can use the Delete key or Ctrl-Backspace keys on the keyboard to correct typing errors on the Call Server Overlay CLI (before pressing <Enter>).

13 You can also establish direct FTP connections from the remote PC to the system elements using the Signaling Server ELAN network.

End of Procedure

Benchmarking

Benchmarks for Element Manager page loading time

Table 63 benchmarks for Element Manager page loading time at 38400 bps over a 33.6 kbps modem connection.

Table 63
Element Manager benchmarks

From	To	Time
Login page	Nortel logo	12 seconds
Login page	Navigation tree (without control objects) <i>Note:</i> The Navigation Tree can be used immediately.	18 seconds
Login page	System Information display and Navigation Tree control objects for System Status and Configuration	26 seconds
Login page	Navigation Tree (with all control objects)	44 seconds
Configuration IP Telephony pages	Node Summary page	15 seconds
Node Summary	Open a select node for editing	18 seconds

Benchmarks for File Transfer time

Table 64 shows the benchmarks for file transfer time at 38400 bps over a 33.6 kbps modem connection. The benchmarks were performed using FTP from a remote PC to the Signaling Server.

Table 64
File Transfer benchmarks

Action	Amount of data	Time	Rate
Puts	1554216 bytes	466.61 seconds	3.33 Kbytes/sec
Gets	1554216 bytes	420.40 seconds	3.70 Kbytes/sec

The **Advanced TCP/IP Properties** window opens (see Figure 28).

Index

Numerics

10BaseT port, 27

A

alarm management on OTM, 22

Alarms

major, 53

minor, 53

remote, 54

system, 53

alarms, causes, 54

alarms, management of, 65

antistatic wrist strap, use of, 19, 20

audits, 158

B

Background Routine, 61

backing up the Call Server, 139

backing up the Gatekeeper, 143

B- and D-channel, maintenance window, 59

Bantam jacks, 52

battery backup, CS 1000S, 19

battery backup, provision, 20

C

Call Server

clearing common faults, 75

faults, 76

Call Server, configure route, 231

call transfer, faults, 91

Card disabled without OVD message, 89

CCBR- see Customer Configuration Backup and Restore

chassis, faults, system impact, 80

circuit card, disabled, OVD, 87

circuit card, self-test, 36

circuit card, status indicators, 36

circuit cards, CS 1000S, 87

circuit cards, faults, 89

circuit cards, handling during maintenance, 20

circuit cards, trunk, 101

command, CHG PDV, 64

command, LMAX, 65

Commands

PRT PDV, 64

commands, Disable, 36

commands, enable, 36

commands, executing, 31

commands, IP line shell, 159

commands, maintenance, 58

commands, rlogin, 135

commands, TEST, 87

components, Call Server, 75

Conference call problems, 91

- conference calls, faults, 91
- connection, Point-to-Point, 85
- connections, LAN, layer 2 and layer 3, 86
- continuity, 124
- CPU or Memory fault, 77
- CTS, contacting, 205
- Customer Configuration Backup and Restore, 79

D

- Daughterboard software replacement
 - scheduled, 126
 - unscheduled, 127
- Diagnostic programs, 60
- Dial pad to keyboard translation, 32
- Dial-up Networking PPP client, 220
- Disabled card indicated by OVD message, 87

E

- electric shock, danger of, 19
- Element Manager, benchmarks, 236
- element manager maintenance, 132
- Equipment
 - replacing, 109
- equipment, replacing, 109
- error messages, ITG System, 152
- event monitor, 65

F

- fault, notification, 72
- fault clearing, with an SDI terminal, 102
- Fault clearing procedures
 - Network faults, 84
- Fault clearing process, 70
- faults, call transfer, 91
- faults, conference call setup, 91
- faults, CS-MG, clearing, 83

- faults, isolating, 84
- faults, MG 1000S, 95
- faults, Music-on-Hold, 91
- faults, network, indicators, 84
- faults, voice media, 90
- faults in circuit cards, 89

G

- Gatekeeper, backing up, 143

H

- Hardware maintenance tools, 35
- hex codes
 - faceplate display, 36

I

- INI (initialization), 61
- Initialize
 - button, 52
 - program, 61
- Install Tool, about, 139
- Interactive diagnostics, 67
- I/O ports, miantenance window, 59
- IP Line shell commands, 159
- ITG-P status, 38
- ITG system error messages, 152
- ITG Trunk LED display, 37

J

- Jacks, 52

K

- Keyboard to dial pad translation, 32

L

- LAN connections, layer 2 and layer 3, 86
- Layer 2 LAN connections, 86

- Layer 3 LAN connections, 86
- LED, ELAN ethernet, 50
- LED, ITG-P, 38
- LED, ITG Trunk display, 37
- LED, maintenance hex display, 36
- LED, NTA09 faceplate, 38
- LED, NTA10 faceplate, 40
- LED, NTA79 faceplate, 42
- LED, NTB50 faceplate, 43
- LED, NTD20 faceplate, 45
- LED, NTD83 circuit card, 48
- LED, NTD99 circuit card, 48
- LED, NTR21 faceplate, 50
- LED, Signaling Server, drive status, 37
- LED, Signaling Server, speed, 37
- LED, Signaling Server, Status, 37
- LEDs, 74, 77
 - faceplate, 36
- LEDs, ethernet activity, 36
- LEDs, faceplate, 36
- Line transfer, 54
- link faults, causes, 88
- link functions, 83
- Local access, 25
- loop-closure, 124

M

- Maintenance
 - telephone, 31
 - tools, 35, 57
- maintenance, element manager, 132
- maintenance, Media Card, 149
- maintenance, software, 57
- maintenance, telephone, use of, 32
- maintenance applications using OTM, 23

- maintenance commands, executing, 30
- maintenance hex display, 36
- maintenance overlays, 31
- Major alarm, 74
- Media Card, 36
- Media Gateway/Expansion card slot assignment, 28
- MG 1000S
 - fault clearing, 95
- Midnight Routine, 61
- modem, configuring for PPP link, 215
- Monitor Jacks, 52
- MTA class of service, 31
- Music-on-Hold, faults, 91
- Music-on-Hold problems, 91

N

- network fault indicators, 84
- Network faults, 83
- network loops, maintenance window, 59
- NT5K21
 - replacing, 122
- NTA02
 - replacing, 112
- NTA03
 - replacing, 113
- NTA09
 - faceplate LEDs, 38
 - removing daughterboards, 115
 - replacing, 114
 - replacing (DTI applications), 120
 - replacing daughterboards, 116
- NTA10
 - faceplate LEDs, 40
 - replacing (DTI applications), 120
- NTA20
 - removing, 115, 118
 - replacing, 116, 119

NTAK79
 faceplate LEDs, 42

NTAK92
 replacing, 124
 wiring diagram, 125

NTAK93
 removing, 115, 118
 replacing, 116, 119

NTBK50
 faceplate LEDs, 43
 removing daughterboards, 118
 replacing, 117
 replacing daughterboards, 119

NTBK51
 removing, 118
 replacing, 119

NTDK20
 CPU or Memory fault, 77
 Data dump fault, 79
 Disabled Peripheral Equipment circuit card, 98
 faceplate LEDs, 45
 More than one Peripheral Equipment card
 disabled, 100
 replacing, 125

NTDK20 circuit card, 75

NTDK20 circuit card faults, 98

NTDK83, NTDK99
 card circuit board LEDs, 48
 replacing, 129

NTRB21
 faceplate LEDs, 50
 replacing (DTI applications), 120

O

Optivity Telephony Manager (OTM), 22

OTM, maintenance applications, 23

OTM, use of, 67

OTM alarm management, 22

OVD message, 87

OVD message, trunks, 102

OVD message indicates disabled card, 87

Overlay
 Loader, 62

overlay, through the OTM system terminal, 23

Overlays, 60

overlays, maintenance, 31, 58

overlays, overview, 133

overload (OVD) message, 87

Overload Monitor, 63

OVL005 message and no overlay access, 79

P

Patches, 67

PE cards, maintenance window, 59

PE units, maintenance window, 59

pinging system elements, 85, 91, 132

Point-to-Point connection, 85

Point-to-Point connections, troubleshooting, 85

power supply, failure of, 19

power supply, location, 19

PPP, 85

PPP, connection, troubleshooting, 85

PPP Client, configuring for remote access, 220

PPP connection, establishing, 213

PPP link, configuring, 215

PPP link, establishing, 213

PPP link, Remote Single Point of Access, 232

Precautions, 19

Q

QoS LAN
 monitoring, 63

R

Remote access, 25

Remote Single Point of Access, via PPP link, 232
remote TTY, 26
Replacing equipment, 109
Resident Trunk Diagnostic, 65
rlogin command, 135

S

SDI port, 25
SDI terminal, purpose, 84, 102
SDI terminal, use of, 67
SDI terminals, using, 58
serial port, configuring for PPP link, 215
serial ports, additional, 26
Signaling Server, about, 81
Signaling Server Gatekeeper, 137
Software maintenance tools, 57
special service prefix (SPRE), 31
SPRE (Special Service Prefix), 31
SSC, maintenance window, 59
SSC, rlogin, 135
SSC card, LEDs, 45
System
 alarms, 53
 Loader, 65
 messages, 72
 monitor, 54
 terminal, 30
system, accessing, 30
system elements, pinging, 85, 91, 132
system terminal, using, 30

T

Technical Assistance Centers, 205
terminals, installing, 25
terminal server, purpose, 27
TEST command, 87

testing, 124
testing for, 124
Tools
 Hardware maintenance, 35
 Software maintenance, 57
Transferring problems, 91
trunk, resident diagnostic, 65
Trunk cannot make or receive calls
 (OVD message received), 102
trunk failure, impact, 65
trunk faults, 105
trunks, E&M, 101
trunks, universal, 101
TTY, remote, 26

U

universal trunks, 101

V

voice media faults, 90

Nortel Communication Server 1000
Communication Server
1000S
Maintenance

Copyright © Nortel Networks Limited 2005
All Rights Reserved

Information is subject to change without notice. Nortel reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant.

Nortel, Nortel (Logo), the Globemark, This is the Way, This is Nortel (Design mark), SL-1, Meridian 1, and Succession are trademarks of Nortel Networks.

Publication number: 553-3031-500
Document release: Standard 3.00
Date: August 2005
Produced in Canada



>THIS IS THE WAY

>THIS IS **NORTEL**™