



Nortel Communication Server 1000

IP Line Fundamentals

Document status: Standard
Document version: 01.01
Document date: 30 May 2007

Copyright © 2003–2007, Nortel Networks
All Rights Reserved.

Sourced in Canada.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

Nortel, Nortel (Logo), the Globemark, SL-1, Meridian 1, and Succession are trademarks of Nortel Networks.

All other trademarks are the property of their respective owners.

Revision history

May 2007

Standard 01.01. This document is issued to support Communication Server 1000 Release 5.0. This document is renamed *IP Line Fundamentals* (NN43100-500) and contains information previously contained in the following legacy document, now retired: (553-3001-365). This document also contains the proposed solution for CR Q01504212. See "[CallPilot](#)" ([page 70](#)).

December 2006

Standard 10.00. This document is up-issued to support CS 1000 Release 4.5. This document addresses the following CRs:

- Q01512086
- Q01452824

July 2006

Standard 9.00. This document is up-issued to address the following CRs:

- Q01368947
- Q01349604

May 2006

Standard 8.00. This document is up-issued to reflect changes to the IPL> CLI default user name and password.

April 2006

Standard 7.00. This document is up-issued to reflect changes in technical content due to the following CRs:

- Q01270071
- Q01285983
- Q01318230

January 2006

Standard 6.00. This document is up-issued to reflect changes in technical content due to the following CRs:

- Q01206792
- Q01259132
- Q01131032

August 2005

Standard 5.00. This document is up-issued following the removal of regulatory data.

August 2005

Standard 4.00. This document is up-issued to support Nortel Communication Server 1000 Release 4.5.

September 2004

Standard 3.00. This document is up-issued to support Nortel Networks Communication Server 1000 Release 4.0.

May 2004

Standard 2.00. This document is up-issued to support the Nortel Networks Mobile Voice Client 2050 (MVC 2050).

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: *IP Line: Description, Installation and Operation* (553-3001-204).

Contents

New in this release **13**

- Features 13
 - Other changes 14
 - Subject 14
 - Structure 14
-

How to get help **17**

- Getting help from the Nortel Web site 17
 - Getting help over the telephone from a Nortel Solutions Center 17
 - Getting help from a specialist by using an Express Routing Code 17
 - Getting help through a Nortel distributor or reseller 18
-

Description **19**

- Contents 19
 - Introduction 19
 - Digital Signaling Processor daughterboards 20
 - Interworking 21
 - Applicable systems 21
 - System requirements 22
 - System configurations 23
 - Software delivery 24
 - Required packages 25
 - Voice Gateway Media Cards 25
 - Media Card 32S 33
 - RUDP 40
 - Secure Real-time Transport Protocol 41
 - Virtual superloops, virtual TNs, and physical TNs 42
 - Licenses 42
 - Zones 44
 - Administration 44
-

Features **47**

- Contents 47
- Introduction 48
- Live Dialpad 50

Diagnostics	51
Unicode support	51
Pop-up and USB keyboard support	51
IP Client cookies	52
New IP Phone Types	53
Unique TN Types for existing IP Phones	53
Automatic IP Phone TN conversion (Flexible Registration)	54
Manual IP Phone TN conversion	55
Active Call Failover for IP Phones	55
DSP peg counter for CS 1000E systems	78
Enhanced UNISim Firmware Download for IP Phones	79
Firmware download using UNISim FTP	107
NAT Traversal feature	114
Corporate Directory	131
Personal Directory, Callers List, and Redial List	132
IP Call Recording	132
pbxLink connection failure detection	141
LD 117 STAT SERV	142
IP Phone support	146
Expansion Module for IP Phone 1100 Series	158
Element Manager support	159
Call Statistics collection	160
Programmable line/DN feature keys (self-labeled)	169
Private Zone configuration	170
Run-time configuration changes	173
Network wide Virtual Office	174
Bandwidth Management for Network wide Virtual Office	177
Requirements	178
Branch Office and Media Gateway 1000B	178
802.1Q support	179
Data Path Capture tool	182
IP Phone firmware	182
Graceful Disable	183
Hardware watchdog timer	184
Codecs	185
Set type checking and blocking	186
Enhanced Redundancy for IP Line nodes	187

Personal Directory, Callers List, and Redial List **189**

Contents	189
Introduction	189
Personal Directory	191
Callers List	192
Redial List	194

IP Phone Application Server configuration and administration	195
IP Phone Application Server database maintenance	198
Call Server configuration	202
Password administration	203

Codecs 205

Contents	205
Introduction	205
Codec configuration	207
Codec registration	209
Codec negotiation	212
Codec selection	215

Installation and configuration summary 219

Contents	219
Introduction	219
Before you begin	219
Installation summary	219
Voice Gateway Media Card installation summary sheet	222

Installation and initial configuration of an IP Telephony node 225

Contents	225
Introduction	225
Equipment considerations	226
Install the hardware components	226
Initial configuration of MC 32S card	241
Configuring the Leader and Follower on the MC 32S	241
Initial configuration of IP Line data	241
Configure the Expansion Module for IP Phone 1100 Series	255
Node election rules	257

Configuration of IP Telephony nodes using Element Manager 259

Contents	259
Introduction	259
Configure IP Line data using Element Manager	260
Transfer node configuration from Element Manager to the Voice Gateway Media Cards	286
Upgrade the Voice Gateway Media Card software and IP Phone firmware	293
Assemble and install an IP Phone	307
Change the default IPL CLI Shell password	307
Configure the IP Phone Installer Passwords	307
Import node configuration from an existing node	307

IP Line administration 311

Contents	311
Introduction	311
IP Line feature administration	312

- Password security 317
- IP configuration commands 333
- TLAN network interface configuration commands 333
- Display the number of DSPs 334
- Display IP Telephony node properties 334
- Packet loss monitor 338
- Transfer files using the CLI 338
- Download the IP Line error log 340
- Reset the Operational Measurements file 340

IP Line administration using Element Manager 341

- Contents 341
- Introduction 341
- Element Manager administration procedures 341
- Backup and restore data 352
- Update IP Telephony node properties 355
- Update other node properties 374
- Telnet to a Voice Gateway Media Card using Virtual Terminal 374
- Check the Voice Gateway Channels 376
- Setting the IP Phone Installer Password 377

IP Line administration using TM 3.1 381

- Contents 381
- Introduction 381
- TM administration procedures 381
- Back up and restore TM data 395
- Add an IP Telephony node in TM by retrieving an existing node 396
- IP Line CLI access using Telnet or local RS-232 maintenance port 399

Voice Gateway Media Card maintenance 401

- Contents 401
- Introduction 401
- Faceplate maintenance display codes 401
- System error messages 405
- IP Line and IP Phone maintenance and diagnostics 410
- IP Line CLI commands 420
- Lamp Audit and Keep Alive functions 448
- Voice Gateway Media Card self-tests 452
- Troubleshoot a software load failure 452
- Troubleshoot an IP Phone installation 455
- Maintenance telephone 456
- Replace the Media Card CompactFlash 456

Voice Gateway Media Card maintenance using Element Manager 457

- Contents 457

Introduction	457
Replace a Voice Gateway Media Card	457
Add another Voice Gateway Media Card	463
Access CLI commands from Element Manager	465
Access the CLI from Element Manager	476
Convert IP Trunk Cards to Voice Gateway Media Cards	477
Contents	477
Introduction	477
Before you begin	478
Convert the IP Trunk cards	478
Add the converted cards to an IP Telephony node	479
Appendix A NAT router requirements for NAT Traversal feature	487
Contents	487
Description	487
Requirements	488
Natcheck output	490
Appendix B I/O, maintenance, and extender cable description	493
Contents	493
Introduction	493
NTMF94EA I/O cable	493
Connector pin assignments	494
NTAG81CA maintenance cable description	497
NTAG81BA maintenance extender cable	498
Replace the NT8D81BA cable with the NT8D1AA cable and install the NTCW84JW special IPE filter	499
Appendix C Product integrity	503
Contents	503
Introduction	503
Reliability	503
Environmental specifications	504
Appendix D Subnet Mask Conversion from CIDR to Dotted Decimal Format	507
Introduction	507
Appendix E Download IP Line files from Nortel Web site	509
Contents	509
Introduction	509
Download files from Nortel Web site	509
Appendix F Moving Voice Gateway Media Cards between systems	511
Contents	511

Introduction	511
Reconfiguring the Voice Gateway Media Card	511
Node has Leader configured	512
Node has no Leader configured	516
Upgrading the software	523

Procedures

Procedure 1	Accessing Ethernet Diagnostics in Element Manager	97
Procedure 2	Accessing the uftpTurboMode command	101
Procedure 3	Accessing the uftpTurboModeShow command	103
Procedure 4	Accessing uftpTurboModeTimeoutSet command	104
Procedure 5	Accessing uftpAutoUpgradeTimeoutSet command	105
Procedure 6	Accessing the call log options	193
Procedure 7	Configuring the IP Phone Application Server on a separate Signaling Server	197
Procedure 8	Backing up the IP Phone Application Server database server manually	199
Procedure 9	Performing a full database recovery	200
Procedure 10	Performing a selective database recovery	201
Procedure 11	Preinstallation and configuration steps	220
Procedure 12	Installing the ITG-P 24-port line card	229
Procedure 13	Installing the CompactFlash card on the Media Card	231
Procedure 14	Installing the Media Card	232
Procedure 15	Replacing the existing I/O Panel Filter Connector	234
Procedure 16	Installing the NTMF94EA ELAN, TLAN, serial interface cable	238
Procedure 17	Installing the Shielded 50-pin to Serial/ELAN/TLAN Adapter onto the Media Card	240
Procedure 18	Configuring the ELAN network interface IP address for the active ELNK	242
Procedure 19	Viewing Element Manager for Zone Configuration	244
Procedure 20	Using Element Manager to configure Voice Gateway channels	246
Procedure 21	Configuring a virtual Superloop in Element Manager	250
Procedure 22	Turning off browser caching in Internet Explorer	261
Procedure 23	Launching Element Manager	263
Procedure 24	Adding an IP Telephony node manually	265
Procedure 25	Configuring SNMP trap destinations	269
Procedure 26	Configuring DSP Profile data	270
Procedure 27	Configuring QoS	274
Procedure 28	Configuring the Call Server ELAN network interface IP address (Active ELNK), TLAN voice port, and routes	276
Procedure 29	Configuring access to the file server	280
Procedure 30	Setting the loss plan for the UK	282
Procedure 31	Adding a card and configuring Voice Gateway Media Card properties	283
Procedure 32	Submitting and transferring the node information	285
Procedure 33	Configuring the Leader IP address for a second or subsequent node	288
Procedure 34	Transmitting node properties to Leader	290

Procedure 35	Configuring the Follower cards 292
Procedure 36	Determining the IP Phone firmware version 295
Procedure 37	Updating Recommended Firmware List 296
Procedure 38	Downloading loadware and firmware from the Nortel Web site 297
Procedure 39	Uploading loadware and firmware files 298
Procedure 40	Upgrading the card loadware 299
Procedure 41	Rebooting the Voice Gateway Media Card 300
Procedure 42	Re-enabling the Voice Gateway Media Card 301
Procedure 43	Upgrading the IP Phone firmware 302
Procedure 44	Importing node files 308
Procedure 45	Configuring the Administrative IP Phone Installer Password 328
Procedure 46	Configuring the temporary IP Phone Installer Password 330
Procedure 47	Resetting the user name and password to default 332
Procedure 48	Retrieving the current OM file from the Voice Gateway Media Card using Element Manager 342
Procedure 49	Viewing IP Line log files 351
Procedure 50	Backing up the Call Server data 353
Procedure 51	Restoring the Call Server data 355
Procedure 52	Updating the IP Telephony node properties 356
Procedure 53	Adding a Voice Gateway Media Card to the node 357
Procedure 54	Deleting a follower Voice Gateway Media Card from the node 362
Procedure 55	Deleting the Leader Voice Gateway Media Card 364
Procedure 56	Changing the IP addresses of an IP Telephony node in Element Manager 365
Procedure 57	Restarting a Voice Gateway Media Card at the CLI 372
Procedure 58	Restarting a Voice Gateway Media Card in Element Manager 373
Procedure 59	Changing the IP address of the Leader card 374
Procedure 60	Accessing a Voice Gateway Media Card using Telnet 375
Procedure 61	Checking the Voice Gateway Channels 377
Procedure 62	Setting the administrative and temporary IP Phone Installer Passwords 377
Procedure 63	Scheduling Reports 383
Procedure 64	Generating reports 385
Procedure 65	Opening an Operational Measurement (OM) report 386
Procedure 66	Retrieving the current OM file from the Voice Gateway Media Card using TM 387
Procedure 67	Viewing IP Line info and error log 395
Procedure 68	Adding a node by retrieving an existing node 396
Procedure 69	Accessing a Voice Gateway Media Card using Telnet 399
Procedure 70	Troubleshooting an IP Phone installation 455
Procedure 71	Removing the CompactFlash 456
Procedure 72	Replacing a Follower Voice Gateway Media Card 458
Procedure 73	Replacing a Leader Voice Gateway Media Card 460
Procedure 74	Add another Voice Gateway Media Card to the system 463
Procedure 75	Accessing the CLI commands from Element Manager 468
Procedure 76	Converting IP Trunk card to Voice Gateway Media Cards 478

Procedure 77	Adding the converted Voice Gateway Media Cards into an existing IP Telephony node 480
Procedure 78	Importing all converted Voice Gateway Media Cards into a new IP Telephony node 482
Procedure 79	Preventing ground loops 496
Procedure 80	Removing an NT8D81BA cable 500
Procedure 81	Installing an NTCW84JA filter and NT8D81AA cable 501
Procedure 82	Converting a subnet mask from CIDR format to dotted decimal format 507
Procedure 83	Downloading files from the Nortel Web site 509
Procedure 84	Reconfiguring a Voice Gateway Media Card running CS 1000 Release 4.5 or later (Follower on original system) 514
Procedure 85	Reconfiguring a Voice Gateway Media Card running CS 1000 Release 4.5 or later (Leader in original system) 515
Procedure 86	Reconfiguring a Voice Gateway Media Card running CS 1000 Release 4.0 or earlier (Leader or Follower) 516
Procedure 87	Reconfiguring the ITG-P 24-port card running CS 1000 Release 4.5 or later (Leader or Follower) 518
Procedure 88	Reconfiguring an ITG-P 24-port card running CS 1000 Release 4.0 (Leader or Follower) 519
Procedure 89	Reconfiguring the Media Cards running CS 1000 Release 4.5 or later (Leader or Follower) 521
Procedure 90	Reconfiguring the Media Cards running CS 1000 Release 4.0 or earlier (Leader or Follower) 522
Procedure 91	Upgrading the software for the ITG-P 24-port card or the Media Card running CS 1000 Release 4.0 or earlier 524

New in this release

The following sections detail what is new in *IP Line Fundamentals* (NN43100-500) for CS 1000 Release 5.0.

- Features
- Other changes

Features

See the following sections for information about the feature changes.

Live Dialpad

Live Dialpad activates the line/DN key when the user makes a call by pressing the keys on the dialpad without lifting the handset, pressing a line/DN key, or pressing the handsfree key. For further information, see ["Live Dialpad" \(page 50\)](#).

Unicode support

Unicode support provides the ability for IP Phone 1110, IP Phone 1120E, IP Phone 1140E, IP Phone 1150E, and IP Phone 2007 to display characters for languages with complex fonts. The following languages are supported on the IP Phones with Unicode capabilities: Traditional Chinese, Simplified Chinese, Arabic, Japanese, Greek, Korean, and Hebrew. For further information, see ["Unicode support" \(page 51\)](#).

IP client cookies

IP client cookies provide transparent data transfer between the CS 1000 and third-party applications, for example, Citrix AG. For further information, see ["IP client cookies" \(page 52\)](#).

New IP Phone types

IP Phones are provided with unique Terminal Number (TN) types. IP Phones are no longer required to emulate one of five IP Phones. For further information, see ["New IP Phone Types" \(page 53\)](#).

Other changes

IP Line: Description, Installation, and Maintenance for CS 1000 Release 5.0. includes the following changes:

- Rebranded OTM 2.2 to TM 3.1.
- Removed the following sections of TM 3.1, which are not supported in CS 1000 Release 5.0:
 - Configuration of IP Telephony nodes using TM 3.1 section
 - Update IP Telephony node properties using TM 3.1
 - Update Voice Gateway Media Card properties
 - Voice Gateway Media Card maintenance using TM 3.1
- Added the Media Card 32S for SRTP support.
- Updated Element Manager with enhancements.
- Added support for Enterprise Common Manager (ECM).
- Added new IP Phones, and Expansion Module for IP Phone 1100 Series.
- Updated IP Phone firmware upgrade process, which is enhanced to be IP Telephony Node specific.
- Removed instances of CS 1000S.
- Removed instances of Meridian 1.
- Removed instances of Media Card 8-port line card.
- Removed instances of IP Phone firmware download from the Voice Gateway Media Card.

Subject

This document:

- describes the physical and functional characteristics of the IP Line application for Nortel Communication Server (CS) 1000 Release 5.0 system and describes its use on Signaling Servers and Voice Gateway Media Cards.
- explains how to engineer, install, configure, administer, and maintain an IP Telephony node that contains Voice Gateway Media Cards.

Structure

This document has separate chapters that are applicable only to either Telephony Manager (TM) 3.1 or Element Manager.

The configuration, administration, and maintenance sections are divided into two chapters. For example, a generic configuration chapter deals with tasks related to the installation and configuration of IP Line. This chapter is followed by the configuration chapter for Element Manager. The administration and maintenance chapters have the same format.

Note on legacy products and releases

This NTP contains information about systems, components, and features that are compatible with Nortel Communication Server 1000 Release 5.0 software. For more information about legacy products and releases, click the Technical Documentation link under Support & Training on the Nortel home page: www.nortel.com

Related information

The following documents are referenced in this document:

- *Converging the Data Network with VoIP Fundamentals (NN43001-260)*
- *Transmission Parameters Reference (NN43001-282)*
- *Signaling Server Installation and Commissioning (NN43001-312)*
- *Branch Office Installation and Commissioning (NN43001-314)*
- *Telephony Manager 3.1 System Administration (NN43050-601)*
- *WLAN IP Telephony Installation and Commissioning (NN43001-504)*
- *Emergency Services Access Fundamentals (NN43001-613)*
- *Element Manager System Reference—Administration (NN43001-632)*
- *Enterprise Common Manager Fundamentals (NN43001-116).*
- *IP Phones Fundamentals (NN43001-368)*
- *Software Input Output Reference—System Messages (NN43001-712)*
- *Communication Server 1000M and Meridian 1 Small System Planning and Engineering (NN43011-220)*
- *Communication Server 1000M and Meridian 1 Large System Planning and Engineering (NN43021-220)*
- *Communication Server 1000M and Meridian 1 Large System Maintenance (NN43021-700)*
- *Communication Server 1000E Planning and Engineering (NN43041-220)*
- *IP Phone 2001 User Guide (NN43115-102)*
- *IP Phone 2002 User Guide (NN43116-104)*
- *IP Phone 2004 User Guide (NN43117-102)*
- *IP Phone 2007 User Guide (NN43118-100)*

- *IP Audio Conference Phone 2033 User Guide (NN43111-100)*
- *IP Softphone 2050 User Guide (NN43119-101)*
- *Mobile Voice Client 2050 User Guide (NN43119-103)*
- *IP Phone 1110 User Guide (NN43110-101)*
- *IP Phone 1120E User Guide (NN43112-103)*
- *IP Phone 1140E User Guide (NN43113-106)*
- *IP Phone 1150E User Guide (NN43114-100)*
- *IP Phone Key Expansion Module User Guide (NN43119-102)*
- *Expansion Module for IP Phone 1100 Series User Guide (NN43130-101)*

How to get help

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

Getting help from the Nortel Web site

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

www.nortel.com

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

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

Getting help over the telephone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support Web site, and you have a Nortel support contract, you can also get help over the telephone from a Nortel Solutions Center.

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

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

www.nortel.com/callus

Getting help from a specialist by using an Express Routing Code

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

www.nortel.com/erc

Getting help through a Nortel distributor or reseller

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

Description

Contents

This section contains the following topics:

- ["Introduction" \(page 19\)](#)
- ["Interworking" \(page 21\)](#)
- ["Applicable systems" \(page 21\)](#)
- ["System requirements" \(page 22\)](#)
- ["System configurations" \(page 23\)](#)
- ["Software delivery" \(page 24\)](#)
- ["Required packages" \(page 25\)](#)
- ["Voice Gateway Media Cards" \(page 25\)](#)
- ["Virtual superloops, virtual TNS, and physical TNS" \(page 42\)](#)
- ["Licenses" \(page 42\)](#)
- ["Zones" \(page 44\)](#)
- ["Administration" \(page 44\)](#)

Introduction

Communication Server (CS) 1000 Release 5.0 requires the IP Line application.

The IP Line application provides an interface that connects IP Phones to a CS 1000 Call Server.

CS 1000 Release 5.0 requires a Signaling Server to operate. You must upgrade your Meridian 1 system, if your system is IP enabled to include a Signaling Server, which in turn becomes a CS 1000M system. CS 1000 Release 5.0 is supported on an analog/digital (TDM) only system without a Signaling Server if the system is not IP enabled. For information about upgrading your system, see *Communication Server 1000M and Meridian 1*

Small System Planning and Engineering (NN43011-220) or Communication Server 1000M and Meridian 1 Large System Planning and Engineering (NN43021-220).

ATTENTION

The IP Line version of software must match the Call Server version.

Digital Signaling Processor daughterboards

CS 1000 Release 5.0 introduces Digital Signaling Processor (DSP) daughterboards, which are placed on the Media Gateway Controller (MGC) to provide DSP resources for connecting IP and Time Divisional Multiplexing (TDM) devices together in a CS 1000E Media Gateway (MG 1000E) system. The following DSP daughterboards are available:

- 32 port daughterboard
- 96 port daughterboard

These daughterboards provide an optional solution to installing the Voice Gateway Media Cards within the CS 1000E Media Gateway (MG 1000E) chassis. However, Voice Gateway Media Cards are still supported within an MG 1000E with a Media Gateway Controller (MGC) and DSP daughterboards. The MGC is only used in a Media Gateway chassis or an Option 11C cabinet.

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

Voice Gateway Media Cards

If a Media Card 32-port card, a Media Card 32S, or an ITG-P 24-port card is running IP Line software, it is known as a Voice Gateway Media Card.

In this document, Media Card 32-port card and Media Card 32S card are referred to as Media Card 32-port cards, unless explicitly stated.

DHCP server

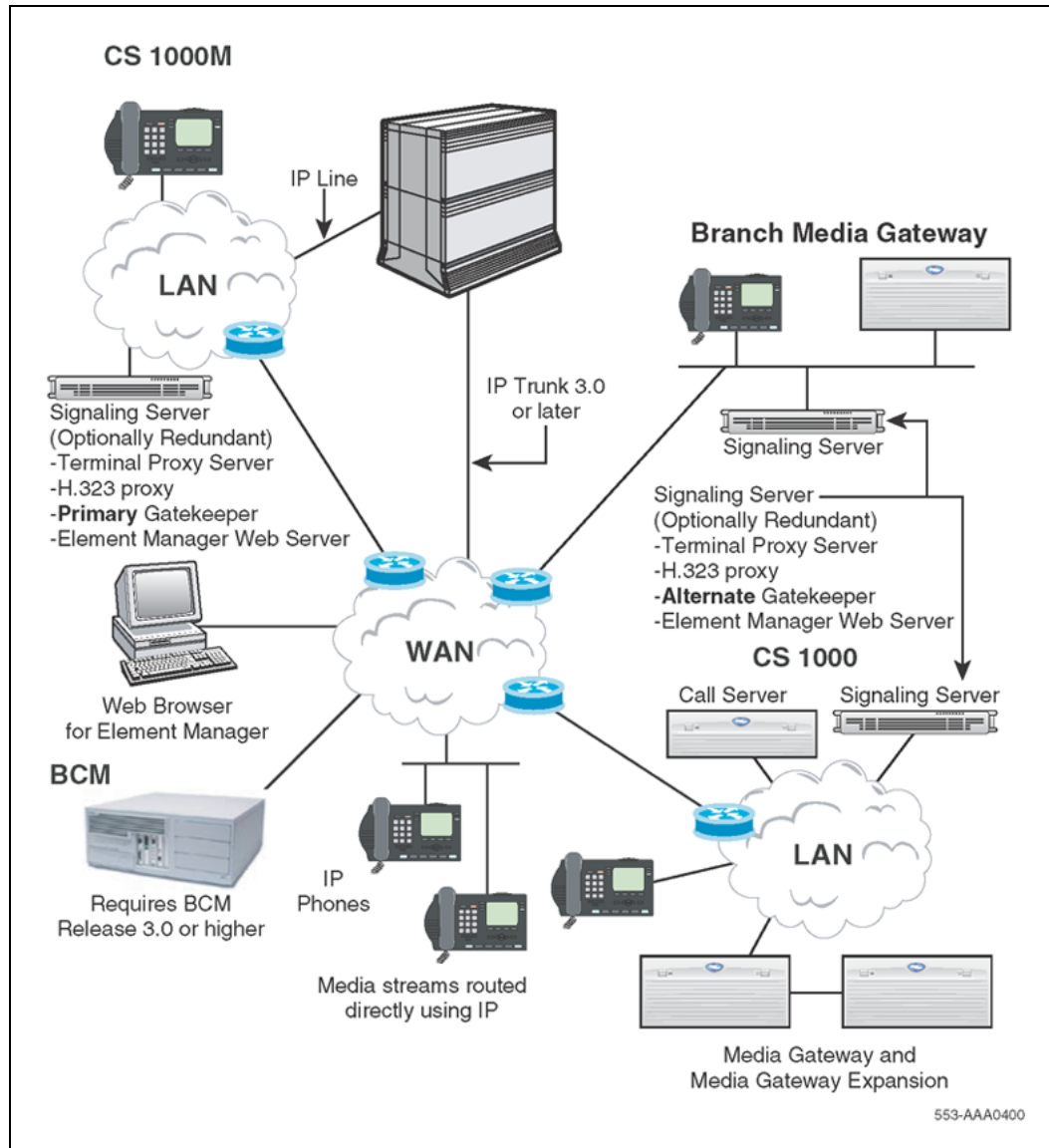
A Dynamic Host Configuration Protocol (DHCP) server can be used to provide the required information so that the IP Phone network connection can connect to the Signaling Server or Line Terminal Proxy Server (LTPS).

For more information about DHCP, see *Converging the Data Network with VoIP Fundamentals (NN43001-260)* and *IP Phones Fundamentals (NN43001-368)*.

Interworking

The IP Phone uses the IP network to communicate with the LTPS and the optional DHCP server. [Figure 1 "System architecture" \(page 21\)](#) shows a diagram of the system architecture.

Figure 1
System architecture



Applicable systems

The CS 1000 system supports the Media Card 32-port line card, Media Card 32S card, and ITG-Pentium 24-port line card.

Unsupported products

The following remote service products do not support the Media Card 32-port line card, Media Card 32S card, and ITG-Pentium 24-port line card:

- Carrier Remote
- Mini-carrier Remote
- Fiber Remote
- Fiber Remote Multi-IPE

System requirements

CS 1000 Release 5.0 software is the minimum system software for IP Line 5.0.

Element Manager and Telephony Manager 3.1

In CS 1000 Release 5.0, Element Manager is the primary interface for Voice Gateway Media Cards and IP Line.

Telephony Manager (TM) 3.1 is used only to obtain Operational Measurement (OM) reports. TM 3.1 is the minimum required version.

CS 1000 systems

Element Manager is used as the configuration, administration, and maintenance interface for IP Line on a CS 1000 system.

If you are trying to use TM 3.1 to perform an action available through Element Manager, then TM 3.1 launches Element Manager automatically.

Corporate Directory

TM 3.1 is necessary for creation of the Corporate Directory database.

SNMP and alarms

Element Manager does not provide a SNMP alarm browser. Nortel recommends you use TM 3.1 Alarm Manager when SNMP alarm collection is required.

System configurations

Although IP Line can be used in different system configurations and its use can vary in those configurations, there are two basic system configurations supported in CS 1000 Release 5.0. See [Table 1 "Possible system configurations" \(page 23\)](#).

Table 1
Possible system configurations

System	Signaling Server present
CS 1000E	Yes
CS 1000M	Yes

CS 1000 systems

CS 1000 systems have a Signaling Server in their network configuration. The Signaling Server is a server that provides signaling interfaces to the IP network. The Signaling Server central processor drives the signaling for IP Phones and IP Peer networking.

In IP Line, the LTPS executes on the Signaling Server, and the voice gateway executes on the Voice Gateway Media Cards. All IP Phones register with the Signaling Server. The Voice Gateway Media Cards only provide access to the voice gateway.

The Signaling Server is the node leader and, by default, acts as a Master for the node.

Signaling Servers

The following Signaling Servers are available for CS 1000 Release 5.0:

- ISP1100
- HP-DL320-G4
- IBM-X306m
- Common Processor Pentium Mobile (CP PM)

For further information about Signaling Server hardware platforms, see *Signaling Server Installation and Commissioning (NN43001-312)*.

In a CS 1000 system, the Signaling Servers can be used in Leader/Follower and Primary/Alternate/Failsafe combinations.

In CS 1000 Release 5.0, the Signaling Servers support the following applications:

- Line Terminal Proxy Server (LTPS)
- Virtual Trunk

- H.323 Gateway
- SIP Gateway
- SIP Redirect Server
- Network Routing Service (NRS)
- Personal Directory
- SIP Proxy Server (SPS)
- Element Manager

Signaling Server redundancy Signaling Server redundancy ensures that telephony services can withstand single hardware and network failures. Several Signaling Servers can load share when the system contains multiple Signaling Servers or Voice Gateway Media Cards. One Signaling Server is a Leader Signaling Server that acts as the primary, or master, Terminal Proxy Server (TPS). The other Signaling Server is a Follower Signaling Server that acts as the backup, or secondary redundant TPS. There are several methods of redundancy for a Signaling Server. See [Table 2 "Methods of Signaling Server redundancy" \(page 24\)](#).

Table 2
Methods of Signaling Server redundancy

Stage	Description
With a Signaling Server to share the load	
1	A Signaling Server, which shares the load, can be configured in a normal configuration.
2	If the primary Signaling Server fails, the Signaling Server, which shares the load, takes over and all IP Phones register with this Signaling Server.
3	If the Signaling Server, which shares the load, fails, one of the Voice Gateway Media Cards is elected to be the node Master.
4	The IP Phones then register to the Voice Gateway Media Cards.
Without a Signaling Server to share the load	
1	If there is no Signaling Server to share the load, and the primary Signaling Server fails, one of the Voice Gateway Media Cards is elected to be the node Master.
2	The IP Phones then register to the Voice Gateway Media Cards.

Software delivery

IP Line supports software delivery through the following formats:

1. CompactFlash
2. Signaling Server CD-ROM
3. Download from the Nortel Web site

Stand-alone IP Line software is not available through CD-ROM.

Download the IP Line software and related documentation (such as *Readme First* documents) from the Nortel Web site.

Required packages

The IP Phones require the software packages listed in [Table 3 "Required packages" \(page 25\)](#).

Table 3
Required packages

Package	Package number
M2000 Digital Sets (DSET)	88
Aries Digital Sets (ARIE)	170

ATTENTION

To configure IP Line in groups five to seven on Option 81C CP PII or CS 1000M MG, the Fibre Network (FIBN) software package 365 is required.

Voice Gateway Media Cards

Voice Gateway Media Card is a term used to encompass the Media Card 32-port card, ITG-P 24-port line card, and the Media Card 32S card. These cards plug into an Intelligent Peripheral Equipment (IPE) shelf in the CS 1000M systems and into a Media Gateway 1000E and Media Gateway 1000E Expander in the CS 1000E system.

The ITG-P 24-port line card occupies two slots, while the Media Card 32-port and the Media Card 32S card occupy one slot.

The Media Card 32S card provides the following features:

- Secure Real-time Transport Protocol (SRTP)
- two Digital Signal Processors (DSP), based on an ARM processor
- channel density of 32 ports
- cost improvement over existing Media Cards

The Media Card 32-port card provides the following features:

- 32-port card packet processing power is greater than that of the ITG-P 24-port line card
- increases the channel density from 24 to 32 ports (for the 32-port version)
- reduces the slot count from a dual IPE slot to a single IPE slot
- supports up to 128 IP Phones in failover scenarios

Table 4 "Card comparison " (page 26) provides a comparison of the ITG-P 24-port line card, Media Card 32-port card, and the MC 32S card.

Table 4
Card comparison

Item	ITG-P 24-port card	Media Card 32-port card	Media Card 32S card
Total DSP Channels	24	32	32
Number of slots the card occupies	2	1	1
Operating System	VxWorks 5.3	VxWorks 5.4	VxWorks 5.5
Processor	Pentium	IXP1200	ARM920T Contains two ARM processors, one that runs VxWorks and one that runs the Mindspeed application.
DSP	8 x TI5409	4 x TI5421	32 DSP channels provided on a second processor
Telogy version	7.01	8.1 High Density version (8 ports for each DSP)	DSP code is provided by Mindspeed.
Number of IP Phones that can register on each LTPS	96	128	128
The IP Phones register to the Signaling Server. If the Signaling Server fails, the IP Phones register to the Voice Gateway Media Card. A Signaling Server can register a maximum of 5000 IP Phones.			
Image file name prefixes shown by swVersionShow command	IPL P	IPL SA	IPL ARM
/C: drive	On board Flash 2 x 4Mb	Plug-in CompactFlash 32 Mb	CompactFlash 128 Mb
Upgrade	Two images files	One image file (no backup)	One zipped package

ATTENTION

In a CS 1000 system, the ELAN (Embedded LAN) subnet isolates critical telephony signaling between the Call Server and the other components. The ELAN subnet is also known as the Embedded LAN subnet. The TLAN (Telephony LAN) subnet carries telephony, voice, and signaling traffic. The TLAN subnet, also known as the Voice LAN subnet, connects to the customer network.

Voice Gateway Media Cards have an ELAN network interface (10BaseT) and a TLAN network interface (10/100BaseT) on the I/O panel.

There is an RS-232 Maintenance Port connection on the faceplates of both the ITG-P 24-port card and the Media Cards. The ITG-P 24-port card has an alternative connection to the same serial port on the I/O backplane.

**CAUTION**

Do not connect maintenance terminals to both the faceplate and the I/O panel serial maintenance port connections at the same time.

Capacity

The Virtual TN (VTN) feature allows each Voice Gateway Media Card to support more IP Phones than there are physical bearer channels. There are 24 bearer channels on each ITG-P card and 32 channels on each Media Card.

Both cards support a 4:1 concentration of registered IP Phones (IP Phone 2001, IP Phone 2002, IP Phone 2004, IP Phone 2007, IP Audio Conference Phone 2033, IP Softphone 2050, Mobile Voice Client [MVC] 2050, IP Phone 1110, IP Phone 1120E, IP Phone 1140E, IP Phone 1150E, WLAN Handset 2210, WLAN Handset 2211, WLAN Handset 2212, WLAN Handset 6120, WLAN Handset 6140 to gateway channels. The ITG-P supports 96 registered IP Phones. The Media Cards supports 128 registered IP Phones (when the card has 32 channels). The IP Phones require the services of the bearer channels only when they are busy on a call that requires a Time Division Multiplexing (TDM) circuit such as an IP Phone-to-digital telephone/trunk/voice mail/conference. When an IP Phone is idle or there is an IP-to-IP call, no gateway channel is required.

When the total number of IP Phones that are registered or are attempting to register reaches the limit (96 on the ITG-P or 128 on the Media Cards), the Voice Gateway Media Card recognizes this, and no more IP Phones are assigned to the card. Each Voice Gateway Media Card is restricted to a total of 1200 call attempts per hour distributed across all the IP Phones associated with the card.

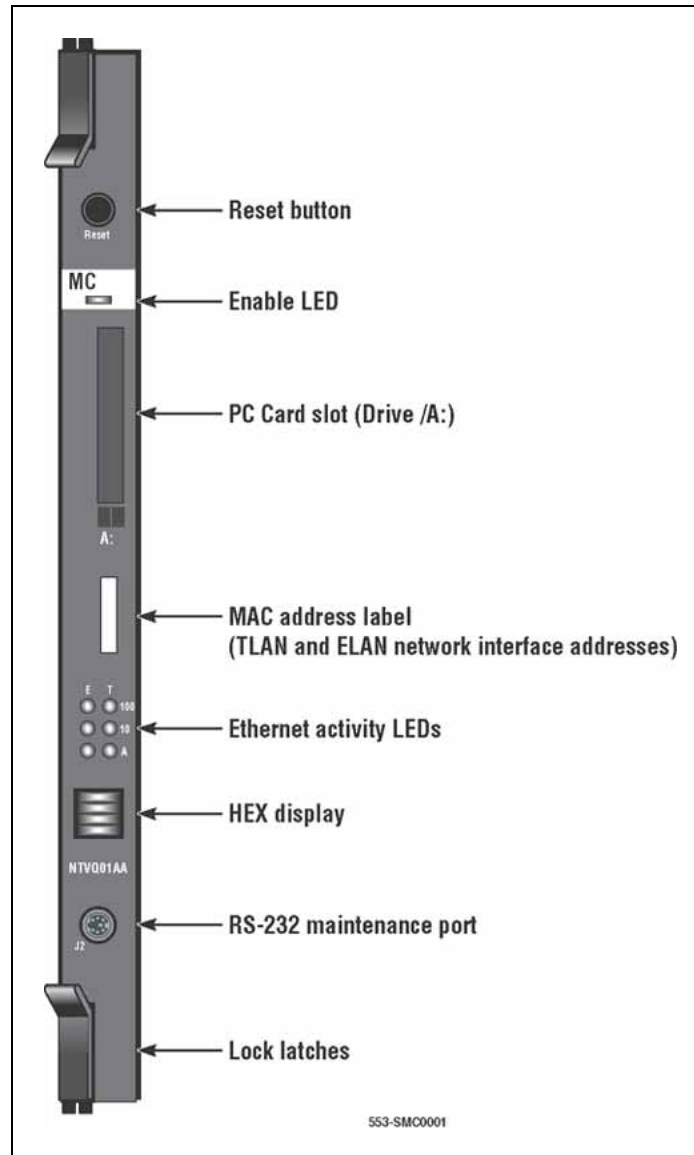
Voice Gateway Media Card controls, indicators, and connectors

The following sections show the faceplates and describe the faceplate components of the following Media Cards:

- [Figure 2 "Media Card 32-port " \(page 28\)](#)
- [Figure 3 "ITG-P 24-port card faceplate" \(page 30\)](#)

- Figure 5 "Media Card 32S card faceplate" (page 36)

Figure 2
Media Card 32-port



Faceplate components

The components on the faceplate of the Media Card 32-port card are described in the following sections.

Reset button

Use the Reset button on the faceplate to manually reset the Media Card. This enables the card to be reset without cycling power to it. The Reset button is used to reboot the card after a software upgrade or to clear a fault condition.

Enable LED

The faceplate red LED indicates the following:

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

PC Card slot

This slot accepts the Type I or Type II standard PC Flash Cards, including ATA Flash cards (3 Mb to 170 Mb). The slot is labeled /A:.

Nortel supplies PC Card adaptors that enable CompactFlash cards to be used in the slot.

**WARNING**

Do not format the PC Card by using a Windows application. As well, only format the PC Card using the type of card on which it is running. For example, a PC Card formatted using a Small System Controller (SSC) card is only readable by the SSC card. It is not readable by the ITG-P 24-port card or the Media Card. A PC Card formatted using a Voice Gateway Media Card (ITG-P 24-port card or Media Card) is only readable by another Voice Gateway Media Card. It is not readable by the SSC card.

MAC address label

The MAC address label on the card faceplate is labeled ETHERNET ADDRESS. It shows the TLAN and ELAN network interface MAC addresses. The Management/ELAN network interface MAC address for each card is assigned during manufacturing and is unchangeable. The MAC address label on the Media Card is similar to the following example:

ETHERNET ADDRESS

TLAN

00:60:38:BD:C9:9C

ELAN

00:60:38:BD:C9:9D

Ethernet activity LEDs

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

1. 100 (100BaseT)
2. 10 (10BaseT)
3. A (Activity)

Maintenance hex display

This is a four-digit LED-based hexadecimal display that provides the role of the card. It also provides an indication of fault conditions and the progress of PC Card-based software upgrades or backups.

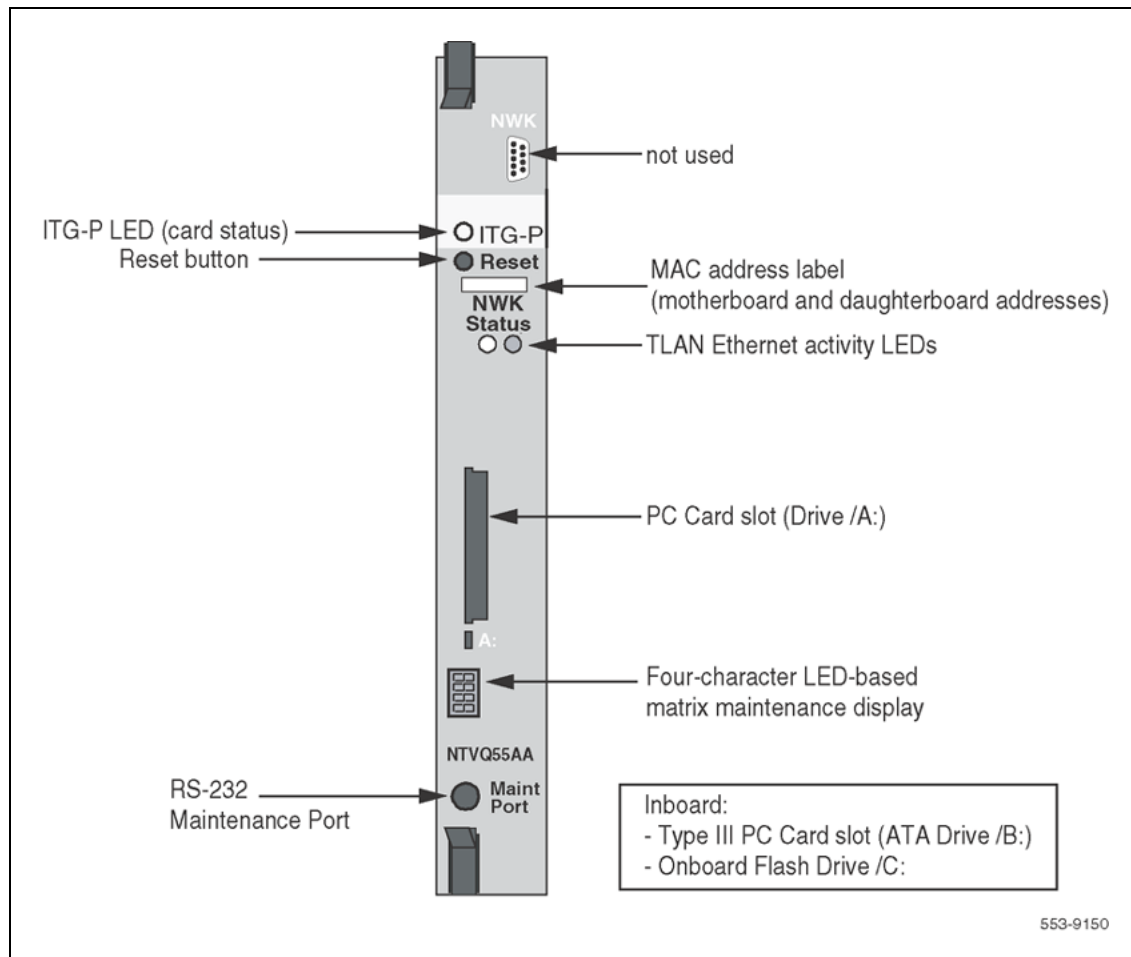
RS-232 Maintenance Port

The Media Card faceplate provides a female eight-pin mini-DIN serial maintenance port connection. The faceplate on the card is labeled J2.

ITG-P 24-port card controls, indicators, and connectors

Figure 3 "ITG-P 24-port card faceplate" (page 30) shows the ITG-P 24-port card faceplate components.

Figure 3
ITG-P 24-port card faceplate

**Faceplate components**

The components on the faceplate of the ITG-P 24-port card are described in the following sections.

NWK

The faceplate connector labeled NWK is a nine-pin, subminiature D-type connector. The connector is not used for the IP Line application.

**WARNING**

The NWK connector looks like a nine-pin serial connector. Do not connect a serial cable or any other cable to it. If a cable is connected to the NWK connector, the TLAN network interface is disabled.

ITG-P LED (card status)

The red status faceplate LED indicates the enabled and 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.

Reset button

Press the Reset button to reset the card without having to cycle power to the card. This button is normally used after a software upgrade to the card or to clear a fault condition.

MAC address label

The MAC address label on the card faceplate shows the motherboard and daughterboard addresses. The ELAN network interface address corresponds to the Management MAC address. The Management MAC address for each card is assigned during manufacturing and is unchangeable. The ELAN network interface MAC address is the MOTHERBOARD Ethernet address found on the label. The MAC address label on the ITG-P 24-port line card is similar to the following example:

ETHERNET ADDRESS

MOTHERBOARD

00:60:38:8c:03:d5

DAUGHTERBOARD

00:60:38:01:b3:cb

TLAN network interface activity LEDs (labeled NWK Status LEDs)

The two NWK Status LEDs display TLAN network interface activity.

- Green—the LED is on if the carrier (link pulse) is received from the TLAN network interface switch.
- Yellow—the LED flashes when there is data activity on the TLAN network interface. During heavy traffic, the yellow LED can stay continuously lit.

There are no Ethernet status LEDs for the ELAN network interface.

PC Card slots

The ITG-P 24-port card has one faceplate PC Card slot (designated Drive /A:). It is used for optional maintenance. The ITG-P 24-port card also has one unused inboard slot (designated Drive /B:). The PC Card slots support high-capacity PC flash memory cards.

**WARNING**

Do not format the PC Card by using a Windows application. As well, only format the PC Card using the type of card on which it runs. For example, a PC Card formatted using a Small System Controller (SSC) card is only readable by the SSC card. It is not readable by the ITG-P 24-port card or the Media Card. A PC Card formatted using a Voice Gateway Media Card (ITG-P 24-port card or Media Card) is only readable by another Voice Gateway Media Card. It is not readable by the SSC card.

Matrix maintenance display

A four-character, LED-based dot matrix display shows the maintenance status fault codes and other card state information. For a list of the fault codes, see [Table 82 "ITG-P 24-port line card faceplate maintenance display codes" \(page 402\)](#) and [Table 83 "Media Card faceplate maintenance display codes" \(page 403\)](#).

RS-232 maintenance port

The ITG-P 24-port line card faceplate provides a female eight-pin mini-DIN serial maintenance port connection, labeled Maint Port. An alternative connection to the faceplate serial maintenance port exists on the NTMF94EA I/O panel breakout cable.

**CAUTION**

Do not connect maintenance terminals or modems to the faceplate and I/O panel DB-9 male serial maintenance port at the same time.

Backplane interfaces

The backplane provides connections to the following:

- ELAN network interface
- TLAN network interface
- alternate connection to the DS-30X serial maintenance port
- Card LAN interface connectors

DS-30X voice/signaling

The DS-30X serial maintenance port carries Pulse Code Modulation (PCM) voice and proprietary signaling on the IPE backplane between the ITG-P 24-port card and the Intelligent Peripheral Equipment Controller (XPEC).

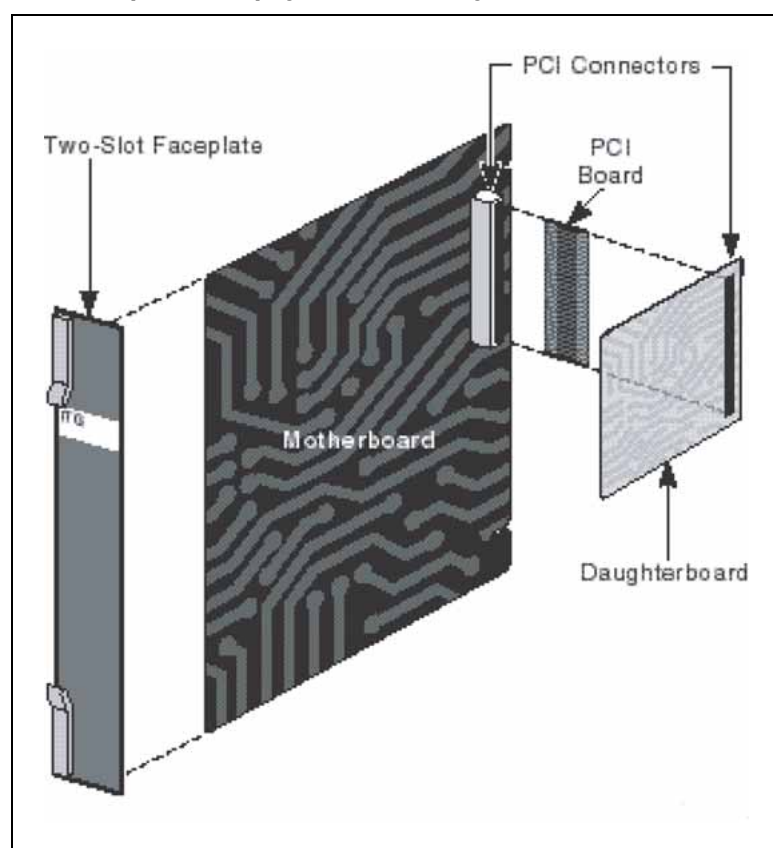
Card LAN

The card LAN carries card polling and initialization messages on the IPE backplane between the ITG-P 24-port card and the Intelligent Peripheral Equipment Controller (XPEC).

Assembly description

The ITG-P 24-port card assembly is a two-slot motherboard and daughterboard combination. A PCI interconnect board connects the motherboard and the DSP daughterboard. See [Figure 4 "ITG-P 24-port card physical assembly"](#) (page 33).

Figure 4
ITG-P 24-port card physical assembly

**Media Card 32S**

The Media Card 32S card (NTDW65AA) provides the following features:

- Secure Real-time Transport Protocol (SRTP)

- two Digital Signal Processors (DSP), based on an ARM processor
- channel density of 32 ports

Secure Real-time Transport Protocol

The Media Card 32S card uses Secure Real-time Transport Protocol (SRTP) to secure the IP media path between the card and the Nortel Phase II IP Phones, IP Phone 1110, IP Phone 1120E, IP Phone 1140E, IP Phone 1150E, another Media Card 32S card, or a DSP daughterboard. When Media Security is configured to On, the Call Server sends a message to the Voice Gateway software on the Media Card 32S card to activate SRTP for the media connection established for that call.

Media Security is configured by the system administrator.

For information about SRTP, see *IP Phones Fundamentals (NN43001-368)* and *System Management Reference (NN43001-600)*.

Processors Two separate processors on the MC 32S card are known as the Control and Signaling Processor (CSP) and the Media Stream Processor (MSP). The CSP runs application and signaling code, whereas the MSP processes the media streams.

[Table 5 "Files downloaded to the MC 32S card" \(page 34\)](#) lists the file names and paths for files that are downloaded from the Signaling Server to the MC 32S card.

Table 5
Files downloaded to the MC 32S card

File name	Path on Signaling Server	Path on MC 32S card	Description
IPL5.00XX.mc32s	/u/fw	/pl	Software binaries
bootp.tab	/u/config	/u/config	bootp parameter file
config.ini	/u/config	/u/config	config file

The software for the MC 32S consists of five files, which are located in the IPL5.00XX.mc32s zipped file stored on the Signaling Server. All Gold versions of firmware are loaded on the MC 32S when the card is shipped from the factory. The Gold Boot Code, the upgradeable Boot Code, the Gold MSP Image, the Gold VxWorks Kernel for CSP Image, the Gold App Image, and the upgradeable Field-programmable Gate Array (FPGA) image

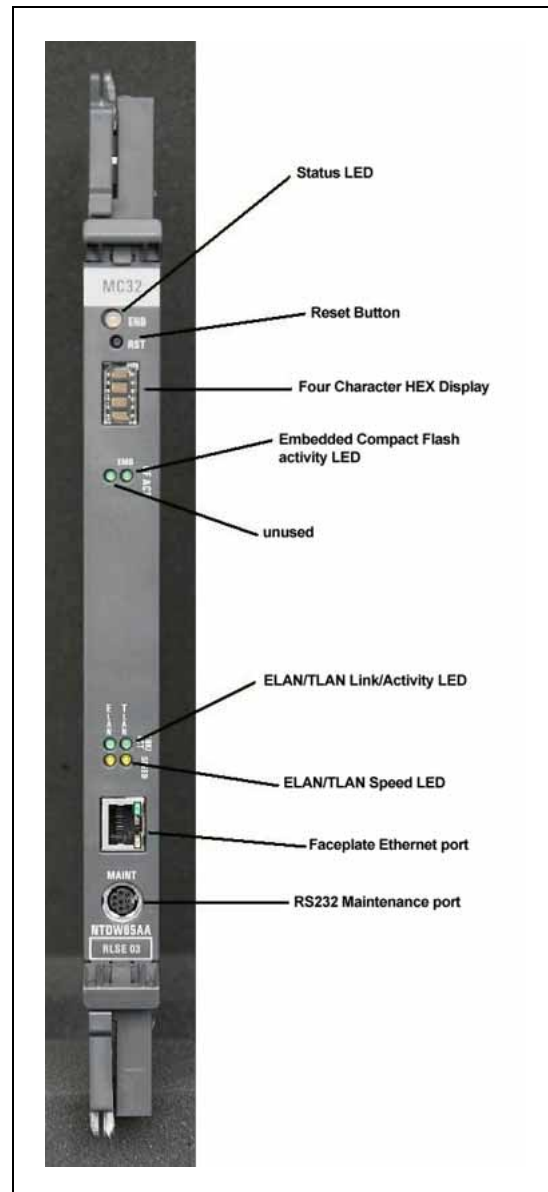
are stored in separate areas of the MC 32S FLASH memory. A new load can be programmed into the appropriate area of FLASH memory under software control.

Table 6
Files within the zipped file

File name	Description
bootrom.bin	MC 32S boot code image
mainos.sys	VxWorks 5.5 Kernel image for the Control and Signaling Processor (CSP). The CSP runs the application and signaling code.
mainos.sym	mainos.sys and mainos.sym files form the CSP image
ldvoice.axf	Media Stream Processor (MSP) load. The MSP runs the media stream processing code. This load is a binary image.
fpga.xsvf	MC 32S board FPGA load

Media Card 32S card controls, indicators, and connectors [Figure 5](#)
["MC32S card faceplate" \(page 36\)](#)

Figure 5
Media Card 32S card faceplate



Faceplate components The components on the faceplate of the MC 32S card are described in the following sections.

Reset button

Use the Reset button on the faceplate to manually reset the card without cycling power to it. The Reset button is used to reboot the card after a software upgrade or to clear a fault condition.

Enable LED

The faceplate red LED indicates the following:

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

Ethernet port

The Ethernet port is used for debugging. It connects to the six-ports layer-2 switch through port three on the card and is mirrored to any other ports of the layer 2-switch.

Four character LED display

This is a four-digit LED-based hexadecimal display that provides the role of the card. It also provides an indication of fault conditions and the progress of PC Card-based software upgrades or backups.

Ethernet activity LEDs

The faceplate contains two Ethernet activity LEDs: one for the ELAN network interface and one for the TLAN network interface. The LEDs indicate the following links on the ELAN network interface and TLAN network interface:

- Link Activity
- Speed

RS-232 Maintenance port

The Media Card 32S card faceplate provides a female eight-pin mini-DIN serial maintenance port connection.

Functional description of the Voice Gateway Media Cards

The Media Cards and ITG-P 24-port line card perform three separate functions, depending on the system in which the card is located, and the type of card:

1. The card acts as a gateway between the circuit-switched voice network and the IP network.
2. The card acts as a Line Terminal Proxy Server (LTPS) or virtual line card for the IP Phones.
3. The Media Card 32S card provides Secure Real-time Transport Protocol (SRTP) to secure the IP media path between the DSP channels and the card.

Gateway functional description

The Gateway performs the following functions:

- registers with the system using the TN Registration messages
- accepts commands from the system to connect or disconnect the audio channel
- uses Real-time Transport Protocol (RTP) and Real-time Control Protocol (RTCP) to transport audio between the gateway and the IP Phone or another gateway
- encodes and decodes audio from PCM to and from the IP Phone format
- provides echo cancellation for the speaker on IP Phones for echoes that originate in the circuit-switched voice network (not applicable to the IP Softphone 2050 or MVC 2050, as they have no handsfree capability)

Gateway functionality on the CS 1000 systems

A Signaling Server is always present in the CS 1000 systems. The LTPS executes on the Signaling Server, and the Voice Gateway executes on the Voice Gateway Media Cards and DSP daughterboards. The Voice Gateway Media Cards only provide the voice gateway access.

Active Master

The LTPS maintains a count of the number of IP Phones registered to the card. Each IP Telephony node has one active Master. The active Master broadcasts to all LTPS and requests a response if it has room for another IP Phone.

IP Phone registration

This section describes the maximum number of IP Phones that can register to an LTPS in a CS 1000 system.

IP Phone registration on a CS 1000 system

On a CS 1000 system, the IP Phones register with the LTPS on the Signaling Server. If more than one Signaling Server exists, the IP Phone registrations are distributed equally among the Signaling Servers to aid in load balancing.

If the primary Signaling Server fails, a secondary Signaling Server takes over (if it exists), and the IP Phones that are registered with the failed Signaling Server re-register with the LTPS on secondary Signaling Server. If no other Signaling Servers exist or if the Signaling Servers fail, the IP Phones register with the LTPS on the Voice Gateway Media Cards.

ATTENTION

Each Signaling Server supports the registration of up to 5000 IP Phones.

For more information about Signaling Server failure and redundancy, see *Communication Server 1000M and Meridian 1 Small System Planning and Engineering (NN43011-220)* and *Signaling Server Installation and Commissioning (NN43001-312)*.

Interactions with IP Phones

The following information describes the process by which an IP Phone registers and unregisters with a CS 1000 system.

Registration

[Table 7 "Registration process" \(page 39\)](#) describes the registration process.

Table 7
Registration process

Step	Description
1	The IP Phone receives the IP address of the Connect Server (colocated with the LTPS) through either DHCP or manual configuration.
2	The IP Phone contacts the Connect Server.
3	The Connect Server instructs the IP Phone to display a message on its display screen requesting the customer IP Telephony node number and TN.
4	The node number and TN are entered. The Connect Server redirects the IP Phone to the Node Master.
5	The IP Phone contacts the Node Master. The Node Master redirects the IP Phone to the LTPS.
6	The IP Phone contacts the LTPS.
7	If the IP Phone is valid, the LTPS registers it with the system.

Unregistration

[Table 8 "Unregistration process" \(page 39\)](#) describes the unregistration process.

Table 8
Unregistration process

Step	Description
1	If the LTPS detects a loss of connection with one of its registered IP Phones, it logs the event.
2	The LTPS then sends an unregister message to the system for that IP Phone.

Signaling and messaging

The IP Line application sends Scan and Signaling Distribution (SSD) messages to the Call Server through the system ELAN subnet. When tone service is provided, the service is signaled to the LTPS by using new SSD messages sent through the ELAN subnet.

Signaling protocols

The signaling protocol between the IP Phone and the IP Telephony node is the Unified Networks IP Stimulus Protocol (UNISim). The Reliable User Datagram Protocol (RUDP) is the transport protocol.

RUDP

RUDP is used for:

- signaling between the Call Server and the LTPS
- signaling between the IP Telephony node and the IP Phones

For more information, see ["ELAN TCP transport" \(page 41\)](#).

Description

Signaling messages between the LTPS and IP Phones use RUDP. Each RUDP connection is distinguished by its IP address and port number. RUDP is another layer on top of User Datagram Protocol (UDP). RUDP is proprietary to Nortel.

The features of RUDP are as follows:

- provides reliable communication system over a network
- packets are resent if an acknowledgement message (ACK) is not received following a time-out
- messages arrive in the correct sequence
- duplicate messages are ignored
- loss of contact detection

When a data sequence is packetized and sent from source A to receiver B, RUDP adds a number to each packet header to indicate its order in the sequence.

- If the packet is successfully transmitted to B, B sends back an ACK to A, acknowledging that the packet has been received.
- If A receives no message within a configured time, it retransmits the packet.
- If B receives a packet without having first received its predecessor, it discards the packet and all subsequent packets, and a NAK (no

acknowledge) message, which includes the number of the missed packet, is sent to A. A retransmits the first missed packet and continues.

UNISlim

The Unified Network IP Stimulus protocol (UNISlim) is the single point of contact between the various server components and the IP Phone.

UNISlim is the stimulus-based protocol used for communication between an IP Phone and an LTPS on the Voice Gateway Media Card or Signaling Server.

Secure Real-time Transport Protocol

The Media Card 32S card uses Secure Real-time Transport Protocol (SRTP) to secure the IP media path between the card and the Nortel Phase II IP Phones, IP Phone 1110, IP Phone 1120E, IP Phone 1140E, or IP Phone 1150E, or another Media Card 32S card, or a DSP daughterboard. When Media Security is configured to On, the Call Server sends a message to the Voice Gateway software on the Media Card 32S card to activate SRTP for the media connection established for that call.

Media Security is configured by the system administrator.

For information about SRTP, see *IP Phones Fundamentals (NN43001-368)* and *System Management Reference (NN43001-600)*.

ELAN TCP transport

Although TCP is used for the signaling protocol between the Call Server and the Voice Gateway Media Card, RUDP remains for the Keep Alive mechanism for the link. This means that RUDP messages are exchanged to maintain the link status between the Call Server and the Signaling Server or the Voice Gateway Media Card.

The TCP protocol enables messages to be bundled. Unlike the RUDP transport that creates a separate message for every signaling message (such as display updates or key messages), the TCP transport bundles a number of messages and sends them as one packet.

Handshaking is added to the Call Server and IP Line software so that the TCP functionality is automatically enabled. A software version check is performed by the IP Line application each time before it attempts to establish a TCP link with the CS 1000 CPUs. TCP transports messages, whereas RUDP establishes and maintains the link.

The IP Line software version must match the Call Server software version; otherwise, IP Line terminates the link and logs an error message.

Virtual superloops, virtual TNs, and physical TNs

Virtual TNs (VTNs) enable configuration of service data for an IP Phone, such as key layout and class of service, without requiring the IP Phone to be dedicated (hard-wired) to a given TN on the Voice Gateway Media Card.

The concentration of IP Phones is made possible by dynamically allocating a port (also referred to as a physical TN) of the Voice Gateway Media Card for a circuit-switched-to-IP Phone call. All system speech path management is done with physical TNs instead of virtual TNs. Calls are made between an IP Phone and circuit-switched telephone or trunks using the full CS 1000 feature set. Digital Signal Processor (DSP) channels are allocated dynamically for this type of call to perform the encoding or decoding required to connect the IP Phone to the circuit-switched network.

The IP Phones (virtual TNs) are defined on virtual superloops. To create an IP Phone using VTNs, create a virtual superloop in LD 97 or in Element Manager. To create the virtual superloop in Element Manager, click System > Core Equipment > Superloops in the Element Manager navigator.

A virtual superloop is a hybrid of real and phantom superloops. Like phantom superloops, no hardware (for example, XPEC or line card) is used to define and enable units on a virtual superloop. As with real superloops, virtual superloops use the time slot map to handle IP Phone (virtual TNs)-to-IP Phone calls.

You can configure up to 1024 VTNs on a single virtual superloop for Large Systems, CS 1000M Cabinet and CS 1000M Chassis systems, and CS 1000E systems.

Each ITG-P 24-port card provides 24 physical TNs, and each Media Card 32-port card provides 32 physical TNs. The physical TNs are the gateway channels (DSP ports), which provide 128 channels. The channels (ports) on the Voice Gateway Media Cards are pooled resources.

Configure the physical TNs (IPTN) in LD 14. They appear as VGW data blocks.

Licenses

There are three types of licenses:

- Temporary IP User Licence for IP Phones configured for Branch Office or Network wide redundancy
- Basic IP User License for the IP Phone 2001, IP Audio Conference Phone 2033, and IP Phone 1110
- IP User License for the IP Phone 2002, IP Phone 2004, IP Phone 2007, IP Phone 1120E, IP Phone 1140E, IP Phone 1150E, IP Softphone

2050, Mobile Voice Client (MVC) 2050, WLAN Handset 2210, WLAN Handset 2211, WLAN Handset 2212, WLAN Handset 6120, and WLAN Handset 6140

If insufficient Temporary IP User Licenses are available, Basic IP User License and IP User License can be used.

If insufficient Basic IP User Licenses are available for the IP Phone 2001, IP Audio Conference Phone 2033, and IP Phone 1110, then the IP User License can also be used.

If there are no Basic IP User Licenses available for the IP Phone 2001, IP Audio Conference Phone 2033, and IP Phone 1110, and IP User Licenses are used, an error message is generated:

"SCH1976: Basic IP User License counter has reached its maximum value. IP User License was used to configure <data> basic IP Phone type 2001. Action: (Recommended) Purchase additional Basic IP User Licenses for IP Phones type 2001, instead of using higher-priced IP User Licenses."

Each time an IP Phone is configured, the system TN ISM counter is decremented.

Customers must purchase one license for each IP Phone installed on CS 1000 system. A new license uses the existing keycode to enable the IP Phone in the system software. The default is zero.

To expand the license limits for the IP Phones, order and install a new CS 1000 keycode. See *Features and Services Fundamentals—Book 4 of 6 (NN43001-106)*.

ATTENTION

Individual licenses are not supported on Functional Pricing. With Functional Pricing, licenses are provisioned in blocks of eight.

License limits

The total number of TNs configured with Temporary IP User Licenses must not exceed 100. The total number of TNs configured with Basic IP User Licenses must not exceed 32 767. The total number of TNs configured with IP User Licenses must not exceed 32 767. The total number of IP phones configured within the system must not exceed the allowable system capacity limit controlled by customer keycodes.

Zones

To optimize IP Line traffic bandwidth use between different locations, the IP Line network is divided into zones, representing different topographical areas of the network. All IP Phones and IP Line ports are assigned a zone number, which indicates the zone to which they belong.

When a call is made, the codecs that are used vary, depending on which zones the caller and receiver are in.

By default, when a zone is created in LD 117 or in Element Manager:

- codecs are selected to optimize voice quality (BQ - Best Quality) for connections between units in the same zone.
- codecs are selected to optimize voice quality (BQ - Best Quality) for connections between units in different zones.

Access zones in Element Manager by clicking IP Network > Zones in the Element Manager navigator.

Configure each zone to:

- optimize either voice quality (BQ) or bandwidth usage (BB - Best Bandwidth) for calls between users in that zone
- optimize either voice quality or bandwidth usage within a zone and all traffic going out of a zone

For more information about shared and private zones, see ["Private Zone configuration" \(page 170\)](#). For more information about zones and virtual trunks, see *IP Trunk Fundamentals (NN43001-563)*. For more information about zones and branch office locations, see *Branch Office Installation and Commissioning (NN43001-314)*. For information about Adaptive Bandwidth Management and Alternative Call Routing, see *Branch Office Installation and Commissioning (NN43001-314)*.

Administration

The Voice Gateway Media Card is administered using multiple management interfaces, including the following:

- Web browser interface provided by Element Manager—Element Manager is used to administer Voice Gateway Media Cards in the systems that use a Signaling Server.
- Command Line Interface (CLI)—The CLI prompt, which displays depends on the type of Voice Gateway Media Card in the system. IPL> prompt displays for the ITG-P 24-port line card, and Media Card 32-port. oam> or LBD> prompt displays for the Media Card 32S card.
- Administration and maintenance overlays of Call Servers.

- IP Line application GUI provided by TM 3.1. TM 3.1 is used to obtain OM reports only.

TM 3.1

IP Line uses TM 3.1 to obtain OM reports only.

Element Manager

Element Manager is a resident Web-based user interface used to configure and maintain CS 1000 components. Element Manager Web interface enables IP Line to be configured and managed from a Web browser.

The Element Manager Web server resides on the Signaling Server or within Enterprise Common Manager (ECM) framework. For further information about Element Manager residing on a Signaling Server, see *Element Manager System Reference—Administration (NN43001-632)*.

Description

Element Manager is a simple and user-friendly Web-based interface that supports a broad range of system management tasks, including:

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

Element Manager has many features to help administrators manage systems with greater efficiency. Examples are as follows:

- Web pages provide a single point-of-access to parameters that are traditionally available through multiple overlays.
- Parameters are presented in logical groups to increase ease-of-use and speed-of-access.
- Administrators see information that relates directly to the task at hand by using the hide or show information option.
- Full-text descriptions of parameters and acronyms help administrators reduce configuration errors.

- Configuration screens offer preselected defaults, drop-down lists, check boxes, and range values to simplify response selection.

You can access Element Manager directly through a Web browser or Telephony Manager 3.1 (TM 3.1). The TM navigator includes integrated links to each network system and their respective instances of Element Manager.

Command Line Interface

The Command Line Interface (CLI) provides a text-based interface to perform specific Signaling Server and Voice Gateway Media Card installation, configuration, administration, and maintenance functions.

Access

Establish a CLI session by connecting a Teletype (TTY) or PC to the card serial port or Telnet through the ELAN or TLAN network interface IP address.

For more information about the CLI commands, see ["IP Line CLI commands" \(page 420\)](#).

Overlays

For information about the overlays, see *Software Input Output Administration (NN43001-611)*.

Features

Contents

This section contains the following topics:

- "Introduction" (page 19)
- "Active Call Failover for IP Phones" (page 55)
- "DSP peg counter for CS 1000E systems" (page 78)
- "Enhanced UNISTim Firmware Download for IP Phones" (page 79)
- "Firmware download using UNISTim FTP" (page 107)
- "NAT Traversal feature" (page 114)
- "Personal Directory, Callers List, and Redial List" (page 132)
- "IP Call Recording" (page 132)
- "pbxLink connection failure detection" (page 141)
- "LD 117 STAT SERV" (page 142)
- "IP Phone support" (page 146)
- "Corporate Directory" (page 131)
- "Element Manager support" (page 159)
- "Call Statistics collection" (page 160)
- "Programmable line/DN feature keys (self-labeled)" (page 169)
- "Private Zone configuration" (page 170)
- "Run-time configuration changes" (page 173)
- "Network wide Virtual Office" (page 174)
- "Branch Office and Media Gateway 1000B" (page 178)
- "802.1Q support" (page 179)
- "Data Path Capture tool" (page 182)
- "IP Phone firmware" (page 182)
- "Graceful Disable" (page 183)

- "Hardware watchdog timer" (page 184)
- "Codecs" (page 185)
- "Set type checking and blocking" (page 186)
- "Enhanced Redundancy for IP Line nodes" (page 187)

Introduction

Table 9 "IP Line 5.0 feature support" (page 48) outlines the IP Line features available for CS 1000 systems with CS 1000 Release 5.0 software.

Table 9
IP Line 5.0 feature support

Feature	CS 1000M	CS 1000E
Support for Media Card	Yes	Yes
Support for Element Manager	Yes	Yes
Support for Signaling Server	Yes	Yes
Support for the following IP Phones:	Yes	Yes
• IP Phone 2001 • IP Phone 2002 • IP Phone 2004 • IP Phone 2007 • IP Audio Conference Phone 2033 • IP Phone 1110 • IP Phone 1120E • IP Phone 1140E • IP Phone 1150E • WLAN Handset 2210 • WLAN Handset 2211 • WLAN Handset 2212 • WLAN Handset 6120 • WLAN Handset 6140		
Node level patching is not provided by TM 3.1. The patching CLI command of the Media Card 32-port card, MC 32S card, and ITG-Pentium 24-port line card can be used.		

Feature	CS 1000M	CS 1000E
Support for the following software clients:	Yes	Yes
- IP Softphone 2050 - Mobile Voice Client (MVC) 2050		
Support for the IP Phone Key Expansion Module (KEM)	Yes	Yes
Support for the Expansion Module for IP Phone 1100 Series (Expansion Module)	Yes	Yes
Live Dialpad	Yes	Yes
Unicode support	Yes	Yes
IP Client cookies	Yes	Yes
New IP Phone Types	Yes	Yes
Active Call Failover	Yes	Yes
DSP peg counter for the CS 1000E	No	Yes
Enhanced UNISTim firmware downloads for IP Phones	Yes	Yes
Support for external server applications	Yes	Yes
Enhanced VLAN support on Phase II IP Phones; support for Voice VLAN hardware filter providing enhanced traffic control on IP Phone and PC port	Yes	Yes
Network Address Translation (NAT) Traversal	Yes	Yes
Personal Directory, Callers List, and Redial List with password protection	Yes	Yes
UNISTim File Transfer Protocol (UFTP) for IP Phone firmware downloads	Yes	Yes
IP Call Recording	Yes	Yes
pbxLink connection failure detection	Yes	Yes
Dynamic Loss Plan	Yes	Yes
Network-wide Virtual Office	Yes	Yes
Patching	Partial	Yes
802.1Q support	Yes	Yes
Corporate Directory	Yes	Yes
Data Path Capture tool	Yes	Yes
Self-labeled line/programmable feature keys	Yes	Yes
Private Zone	Yes	Yes
Node level patching is not provided by TM 3.1. The patching CLI command of the Media Card 32-port card, MC 32S card, and ITG-Pentium 24-port line card can be used.		

Feature	CS 1000M	CS 1000E
Graceful TPS Disable	Yes	Yes
Run-time download	Yes	Yes
Watchdog Timer	Yes	Yes
Password Guessing Protection	Yes	Yes
Ringer and buzzer volume adjustment	Yes	Yes
Set-based installation	Yes (Small Systems only)	Yes
Maintenance Audit enhancement	Yes	Yes
Multi-language support	Yes	Yes
Enhanced Redundancy for IP Line nodes	Yes	Yes
IP Softphone 2050 user-selectable codec (not applicable to MVC 2050 as it only supports G.711 codec)	Yes	Yes
Node level patching is not provided by TM 3.1. The patching CLI command of the Media Card 32-port card, MC 32S card, and ITG-Pentium 24-port line card can be used.		

Live Dialpad

IP Line provides support for the Live Dialpad feature. Live Dialpad activates the primary line/DN key when the user makes a call by pressing the keys on the dialpad without lifting the handset, pressing a line/DN key or the handsfree key.

The Live Dialpad feature is supported on the following IP Phones:

- IP Phone 2001
- IP Phone 2002
- IP Phone 2004
- IP Phone 2007
- IP Audio Conference Phone 2033
- IP Softphone 2050
- WLAN Handset 2210/2211/2212/6120/6140
- IP Phone 1110
- IP Phone 1120E
- IP Phone 1140E
- IP Phone 1150E

Live Dialpad is enabled and disabled in the Telephone Options menu on the IP Phone. Feature processing is performed on the LTPS. The on or off state for the Live Dialpad feature is stored on the Call Server.

Diagnostics

Output of vxWorksShell command `ed2setShow` contains a state of the Live Dialpad feature.

Unicode support

IP Line provides Unicode capabilities on the IP Phone 2007, IP Phone 1110, IP Phone 1120E, IP Phone 1140E, and IP Phone 1150E. Using the Unicode feature the Call Server can easily display multilingual text on the IP Phones for the following languages:

- Japanese
- Greek
- Traditional Chinese
- Simplified Chinese
- Arabic
- Korean
- Hebrew

These languages are not available on IP Phones without Unicode capabilities. Japanese is available in Katakana version.

If an IP Phone without Unicode support registers to a TN with Unicode-only language configured, the IP Phone falls back to English. The information stored on the Call Server is not changed unless the user explicitly changes the language.

Personal Directory, Callers List, Redial List, and user-defined feature key labels support Unicode. Corporate Directory and Calling Party Name Display (CPND) do not support Unicode.

Pop-up and USB keyboard support

Only a limited subset of Unicode characters can be input using the dialpad. The Special Characters Input Screen includes the character set which is used by the current language. For languages with a large amount of characters, such as Traditional Chinese, Japanese, and Korean, localized input is not supported. The Pop-up and USB keyboard supports English input only.

Language synchronization

Language synchronization is handled strictly through UNISTim messaging. If the IP Phone receives an Assign IT Language from the Call Server, the IP Phone changes its local prompts to match the specified language. If a user sets the IP Phone language using the Telephone Options menu, the IP Phone sends a UNISTim Assign NI Language message to the Call Server. The Call Server then synchronizes its language with the IP Phone. The Call Server can use the Query IT Language message at any time to determine the current language of the IP Phone. If there is no default or programmed mapping for a language specified by the Call Server, then the IP Phone uses the same language that is previously used. It is up to the Call Server to only specify languages for which the IP Phone has fonts and font mappings. The Call Server retrieves a list of language codes using the Display Manager Query Supported IT Languages.

Virtual Office interaction

Virtual Office log on can be performed from an IP Phone without Unicode support to an IP Phone with Unicode entries in the Personal Directory. <Unicode name> is displayed instead of the name of the entry. The entry cannot be edited, but it can be deleted.

IP Client cookies

IP Client cookies provide a transparent transfer of data from the Call Server to third-party applications, for example, Citrix AG. The cookies are a set of UTF-8 variable names and values, which are duplicated and synchronized between the LTPS and the IP Phone. IP Line uses public cookies which are visible to both the IP Phone and third-party applications. IP Client cookies are not supported on Nortel Phase I IP Phones, and third-party IP Phones, such as WLAN Handset 2210/2211/2212/6120/6140, and IP Audio Conference Phone 2033.

Table 10
Cookie definitions

Cookie name	Description
PrimeDN	A string of digits containing the current primary DN of the IP Phone.
AgentPosition	A string of digits containing the current agent position of the IP Phone. This string is empty if the agent is not logged on.
CallState	A UTF-8 string indicating the current call processing state of the IP Phone. The following are possible values: - BUSY—an active call is established - IDLE—no active calls (there can be calls on hold) - RINGING—IP Phone is ringing
CustNo	A string of digits indicating the IP Phone customer number.

Zone	A string of digits indicating the IP Phone zone.
VPNI	A string of digits containing the Virtual Private Network Identifier configured for the IP Phone.
TN	UTF-8 string containing the TN currently associated with the IP Phone in hexadecimal format. The maximum number of TNs is FFFF.
Although cookie names and values are UTF-8 strings, it is not necessary for the IP Phone to support Unicode.	

Output of the `ed2setShow` command shows the contents of the IP Phone cookie storage associated with the IP Phone. This command is only available from the VxWorksShell.

New IP Phone Types

IP Line introduces support for new TN types. This feature provides the following functionality:

- unique TN types for each IP Phone
- special emulation mode for IP Phones that are not known to the TPS
- automatic and manual IP Phone TN type conversion
- existing IP Phone TN types are renamed to match the brand name of the IP Phone
- enhanced Model Names support is accessed from LD 20 and TM 3.1

Unique TN Types for existing IP Phones

The names of existing IP Phone TN types are updated with a naming convention to match the brand name of the IP Phone.

Table 11
CS 1000 Release 5.0 TN Type naming convention

IP Phone model name	CS 1000 Release 4.5 TN_TYPE	CS 1000 Release 5.0 TN_TYPE
IP Phone 2001	i2001	2001P2
IP Phone 2002 Phase I	i2002	2002P1
IP Phone 2002 Phase II	i2002	2002P2
IP Phone 2004 Phase 0/I	i2004	2004P1
IP Phone 2004 Phase II	i2004	2004P2
IP Audio Conference Phone 2033	i2001	2033
IP Softphone 2050	i2050	2050PC
Mobile Voice Client 2050	i2050	2050MC

WLAN Handset 2210	i2004	2210
WLAN Handset 2211	i2004	2211
WLAN Handset 2212	i2004	2212
WLAN Handset 6120	Not applicable	6120
WLAN Handset 6140	Not applicable	6140
IP Phone 2007	i2004	2007
IP Phone 1110	Not applicable	1110
IP Phone 1120E	i2002	1120
IP Phone 1140E	i2004	1140
IP Phone 1150E	IPACD	1150

Emulation Mode

During IP Phone registration, the LTPS determines the IP Phone TN Type (TN_TYPE) by looking up its User Interface capabilities (UI_TYPE) and Firmware ID (FW_ID) in a mapping table. The mapping table is used to map the IP Phone UI_TYPE and FW_ID with TN_TYPE. If an IP Phone has a known UI_TYPE but an unknown UI_TYPE and FW_ID combination, the IP Phone registers in Emulation Mode.

Use the `isetShow` command or LD 20 to list the IP Phones registered in Emulation Mode.

Automatic IP Phone TN conversion (Flexible Registration)

Flexible Registration Class of Service (CLS) for all IP Phones is configured in LD 11. Flexible Registration CLS can be set to one of the following values:

- FRA-Flexible Registration Allowed (default)
- FRU-Flexible Registration on Upgrade
- FRD-Flexible Registration Denied

Use LD 81 to list the IP Phone TNs which have Flexible Registration Allowed (FRA), Flexible Registration on Upgrade (FRU), and Flexible Registration Denied (FRD) CLS.

When the LTPS attempts to register an IP Phone with the Call Server, the following occurs:

1. If the TN has FRD CLS, the Call Server checks the IP Phone type against the TN type. Registration is rejected if the types do not match. Furthermore, the Call Server checks the Emulation Flag and blocks registration in the Emulation Mode.

2. If the TN has FRA CLS, the Call Server checks the IP Phone type against the TN type. If the types are compatible, the TN is converted, and the IP Phone registers.
3. If the TN has FRU CLS, the Call Server checks the IP Phone type against the VTN type. If the types are compatible, the TN is converted and the IP Phone registers. After the TN is converted, the Flexible Registration CLS is set to FRD. The Call Server checks the Emulation Flag and blocks registration in the Emulation Mode.

Manual IP Phone TN conversion

Manual IP Phone TN conversion lowers the administrative effort required to replace an IP Phone with another model while preserving the IP Phone features. Use LD 11 to convert an IP Phone TN to another IP Phone TN while preserving the IP Phone features.

Table 12
LD 11 IP Phone interface commands

Prompt	Response	Description
REQ	CHGTYP	Change the IP Phone TN type
TYPE	2004P1, 2004P2, 2002P1, 2002P2, 2001P2, 2050PC, 2050MC, 2033, 2210, 2211, 2212, 6120, 6140, 2007, 1120, 1140, 1150	Type of TN block to convert
TN	lscu	For Large Systems
NEWTYP	2004P1, 2004P2, 2002P1, 2002P2, 2001P2, 2050PC, 2050MC, 2033, 2210, 2211, 2212, 6120, 6140, 2007, 1110, 1120, 1140, 1150	TN_TYPE to convert The Call Server lists the features that are lost if the administrator proceeds.
PROCEED	YES No	Perform or reject the IP Phone TN conversion

Active Call Failover for IP Phones

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

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

IP/IP calls means both parties are IP Phones. IP/TDM calls means one party is an IP Phone and the other party is a TDM telephone or trunk.

- IP and IP/TDM calls survive Signaling Server restarts.

The IP/TDM call does not survive if the Voice Gateway Media Card with the DSP resource used for the call fails.

- IP and IP/TDM calls survive LTPS ELAN subnet failures.
- IP calls survive a Call Server cold start and Call Server failures in system configurations with a redundant Call Server of the following types
 - Media Gateway 1000B for a branch office configuration
 - Geographic Redundancy Secondary Call Server. The feature addresses the Primary Call Server failures.

IP Phone to IP Phone calls survive the Call Server failures listed above.

ATTENTION

IP Phone to Media Gateway calls through IP Peer virtual trunk routes are preserved on the TDM side of the Media Gateway, in some cases, when the IP Phone is redirected in ACF mode from the main office CS 1000 to the MG 1000B at the branch office location, or from the Geographic Redundancy Primary to the Secondary Call Server.

IP Phone to Media Gateway calls are preserved if the Media Gateway to which the call is established is not affected by the failure, or if there is cold restart of the Call Server that controls the Media Gateway where the IP Peer virtual trunk call is established.

- For Call Server call processor types CP PII, CP PIV, and CP-PM:
 - IP/IP calls survive a cold start on all systems.
 - IP/IP and IP/TDM calls survive a warm start on all systems.
 - Graceful switchover and graceful failover to the redundant Logical Call Processor (LCP) side of the Call Server makes the failure transparent and allows all the calls to survive without any loss.

When the IP Phone with an active call re-registers, the call data is rebuilt if the Call Server does not know about the call, using the internal IP Phone information.

The ACF feature for IP Phones meets Joint Interoperability Test Command (JITC) requirements if the LAN/WAN network is engineered to provide full redundancy: that is, if a LAN/WAN network component fails, an alternate path between the clients and LTPS server is provided.

Minimum requirements

The ACF feature for IP Phones has the following minimum requirements:

- Call Server must be running CS 1000 Release 4.5, or later software.
- IP Phones (including IP Softphone 2050) must support Unistim version 2.9. (Use the `isetShow` command to determine the Unistim version. One of the columns in the `isetShow` output is UNIStimVsn.)

ACF mode

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

The ACF mode preserves the following:

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

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

The IP Phone uses this new mode of re-registration only when the Call Server explicitly tells the IP Phone to do so. IP Phones clear all call information if they register to a Call Server or LTPS that does not support the ACF feature.

IP Phone ACF timer

It is possible that there may be an LTPS supporting the ACF feature and an LTPS that does not support the feature in the same system.

A situation can exist where it takes a long time to fix a failure and no failover Call Server is available. During this time, if the user released the call by pressing the Release key or hanging up the telephone, the call-associated resources are not used. The call-associated resources still exist on the Call Server because they are not released. To prevent this, the 10-minute Call Server ACF timer is introduced for each call. The timer prevents call processing-related resources from being unnecessarily used when an IP Phone that had an active call unregisters and never re-registers.

The timer is set if:

- the ACF call status is UNREGISTERED; that is, when both parties go offline.
- only one of the parties is offline, and the other party does not support disconnect supervision.

ACF scenarios

Table 13 "ACF behaviors" (page 58) describes ACF behavior in different scenarios.

Table 13
ACF behaviors

Scenario	Result
TLAN subnet failure - A call is established between IP Phones A and B registered with the same node. - TLAN subnet goes down. - The IP Phones detect the connection is lost and periodically try to re-register. - The TLAN subnet is up shortly (less than 10 minutes), or an election is called and another accessible LTPS node acquires the node IP address. The IP Phones re-register with the node again.	The call is not lost as the IP Phones re-register. In this scenario, the call exists on the Call Server during the failover time and has the following transitions: UNREGISTERED -> HALF-REGISTERED -> NO ACF
Signaling Server/Voice Gateway Media Card platform failure - A call is established between IP Phones A and B registered with the same node. - The LTPS node goes down. - The IP Phones detect the connection is lost and periodically try to re-register. - The LTPS node is up shortly (less than 10 minutes), or an election is called and another accessible LTPS node acquires the node IP address. The IP Phones re-register with the node again.	The call is not lost as the IP Phones re-register. The scenario is similar to the TLAN subnet failure, but the ACF call transition on the Call Server is instantaneous, because Offline events are generated in a group as the ELAN subnet goes down.
Call Server warm restart - A call is established between IP Phones A and B registered with the same Call Server. - The Call Server warm restart (INI) occurs. - The users of IP Phones A and B do not go on-hook or press any keys during the Call Server restart.	The call is not lost. The call is rebuilt after the warm restart and has the following transitions: UNREGISTERED->HALF REGISTERED->NO ACF. The transition is almost instantaneous because the Online messages are sent in a group as a response to the Sync Request.

Scenario	Result
Call Server cold restart - A call is established between IP Phones A and B registered with the same Call Server. - The Call Server cold restart (SYSLOAD) occurs. - The users of IP Phones A and B do not go on-hook or press any keys during the Call Server warm restart.	The call is not lost. The call cannot be rebuilt after the SYSLOAD. The PARTIAL REBUILT -> REBUILT transition is almost instant since the Online messages are sent in a group as a response to the Sync Request.
Main office failure for branch office (scenario 1) - Branch IP Phones A and B register with the Media Gateway 1000B and are redirected to the main office. - IP Phones A and B registered with the main office establish a call. - A serious main office failure occurs. The active Branch IP Phones cannot re-register with the main office and re-register with the branch office in local mode. IP Phone A re-registers in local mode first.	The call is not lost. The HALF REBUILT -> REBUILT transition occurs since the far end is known to the Call Server gateway to the Media Gateway 1000B.
Main office failure for branch office (scenario 2) - IP Phones A and B register with the Media Gateway 1000B and are redirected to the main office. - Branch office warm or cold starts. - Branch users A and B registered with the main office establish a call. - A serious main office failure occurs so the active branch IP Phones cannot re-register with the main office and they re-register with the Branch office in local mode. IP Phone A re-registers in local mode first.	The call is not lost. Although the branch office LTPS wrote the IP Phones A and B data to its RLM table when it redirected the IP Phones to the main office, the RLM data is lost and cannot be restored when the branch office restarts. The transition is similar to a Call Server cold start: PARTIAL REBUILT -> REBUILT.

Scenario	Result
Primary Call Server failure (WAN geographically redundant system) - A call is established between IP Phones A and B that are registered with the primary site in the geographically redundant system. - The primary site fails. - The IP Phones are re-registered with the secondary site. IP Phone A re-registers first.	The call is not lost. IP Phones can be configured in 2 ways: - Site 1 is the secondary site and Site 2 is not configured. In this case the scenario is the same as main office failure for branch office (scenario 1): the HALF REBUILT-> REBUILT transition. - IP Phones have Site 1 defined as the primary site while Site 2 is defined as the secondary site. Registration by Site 1 fails. In this case, the secondary site Call Server does not have the RLM entries for the re-registering IP Phones and the scenario is the same as main office failure for branch office (scenario 2): the PARTIAL REBUILT -> REBUILT transition.
Virtual Office logon failure (scenario 1) - IP Phone A logs into IP Phone C and establishes a call with IP Phone B. All three IP Phones are registered with the same Call Server. - TLAN subnet failure occurs. IP Phone A goes offline first, then IP Phone B. - Active IP Phones A and B re-register with the system when the TLAN subnet comes back up. IP Phone A re-registers first and then IP Phone B.	The call is not lost. The following ACF transitions occur: NO ACF -> PARTIAL REBUILT -> IDLE -> HALF REBUILT -> REBUILT

Scenario	Result
Virtual Office logon failure (scenario 2): - IP Phone A logs into IP Phone C and establishes a call with IP Phone B. All three IP Phones are registered with the same Call Server. - TLAN subnet failure occurs. IP Phone B goes offline first, then IP Phone A. - Active IP Phones A and B re-register with the system when the TLAN comes back up. IP Phone A re-registers first and then IP Phone B.	The call is not lost. The following ACF transitions occur: NO ACF -> HALF REGISTERED -> IDLE -> HALF REBUILT -> REBUILT
Virtual Office logon failure (scenario 3): - IP Phone A logs into IP Phone C and establishes a call with IP Phone B. All three IP Phones are registered with the same Call Server. - TLAN subnet failure occurs. IP Phones A and B fail and IP Phone C does not fail. - IP Phone C tries to log into its home TN before IP Phones A and B go offline.	IP Phone C cannot log into its home TN if another active IP Phone is logged on its TN. IP Phone C can log into its home TN only when the call register is released or becomes PARTIAL REBUILT. See Virtual Office login failure (scenario 1) and Virtual Office login failure (scenario 2).
Network TLAN subnet failure - IP Phone A has an IP Peer call with a remote user over a virtual trunk. - IP Phone A TLAN subnet connection fails. - Active IP Phone A re-registers with the Call Server when the TLAN subnet comes back up.	The call is not lost. The scenario is the same as if the far end were a local IP Phone. See TLAN subnet failure.
Network Call Server warm start - IP Phone A has an IP Peer call with a remote user over a virtual trunk. - The Call Server warm starts. - Active IP Phone A re-registers with the Call Server as the TLAN subnet comes back up.	The call is not lost. The scenario is the same as if the far end were a local IP Phone. See Call Server warm restart.

Scenario	Result
Network Call Server cold start - IP Phone A has an IP Peer call with a remote user over a virtual trunk. - The Call Server cold starts. - Active IP Phone A re-registers with the Call Server as the TLAN subnet comes back up.	The call is lost as the Call Server comes up.
Network branch office - Branch IP Phones A and B belong to different branches – Branch A and Branch B respectively. IP Phones A and B are registered on the main office Call Server. - A call is established between IP Phones A and B. - Main office Call Server failure occurs and IP Phones A and B register with their branches in local mode.	The call is not lost. The scenario for each branch is the same as the first 3 steps of Main office failure for branch office (scenario 2). Branch A does not know about IP Phone B and Branch B does not know about IP Phone A. Therefore, each branch builds the PARTIAL REBUILT call. Two local PARTIAL REBUILT calls exist on the branches as the IP Phones re-register in local mode. The calls are never transitioned to the REBUILT state and exist until the IP Phones release the call.
IP/TDM call with TLAN subnet failure - IP Phone A has a call with a TDM telephone or trunk B. - IP Phone A TLAN subnet connection fails. - Active IP Phone A re-registers with the Call Server as the TLAN subnet comes back up.	The call is not lost. The scenario is the same as TLAN subnet failure and Network TLAN subnet failure. The call has the following transitions: NO ACF -> HALF REGISTERED -> UNREGISTERED.
Network Call Server warm start - IP Phone A has an IP Peer call with a remote user over a virtual trunk. - The Call Server warm starts. - Active IP Phone A re-registers with the Call Server as the TLAN subnet comes back up.	The call is not lost. The scenario is same as if the far end were a local IP Phone. See Call Server warm restart.
Network Call Server cold start IP Phone A has an IP Peer call with a remote user over a virtual trunk.	The call is lost as the Call Server comes back up.

Scenario	Result
- The Call Server cold starts. - Active IP Phone A re-registers with the server as the TLAN subnet comes back up.	

Firmware downloads

If the IP Phone has an active media stream, the LTPS does not request the firmware download in order to avoid resetting the IP Phone and losing the call. Therefore, it is possible that a system has IP Phones with a mixture of firmware versions registered with it. The firmware can be downloaded later, after the idle IP Phone registers again or can be downloaded manually using appropriate CLI commands.

WLAN Handsets 2210/2211/2212/6120/6140

The Wireless LAN (WLAN) Handsets 2210/2211/2212/6120/6140 support Active Call Failover in the same manner as Phase II IP Phones if their firmware supports UNISim 2.9.

Operating parameters

IP Peer calls

IP Peer calls survive the following failure types:

- TLAN subnet failures.
- Signaling Server platform failures/restarts. When the Signaling Server reboots after the failure, all sessions are lost. Therefore, when the local IP Phone or far-end telephone releases the call, no RELEASE message is sent to the other party. The other party must go on-hook to become idle.
- Call Server warm starts.

IP Peer calls do not survive the Call Server cold start; all virtual trunks are idled as the Call Server comes back up after the cold start. In this case, the local IP Phone must go on-hook to become idle.

IP/TDM calls

IP/TDM calls do not survive a Call Server cold start; all DSP channels are closed as the Call Server comes back up after the cold start. In this case, the local IP Phone must go on-hook to become idle.

Dialing state

Only established calls survive failures. All calls having the DIALING state on the Call Server are released when an LTPS or signaling failure occurs that causes an IP Phone to unregister.

Calls that are ringing are handled as follows:

- If the IP Phone originating the ringing call unregisters, the call is released by the Call Server.
- If the IP Phone receiving the call unregisters, the call receives CFNA treatment if possible.

Held calls

From the ACF feature perspective, held calls are considered to be established. This means that the call is preserved on the Call Server despite TLAN subnet or LTPS failure. The IP Phone itself is unaware of the state of any held call.

Phase 0/1 IP Phones

Phase 0/1 phones do not support ACF.

Feature key labels

If user-defined feature key labels have been changed but no datadump has been performed, the changes are lost if there is a Call Server failure.

SIP telephones

SIP telephones appear as IP Peer endpoints to the system. See ["IP Peer calls" \(page 63\)](#).

NAT devices

The ACF feature cannot handle the case of a NAT device changing the media path mapping between the IP Phone private address and public address during the failover period. There is no way to discover the mapping while the port is in use. For instance, if a main office failure occurs and the user re-registers in local mode, NAT mapping is changed and the active call cannot survive.

Control messages

The LTPS sends the Audio Stream Control and LEDs Control commands in separate messages. If a failure occurs in the time between the two messages, the Audio Stream and LEDs states may not be synchronized. For example, it is possible for the Audio Stream to be muted and a network failure to occur at just the right moment to prevent the LED Control message for the mute LED from being received by the IP Phone.

Held Calls

When an idle IP Phone (one without an active speech path) re-registers, a firmware download can occur, if needed. If that IP Phone actually had calls on hold, this means the held calls cannot be retrieved until after the firmware download is finished.

Voice Gateway Media Cards

The ACF feature does not handle failures of the Voice Gateway functionality of the Voice Gateway Media Cards.

ELAN and TLAN subnet failures that affect the signaling with the IP Phones registered to a Voice Gateway Media Card are addressed in the same manner as failures affecting the Signaling Server. However, if there is a failure affecting the speech path to an IP Phone, such as when a PBX link failure occurs and the 10-minute PBX link timer expires, the Voice Gateway calls are released.

Codecs

Not all the codec properties are restored for the failed-over call. The following default codec properties are used for the active failover call:

- VAD is OFF
- G.723 Working Rate is 5.3 kb/s
- G.729 Annex is Annex A

QoS monitoring

The QoS monitoring is always disabled for the failover call. This is only for the period of the failover call; for all subsequent calls, the QoS monitoring works as configured.

Virtual Office

Active Call Failover is not supported for the active call from an IP Phone logged on another IP Phone to a TDM resource or virtual trunk. Such a call is released when the LTPS detects that the connection to the IP Phone is lost.

For example, IP Phone A is logged on to IP Phone B and talking to a TDM resource or a virtual trunk. If a TLAN subnet failure occurs and IP Phone A re-registers with its home TN, the active call is released as IP Phone A re-registers.

Handsfree

Scenario: IP Phone A has handsfree denied and IP Phone B has handsfree allowed. IP Phone A is logged on IP Phone B and talks to IP Phone C using handsfree.

If a TLAN subnet failure occurs and IP Phone A re-registers with its home TN (with handsfree disabled), the handsfree functionality is turned off and IP Phone A must go off-hook to continue the conversation.

ELAN subnet failure

The ACF state cannot be determined on the LTPS side during an ELAN subnet failure. This is because the ACF state is stored on the Call Server and it is not possible to send the ACF state on the LTPS side when the ELAN subnet has failed.

When the ELAN subnet is down, the `isetShow` command always outputs the ACF state as UNKNOWN for all established calls (the state is shown as busy-UNK).

Feature interactions

This section shows the ACF feature interactions with Virtual Office and Branch Office.

Branch Office

When the first failed IP Phone re-registers in local mode, the branch office Call Server looks up the far-end branch IP Phone local TN using the specified far-end IP address and builds a local call.

The call can be rebuilt only if both the IP Phones are branch users of the same branch office.

Example: A regular main office IP Phone talks to the branch IP Phone registered with the main office. A failure occurs on the main office, so that the branch IP Phone cannot register in normal mode again, and re-registers in local mode. Even if the main office IP Phone survives the failure, the call cannot be rebuilt because the call becomes an IP Peer call between the branch office and main office. This call becomes Partial Rebuilt and exists until released.

Virtual Office

It is possible that active IP Phone A, that was logged on to IP Phone B before the failure, cannot re-register with the Call Server, because IP Phone C performed a Virtual Office logon and uses IP Phone A TN. In this case, the Signaling Server/Voice Gateway Media Card locally handles the Release, Onhook and Mute events coming from IP Phone A in the Logged Out state.

Survivable Remote Gateway

The Survivable Remote Gateway (SRG) 1.0 and SRG50 do not support ACF. If the IP Phone is an SRG user, the active call, either in normal mode or local mode, does not survive a failure.

NAT

The NAT discovery is delayed for an IP Phone with an active call when it re-registers. NAT discovery messages are sent through the port used for the RTP stream. NAT discovery is not initiated if the LTPS detects that the IP Phone has an active RTP stream.

Personal Directory, Callers List, Redial List

The display content is cleared and the Personal Directory/Callers List/Redial List applications are reset when the active call failover process starts. The applications can be used again only after the IP Phone re-registers. A user that is using one of the Personal Directory/Callers List/Redial List menus sees the display clear and loses any data in that transaction that was not selected or saved with the Personal Directory/Callers List/Redial List feature.

ACF implementation does not maintain data present only on the Signaling Server/Voice Gateway Media Card. Transient data (for example, the Services key submenu the user is currently in) is lost when the failover occurs and the IP Phone re-registers.

Converged Desktop

If the Call Server maintains the active call information during the active call failover, and the SIP Gateway maintains the link and information with the MCS 5100 (the SIP Gateway has not failed or is not on the Signaling Server that reboots if that is the failure mode), a Converged Desktop call is maintained when the involved IP Phone re-registers to the system. If the Call Server loses the call information or the SIP Gateway Signaling Server reboots, the Converged Desktop call is impacted.

A Converged Desktop consists of a telephone and multimedia PC Client (PCC) software.

The following are scenario examples.

Example 1: The IP Phone TLAN subnet fails and the IP Phone re-registers with the same or a different TPS.

In this case, both the voice and multimedia sessions survive: if a SIP call is established with the other party in the SIP domain, the call is not released as the IP Phone re-registers. The multimedia applications still work: the presence is updated on PCC after the telephone re-registers.

If the unregistered converged IP Phone releases the call during the TLAN subnet failure, the Presence status is updated on PCC as the idle converged IP Phone re-registers.

Example 2: The IP Phone Signaling Server fails and the IP Phone re-registers with the same or a different TPS (active converged IP Phone and SIP Gateway are on different Signaling Servers in the same node).

In this case, both the voice and multimedia sessions survive; the scenario is the same as the TLAN subnet failure in Example 1.

Example 3: The IP Phone ELAN subnet fails and the IP Phone re-registers with the same or a different TPS.

The voice session survives. If the ELAN subnet comes back up before the IP Phone changes the call state (that is, releases the call), then the multimedia session is not impacted.

If the IP Phone releases the call when the ELAN subnet is still down, the PCC status update happens when the idle converged IP Phone re-registers with the system.

If the call is released by the supervisory timer, the status is updated on PCC after the ELAN subnet comes back up and the Converged Desktop AML ELAN subnet link is enabled (the CSA104 message is output on the Call Server when this happens).

Example 4: Call Server warm start.

The voice and multimedia sessions survive. The Presence status is updated on PCC as the converged IP Phone releases the call after the warm start.

Example 5: Call Server cold start.

The voice and multimedia sessions are closed as the Call Server comes up. The Presence status becomes Connected - Idle even if the call is rebuilt and active after the Call Server cold start.

IP Phone firmware downloads

The firmware is not downloaded to an IP Phone that has an active RTP stream open when it registers with the failover system. The firmware is downloaded later when the idle IP Phone registers again or by using appropriate CLI commands.

IP Phone as ACD agent or supervisor telephone

If an IP Phone is used as an ACD agent (or supervisor) and the Call Server fails:

- In the case of a Call Server warm start (INI), the active calls are retained on the agent telephone.

- In the case of a Call Server cold start (SYSLOAD), the active calls are dropped and the agents are logged out.

This applies to both the In-calls (PRIMARY) key and any secondary DN key on the ACD telephone.

TPS failures do not impact general ACD functionality, because the ACD feature is implemented on the Call Server.

CS 1000 base features

No feature works when the active IP Phone is disconnected and trying to re-register with the Call Server. All the features can be used in the context of the failover call after the IP Phone re-registers (if it is not a PARTIAL REBUILT call).

The feature context is lost on the Call Server if the Call Server fails.

The feature context is not lost on the Call Server in a case of TLAN/ELAN subnet failure. Only the feature data on the IP Phone display is lost.

Feature context in Call Server failures

The context of any feature is lost on the Call Server in cases of Call Server failure (Call Server warm or cold start). The LTPS IP Phone display is lost as the IP Phone re-registers. This means if a feature is activated and the Call Server fails, all the user input and data is lost.

Example: IP Phone A is in a call; the user presses the Transfer key and starts dialing a DN. The Call Server cold or warm starts. Therefore, IP Phone A does not accept the user input and tries to re-register with the Call Server. When the Call Server comes back up and the IP Phones re-register, IP Phone A does not have the Call Transfer activated. The held call is also lost: it is not rebuilt after INI or by the ACF feature, because the call is not active.

TLAN/ELAN subnet and LTPS failures

When a network or Signaling Server/Voice Gateway Media Card failure occurs and the active IP Phone has some feature activated, the feature context and data is not lost on the Call Server. The user can proceed with the feature after the IP Phone re-registers. Only the LTPS display is lost when the IP Phone re-registers.

Example: IP Phone A is in a call; the user presses the Transfer key, and starts dialing a DN. A TLAN subnet failure occurs when the first digit is dialed. The user is unaware of the failure and continues dialing the DN. The digits dialed after the failure are ignored, the IP Phone detects the failure, clears the display, and tries to re-register with the server.

The TLAN comes up again and the IP Phone re-registers. Although the IP Phone is now idle and the display is cleared, the IP Phone can resume dialing the DN starting from the second digit. The IP Phone can also return to the held call by pressing the held call DN key.

CDR

No ACF-specific information is added to the Call Detail Record (CDR) records.

In the case of Call Server failure, the CDR records for the call before the failure occurred are lost. CDR is restarted as the active IP Phone re-registers. Therefore, the records are generated only for the post-failure period of time.

In the case of the LTPS or network failure, CDR continues. The CDR is then stopped only if:

- the Call Server supervisory timer expires
- the IP Phone is idle when it re-registers
- the active IP Phone re-registers and then the call is released

The records include the failover time as well. This means that the user can be under-charged in case of Call Server failure and over-charged in a case of LTPS/network failure.

CallPilot

ACF considers CallPilot to be a TDM resource and interaction of an IP Phone with CallPilot as an IP/TDM call. See ["IP/TDM calls" \(page 63\)](#) and [Table 13 "ACF behaviors" \(page 58\)](#).

Example: IP Phone A calls telephone B and is redirected to CallPilot on no answer. The IP/TDM call is established between the IP Phone A and CallPilot.

The media session between IP Phones and CallPilot is dropped due to INI, which can be initiated by, for example, cold start, warm start, or ungraceful switchover.

Note that during any failure, user input is not passed to CallPilot. The user must resume entering responses after the IP Phone re-registers.

Interactions considered as IP/TDM calls

The ACF feature also considers interaction of an IP Phone with the following to be an IP/TDM call:

- CallPilot Mini
- Meridian Mail

- Meridian Mail Card Option
- Companion DECT Telephones (DMC8 version)
- Remote Office 9150
- Mini Carrier Remote
- Carrier Remote
- Periphonics Open IVR (VPS/is)
- Integrated Call Assistant
- Integrated Conference Bridge
- Integrated Recorded Announcer
- Integrated Personal Call Director
- Integrated Voice Services

Contact Center Management Server

The feature interacts with the Contact Center Management Server (CCMS) environment in the following cases:

- Acquired ACD agent is an IP Phone.
 - If a failure occurs when the IP Phone is active, the ACD IP Phone behaves as described in ["IP Phone as ACD agent or supervisor telephone"](#) (page 68).
 - If the active unregistered ACD agent changes the call state during the failure period (for example, releases the call), the status message is sent to the Symposium and CTI applications as the idle agent re-registers with the system.
- Associated non-ACD telephone is an IP Phone.
 - If a failure occurs when the IP Phone is active, the ACD IP Phone behaves as any other IP Phone. If the active associated IP Phone changes the call state during the failure period (for example, releases the call), the status message is sent to the Symposium and CTI applications as the idle telephone re-registers with the system.

MCS 5100

The SIP calls between the CS 1000 IP Phone and a SIP party on the MCS 5100 side are considered to be IP Peer calls. Such calls survive any type of failure except a Call Server cold start.

Installation and configuration

The feature for IP Phones requires no installation. It is active by default on any CS 1000 system running the CS 1000 Release 4.5, or later software.

On a system running CS 1000 Release 4.5, or later software, every node running the CS 1000 Release 4.5 or later LTPS software has the ACF feature enabled for the IP Phones that register to it.

Configurable RUDP Timeout and Retries Count

When a network failure occurs and the IP Phone connection is lost, the IP Phone does not instantly start the failover process. The IP Phone waits for a length of time for a reply from the server (the length of time is the value of RUDP timeout in ms). If the IP Phone does not receive a reply from the server in that length of time, the IP Phone retransmits the message. The IP Phone retransmits the message for the number of times of the Retries count value, and then starts the failover process: the IP Phone tries to reconnect to S1, then to S2 and so on.

Previously, the RUDP timeout was hard-coded to 500 msec, which meant that the IP Phone detected the connection failure after a 5-second delay, and Retries count was hard-coded to 10 retries. During that time, the IP Phone appeared frozen to the user. Now the time-out and number of retries can be configured in the OAM and PDT shells of the Signaling Server. See [Table 14 "RUDP Timeout and Retries Count commands" \(page 72\)](#).

Table 14
RUDP Timeout and Retries Count commands

Command	Description
usiSetPhoneRudpRetries	Configure the RUDP Retries Count maximum for IP Phones 1 – (10) – 20
usiGetPhoneRudpRetries	Display the RUDP Retries Count maximum for IP Phones
If the customer has a network with low network delays, one or both parameters can be reduced to make an IP Phone more responsive to failures. If the network delay values are high, the parameters can be increased to prevent the IP Phones from being reset due to significant network delay.	

Command	Description
usiSetPhoneRudpTimeout	Configure the RUDP Timeout value (in ms) for IP Phones 50 – (500) – 1000 in increments of 50 milliseconds
usiGetPhoneRudpTimeout	Display the RUDP Timeout value (in ms) for IP Phones
If the customer has a network with low network delays, one or both parameters can be reduced to make an IP Phone more responsive to failures. If the network delay values are high, the parameters can be increased to prevent the IP Phones from being reset due to significant network delay.	

The RUDP Timeout and Retries Count commands are found in the usi group. If **help** is typed at the OAM prompt, the following is output.

```
oam> help
For help on a particular command group type:  help 'group'
Available command groups are:
.....
DLOG          f/w download log file commands
usi           UNISTIM related commands
vte           Virtual Terminal Emulator related
commands
```

The configured values are saved in the [usiLib] section of the TPS.ini file and downloaded to all UNiStim IP Phones registered to the Signaling Server or Voice Gateway Media Card where the value was configured. When a supported IP Phone registers with the Signaling Server or Voice Gateway Media Card, the IP Phone downloads the new values.

It is necessary to configure these values on every Signaling Server and Voice Gateway Media Card in the node.

Overlay and command modifications

Because call failover is an exceptional situation, ACF information is output only if it exists.

Status definitions

UNREG

The ACF call is UNREGISTERED (UNREG). This occurs when both parties go offline. This state is always monitored by the 10-minute ACF timer. The call is released if the Call Server ACF timer expires.

HREG

The ACF call is HALF-REGISTERED (HREG). This occurs when one of the telephones involved in the call is registered with the Call Server, but the other telephone fails or is not connected to the Call Server. The CS ACF timer is started only if the other party does not support disconnect supervision.

HREB

The ACF call is HALF-REBUILT (HREB). This is when no call-associated data was found and the Call Server creates the data. HREB happens when the first of the two telephones involved registers with the Call Server, while another telephone is still not connected to the Call Server. When the far-end telephone registers, the partially-rebuilt call is promoted to REBUILT state.

PREB

The ACF call is PARTIAL-REBUILT (PREB). This is when no call-associated data is found. The far-end IP address is not known on the Call Server, or the far-end IP address is translated to the virtual trunk TN or Voice Gateway TN. The Call Server creates the data leaving the far-end TN undefined.

This scenario happens when:

- the far-end telephone is a local telephone, but while it was registered with the remote Call Server, the local Call Server was cold-started and TN-to-IP address associations were lost.
- the far-end telephone is a remote telephone.

The terminating-party TN in the PREB call is 0.

ATTENTION

No signaling is passed to the far-end telephone involved in the HREG, HREB, and PREB calls. This means any features that involve both parties do not work with such calls.

REB

The ACF call is REBUILT (REB). This means the calls have both parties available, but all call data except bandwidth and connected transducers is lost.

LD 32 STAT command

If ACF information exists for the requested IP Phone, it is output as follows:

```
ACF STATUS <status> TMR <timer>
```

where <status> is:

- UNREG for unregistered calls
- HREG for half-registered calls
- REB for rebuilt calls

- PREB for partially-rebuilt calls

where <timer> is:

- an integer value if the timer exists for the call
- N/A if there is no Call Server ACF timer attached

See [Figure 6 "LD 32 STAT output with ACF example" \(page 75\)](#).

Figure 6
LD 32 STAT output with ACF example

```
.stat 81 1
BUSY UNREGISTERED 00
ACF STATUS UNREG TMR 110

.stat 81 2
BUSY REGISTERED 00
ACF STATUS HREG TMR N/A

.stat 81 3
BUSY REGISTERED 00
ACF STATUS REB TMR N/A
```

LD 80 TRAC command

If ACF information exists for the requested IP Phone, it is output as follows:

```
ACF STATUS <status> TMR <timer> ORIG <orig_state> TERM
<term_state>
```

where <status> is:

- UNREG for unregistered calls
- HREG for half-registered calls
- REB for rebuilt calls
- PREB for partially-rebuilt calls

where <timer> is:

- an integer value if the timer exists for the call
- N/A if there is no Call Server ACF timer attached

ORIG <orig_state> and TERM <term_state> can be REGISTERED or UNREGISTERED.

[Figure 7 "LD 80 TRAC with ACF example" \(page 76\)](#) is a sample output for IP Phones involved in UNREGISTERED and PARTIAL-REBUILT calls.

Figure 7
LD 80 TRAC with ACF example

```
.TRAC 0 8100

ACTIVE TN 081 0 00 00 V PHYSICAL TN 003 0 00 04
ORIG 008 0 00 00 0 SCR MARP 0 5500 2616
TERM 081 0 00 00 V PHYSICAL TN 000 0 00 00 0 SCR MARP RING ON 0
8100 I2004
DIAL DN 8100
MAIN_FM ESTD
TALKSLOT ORIG 17 TERM 14
EES_DATA:
NONE
QUEU NONE
CALL ID 0 197
ACF STATUS UNREG TMR 110 ORIG UNREGISTERED TERM UNREGISTERED

.TRAC 0 8100

ACTIVE TN 081 0 00 00 V PHYSICAL TN 003 0 00 04
ORIG 008 0 00 00 0 SCR MARP 0 5500 2616
TERM 000 0 00 00 V PHYSICAL TN 000 0 00 00 0
DIAL DN 8100
MAIN_FM ESTD
TALKSLOT ORIG 17 TERM 14
EES_DATA:
NONE
QUEU NONE
CALL ID 0 201
ACF STATUS PREB TMR N/A ORIG REGISTERED TERM UNREGISTERED
```

LD 117 STIP ACF command

A sub-command **ACF** is added to the existing LD 117 STIP command.

Table 15
LD 117 STIP ACF command

Command	Description
STIP ACF <status>	Displays the Active Call Failover (ACF) information. <status> – optional parameter. Specifies the status to be output. Outputs all IP Phones involved in the following types of calls: • UNREG - UNREGISTERED calls • HREG - HALF-REGISTERED calls • REB - REBUILT calls • HREB - HALF-REBUILT calls • PREB - PARTIAL-REBUILT calls • ALL – all types of ACF calls

Command	Description
	If no status parameter is entered, all types of ACF calls are output.

Output

The output is similar to the existing LD 117 STIP output, with the addition of a column titled ACF STATUS. If the call is in an inactive state, the value of the Call Server ACF timer follows that status, separated by a colon (:).

LD 117 STIP ACF in Element Manager

Support for the STIP ACF command in LD 117 is provided by Element Manager. Click **System > Maintenance**. Select **LD 117 - Ethernet and Alarm Management**. Select **Ethernet Diagnostics**. The Ethernet Diagnostics window appears.

Figure 8 "LD 117 STIP ACF in Element Manager" (page 77) illustrates the placement of the **STIP ACF** command with the other STIP commands.

Figure 8
LD 117 STIP ACF in Element Manager

CS 1000 ELEMENT MANAGER Help | Logout

Managing: 192.167.102.3
System > Maintenance > Ethernet Diagnostics

Ethernet Diagnostics

Status Commands [-- Filters]	Command Parameters
STAT LINK IP - Link status -- IP	Submit
STAT SRV - Server status	Submit
STIP ACF - IP status - Active Call Failover	All Submit
PRT IPDN - Print DNS with a given IP address	Submit
ECNT FW - Ethernet Count FWID Major/Ver Minor/Ver Filter	Submit
RST ZONE - Reset IP Phone Zone START/STOP HH/MM	Submit
STAT IFMG - Print status of the given or all IPMGs	Submit
STAT RHC2833 - RHC2833 Status - IN	Submit

Instruction: Select command, add value and click on [Submit]

A list of command parameters are made available after the STIP ACF command is selected. The ALL command parameter is displayed as the default.

Click the **Submit** button after selecting one of these available parameters to execute the command. The output from the command is displayed in the text box located in the lower portion of the Web page.

Online Help describes the various parameters available for the **STIP ACF** command.

isetShow command

If the ACF status exists for the requested IP Phone, it is provided in the State field of the **isetShow** command output. The ACF status is separated from the state by '-' (dash). The ACF status is any value described in the LD 80 output. The Call Server ACF timer value is not provided in the output.

See [Figure 9 "isetShow command output with ACF example" \(page 78\)](#).

Figure 9
isetShow command output with ACF example

```
-> isetShow
```

Set Information						
IP Address	NAT Type	RegType	State	Up Time	...cont...	
192.168.29.51	12004	Regular	busy-BREG	0 01:16:42	..	..
192.168.29.53	12004	Regular	busy-BREB	0 01:16:42	..	..
192.168.29.99	12004	Regular	busy	0 01:16:42	..	..

DSP peg counter for CS 1000E systems

The conversion of TDM voice to IP packets is performed by Digital Signaling Processor (DSP) resources residing on a Voice Gateway Media Card in the IP Media Gateway (IPMG) of a CS 1000E system. The Voice Gateway Media Cards have a limited number of DSP resources that actually perform the conversion. When all DSP resources are busy, IP-to-TDM calls and TDM-to-TDM calls between different IPMGs are blocked. IP-to-IP calls are not blocked.

The DSP Peg Counter feature provides three counters. The first peg counter provides a count of the number of attempts to allocate a DSP resource on an IPMG. The second provides a count of the number of times calls were blocked on an IPMG due to a lack of DSP resources. If the call failed due to a lack of bandwidth, this is reflected in the third peg counter. The counters are a part of customer traffic measurement in LD 2.

For more information, see *Traffic Measurement: Formats and Output Reference (NN43001-750)* and *Software Input Output Administration (NN43001-611)*.

Enhanced UNiStim Firmware Download for IP Phones

Prior to CS 1000 Release 5.0, firmware files were downloaded to the Voice Gateway Media Cards. In CS 1000 Release 5.0, firmware files are stored on and are downloaded from the Signaling Server.

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

Specifically, this feature introduces the following functionality:

- Enhanced firmware file header that includes the IT_TYPE and name string for each IP Phone type. Element Manager and the LTPS can read this information and automatically display the mapping to the administrator.
- Revised definition of the IP Client IP Phone identification.
- New Maintenance Mode for the Signaling Server that allows even more simultaneous firmware downloads from the UFTP server. Maintenance Mode (Turbo Mode) is manually initiated by the administrator in which premarked node Signaling Servers utilize all possible resources for processing firmware upgrade jobs.
- Improved identification of the registered IP Phones using string names and providing more detailed identification of IP Phones that register in Emulation Mode.
- UNiStim IP Phones are allowed to register with an older version of firmware if the UFTP servers are busy, then periodically offers the option to start the firmware upgrade to the IP Phone user.
- Introduction of missing firmware file retrieval to the Branch Office from the Main Office.

System management commands are provided to collect information about registered IP Phones, their models, and their firmware.

Operating parameters

Enhanced UNiStim Firmware Download feature is supported on the following systems running CS 1000 Release 4.5 or later software.

- CS 1000M HG
- CS 1000M SG
- CS 1000M MG
- CS 1000E

The Enhanced UNISlim Firmware Download feature has the following operating parameters:

- It supports only firmware downloads performed by the UFTP server to the UNISlim IP Phones supporting the UFTP download protocol.
- Enhanced functionality is provided only if the recommended commands are used. For example, use of the VxWorks shell `copy` command instead of the `firmwareFileGet` command bypasses the other features and is therefore not supported.
- Firmware retrieval mechanism described for the Branch Office LTPS retrieves only firmware files it finds missing. It does not compare the list of firmware on the Branch Office LTPS and Main Office LTPS to determine whether the Branch Office has the latest firmware, or perform any automatic compare and update operations. The Branch Office LTPS only receives firmware files when the `umsUpgradeAll` command was issued on the Main Office LTPS.

Feature interactions

Active Call Failover for IP Phones

The Active Call Failover feature handles cases when an IP Phone registers with an active RTP stream (has a call active at the time of registration). The check of IP Phone firmware is skipped in this case, and the IP Phone registers with the LTPS.

The Active Call Failover scenario is the same as the postponed firmware upgrade scenario described in [Table 19 "IP Phone registration and download scenarios" \(page 83\)](#). After the call ends, the user is prompted to start the firmware upgrade.

For more information about Active Call Failover for IP Phones, see ["Active Call Failover for IP Phones" \(page 55\)](#).

System view

IP Phone firmware upgrades

Each IP Phone registering with the LTPS is queried for its firmware ID and IT_TYPE. The system response depends on the results of the query. See [Table 16 "System response" \(page 80\)](#).

Table 16
System response

Query result	Response
LTPS software supports the reported IT_TYPE (see Table 17 "Supported IT_TYPES" (page 81)) and the Upgrade Manager has firmware for the given firmware ID.	Registration of the IP Phone continues. The IP Phone firmware upgrade is performed if possible.

Query result	Response
LTPS software supports the reported IT_TYPE, but the Upgrade Manager has no firmware for the given firmware ID.	Registration of the IP Phone continues with no firmware download.
LTPS software does not support the IT_TYPE reported.	Registration of the IP Phone is rejected.
The branch office IP Phone is upgraded at the branch office before the IP Phone is redirected to the main office.	If the branch office does not have the necessary firmware file, an attempt is made to download the firmware file from the main office.

Firmware file management

To manage available firmware, the following information is collected about each firmware file on the Signaling Server or Voice Gateway Media Card:

- firmware ID
- firmware version
- applicable IT_TYPE (see [Table 17 "Supported IT_TYPES" \(page 81\)](#))
- applicable model names

IT_TYPES

[Table 17 "Supported IT_TYPES" \(page 81\)](#) lists the IT_TYPES supported by the Upgrade Manager for CS 1000 Release 5.0

Table 17
Supported IT_TYPES

IT_TYPE	IP Phone
0x02	IP Phone 2004, IP Phone 2007, WLAN 2210/2211/2212/6120/6140, IP Phone 1140E
0x03	IP Phone 2002, IP Phone 1120E
0x04	IP Phone 2001, IP Audio Conference Phone 2033, IP Phone 1110
0x20	IP Softphone 2050, Mobile Voice Client 2050
0x06	IP Phone 1150E

Two events trigger data about firmware files to be updated by the LTPS:

1. LTPS reboot
2. new firmware file upload from either the LTPS Command Line Interface (CLI) or Element Manager

In the first case, the LTPS explores possible locations of firmware files and collects information about found files in its internal database. In the second case, when a new firmware file is uploaded, the LTPS updates the internal database with information extracted from the file.

Element Manager uses data from the firmware file to provide information about the firmware file and the IP Phones to which it can be downloaded.

Firmware file names

Firmware file names are originally in the format **SSFFYxx.bin**. See [Table 18 "Original firmware file name format" \(page 82\)](#).

Table 18
Original firmware file name format

Designator	Definition	Values
SS	Site code where firmware was built	06 – Calgary 30 – Ottawa
FF	Firmware type	02 – Phase 0/1 IP Phone 2004 03 – Phase 1 IP Phone 2002 04 – Phase 2 IP Phone 2001/2002/2004
Y	Alpha character	A – 0 B – 1 C – 2 D – 3 (and so on)
XX	Release number	2-digit decimal integer (for example,.38)

The files are renamed according to the following rules:

- Phase 0/1 IP Phone 2004 firmware is renamed to **x00.fw**
- Phase 1 IP Phone 2002 firmware is renamed to **x01.fw**
- All other firmware files are renamed to **xNN.fw**, where:
 - **x** emphasizes that NN is a hexadecimal number
 - **NN** is the firmware ID for that file

The xNN.fw format also applies to the firmware file for the Phase 2 IP Phone 2001, IP Phone 2002, and IP Phone 2004. The file was named IPP2SET.fw but is renamed to x02.fw to conform to the naming convention.

Download maximums

The following modifications are available on the Signaling Server to the Upgrade Manager:

- The default number of allowed simultaneous downloads is increased to 100.
- Maintenance Mode (Turbo Mode) that is manually initiated by the administrator is available in which premarked node Signaling Servers utilize all possible resources for processing firmware upgrades. The following commands are used to manage the Maintenance Mode:
 - uftpTurboMode
 - uftpTurboModeTimeoutSet
 - uftpTurboModeShow

The uftpTurboMode command is used in conjunction with RST FW (hard-resets all IP Phones with specified F/W ID) and RST ZONE (hard-resets all IP Phones) commands in LD 117. For more information about commands in a specified zone, see [Table 20 "Maintenance Mode commands" \(page 86\)](#).

For more information about Maintenance Mode, see ["Maintenance Mode" \(page 85\)](#).

Immediate and delayed firmware downloads

The IP Phones display various messages to indicate the status of IP Phone registration and firmware downloads. [Table 19 "IP Phone registration and download scenarios" \(page 83\)](#) lists some scenario examples with the resulting IP Phone displays.

Table 19
IP Phone registration and download scenarios

Scenario	Result
Normal firmware download for known IP Phone type	IP Phone displays message that IP Phone is connecting to the LTPS. IP Phone displays message that firmware download is initiated. If download is successful, IP Phone continues with normal registration.

Scenario	Result
Postponed firmware upgrade	IP Phone displays message that IP Phone is connecting to the LTPS. IP Phone cannot download firmware. It is allowed to proceed with registration using old firmware. At the completion of call (if download resources are available), IP Phone displays message Upgrade F/W now? IP Phone displays Yes and No soft keys to use to select choice. If Yes is selected, firmware download begins. If no choice is made, IP Phone proceeds with firmware download after timer expiration. If No is selected, IP Phone display returns to idle state. Off-hook dialing, on-hook dialing, and external events such as an incoming call imply a No response.
Unknown firmware ID for known IT_TYPE	IP Phone displays message that IP Phone is connecting to the LTPS. No firmware upgrade is performed, but IP Phone is allowed to register.
Unknown IT_TYPE	IP Phone has no display. The IP Phone just resets continuously. IP Phone registration is not allowed. Log message is sent to LTPS administrator.
Branch Office LTPS determines IP Phone requires firmware upgrade	IP Phone displays message that firmware download is initiated. IP Phone is placed into local mode. Message is displayed until firmware is downloaded. IP Phone upgrade process is initiated. If firmware download is unsuccessful after 10 retries, IP Phone remains in local mode.

Maintenance Mode

When a Signaling Server is placed into Maintenance Mode, the allowable maximum number of simultaneous firmware downloads increases. Maintenance Mode enables the UFTP server to utilize most of its processing resources to deal with the downloads.

The actual number of simultaneous downloads is determined by measuring the CPU idle time, so each new firmware download session is launched if there are less than 100 download sessions for the Signaling Server already taking place and one of the following is true:

- there are less than five download sessions currently active
- Signaling Server is in regular mode (not in Maintenance Mode) and its CPU usage is less than 85%
- Signaling Server is in Maintenance Mode and its CPU usage is less than 100%

The UMS tries to launch a pending download session every 5 seconds.

ATTENTION

When Maintenance Mode is enabled, call processing signaling could be impacted by the UFTP download processes.

After Maintenance Mode is enabled, it can be exited in several ways:

- manually, by using the `uftpTurboMode "stop"` command
- automatically, after the Upgrade Manager is idle for MM minutes after at least one download has been started
This prevents a time-out from occurring while the system is being configured and the downloads start. After a download starts, if MM minutes pass with no new firmware upgrade jobs starting, the normal mode of operation resumes. The idle timeout timer is configured using the `uftpTurboModeTimeoutSet` command.

- automatically, after expiration of the Maintenance Mode period

Active firmware upgrade jobs are not cancelled when the Maintenance Mode exits. No new jobs are added until the number of active jobs is below the default value.

Maintenance Mode can be enabled only on the Signaling Server. Maintenance Mode affects only Signaling Servers designated for Maintenance Mode. This allows some Signaling Servers in the node to operate in Maintenance Mode while others do not. The Signaling Server is designated for Maintenance Mode with the `uftpTurboMode "on"` command. The Maintenance Mode designation is saved and maintained even if the Signaling Server is power-cycled or is rebooted.

Call processing for Signaling Servers operating in normal mode is not impacted by the firmware download process.

Postponed firmware upgrades are not performed when at least one Signaling Server is in Maintenance Mode.

Table 20 "Maintenance Mode commands" (page 86) lists the commands used for Maintenance Mode.

Table 20
Maintenance Mode commands

Command	Description
uftpTurboMode <"HH:MM/start/stop/on/off">, <MM> <"show">	Configures Maintenance Mode "HH:MM" – time to enter Maintenance Mode in 24-hour format "start" – enter Maintenance Mode immediately "stop" – stop Maintenance Mode "on" – allow Signaling Server to enter Maintenance Mode "off" – do not allow Signaling Server to enter Maintenance Mode MM – optional parameter that defines the length of time in minutes that Maintenance Mode is to be maintained "show" – displays the same output as uftpTurboModeShow If no parameter is entered, Upgrade Manager defaults to uftpTurboMode "start".
uftpTurboModeTimeoutSet <MM>	Configures the idle timeout timer for Maintenance Mode MM – optional parameter that defines the number of minutes the Upgrade Manager waits after the last firmware download job is started before returning the Signaling Server to normal mode If this parameter is configured as 0 (zero), the Upgrade Manager never exits Maintenance Mode unless the umsUpgradeModeSet command is issued with the "stop" parameter.

Command	Description
	If no parameter is entered, then the current timeout setting is displayed.
uftpTurboModeShow	Displays current status of Maintenance Mode.

The following is an example of output when Maintenance Mode is to start at 11 p.m.

```
oam> uftpTurboMode "23:00"
oam> 28/07/04 08:23:56 LOG0006 shell: F/W upgrade
Maintenance Mode will start after 52564 seconds
```

Call Server commands

LD 20

A response **ISSET** is introduced to the LD 20 **TYPE** prompt. When ISET is entered, the prompt **MODEL_NAME** is displayed. The MODEL_NAME prompt allows a user to specify the Short Model Name mnemonic for filtering the output of TN blocks. If only the ISET response is used, printed TN blocks contain the long IP Phone Model Name in the output.

LD 20 Listing or printing TN blocks of specified IP Phone model

Prompt	Response	Description
REQ	LTN	List TN blocks.
	PRT	Print TN blocks.
TYPE	ISSET	Enable filtering by IP Phone model name.
...	...	
MODEL_NAME	xxxxxxx	IP Phone model
		For example, 2004P2
...	...	

The following is an example of the input and output.

```
>ld 20
REQ: PRT
TYPE: ISET
TN
CUST
TEN
DATE
PAGE
DES
MODEL_NAME: 2004P2
KEM_RANGE
IP_PHONE_MODEL: IP PHONE 2004 PHASE2
```

```
DES FAKE
TN 064 0 00 00 VIRTUAL
TYPE 2004P2
CDEN 8D
CUST 0
ZONE 000
FDN
TGAR 1
LDN NO
NCOS 0
SGRP 0
RNPG 0
SCI 0
SSU
XLST
SCPW 6400
SFLT NO
CAC_CIS 3
CAC_MFC 0
CLS CTD FBD WTA LPR MTD FND HTD ADD HFD CRPD
MWD LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
POD DSX VMD CMSD SLKD CCSD SWD LND CNDD
CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBF
ICDD CDMD LLCN MCTD CLBD AUTU
GPUD DPUD DNDD CFXD ARHD CLTD ASCD
CPFA CPTA HSPD ABDD CFHD FICD NAID DNAA RDLA BUZZ AGRD MOAD
UDI RCC HBTD AHD IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
DRDD EXR0
USMD USRD ULAD CCBF RTDD RBDD RBHD PGND FLXD FTTC DNDY DNO3
MCBN
FDSF NOVF VOLA VOUA CDMR
CPND_LANG ENG
HUNT
PLEV 02
CSDN
AST
IAPG 0
AACS NO
ITNA NO
DGRP
MLWU_LANG 0
DNDR 0
KEY 00 SCR 640 0 MARP
ANIE 0
01
02
03
04
05
06
```

```
07
08
09
10
11
12
13
14
15
16
17 TRN
18 AO6
19 CFW 16
20 RGA
21 PRK
22 RNP
23
24 PRS
25 CHG
26 CPN
27
28
29
30
31
DATE 8 JUL 2004
NACT
```

LD 117

LD 117 commands are as follows:

- STIP FW <XX> <A> <BB> <FF> – list IP Phones with specified firmware ID and, optionally, firmware version. If no parameters are entered, output is a list of available model names.
- STIP MODL <MMMM> – list IP Phones of specified model name
- RST ZONE <ZoneNumber> <START/STOP> <HH:MM> – reset IP Phones in specified zone
- RST FW <FWID> <START/STOP> <HH:MM> – reset IP Phones with specified F/W ID

See Table 21 "LD 117 commands" (page 90).

Table 21
LD 117 commands

Command	Description
STIP FW <XX> <A> <BB> <FF>	Displays information from the Resource Locator Module (RLM) for IP Phones with specified firmware ID and running specified firmware version. <XX> – firmware ID <A> – major version designator <BB> – minor version designator <FF> – filter to apply on firmware version; can be one of the following: = – equal to ~ – not equal to < – less than > – greater than Only the XX parameter is required. STIP FW <XX> <A> <BB> is equivalent to STIP FW <XX> <A> <BB> EQ. STIP FW <XX> <A> lists all registered IP Phones with firmware ID equal to <XX> and major version designator equal to <A>. STIP FW <XX> lists all registered IP Phones with firmware ID equal to <XX>.

Command	Description
STIP MODL <MMMM>	Displays information from the RLM for all IP Phones of the specified model, where: • MMMM = IP Phone model If the <MMMM> parameter is omitted, a table of existing model names and associated mnemonics is displayed.
RST ZONE <ZoneNumber>	Immediately hard-resets all IP Phones, where: • ZoneNumber = zone number
RST ZONE <ZoneNumber> <START/STOP> <HH:MM>	Schedule or cancel hard-resets of all IP Phones in specified zone. <ZoneNumber> – zone number in which to reset IP Phones START/STOP – IP Phones reset, where: • START – configures reset time schedule • STOP – cancels scheduled reset If START is specified and the last parameter is omitted, then IP Phones are reset immediately. <HH:MM> – hour and minute when IP Phones are to be reset With only the first parameter, or no parameters, the schedule of IP Phones re-sets is printed.
RST FW <FWID> <START/STOP> <HH:MM>	Hard-resets all IP Phones with specified firmware ID. <F/W ID> – firmware ID of IP Phones that should be reset <START/STOP> – schedules or cancels IP Phones hard-reset. If START is specified and the last parameter is omitted, then IP Phones are reset immediately.

Command	Description
	<HH:MM> – hour and minute when IP Phones should be reset With only the first parameter, or with no parameters specified, the schedule of IP Phones resets is printed.

LTPS CLI commands

LTPS CLI commands are as follows:

- firmwareFileGet
- uftpAutoUpgradeTimeoutSet
- isetFWShow
- isetFWGet

See [Table 22 "LTPS CLI commands" \(page 92\)](#).

Table 22
LTPS CLI commands

Command	Description
firmwareFileGet <"ServerIP">, <"UserID">, <"Password">, <"/path/to/file">, <"file name">	Initiates a firmware download from a specified FTP server. After the download is completed, the downloaded file is checked for Enhanced Header (or proper naming). If the file is considered a valid firmware file, the UMS database is updated accordingly. ServerIP – FTP server IP address from where the firmware is retrieved UserID, Password – credentials for logging on to the FTP server /path/to/file – absolute or relative path to the firmware file (does not include the file name itself) file name – name of the firmware file on the FTP server Use the firmwareFileGet command instead of firmwareFileGetI2004, firmwareFileGetI2002, and firmwareFileGetIPP2.

Command	Description
uftpAutoUpgradeTimeoutSet <MM>	Configures the length of time the IP Phone waits for a user response after the "Upgrade F/W now?" message is displayed before automatically beginning the firmware upgrade. MM – user response timeout in minutes. A value of 0 (zero) means "Print current settings". If no parameter is entered, the current value is printed.
isetFWShow	Displays the status of IP Phones firmware.
isetFWGet <filter>	Filters the output of the isetFWShow command by one of that command output field names. Field names include: • IP • Model Name • Type • FWID • Supported • FWVsn • UNiStim • TN

firmwareFileGet example

```
pdt>firmwareFileGet "192.168.0.1","admin1","0000
","/u/fw","0604D45.BIN"
```

firmwareFilePut example

```
pdt>firmwareFilePut "192.168.0.1","admin1","0000
","/u/fw","0604D45.BIN"
```

uftpAutoUpgradeTimeoutSet output example

```
pdt> uftpAutoUpgradeTimeoutSet 4
pdt> 25/08/04 06:22:23 LOG0006 shell: New value of auto F/W
upgrade timeout is 240 seconds.
pdt> uftpAutoUpgradeTimeoutSet
pdt> 25/08/04 06:22:23 LOG0006 shell: Current value of
auto F/W upgrade timeout is 240 seconds.
```

isetFWShow output example

```
oam> isetFWShow
```

```

Set Information
-----
IP Address Model ItType FWID Supported FWVsn UNIStimVsn TN
-----
-----
192.168.29.56 Polycom 2033 2033 0x10 No A.10 2.9 064-00
Total sets = 1
oam>

```

isetFWGet output example

```

oam> isetFWGet "FWID==0x10"
Set Information
-----
IP Address Model ItType FWID Supported FWVsn UNIStimVsn TN
-----
-----
192.168.29.56 Polycom 2033 2033 0x10 No A.10 2.9 064-00
Total sets = 1
oam>

```

Modified LTPS CLI commands

The output of the following commands has been changed to print IP Phone model name (long or short), firmware ID, firmware version, and so on:

- isetShow
- uftpShow
- umsPolicyShow
- isetGet

Short model name example is "2004P2". Long model name example is "IP Phone 2004 Phase 2".

isetShow output example

The output has been modified to display the IP Phone Model Name and firmware version in ABB format.

```

oam> isetShow
Set Information
-----
IP Address NAT Model ItType RegType State Up Time Set-TN
Regd-TN HWID FWVsn UNIStimVsn SrcPort DstPort
-----
-----
-----
192.168.29.56 IP Phone 2004 2004P2 Regular online 0 00:00:32
064-00 064-00 18-006038ddc6b6-6600 B.65 2.8 5100 5000
Total sets = 1
oam>

```

uftpShow output example

The output has been modified to display the IP Phone Model Name, firmware ID, and firmware version in ABB format.

```
oam> uftpShow
----- UFTP Server Configuration -----
UFTP Server IP address..... 192.168.29.42 [port: 5105]
Concurrent downloading limit.... 15 sets
Total firmware = 5
FW ID FWVsn Model PolicyName file name
-----
----- 0x00 B.65 IP Phone 2004 DEFAULT
/ums/i2004.fw
0x00 B.65 IP Phone 2002 DEFAULT /ums/i2002.fw
0x02 D.44 IP Phone 2001 DEFAULT /ums/x02.fw
0x02 D.44 IP Phone 2002 Ph2 DEFAULT /ums/x02.fw
0x02 D.44 IP Phone 2004 Ph2 DEFAULT /ums/x02.fw
----- Run Time Data -----
Last UFTP reset..... 1/14/2096 08:38:19
Cumulation Period..... 0004 01:55:01
Successful downloads..... 1
Fail downloads..... 0
----- Active Downloads -----
Current downloading sets..... 0
Model IP Address Downloaded[KByte]
```

umsPolicyShow output example

The output has been modified to display the IP Phone Model Name, firmware ID, and firmware version in ABB format.

```
oam> umsPolicyShow
Total policies = 1

Name          Upgrade    Protocol  Retries
-----
DEFAULT       ANY        UFTP      -1

Available firmware:
FW ID  FWVsn  Model
-----
0x00   B76   IP Phone 2004 Phase 0/1
0x00   B76   IP Phone 2002 Phase 1
0x02   DBB   IP Phone 2004 Phase 2
0x02   DBB   IP Phone 2002 Phase 2
0x02   DBB   IP Phone 2001 Phase 2
0x21   C4C   IP Phone 2007 Phase 2
0x24   C46   IP Phone 1120E
0x25   C46   IP Phone 1140E
0x27   C46   IP Phone 1150E

Policy Name    File name
-----
DEFAULT        /u/fw/x00.fw
DEFAULT        /u/fw/x01.fw
DEFAULT        /u/fw/x02.fw
DEFAULT        /u/fw/x02.fw
DEFAULT        /u/fw/x02.fw
DEFAULT        /u/fw/x02.fw
DEFAULT        /u/fw/x21.fw
DEFAULT        /u/fw/x24.fw
DEFAULT        /u/fw/x25.fw
DEFAULT        /u/fw/x27.fw

Total firmware = 7
```

isetGet output

The output has been modified to display the IP Phone Model Name and firmware version in ABB format.

Element Manager

To support the Enhanced UNiStim Firmware Download for IP Phones feature, the following changes have been made to Element Manager:

- Extraction and display of information from the Enhanced firmware file. For example, when new firmware is downloaded to Element Manager firmware location from the FTP server, Element Manager examines the file for the text string containing firmware ID, firmware version, applicable IT_TYPES, and model names.
- Ability to upload a new firmware file to the LTPS using the `firmwareFileGet` command.
- Addition of an interface for initiating or obtaining the status for the firmware download Maintenance Mode using the CLI commands `uftpTurboMode`, `uftpTurboModeShow`, and `uftpTurboModeTimeoutSet`.

The `uftpTurboMode` CLI commands are used in conjunction with `RST FW` and `RST ZONE` commands.

- Addition of an interface for resetting IP Phones by firmware ID and zone using the LD 117 commands `RST FW` and `RST ZONE`.

See [Table 20 "Maintenance Mode commands" \(page 86\)](#)

- Output of either ECNT MODL is parsed to obtain the list of available IP Phone models. This output can be used to allow a user to transparently specify the model name; that is, Element Manager replaces the actual model name with associated mnemonic.
- Addition of an interface for displaying the output of the LD 117 commands `ECNT MODEL`, `ECNT FW`, `ECNT PEC`, `STIP MODEL`, and `STIP FW`.
- Management of the compatibility matrix of different firmware versions with the Call Server and LTPS software release using the output of these LD 117 commands.
- Interaction with the Nortel Software Download Web site to download bundles of firmware files.

IP Phone firmware management in Element Manager

For information about updating the IP Phone firmware in Element Manager, see ["Upgrade the Voice Gateway Media Card software and IP Phone firmware" \(page 293\)](#).

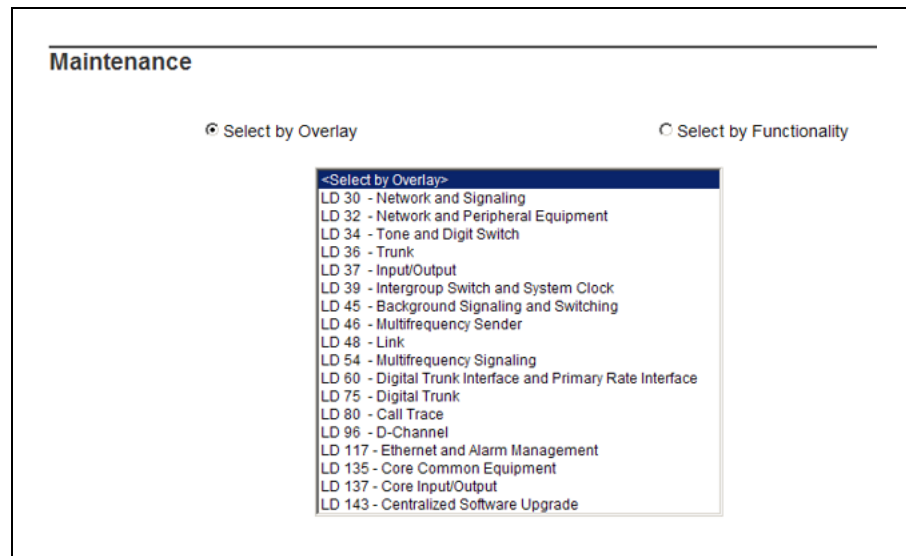
Ethernet Diagnostics in Element Manager

To access Ethernet Diagnostics in Element Manager, follow the steps in [Procedure 1 "Accessing Ethernet Diagnostics in Element Manager" \(page 97\)](#).

Procedure 1**Accessing Ethernet Diagnostics in Element Manager****Step Action**

- 1 In the Element Manager navigator, select **System > Maintenance**.
The **Maintenance** window appears. See [Figure 10 "Maintenance window"](#) (page 97).

Figure 10
Maintenance window



By default, the **Select by Overlay** radio button is selected.

- 2 Select **LD 117 – Ethernet and Alarm Management** in the **<Select by Overlay>** list and then select **Ethernet Diagnostics** in the **<Select Group>** list.

The **Ethernet Diagnostics** window appears. See [Figure 11 "Ethernet Diagnostics window"](#) (page 98).

Alternatively, select the **Select by Functionality** radio button.

Select **Ethernet Diagnostics** from the **<Select by Functionality>** list. See [Figure 12 "Select by Functionality list"](#) (page 98).

The **Ethernet Diagnostics** window appears.

Figure 11
Ethernet Diagnostics window

Status Commands [- Filters]	Command Parameters
STAT LINK IP - Link status -- IP	Submit
STAT SERV - Server status	Submit
STIP TN - IP Status -- TN	Submit
PRT IPDN - Print DNS with a given IP address	Submit
ECNT FW - Etherset Count -- FWID MajorVer MinorVer Filter	Submit
RST ZONE - Reset IP Phone -- Zone START/STOP HH:MM	Submit
STAT IPMG - Print status of the given or all IPMGs	Submit
STAT RFC2833 - RFC2833 Status -- TN	Submit

Instruction: Select command, add value and click on [Submit]

Cancel

Figure 12
Select by Functionality list

☐ Select by Overlay ☒ Select by Functionality

<Select by Functionality>

- AML Diagnostics
- Background Signaling and Switching
- Call Trace Diagnostics
- Centralized Software Upgrade
- Clock Controller Diagnostics
- Core Common Equipment Diagnostics
- Core Input/Output Diagnostics
- D-Channel Diagnostics
- D-Channel Expansion Diagnostics
- Digital Trunk Diagnostics
- Digital Trunk Maintenance Diagnostics
- Emergency Services Diagnostics
- Ethernet Diagnostics
- Ethernet Quality of Service Diagnostics
- Geographic Redundancy Diagnostics
- Input/Output Diagnostics
- InterGroup Switch and System Clock
- MSDL Diagnostics
- Multifrequency Sender Diagnostics
- Multifrequency Signaling Diagnostics
- Network and Peripheral Equipment Diagnostics
- Network and Signaling Diagnostics
- TMDI Diagnostics

—End—

For more information about the LD 117 commands, see "LD 117" (page 89).

ECNT commands

The following commands are available in LD 117 under ECNT in the Status Command list. See Figure 13 "ECNT commands" (page 99).

- ECNT FW
- ECNT MODL
- ECNT PEC
- ECNT CARD
- ECNT NODE
- ECNT SS
- ECNT ZONE

ATTENTION

ECNT CARD, ECNT NODE, ECNT SS, and ECNT ZONE were formerly found in LD 32.

Figure 13
ECNT commands

The screenshot shows the 'CS 1000 ELEMENT MANAGER' interface. The 'Ethernet Diagnostics' section is active. Under 'Status Commands [-- Filters]', the following commands are listed:

Status Commands [-- Filters]	Command Parameters
STAT LINK IP - Link status -- IP	Submit
STAT SERV - Server status	Submit
STIP TN - IP Status -- TN	Submit
PRT IPDN - Print DNS with a given IP address	Submit
ECNT FW - Etherset Count -- FWID, MajorVer, MinorVer, Filter	Submit
ECNT MODL - Etherset Count -- Model	Submit
ECNT PEC - Etherset Count -- PEC	Submit
ECNT ZONE - Etherset Count -- Zone, Customer#	Submit
ECNT CARD - Etherset Count -- Loop Shelf Card, Customer#	Submit
ECNT NODE - Etherset Count -- Node ID	Submit
ECNT SS - Etherset Count -- HostName	Submit

Instruction: Select command, add value and click on [Submit]

STIP commands

STIP MODL and STIP FW are listed in the STIP commands in the Status Command list. See Figure 14 "STIP commands" (page 100).

Figure 14
STIP commands

Ethernet Diagnostics

Status Commands [- Filters]	Command Parameters
STAT LINK IP - Link status -- IP	Submit
STAT SERV - Server status	Submit
STIP TN - IP Status -- TN	Submit
STIP TN - IP Status -- TN	Submit
STIP TYPE - IP Status -- Type	Submit
STIP ZONE - IP Status -- Zone	Submit
STIP NODE - IP Status -- Node ID	Submit
STIP HOSTIP - IP Status -- Host IP	Submit
STIP ACF - IP status -- Active Call Failover	Submit
STIP TERMIP - IP Status -- Term IP	Submit
STIP FW - IP Status -- FWID MajorVer MinorVer Filter	Submit
STIP MODL - IP Status -- ModelName	Submit

Instruction: Select command, add value and click on [Submit]

RST commands

RST ZONE and RST FW are listed in the RST commands in the Status Command list. Both RST commands reset IP Phones for the parameters specified. See [Figure 15 "RST commands" \(page 100\)](#).

Figure 15
RST commands

Ethernet Diagnostics

Status Commands [- Filters]	Command Parameters
STAT LINK IP - Link status -- IP	Submit
STAT SERV - Server status	Submit
STIP TN - IP Status -- TN	Submit
PRT IPDN - Print DNs with a given IP address	Submit
ECNT FW - Etherset Count -- FWID MajorVer MinorVer Filter	Submit
RST ZONE - Reset IP Phone -- Zone START/STOP HH:MM	Submit
RST ZONE - Reset IP Phone -- Zone START/STOP HH:MM	Submit
RST FW - Reset IP Phone -- FWID START/STOP HH:MM	Submit
STAT RFC2833 - RFC2833 Status -- TN	Submit

Instruction: Select command, add value and click on [Submit]

Maintenance Mode commands in Element Manager

The Signaling Server Maintenance Mode (Turbo Mode) commands are as follows:

- uftpTurboMode
- uftpTurboModeShow
- uftpTurboModeTimeoutSet
- uftpAutoUpgradeTimeoutSet

uftpTurboMode

Use the uftpTurboMode command to designate one of more Signaling Servers for firmware upgrade Maintenance Mode, or to schedule Maintenance Mode on the designated Signaling Server to either start immediately or at a specific time. See [Figure 18 "uftpTurboMode window in Element Manager" \(page 102\)](#).

To access the uftpTurboMode command, follow the steps in [Procedure 2 "Accessing the uftpTurboMode command" \(page 101\)](#).

Procedure 2

Accessing the uftpTurboMode command

Step	Action

- 1 In the navigator, select **IP Network > Maintenance and Reports**.

The **Node Maintenance and Reports** window appears. See [Figure 16 "Node Maintenance and Reports window" \(page 101\)](#).

Figure 16
Node Maintenance and Reports window

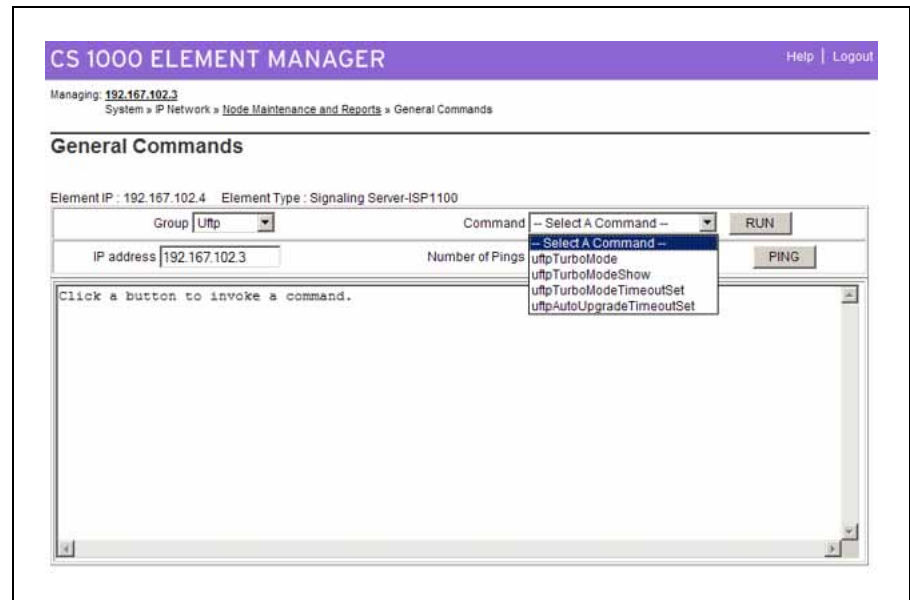
Node Maintenance and Reports							
- Node ID: 9		Node IP: 192.167.103.3		Total elements: 2			
Index	ELAN IP	Type	TN	ELAN			
CS1000E_PIV	192.167.102.4	Signaling Server-ISP1100	NO TN	GEN CMD	RPT LOG	OM RPT	Reset
mc32s_pliv	192.167.102.18	MC32S Card	4 0 1 0	GEN CMD	RPT LOG	OM RPT	Reset
				Virtual Terminal	Status		

- 2 Click the plus sign (+) to the left of the Node ID of the desired node to view the node elements.

- 3 Click the **GEN CMD** button for the desired Signaling Server.

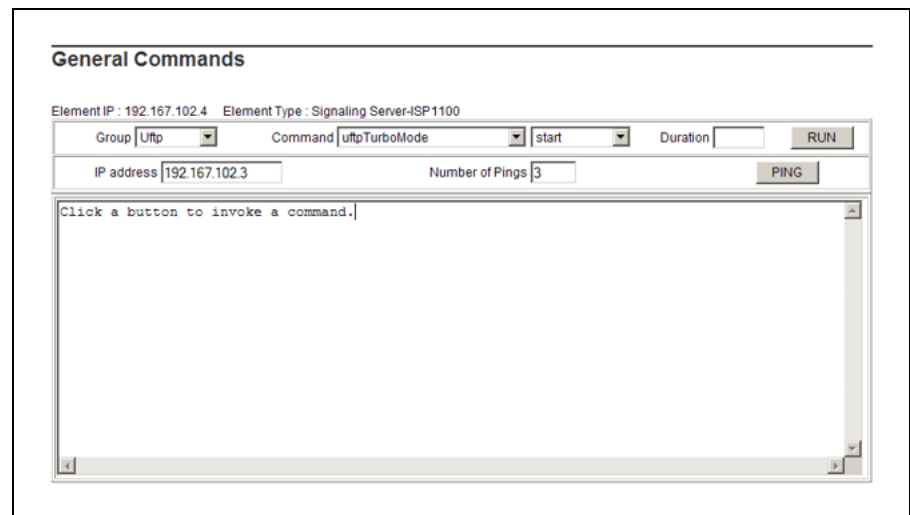
The **General Commands** window appears. See [Figure 17 "General Commands window" \(page 102\)](#).

Figure 17
General Commands window



- 4 From the **Group** drop-down list, select **uftp**.
- 5 From the **Command** drop-down list, **uftpTurboMode**.
- 6 If you select the **HH:MM** option, enter the time in the Hours and Minutes text boxes. No other option requires parameters.

Figure 18
uftpTurboMode window in Element Manager



- 7 Click **Run**.
- The command output is displayed in the pane below the command.

—End—

uftpTurboModeShow

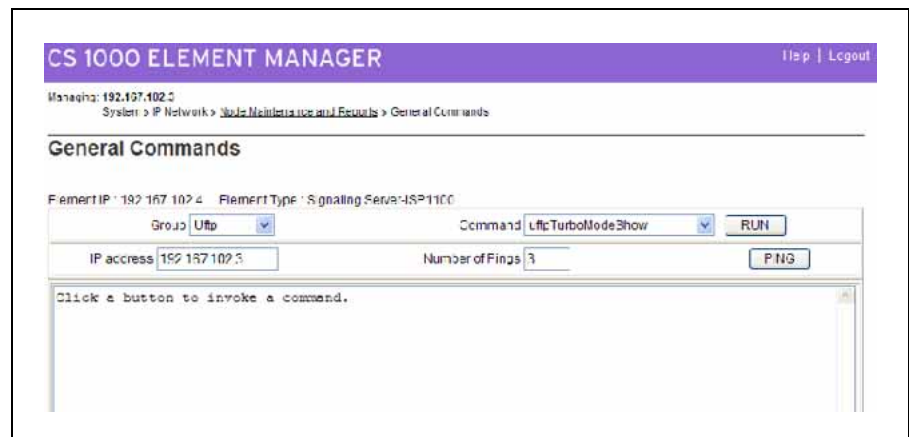
The uftpTurboModeShow command displays the current status of Maintenance Mode (None/Active/Scheduled). To access the uftpTurboModeShow command using Element Manager, follow the steps in [Procedure 3 "Accessing the uftpTurboModeShow command" \(page 103\)](#).

Procedure 3

Accessing the uftpTurboModeShow command

Step	Action
1	In the navigator, select IP Network > Maintenance and Reports . The Node Maintenance and Reports window appears. See Figure 16 "Node Maintenance and Reports window" (page 101) .
2	Click the plus sign (+) to the left of the Node ID of the desired node to view the node elements.
3	Click the GEN CMD button for the desired Signaling Server. The General Commands window appears. See Figure 17 "General Commands window" (page 102) .
4	From the Group drop-down list, select uftp .
5	From the Command drop-down list, select uftpTurboModeShow . See Figure 19 "uftpTurboModeShow window in Element Manager" (page 103) .

Figure 19
uftpTurboModeShow window in Element Manager



The command output is displayed in the pane below the command.

- 6 Click **Run**.

—End—

uftpTurboModeTimeoutSet

The uftpTurboModeTimeoutSet command sets the idle timer for Maintenance Mode. To access the uftpTurboModeTimeoutSet command using Element Manager, follow [Procedure 4 "Accessing uftpTurboModeTimeoutSet command"](#) (page 104).

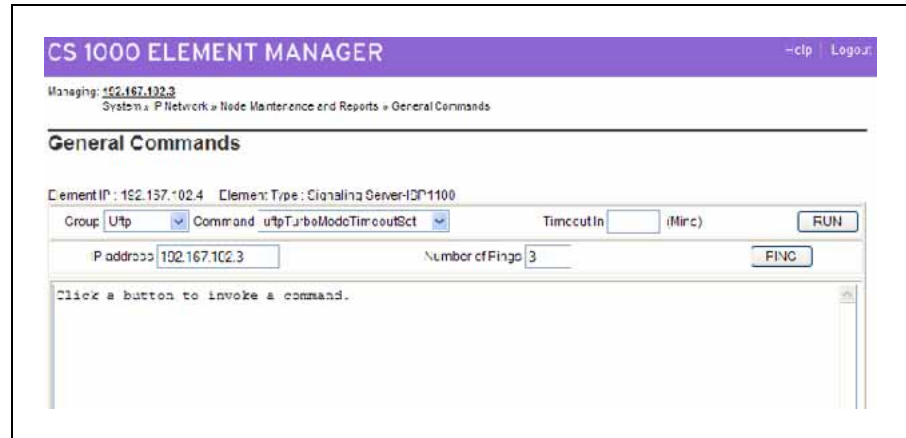
Procedure 4

Accessing uftpTurboModeTimeoutSet command

Step	Action
1	In the navigator, select IP Network > Maintenance and Reports . The Node Maintenance and Reports opens.
2	Click the plus sign (+) to the left of the Node ID of the desired node to view the node elements.
3	Click the GEN CMD button for the desired Signaling Server. The General Commands window appears. See Figure 17 "General Commands window" (page 102).
4	From the Group drop-down list, select uftp .
5	From the Command drop-down list, select uftpTurboModeTimeoutSet . See Figure 20 "uftpTurboModeTimeoutSet window" (page 105).

This command accepts the MM parameter.

Figure 20
uftpTurboModeTimeoutSet window



- 6 Enter the time in minutes in the **Timeout In** text box.
- 7 Click **Run**.
The command output is displayed in the pane below the command.

—End—

uftpAutoUpgradeTimeoutSet

The uftpAutoUpgradeTimeoutSet command sets the idle timer for starting the firmware download. To access the uftpAutoUpgradeTimeoutSet command using Element Manager, follow [Procedure 5 "Accessing uftpAutoUpgradeTimeoutSet command"](#) (page 105).

Procedure 5

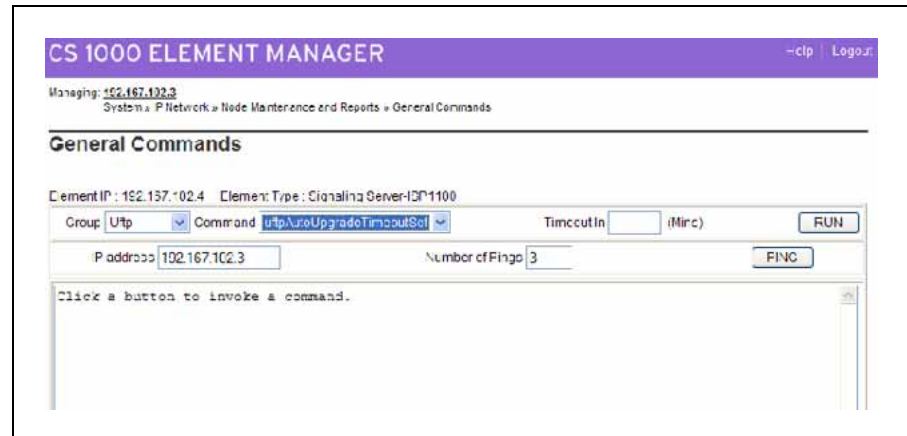
Accessing uftpAutoUpgradeTimeoutSet command

Step	Action
1	In the navigator, select IP Network > Maintenance and Reports . The Node Maintenance and Reports opens.
2	Click the plus sign (+) to the left of the Node ID of the desired node to view the node elements.
3	Click the GEN CMD button for the desired Signaling Server. The General Commands window appears. See Figure 17 "General Commands window" (page 102).
4	From the Group drop-down list, select uftp .

- 5 From the **Command** drop-down list, select **uftpAutoUpgradeTimeoutSet**. See [Figure 21 "uftpAutoUpgradeTimeoutSet window in Element Manager"](#) (page 106).

This command accepts the MM parameter.

Figure 21
uftpAutoUpgradeTimeoutSet window in Element Manager



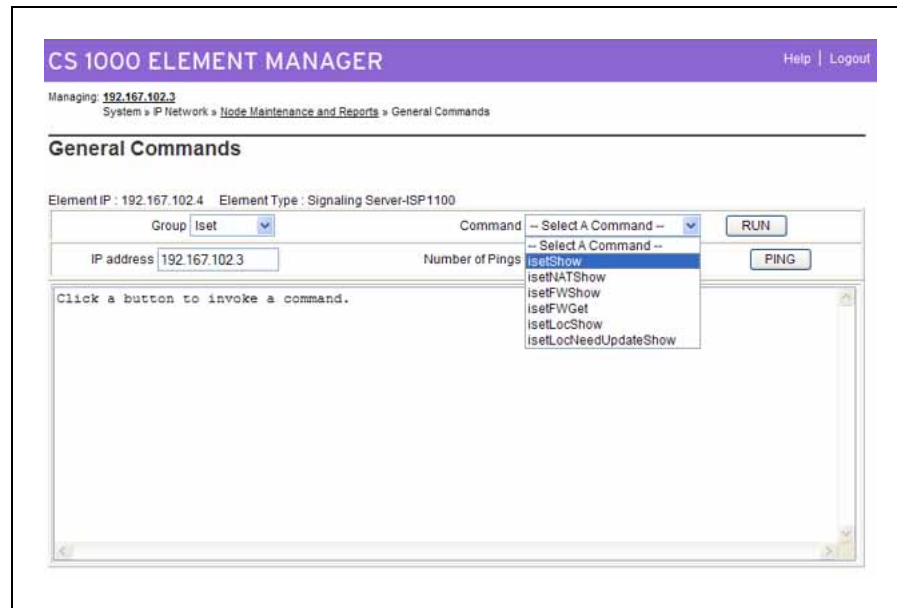
- 6 Enter the time in minutes in the **Timeout In** text box.
 - 7 Click **Run**.
- The command output is displayed in the pane below the command.

—End—

iset commands in Element Manager

Access **isetFWShow** and **isetFWGet** in the **General Commands** window from the **iset** group in the **Group** drop-down list. See [Figure 22 "iset commands"](#) (page 107).

Figure 22
iset commands



Firmware download using UNISlim FTP

Previously, IP Phones on CS 1000 systems downloaded their firmware using Trivial File Transfer Protocol (TFTP). Firewalls often have their well-known TFTP port (port 69) disabled to maintain security. When port 69 is blocked, IP Phones cannot obtain firmware downloads. This situation prevents the IP Phone from registering and coming into service.

In order to eliminate the file transfer problem with the firewalls and TFTP, a UNISlim File Transfer Protocol (UFTP) download solution is implemented.

UFTP enhances security, because it is a proprietary protocol, as opposed to TFTP which is an open protocol. It enables end users to improve their firewall security by closing port 69 to block TFTP in their firewall and policy-based switches and routers.

ATTENTION

For the UFTP IP Phone firmware download to work, it is necessary to explicitly open port 5100 (UNISlim signaling) and port 5105 (UFTP signaling).

If a network firewall is in use, ports 5100 (UNISlim signaling) and 5105 (UFTP signaling) must be explicitly opened in the IP Phone-to-UFTP server direction. Opening these ports enables UNISlim and UFTP firmware

download messages to travel through the firewall. Both of these ports can be safely enabled by firewalls. See [Table 23 "Source/destination port usage on either side of the connection"](#) (page 108).

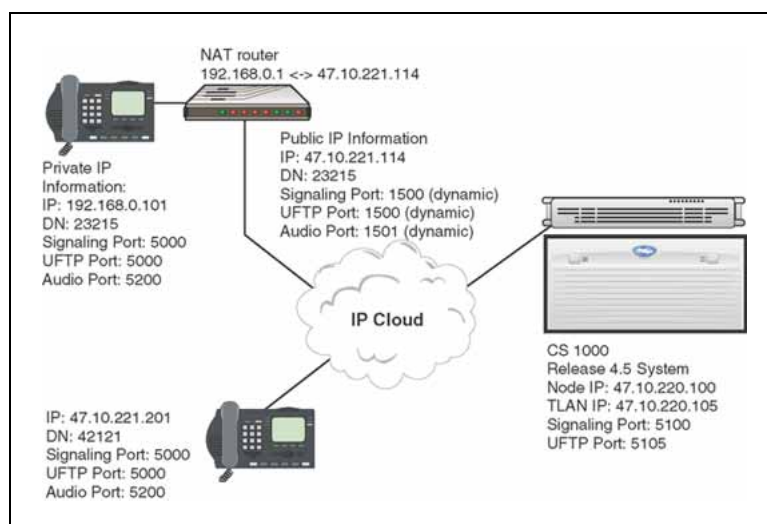
Table 23
Source/destination port usage on either side of the connection

Port	IP Phone signaling	IP Phone UFTP	UFTP Server
Source port	5000 (see below)	5000 (see below)	5105
Destination port	5100	5105	5000 (see below)

ATTENTION

The UFTP firmware download is compatible with the NAT Traversal feature. If the IP Phone is behind a Network Address Translation (NAT) device, then a different public signaling port is used. The public signaling port is assigned dynamically. See [Figure 23 "Using NAT with UFTP"](#) (page 108).

Figure 23
Using NAT with UFTP



Two Download log files log the results of the UFTP firmware downloads: "uftplog0.txt" and "uftplog1.txt". One file is active and one file is inactive. When a file is full, it becomes the inactive file, and the other file is written to. The active file displays the most recent entries.

On Voice Gateway Media Cards, the log files are located in the /C:/LOG directory. The Download log files are limited to 10K each for a total of 20K. Approximately 128 log messages can be saved in each log file.

On the Signaling Server, the log files are located in the /U/LOG directory. The Download log files are limited to 400K each, for a total of 800K. Approximately 5000 log messages can be saved in each log file.

The Download log files are generated during initialization of the UFTP Server task. If the Download log files do not exist during the start-up of the UFTP Server task, new Download log files are created.

The Download log file is a circular file, writing over the oldest information when the log file is full. Each log file entry contains the following download information about the IP Phone:

- F/W download date
- F/W download start time
- F/W download status (specifies if the download succeeded or failed)
- IP Address of the IP Phone
- IP Phone type
- F/W download error code. If the F/W download was successful, this field is empty. The following is the list of all possible error codes:
 - 00 = F/W not exist
 - 01 = F/W size is 0
 - 02 = F/W corrupted
 - 03 = RUDP connection down
 - 04 = Response time out
 - 05 = Reason: Unknown

The format of the download log message is:

<Date> <Download start time> <Download Status> <IP address of the IP Phone> < IP Phone type> <Error Code>

The following is an example of the Download log message:

```
31/01/04 17:04:36 F/W Dnld fail:(47.11.215.44) i2004 Ph2
(F/W Corrupted)
31/01/04 17:05:46 F/W Dnld success:(47.11.215.44) i2004
```

CLI commands

The following CLI commands support UFTP firmware downloads:

- uftpNodeShow
- uftpShow
- uftpRunTimeDataReset
- activeDlogShow
- inactiveDlogShow
- dnldFailShow

uftpNodeShow

The **uftpNodeShow** command provides a complete UFTP IP Phone firmware download summary of each node. This includes the configured cards in the node that are not responding.

Each node summary contains the following information:

- Index
- TN - LL S CC or C C
- Host Type
- TLAN IP Address
- Data Period
- Active Download Count (Act)
- Server Up Time (Srv Up Time)
- Successful Download Count (Ok)
- Failure Download Count (Fail)

Figure 24 "uftpNodeShow command output" (page 110) is an example of output from the **uftpNodeShow** command.

Figure 24
uftpNodeShow command output

```
oam> uftpNodeShow
```

Retrieving information form the peer(s), please wait!

----- UFTP IP Phone Firmware Download Summary for Node 5488 -----							
Index	TN	Host Type	TLAN IP Addr	Act	Srv Up Time	Ok	Fail
01		ISP 1100	47.11.213.83	002	0000 01:36:12	00070	00001
02	100 1 15	SMC	47.11.213.79	001	0000 02:25:10	00050	00001
03	20 1 2	ITG-P	47.11.213.103	001	0000 05:23:10	00048	00001
Total				004		00168	00003

----- card in node configured that are not responding -----			
Index	TN	Host Type	TLAN IP Addr
04	20 1 7	SMC	47.11.213.158

uftpShow

The **uftpShow** command displays the following information:

- configuration information about UFTP

- count of successful downloads because the Signaling Server/Voice Gateway Media Card reboot
- count of downloads that failed or prematurely ended because the Signaling Server/Voice Gateway Media Card reboot
- number of active downloads, and a list of each, including:
 - type of IP Phone
 - IP addresses of the IP Phones that downloaded firmware
 - number of bytes downloaded

Figure 25 "uftpShow command output" (page 111) is an example of output from the `uftpShow` command.

Figure 25
uftpShow command output

```
oam> uftpShow

----- UFTP Server Configuration -----
UFTP Server IP address ..... 192.167.103.2 [port: 5105]
Concurrent downloading limit ..... 100 sets
FirmWare ModelName PolicyName FileName
-----
-
B76 IP Phone 2004 Phase 0/1 DEFAULT /u/fw/x00.fw
B76 IP Phone 2002 Phase 1 DEFAULT /u/fw/x01.fw
DBB IP Phone 2004 Phase 2 DEFAULT /u/fw/x02.fw
DBB IP Phone 2002 Phase 2 DEFAULT /u/fw/x02.fw
DBB IP Phone 2001 Phase 2 DEFAULT /u/fw/x02.fw
C4C IP Phone 2007 Phase 2 DEFAULT /u/fw/x21.fw
C46 IP Phone 1120E DEFAULT /u/fw/x24.fw
C46 IP Phone 1140E DEFAULT /u/fw/x25.fw
C46 IP Phone 1150E DEFAULT /u/fw/x27.fw

Total firmware = 9

----- Run Time Data -----
Last UFTP reset ..... 2/21/2007 20:43:39
Cumulation Period ..... 0005 13:53:44
Successful downloads ..... 0
Fail downloads ..... 0

----- Active Downloads -----
Current downloading sets ..... 0

TermType IP Address Downloaded[KByte]
-----
```

uftpRunTimeDataReset

The `uftpRunTimeDataReset` command is used to reset the run time data field in the UFTP data block.

Figure 26 "uftpRunTimeDataReset command output" (page 112) is an example of output from the `uftpRunTimeDataReset` command.

Figure 26
uftpRunTimeDataReset command output

```
oam> uftpRunTimeDataReset
Run time data reset OK.
----- Run Time Data -----
Successful downloads ..... 0
Fail downloads ..... 0
```

activeDlogShow

The **activeDlogShow** command displays the active log file information for UFTP IP Phone firmware downloads. When no parameter is entered, the output displays the contents of the entire active log file. When a line number is entered, **activeDlogShow[numOfLine]**, the output displays the active log file by the number of lines.

Figure 27 "activeDlogShow command output" (page 112) is an example of output from the **activeDlogShow** command.

Figure 27
activeDlogShow command output

```
oam> activeDlogShow
Active F/W download file: /u/log/UFTPLOG0.TXT
Space remaining:      55

/u/log/UFTPLOG0.TXT
-----
12/29/03 19:58:41 f/w dnld success: (47.11.217.11) I2004
12/29/03 20:24:30 f/w dnld success: (47.11.217.12) I2004
12/29/03 21:42:11 f/w dnld success: (47.11.217.15) I2002
12/29/03 22:17:40 f/w dnld success: (47.11.217.20) I2004
```

inactiveDlogShow

The **inactiveDlogShow** command displays the nonactive dlog file information for UFTP IP Phone firmware downloads. When no parameter is entered, the output displays the contents of the entire file. When a line number is entered, **inactiveDlogShow [numOfLine]**, the output displays the nonactive dlog file by the number of lines.

Figure 28 "inactiveDlogShow command output" (page 113) is an example of output from the **inactiveDlogShow** command.

Figure 28
inactiveDlogShow command output

```
oam> inactiveDlogShow
inactiveDlogShow
Active F/W download file: /u/log/UFTPLOG0.TXT
Space remaining:      399755

Inactive F/W download file: /u/log/UFTPLOG1.TXT
/u/log/UFTPLOG1.TXT
-----
12/27/03 19:58:41 f/w dnld success: (47.11.217.11) I2002
12/27/03 20:24:30 f/w dnld success: (47.11.217.12) I2002
12/27/03 21:42:11 f/w dnld success: (47.11.217.15) I2002
12/27/03 22:17:40 f/w dnld success: (47.11.217.20) I2004
```

dnldFailShow

The **dnldFailShow** command displays the "download failed" status logged in the active and inactive files. When no parameter is entered, the output displays the all the failed UFTP download information in the active and inactive files. When a line number is entered, **dnldFailShow[numOfLine]**, the output displays the download fail status in the active and inactive files by the number of lines.

Figure 29 "dnldFailShow command output" (page 113) is an example of output from the **dnldFailShow** command.

Figure 29
dnldFailShow command output

```
oam> dnldFailShow
Active F/W download file: /u/log/UFTPLOG0.TXT
-----
12/29/03 19:58:41 F/W dnld fail: (47.11.217.11) I2004 (F/W not exist)
12/29/03 20:24:30 F/W dnld fail: (47.11.217.12) I2004 (F/W size is 0)
12/29/03 21:42:11 F/W dnld fail: (47.11.217.15) I2002 (RUDP connection down)
12/29/03 22:17:40 F/W dnld fail: (47.11.217.20) I2004 (Response time out)

Inactive F/W download file: /u/log/UFTPLOG1.TXT
-----
12/28/03 19:58:41 F/W dnld fail: (47.11.217.11) I2004 (RUDP connection down)
12/28/03 20:24:30 F/W dnld fail: (47.11.217.12) I2004 (RUDP connection down)
12/28/03 21:42:11 F/W dnld fail: (47.11.217.15) I2002 (RUDP connection down)
12/28/03 22:17:40 F/W dnld fail: (47.11.217.20) I2004 (Response time out)
```

NAT Traversal feature

Network Address Translation (NAT) provides the following benefits:

- the ability to network multiple sites with overlapping private address ranges
- added security for servers on a private network
- conservation of public IP address allocation

A NAT device (router) exists between a private network and a public network. The NAT device maps private addresses to public addresses.

With the NAT Traversal feature, several IP Phones are now supported behind a single Cone NAT router with, or without, Virtual Private Network (VPN) capabilities. This support enables large-scale deployment of Voice over Internet Protocol (VoIP) in teleworking and Small Office/Home Office (SOHO) environments.

Supported Cone NAT routers include:

- Full Cone
- Restricted Cone
- Port Restricted Cone

ATTENTION

A Cone NAT router with more than one IP Phone connected to it must support hairpinning. Hairpinning occurs when an IP Phone behind a NAT router can send packets to the Public IP address and port of another IP Phone connected to the same NAT router.

ATTENTION

Symmetric NAT routers are not supported. If the IP Phone is behind a Symmetric NAT, IP Phone registration is unsuccessful and the IP Phone displays a "NAT Error! ITG3053" message.

Echo Servers

NAT Traversal is a function of the CS 1000 Release 4.5 or later software, and not a function of the NAT router. NAT Traversal uses two Echo Servers residing on the Signaling Server. Echo Server 1 detects the presence of a NAT router, while Echo Server 2 detects the type of NAT router. Both Echo Server 1 and Echo Server 2 are required for the NAT Traversal feature to function properly.

If a compatible NAT router is detected, successful IP Phone registration occurs and the software invokes the NAT Mapping Keep Alive function to prevent loss of the IP connection. If an incompatible NAT is detected, an error is displayed on the IP Phone display and the IP Phone is not allowed to register.

Mapping

When an IP Phone is used in a private network behind a NAT device, the NAT router strips the IP Phone private IP address and private port number and assigns it a public IP address and public port number.

To support multiple IP Phones behind one NAT device, NAT must map between public/private IP addresses, and ports for each IP Phone behind it. There is a mapping for both a signaling port and a media (voice) port.

Placing an IP Phone behind Multiple NAT devices is an unsupported configuration. If it is necessary to have a configuration with multiple NATs between the IP Phone and the Voice Gateway Media Card, all NATs on the path must follow the rules described in the following sections for signaling and media streams.

Mapping is configured and implemented using the NAT device. The IP Line application does not implement any of the mappings.

NAT and signaling

NAT hides the true identity of the IP Phone from the LTPS. The LTPS is only aware of any IP Phone based on the public IP address and port of the signaling messages. A signaling message originates from the IP Phone on the private side from port 5000. That signaling message is then mapped from the private side to a public IP and port; that is the IP address seen by the LTPS.

Signaling messages between the Voice Gateway Media Card and IP Phones are carried by RUDP. Each RUDP connection is distinguished by its IP address and port number.

The NAT device performs private-to-public mapping for the signaling port for each IP Phone behind it to support multiple IP Phones. The TPS uses fixed port numbers for signaling. The NAT device must perform consistent private-to-public mapping for these port numbers. [Table 24 "Signaling UDP Ports" \(page 115\)](#) lists the UDP port number used.

Table 24
Signaling UDP Ports

UDP Port	Device	Use
5000	IP Phone	incoming signaling messages to the IP Phones, including UFTP messaging
5100	LTPS	incoming call processing messages to the LTPS

UDP Port	Device	Use
5105	UFTP	incoming UFTP packets to the UFTP server
4100	LTPS	incoming registration message to Connect Server
7300	LTPS	incoming registration messages to node Master

Port numbers on the Voice Gateway Media Card use a fixed numbering scheme where the starting number for the port range is configurable. The first port on the card uses the configured starting port number; the rest of the port numbers follow in sequence. Each port has two sequential numbers: one for RTP and one for RTCP.

Do not change this port at any time. Map this port to port 5200 on the IP Phones.

Table 25
IP Line UDP Ports

UDP Port	Device	Use
5200-5262	Media Card	RTP packets (configurable starting port number – IP Phone port matches it)
5201-5263	Media Card	RTCP packets into Media Card (port number is RTP port number + 1)
5200-5246	ITG-P 24-port line card	RTP packets (configurable starting port number – IP Phone port matches it)
5201-5247	ITG-P 24-port line card	RTCP packets into Media Card (port number is RTP port number + 1)
5200	IP Phone	RTP packets into IP Phone (port matches first RTP port of the Voice Gateway Media Card)
5201	IP Phone	RTCP packets into IP Phone (port matches first RTCP port of the Voice Gateway Media Card)

NAT Mapping Keep Alive

The normal operation of the LTPS and the IP Phone requires the LTPS to send a periodic Watchdog Reset UNISTIM message. This message resets the hardware watchdog timer running on the IP Phone and specifies the period for the timeout. If the LTPS does not send the Watchdog Reset message before the watchdog timer expires, the IP Phone resets and begins a new registration cycle with the LTPS.

To avoid loss of the IP connection, the NAT Mapping Keep Alive function sends the Watchdog Reset message more frequently. Default values are recommended. However, if it is necessary to increase the frequency of the Reset Watchdog message, increase the NAT Mapping Keep Alive timer value.

NAT Traversal can be configured to provision the length of time the audio and signaling port mapping is refreshed. This configuration can be done in Element Manager, on the Call Server in LD 117, or in TM through a window to the Call Server.

By default, all IP Phones behind a NAT device have the signaling and audio path kept alive. The default value is 30 seconds. The value can be decreased to 20 seconds or increased to 600 seconds.

Mute and Hold considerations

IP Line software has two special situations when interworking with NAT: Mute and Hold.

Mute

[Table 26 "Mute process" \(page 117\)](#) describes the Mute process.

Table 26
Mute process

	Description
Problem	
1	When a user enables Mute, the LTPS sends a Mute Transmit (Tx) command to the IP Phone. That command forces the IP Phone to generate silence in the transmit direction.
2	If the IP Phone is using an evocator that implements silence suppression, for example G.729AB, the IP Phone sends one silence frame to the far end, and then stops sending any further frames until Mute is cancelled.
3	Data sent from the IP Phone stops.
4	The NAT device sees that the IP Phone UDP connection is not active in the transmit direction and starts aging the translation.
5	Depending on the length of time the call is muted and the duration of the NAT translation aging timeout value, the NAT device might timeout the translation and drop the connection.
6	All packets coming from the far end are dropped by the NAT device.
7	When mute is cancelled, the IP Phone starts transmitting again.
8	NAT considers this to be a new connection and creates a new translation. NAT sends data to the far end using this new translation, resulting in half-duplex voice connection between the IP Phone and the far-end device.

	Description
9	Data sent to the far end device gets there but the data coming back is lost.
Solution	
1	The IP Phone periodically sends an extra non-RTP packet to the far end to keep the NAT translation alive, ensuring that the NAT session timeout does not expire.
2	The non-RTP packet is constructed to fail any RTP validation tests so it is not played out by the far-end device (IP Phone or gateway channel).

Hold

The Hold function differs from the Mute function as Hold does not cause problems with the audio stream. [Table 27 "Hold process" \(page 118\)](#) describes the Hold process.

Table 27
Hold process

	Description
1	When an IP Phone user places a call on Hold, the audio stream in both the Transmit (Tx) and Receive (Rx) directions closes.
2	The NAT device begins aging the translation. When the audio stream is closed and no voice path is present, the IP Phone defaults to sending periodic non-RTP packets to keep the NAT translation alive. Therefore, when a call is put on Hold, the IP Phone defaults to sending these non-RTP packets.
3	When the call is retrieved from Hold, a new set of open audio-stream messages is issued by the LTPS and new connections are established reusing the same NAT translation.

NAT and VLANs

Support of Virtual LANs (VLANs) is entirely dependent on the Layer 2 switch to which the IP Phone is immediately connected. Users behind a NAT router may find that the configuration of a VLAN ID is unsupported by their NAT router. See the documentation of the NAT router to determine if a VLAN ID is supported.

Users who attempt to use an IP Phone with VLAN enabled on a NAT router that does not support VLANs cannot connect to the CS 1000 system. If DHCP is used, the IP Phone cannot even obtain an IP address.

ATTENTION

Most NAT routers do not support 802.1Q Tagging. If 802.1Q Tagging is not supported on the NAT device, the check box **Enable 802.1Q support** in Element Manager Node Summary Page under the "QoS" Section must be left unchecked. See [Figure 30 "802.1Q Tagging on Node Summary page in Element Manager" \(page 119\)](#). If 802.1Q Tagging is enabled for IP Phones behind NAT, the IP Phones can send the initial "Resume Connection" message, but then the IP Phones reset and no call path is established.

Figure 30
802.1Q Tagging on Node Summary page in Element Manager

The screenshot shows the 'Edit' configuration page for Node ID 9 in the CS 1000 ELEMENT MANAGER. The interface includes a top navigation bar with 'CS 1000 ELEMENT MANAGER' and a 'Logout' link. Below the navigation bar, the 'Managing: 192.167.102.3' and 'Import Node Files' links are visible. The main configuration area is titled 'Edit' and contains several sections:

- Save and Transfer** and **Cancel** buttons at the top.
- IP Telephony Node** section:
 - Node ID: 9
 - Telephony LAN (TLAN) Node IP address: 192.167.103.3
 - Embedded LAN (ELAN) gateway IP address: 192.167.102.1
 - Embedded LAN (ELAN) subnet mask: 255.255.255.0
 - Voice LAN (TLAN) subnet mask: 255.255.255.0
- + VGW and IP phone codec profile** section.
- QoS** section:
 - Diffserv Codepoint(DSCP) Control packets: 40 (0 - 63)
 - Diffserv Codepoint(DSCP) Voice packets: 46 (0 - 63)
 - Enable 802.1Q support: ☐
 - 802.1Q Bits value (802.1p): 6 (0 - 7)
- + LAN configuration** section.

NAT Traversal and Proactive Voice Quality Management

Real-Time Control Protocol (RTCP) signaling provides statistics (for example, latency, packet loss, and jitter) about the Real-Time Transfer Protocol (RTP) stream. For the RTCP signaling to be successful, the PUBLIC RTCP port number must be the RTP port number + 1. For example, if the PUBLIC RTP port is 12000, then the PUBLIC RTCP port must be 12001.

The NAT router typically assigns the RTCP port number as RTP port number + 1. However, the NAT router is not guaranteed to properly assign the RTCP port number. When the RTCP port number is not properly assigned, the RTCP message exchange fails and the Proactive Voice Quality Management feature does not receive the required RTCP data. A message is printed to the LTPS console and syslog file and an SNMP trap (ITG3054) is generated.

The NAT Traversal feature attempts a "best effort" approach to initiate the NAT router to properly assign the RTPC port number. The "best effort" approach is dependent on the NAT router implementation, may vary from NAT router to NAT router, and cannot be guaranteed by the NAT Traversal feature.

Configuring NAT Traversal in Element Manager

To configure the Echo Servers IP addresses/port numbers and NAT Keep Alive time-out setting using Element Manager, in the Element Manager navigator select **IP Network > Network Address Translation**.

See [Figure 31 "NAT configuration" \(page 120\)](#).

Figure 31
NAT configuration

CS 1000 ELEMENT MANAGER - cli | Logout

Managing: [162.167.102.3](#)
System » IP Network » Network Address Translation (NAT)

Network Address Translation (NAT)

Input Description	Input Value	
Echo Server 1 IP Address	0.0.0.0	
Echo Server 1 Port	10000	Range: 1000 to 65535
Echo Server 2 IP Address	0.0.0.0	
Echo Server 2 Port	10000	Range: 1000 to 65535
NAT Session Timeout Value (seconds)	30	Range: 20 to 600

Note: IP address 0.0.0.0 means that the default local Echo Server will be enabled

Configuring NAT Traversal in LD 117

Commands are available in LD 117 to configure and print the Echo Servers IP addresses/port numbers and NAT Keep Alive time-out setting.

No configuration is required for the Echo Servers to work. The default IP address of 0.0.0.0 means that Echo Server 1 uses the TLAN network interface IP address. The default IP address of 0.0.0.0 means that Echo Server 2 uses the Node IP address.

An IP address of 0.0.0.0 means the default local Echo Server is enabled.

ATTENTION

The NAT Traversal feature is essentially automatic. Changing the IP addresses or ports must only be done in exceptional cases when an Echo Server external to the CS 1000 system is used.

If IP addresses are specified, they must be for servers external to the system. The IP addresses cannot be the same. Duplicate IP addresses can only be used if the default of 0.0.0.0 is used. If the IP addresses are the same (and not 0.0.0.0), an error message is generated and the input is not accepted.

Table 28
LD 117 commands for NAT

Command	Description
CHG ES1 <Echo Server 1 IP Address> <Echo Server 1 Port>	Change Echo Server 1 IP address and port number, where: • Default Echo Server 1 IP Address = 0.0.0.0 • Default Echo Server 1 Port number = 10 000 Echo Server 1 default IP address uses the TLAN IP address of the LTPS.
CHG ES2 <Echo Server IP Address> <Echo Server Port>	Change the Echo Server 2 IP address and port number, where: • Default Echo Server 2 IP Address = 0.0.0.0 • Default Echo Server 2 Port number = 10 000 Echo Server 2 default IP address uses the node IP address on the node master card.
PRT ES1	Print Echo Server 1 IP address and port number.
PRT ES2	Print Echo Server 2 IP address and port number.
PRT ESS	Print both Echo Servers IP addresses and port numbers.
CHG NKT <time-out setting>	Change NAT Mapping Keep Alive Time-out setting of port mapping for devices behind a NAT router, where: time out setting = 20-(30)-600 seconds
PRT NKT	Print NAT Mapping Keep Alive Time-out setting of port mapping for devices behind a NAT router.

CHG ES1/CHG ES2

If the IP addresses entered for ES1 and ES2 are the same and both are not 0.0.0.0 or for external servers, an error message is generated and the input is not accepted. Any value between 1000 and 60000 can be entered for the port. If the port value is outside of that range, an error message is generated. Just the port (and not the IP addresses) can also be configured. This is accomplished by entering data similar to the following:

```
=>chg es1 0 5400
```

The value 0 for the IP address is interpreted as: 0.0.0.0. This means the Echo Server runs locally using the configured port value.

The port values both default to 10 000. If an IP address is configured, it is also necessary to configure the port. An error message is generated if no port is configured but an IP address is configured.

If both Echo Servers are not configured, then the LTPS on the Signaling Server or the Voice Gateway Media Card uses two local instances of the Echo Server. If both Echo Servers are configured, then the LTPS uses the external Echo Servers. If an external Echo Server fails, that functionality is lost unless the external Echo Server implements a transparent redundancy scheme. The external Echo Server is responsible for its redundancy and reliability.

PRT commands

[Figure 32 "PRT commands output" \(page 123\)](#) is an example of the output of the PRT commands when the defaults are used. If other IP addresses or port numbers have been configured, then these appear in place of the 0.0.0.0 or 10 000 in the examples in [Figure 32 "PRT commands output" \(page 123\)](#).

Figure 32
PRT commands output

```

=>
=>PRT ESS
Echo Server      IP Address      Port
-----
1                0.0.0.0          10000
2                0.0.0.0          10000
Time-out: 30 seconds
=>

=>
=>PRT ES1
Echo Server      IP Address      Port
-----
1                0.0.0.0          10000
=>

=>
=>PRT ES2
Echo Server      IP Address      Port
-----
2                0.0.0.0          10000
=>

=>
=>PRT NKT
NAT Keep alive time-out: 30 seconds
=>

```

CLI commands

The CLI commands described in this section provide information about IP Phones behind a NAT device and the Echo Servers.

isetShow

When the isetShow command is used, a NAT column lists the NAT type if an IP Phone is behind a NAT, where:

- C – Cone NAT
- S – Symmetric NAT
- U – Unknown. Behind a NAT of unknown type (response received from only Echo Server 1).
- P – Pending. Waiting for response from the IP Phone or the IP Phone never received a response from Echo Server 1.
- .. – Blank space. Indicates the IP Phone is not behind any kind of NAT (normal case).

For example (partial output from the left side of the screen):

```
IP Address  NAT Type  RegType
47.11.215.183  i2001 Regular
47.11.179.168  C i2004 Regular
47.11.179.167  C i2004 Regular
```

isetReset

The **isetReset** command resets an IP Phone based on the entered IP address or TN. The IP address must be the Public IP address for IP Phones behind a NAT. If the entered IP address identifies an IP Phone that is behind a NAT and no other IP Phone are sharing the address, then the IP Phone is reset.

However, if the entered IP address identifies multiple IP Phones (multiple IP Phones behind a NAT sharing the same public IP address), then an error message is printed. This message indicates there is more than one IP Phone with the IP address, lists the IP Phones and their TNs, and recommends using the **isetReset** TN command.

For example:

```
oam> isetReset "47.11.217.102"
WARNING: There are 2 IP Phones that use the public IP address
of 47.11.217.102 Please reset the IP Phone using the TN:
isetReset "TN".
```

The number of IP Phones that share the same public IP address is printed.

Commands such as **isetScpwQuery**, **isetScpwModify**, and **isetScpwVerify** have the same error handling as **isetReset**. If an IP address is entered that multiple IP Phones are using, an error message prints. For example,

```
WARNING: There are 2 IP Phones that use the public IP address
of 47.11.217.102.
```

isetGet

The **isetGet** command can search on the NAT type.

NAT = xxx where x is:

- C – the IP Phone is behind a Cone NAT
- S – the IP Phone is behind a Symmetric NAT
- U – the IP Phone is behind a NAT of unknown type (response only received from Echo Server 1)
- P – waiting on a response from the IP Phone, or the IP Phone never received a response from Echo Server 1
- .. – Blank space: the IP Phone is not behind any kind of NAT (normal case)

- Y – true when an IP Phone NAT is C, S or U
- N – true when an IP Phone NAT is . . (blank), meaning no NAT is detected

For example:

```
IPL> isetGet "NAT == Y"
```

returns the output (partial output from the left side of the screen):

```
IP Address  NAT Type RegType State Up Time
47.11.179.168 C i2004 Regular online 0 04:20:34
47.11.179.167 C i2004 Regular online 0 03:48:17
```

isetNATShow

The **isetNATShow** command outputs information about IP Phones behind a NAT device.

The public and private IP address and ports are provided for both signaling and media.

In most cases, the private signaling port information is available. If the firmware on the IP Phone is outdated, the private signaling port information is not printed.

If the IP Phone is found to be behind a Symmetric NAT device, the media IP information is not printed out.

The following is an example of output for a Symmetric NAT device.

```
Signalling          Media
Public IP Addr:Port  Public IP Addr:Port
(Private IP Addr:Port) (Private IP Addr:Port) NAT
Type RTCP Type Set-TN Regd-TN
-----
47.11.217.102:10000 <<No Speech Possible>> Symmetric Y i2002
Ph2 061-08 061-08
(192.168.1.3:5000)
```

The type of NAT is indicated, as detected by Echo Server 2. The support of RTCP signaling is indicated by Y; if N is displayed, then features that depend on RTCP, such as Proactive Voice Quality Management (PVQM), will not work.

An IP Phone TN or public signaling IP address can be entered after the command. Entering the **isetNATShow** command at the CLI of any card in an IP Telephony Node along with the TN or IP address of a particular IP Phone displays the information shown in the previous example, as well as the identification of the card with which the IP Phone is registered. This is useful when it is necessary to identify the card on which to enable a message monitor, or to connect a sniffer, when debugging a specific IP Phone problem.

Figure 33 "isetNATShow sample output" (page 126) shows a sample output.

Figure 33
isetNATShow sample output

```
IPL> isetNATShow "47.11.217.102"

value = 0 = 0x0

IPL>

Signalling Media

Public IP Addr:Port Public IP Addr:Port

(Private IP Addr:Port) (Private IP Addr:Port) NAT Type RTCP Type Set-TN Regd-TN
-----

->Found on Card TN 009-00 ,ELAN IP 47.11.217.21,TLAN IP 47.11.216.185 :

47.11.217.102:10000 47.11.217.102:10354 Cone Y i2002 Ph2 061-08 061-08

(192.168.1.3:5000) (192.168.1.3:5200)

->Found on Card TN 009-00 ,ELAN IP 47.11.217.21,TLAN IP 47.11.216.185 :

47.11.217.102:10006 47.11.217.102:10007 Cone Y i2004 061-00 061-00

(192.168.1.4:5000) (192.168.1.4:5200)
```

The command "isetShow" and "isetNATShow" can display the information about an IP Phone based on IP or TN. The "IP" is the Public IP address used for signaling. If "isetShow" or "isetNATShow" is typed with a Public IP address used by multiple IP Phones, then all those IP Phones are displayed, even if the IP Phones are registered to different cards. Therefore, the "isetShow" and "isetNATShow" now display the information similar to the following example:

```
Signaling....
Public...
(Private...
----
->Found on Card TN 009-00, ELAN IP....
47.11.217.102....
```

Notice how the "Found on" line is below the title, and is displayed before every IP Phone.

If a PVQM command is entered with an IP address that multiple IP Phones are using, then an error message is also printed.

WARNING: There are 2 IP Phones that use the public IP address of 47.11.217.102

These PVQM commands include:

- RTPStatShow
- RTPTraceShow
- RTPTraceStop
- rPing
- rPingStop
- rTraceRoute
- rTraceRouteStop
- eStatShow
- RUDPStatShow
- isetInfoShow

echoServerShow

The **echoServerShow** command provides both configuration information about the Echo Servers and information about interactions with the Echo Servers for the IP Phones on a specific LTPS. Use this command on an LTPS card to investigate a problem with an IP Phone registered to that LTPS card. This is a per-card command that provides information about the Echo Servers from the viewpoint of the LTPS on the card where the command is entered.

The command has one optional parameter, "action"; the only valid value is 99. When **echoServerShow 99** is entered, the counter values are reset after they are displayed. When just **echoServerShow** is entered, the counter values are displayed without being reset.

The output for each Echo Server displays the following information:

- Configured – the IP address: port configured for this Echo Server in LD 117
- Actual – the IP address: port used for this Echo Server, followed by an explanation in parenthesis. This is different from the "Configured" parameter only when the default address (0.0.0.0) has been configured. The explanation in parenthesis is one of the following:
 - (TLAN IP, this card) – the IP address used is the TLAN network interface of this card; the Echo Server is active on this card.

- (node IP, this card) – the IP address used is the Node IP address; the Echo Server is active on this card because it is the node master.
 - (node IP, other card) – the IP address used is the Node IP address, but another card is currently the Node master; the Echo Server is not active on this card.
 - (not this card) – the IP address is not the card TLAN IP address or the Node IP address; the Echo Server is not active on this card.
- LTPS request sent – the number of **Resolve Port Mapping Request** messages sent from the LTPS to IP Phones, with this Echo Server identified as the one to contact.
 - Failed resp rec.d – the number of **Resolve Port Mapping Ack** messages received from the IP Phones that had the public IP address and port configured as 0.0.0.0:0000. Each increment of this counter indicates an IP Phone never received the **Discover Port Mapping Ack** response from the Echo Server (all 10 attempts failed).

The two peg counts give an indication of the interaction this LTPS is having with the Echo Server. It is not a direct sign of the health of the Echo Server; network conditions for IP Phones registered to this LTPS may be preventing communication with this Echo Server while another LTPS IP Phones have no problem. The **echoServerShow** command output can help to understand why a particular IP Phone registered to a LTPS may be having difficulties or helps to uncover patterns of communication problems between IP Phones and Echo Servers.

A sample output is shown in [Figure 34 "echoServerShow sample output" \(page 129\)](#).

Figure 34
echoServerShow sample output

```
->echoServerShow

Echo Server 1
-----
Configured:          0.0.0.0:10000
Actual:              47.11.212.54:10000 (TLAN IP, this card)
LTPS request sent: 112665
Failed resp rec'd: 0

Echo Server 2
-----
Configured:          0.0.0.0:10000
Actual:              47.11.212.60:10000 (node IP, other card)
LTPS request sent: 82201
Failed resp rec'd: 0
NAT Timeout: 30 seconds
```

When the **echoServerShow** command with the reset parameter 99 is entered, the counter values are displayed and then reset. If the **echoServerShow** command is entered again and no requests have since been sent, the counter values are displayed as 0.

A sample output is shown in [Figure 35 "echoServerShow 99 sample output" \(page 130\)](#).

Figure 35
echoServerShow 99 sample output

```

->echoServerShow 99

Echo Server 1
-----
Configured:          0.0.0.0:10000
Actual:              47.11.212.54:10000 (TLAN IP, this card)
LTPS request sent: 81563
Failed resp rec'd: 40

Echo Server 2
-----
Configured:          0.0.0.0:10000
Actual:              47.11.212.60:10000 (node IP, other card)
LTPS request sent: 50199
Failed resp rec'd: 4
NAT Timeout: 30 seconds

->echoServerShow

Echo Server 1
-----
Configured:          0.0.0.0:10000
Actual:              47.11.212.54:10000 (TLAN IP, this card)
LTPS request sent: 0
Failed resp rec'd: 0

Echo Server 2
-----
Configured:          0.0.0.0:10000
Actual:              47.11.212.60:10000 (node IP, other card)
LTPS request sent: 0
Failed resp rec'd: 0
NAT Timeout: 30 seconds

```

vgwShow

The **vgwShow** command has been modified to allow the optional entry of an IP Phone IP address and port. A search is made of all the Voice Gateway Media Cards in the node to find the IP Phone IP address and port. With the introduction of NAT Traversal, more than one IP Phone may map to a single IP address. The command input is modified to allow the entry of the public port number for a specific IP Phone.

vgwShow <"IPAddr">, <port>

If no port number is entered, the first entry found with the specified IP address on a Voice Gateway Media Card is returned. An example is shown in [Figure 36 "vgwShow with IP address command output" \(page 131\)](#).

Figure 36
vgwShow with IP address command output

```

-> vgwShow "47.11.215.136"
value = 0 = 0x0
-> Found on Card TN 005-00 , HLAN IP 47.11.216.174, TLAN IP 47.11.215.143 , number of matches 2

```

Chan	ChanState	DspMode	Codec	TN	Reg	AirTime	rxTsap	txTsap
17	Busy	Voice	G.711-20	0x0505	yes	21	47.11.215.143:5234	47.11.215.136:2237

```

-> Found on Card TN 003-00 , HLAN IP 47.11.216.175, TLAN IP 47.11.215.146, number of matches 1

```

Chan	ChanState	DspMode	Codec	TN	Reg	AirTime	rxTsap	txTsap
1	Busy	Voice	G.711-20	0x0307	yes	21	47.11.215.145:5202	47.11.215.136:5200

When the IP address is found in the list of VGW channels for a card other than the card where the command was entered, the VGW channel information for the first occurrence is returned, plus a count of the number of times the IP address occurs in that card list. Multiple instances can occur when the customer network is configured so that multiple IP Phones are behind a NAT device sharing the NAT device public IP address.

If there is more than one match, the administrator can log into that specific card and enter the **vgwShow** command without entering an IP address and port number. That will print all the busy channels on the card. To quickly find a particular IP Phone, use the IPDN or DNIP commands in LD 117 to obtain the IP Phone media stream public IP address and port number; then enter the public IP address and port number as parameters for the **vgwShow** command.

Corporate Directory

The Corporate Directory feature is based on the M3900 telephone Corporate Directory feature.

The Corporate Directory database is created using TM 3.1 and is generated from one of the following:

- the configured DN information from the Call Server
- the data from a corporate LDAP server

The database is downloaded and stored on the Call Server. It is then accessible to the IP Phones. The Signaling Server can support Corporate Directory access for the same number of IP Phones that are registered.

The Directory key on the IP Phone is used to access the directory, select a listing, and then dial a number from the Corporate Directory. The Navigation keys are used to refine the search within the Corporate Directory.

Corporate Directory is configured in LD 11. LD 11 accepts CRPA/CRPD class of service for the IP Phones (see [Table 75 "Corporate Directory: LD 11 configuration" \(page 312\)](#)).

For more information about the operation of the Corporate Directory feature, see *Telephony Manager 3.1 System Administration (NN43050-601)* or *IP Phones Fundamentals (NN43001-368)*.

Personal Directory, Callers List, and Redial List

The Personal Directory, Callers List, and Redial List features are supported on CS 1000 systems running CS 1000 Release 5.0 software.

The Personal Directory allows a user to enter or copy names to a personal directory, and to edit and delete those entries if desired.

The Callers List and Redial List are call log features. The content of these lists is generated during call processing. A user can scroll through the Callers List to see who has called. The user can dial a number from the Redial List.

The Personal Directory, Callers List, and Redial List use a separate central database, called the IP Phone Application Server, to store directory data and user profile options.

ATTENTION

Because the IP Phone Application Server is part of the IP Line software on the Signaling Server, the Personal Directory, Callers List, and Redial List are only supported on CS 1000 systems.

Password protection is available to control access to a user Personal Directory, Callers List, and Redial List.

ATTENTION

Calling Party Name Display (CPND) must be configured on the system to enable Personal Directory, Callers List, and Redial List.

For more information, see ["Personal Directory, Callers List, and Redial List" \(page 189\)](#).

IP Call Recording

IP Call Recording provides the IP address and port information for an IP Phone in Information Elements (IE) over Application Module Link (AML) for Meridian Link Services (MLS). This information correlates the TN of a specific IP Phone with its associated IP address for a call recording application. When enabled in LD 17, IP Call Recording sends a modified

AML message for each call. The modified message identifies the call IP endpoint and makes it possible to correlate the RTP packets for that call to a particular IP Phone

IP Call Recording introduces the IE pair:

- This Party IP IE (monitored party)
- Other Party IP IE (remote party)

The IP IE pair is similar to the existing IE pairs:

- For DNs: This Party DN IE, Other Party DN IE
- For TNs: This Party TN IE, Other Party TN IE

The IP IEs are optional in the Unsolicited Message Status (USM) (Active) and USM (Restore) messages. Note the following:

- If the USM message applies to a monitored key on a digital telephone, then the IP IEs are not sent.
- If the USM message applies to a monitored key on an IP Phone, then the IP IEs are sent: one for the monitored party and one for the remote party.

A call recording application is provided with status update messages for the call keys of any IP Phone it is monitoring. These USM messages contain the IP address and port number information for the monitored IP Phone and the remote party in the active call. By using a Layer 2 switch that supports port mirroring, the call recording device can monitor the media stream for the active call and record it.

Enhanced IP Call Recording

IP Call Recording provides a direct method of capturing and recording VoIP calls. The feature enhancement implements a mechanism to record the IP media stream to an external media-recording device by instructing the IP Phone to send a duplicate media stream to a third-party call-recording application. The third-party call-recording application provides the recording and playing function for the IP calls.

This feature enhancement is supported on the Phase II IP Phone 2001, IP Phone 2002, IP Phone 2004, IP Softphone 2050, IP Audio Conference Phone 2033, IP Phone 2007, IP Phone 1110, IP Phone 1120E, IP Phone 1140E, IP Phone 1150E, WLAN Handset 2210/2211/2212/6120/6140.

The IP Call Recording enhancement enables the following types of recording:

- Bulk Call Recording – All calls are automatically recorded for a particular IP Phone. The Call Recording application issues a Start Recording Request message for the User ID, and all calls are recorded until the Call Recorder application issues a Stop Recording Request.

- Quality Monitor Recording – The Call Recorder records conversation for a particular call. The Call Recording application can monitor the Call Recording application (CR) data such as Calling Line ID (CLID) or Automatic Number Identification (ANI) to determine if it needs to record a specific call. The Call Recording application issues a Start/Stop Recording Request to the User ID for only the duration of the specific call. Quality monitor recording enables manual recording of individual calls with the following options:
 - Call recording can be started or stopped at any time during a call.
 - Call recording can also be paused and restarted repeatedly during a call, enabling excerpts from a conversation to be recorded.
 - Call recording can begin retroactively. At any time during the conversation, the entire call can be saved; it is not necessary to start recording when the call begins.
 - Call recording can be configured to maintain ACD Emergency key functionality.

The IP Call Recording is initiated by the CR. A Start Recording Request message is sent that contains the User ID to be recorded and the IP addresses and port information of where the duplicate media stream is to be sent.

In LD 11, the Class of Service ICRA/ICRD (IP Call Recording Allowed/IP Call Recording denied) is available for the IP Phones that support IP Call Recording. The default is ICRD. See "[LD 11](#)" ([page 138](#)).

Warning tones

If Recording Warning Tone is required, this tone can be turned on or off on the Call Server using the existing UNISim message Stream Based Tone on or off. The message requires the predefined parameters for the tone, such as tone ID, frequency and volume.

Bandwidth requirements

The use of IP Call Recording doubles the bandwidth requirements of the call.

For example, in a call using the G.711 codec, one voice packet data stream requires approximately 80 kb/s. As the IP Call Recorder uses two separate streams for the in/out calls, there are four streams requiring a total of 320 kb/s for the voice packet data. In a typical 100 Mb/s LAN network environment, if 80% of the bandwidth was configured for voice data, then this network could support a maximum of 500 simultaneous IP Phone calls.

$$(100 \times 1000 \times 0.8 / 160) = 500$$

When the IP Call Recording feature is enabled, that same network is limited to a maximum of 250 calls.

For remote users connecting to the IP Call Recorder Server through a WAN connection, the impact of the bandwidth usage to the QoS must be considered. In this case, the IP Call Recorder Server must provide the QoS parameters when instructing the IP Phone to echo the voice data.

Depending on the IP Call Recorder Server ability to handle the RTP stream, more than one IP Call Recorder Server can be required in a large call center environment. Middleware (software that connects two sides of an application and passes data between them) must have an algorithm to balance the traffic between the different servers.

Feature interactions

Mute key

When the Mute key is pressed, the IP Phone keeps both the primary and the duplicate audio stream open. When Mute is pressed, the recording state remains active, but only the incoming conversation is recorded. Pressing the Mute key a second time resumes normal recording.

Hold key

When the Hold key is pressed, a Stop Recording Request message is sent from the Call Server, and the duplicate media stream is closed. A new audio stream is opened for the other active call. When the hold is released, a new Start Recording Request is sent from the Call Server to the IP Phone and recording begins again.

Transfer key

After the Transfer key is pressed and the transfer accepted, the current audio stream is closed. A new audio stream for the new call is opened, followed by a Start Recording Request message. If the IP Phone that accepted the transferred call does not have call recording enabled, the transferred call is not recorded.

Call Forward

When a call is forwarded, the audio stream is opened for the destination IP Phone. If the destination IP Phone does not have call recording enabled, the forwarded call is not recorded.

Conference call

In a conference call, each IP Phone opens a media stream. The IP Phone duplicate media stream to the CR is maintained as long as that IP Phone is part of the conference.

Agent Observe injects a tone which interferes with the Recording Warning tone.

Identifying the IP Phone

IP Call Recording requires the unique identification of each IP Phone to be recorded.

In an Multiple Appearance Directory Number (MADN) configuration, the Call Server enables the association of two MADN keys on a particular TN. There is a maximum of two associated (AST) keys per TN.

In a Multiple Appearance DN Redirection Prime (MARP) configuration, the Call Server enables the association of MARP DN's on different TN's. There is a maximum of two associated (AST) keys per TN.

The following table provides an example of AST configuration in LD 11.

LD 11 AST configuration

Prompt	Response	Description
...		
AST	ASTKEY1	Key numbers to be associated on this TN.
	ASTKEY2	((ASTKEY1 and ASTKEY2 are the numbers of the keys to be associated. In this example, consider ASTKEY1 = 0 and ASTKEY2 = 1.)
...		
KEY	KEY 0 SCR XXXX	XXXX is the DN which is a MARP and already configured on another TN.
	MARP ON TN L S C U	
	MARP	
	CPND	
	VMB	
	ANIE	

Prompt	Response	Description
KEY	KEY 1 SCR XXXX	XXXX is the same DN as configured on KEY 0.
	MARP ON TN L S C U	
	MARP	
	CPND	
	VMB	
	ANIE	
...		

Administration

LD 17

LD 17 provides the Enhanced Unsolicited Status Message (USM) IE enable (IPIE) prompt.

The IPIE prompt enables or disables IP Call Recording on a system-wide basis. The functionality is disabled by default. When enabled, a modified Application Module Link (AML) message that identifies the IP endpoint is sent for each call. The IPIE prompt is in LD 17 under system parameters (PARM).

LD 17 IP Call Recording

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	PARM	Change system parameters.
LPIB	96 - 7500	Low priority Input Buffers
...		
NDRG	(NO) YES	New Distinctive Ringing
MARP	(YES) NO	Multiple Appearance Redirection Prime feature allowed.
IPIE	(NO) YES	Enhanced Unsolicited Status Message (USM) IE enable.
		YES = Allow "This Party IP IE" and "Other Party IE" to send with USM.
FRPT	(NEFR) OLFR	(Deny) or allow access to incoming calls by FRE station.
...		

TM and Element Manager do not support LD 17 for PARM. However, TM does support the corresponding print overlay, LD 22, which prints the prompt IPIE.

LD 11

The CLS ICRD/ICRA responses are used to configure whether or not an IP Phone allows call recording.

LD 11 Service change request for CLS ICRA/ICRD

Prompt	Response	Description
REQ	ADD CHG	Add new data. Change existing data.
TYPE	aaaa	Supported IP Phone type aaaa = 2001P2, 2002P2, 2004P2, 2007, 2050PC, 2050MC, 2033, 1120, 1140, 1150, 2210, 2211, 2212, 6120, 6140
TN	l s c u	Terminal Number of IP Phone Where l = loop, s = shelf, c = card, u = unit
...		
CLS	ICRA (ICRD)	IP Call Recording allowed IP Call Recording denied
...		

If the ICRA class of service is applied to a non-IP Phone, error SCH1599 message is generated.

If the class of service on an IP Phone is changed during an active call, the Call Server tears down the call. As well, if an IP Phone TN is deleted during an active call on that IP Phone, the Call Server tears down that call.

LD 20

The CLS options ICRA/ICRD are displayed in LD 20 when requesting a printout for an IP Phone, as shown in the following example.

```
> ld 20
REQ: PRT
TYPE: TNB
CUST: 0
.....
CLS CTD FBD .....
.....
ICRD (or ICRA)
```

```

.....

LD 80
In LD 80, the output of the call trace command includes IP Call
Recording-related information.
trak <TN>
.trak 61 9
ACTIVE VTN 061 0 00 09
ORIG VTN 061 0 00 02 KEY 0 SCR MARP CUST 0
DN 4002 TYPE I2002
MEDIA ENDPOINT IP: 47.11.215.40 PORT: 5200
TERM VTN 061 0 00 09 KEY 0 SCR MARP CUST 0
DN 4009 TYPE I2004
MEDIA ENDPOINT IP: 47.11.215.47 PORT: 5200
IPCR Tx MEDIA FAREND ENDPOINT IP: 47.11.181.174
PORT: 5000 *
IPCR Rx MEDIA FAREND ENDPOINT IP: 47.11.181.174
PORT: 5001 *
MEDIA PROFILE: CODEC G.711 MU-LAW PAYLOAD 20 ms VAD OFF
DIAL DN 4009
MAIN_PM ESTD
TALKSLOT ORIG 19 TERM 21
EES_DATA:
NONE
QUEU NONE
CALL ID 500 799
.....

```

The asterisk (*) indicates Call Recording information.

LD 81

Use the ICRA/ICRD responses to the FEAT prompt in LD 81 to count the number of IP Phones with the class of service ICRA or ICRD.

LD 81 Count the IP Phones with CLS ICRA or ICRD

Prompt	Response	Description
REQ	LST	List the IP Phones
	CNT	Count the IP Phones
CUST	xx	Customer number
...		
FEAT	ICRA	IP Phones with IP Call Recording allowed
	ICRD	IP Phones with IP Call Recording denied
...		

LD 83

In LD 83, the ICRA/ICRD class of service is displayed when the IP Phone TNB is printed.

LD 117

In LD 117, the output of the following STIP commands includes IP Call Recording-related status information.

- STIP NODE – Displays the Resource Locator Module information for the specified node
- STIP TN – Displays the Resource Locator Module information for the specified TN or group of TNs
- STIP TYPE – Displays the Resource Locator Module information for the specified TN type
- STIP ZONE – Displays the Resource Locator Module information for the specified zone
- STIP TERMIP – Displays the Resource Locator Module information for the specified IP address

Examples of STIP output**Example 1:**

```
=> stip termip 47.11.215.101
TN      type HWID          STATUS  HOSTIP      SIGNALING IP
61 0 0 1 i2001 MAC:        REG     47.11.216.138
47.11.215.101:5000
      18000ae401da5f6602
CODEC(BW): G711u noVAD(1904), G711a noVAD(1904),
G729A(784), G723(544)
MODEL:   IP Phone 2001 Phase 2      FWID: 2  FWVer:
D99 PEC:  NTDU90AA
Under Recording: No      Warning Tone: Not Required
  IPCR Tx Path: 47.11.181.174:6000  IPCR Rx Path:
47.11.181.174:6001
(Italics indicate the IP Call Recording information)
```

Example 2:

```
=> stip termip 47.11.215.101
TN      type HWID          STATUS  HOSTIP      SIGNALING IP
61 0 0 1 i2001 MAC:        REG     47.11.216.138
47.11.215.101:5000
      18000ae401da5f6602
CODEC(BW): G711u noVAD(1904)*, G711a noVAD(1904),
G729A(784), G723(544)
MODEL:   IP Phone 2001 Phase 2      FWID: 2  FWVer:
D99 PEC:  NTDU90AA
Under Recording: Yes      Warning Tone: Not Required
```



```

    IPCR Tx Path: 47.11.181.174:6000    IPCR Rx Path:
47.11.181.174:6001
(Italics indicate the IP Call Recording information)

```

Example 3:

```

=> stip tn 61 9
TN      type HWID          STATUS  HOSTIP      SIGNALING IP
61 0 0 9 i2004 MAC:        REG     47.11.216.138
47.11.215.47:5000
        18000ae401ddb26602
CODEC(BW):  G711u noVAD(1904)*, G711a noVAD(1904),
G729A(784), G723(544)
MODEL:     IP Phone 2004 Phase 2      FWID:  2  FWVer:
D99  PEC:   NTDU92AA
Under Recording: Yes          Warning Tone: On
    IPCR Tx Path: 47.11.181.174:5000    IPCR Rx Path:
47.11.181.174:5001
(Italics indicate the IP Call Recording information)

```

pbxLink connection failure detection

The pbxLink Connection Failure Detection feature provides a means of detecting the link status of 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 Call Server monitors the pbxLink.

The Call Server maintains a list of all known registered elements (Signaling Servers and Voice Gateway Media Cards). When booted, a Call Server has a 5-minute delay to enable these known elements to reestablish contact with the Call Server.

If a known element fails to register with the Call Server, an ELAN0028 alarm is generated.

If an unknown Signaling Server or Voice Gateway Media Card registers with the Call Server, an ELAN0029 alarm is generated.

Displaying pbxLink information

Element Manager

For CS 1000 systems, use the Element Manager **IP Network > Maintenance and Reports > Gen Cmds > Group - pbxLink > Command - pbxLinkShow** window to display the pbxLink information. See [Figure 37 "pbxLinkShow in Element Manager"](#) (page 142).

Figure 37
pbxLinkShow in Element Manager

The screenshot shows the 'CS 1000 ELEMENT MANAGER' web interface. At the top, there is a navigation bar with 'Help' and 'Logout' links. Below the header, the breadcrumb trail reads: 'Managing: 192.167.102.3 > System > IP Network > Node Maintenance and Reports > General Commands'. The main section is titled 'General Commands'. It displays 'Element IP: 192.167.102.4' and 'Element Type: Signaling Server-IP1100'. Below this, there is a form with two rows of input fields. The first row has 'Group' set to 'pbxLink' and 'Command' set to 'pbxLinkShow', with a 'RUN' button. The second row has 'IP Address' set to '192.167.102.3' and 'Number of Pings' set to '3', with a 'PING' button. At the bottom of the form, there is a text area containing the instruction: 'Click a button to invoke a command.'

CLI

For a CS 1000 system, use the LD 117 STAT SERV command at the Command Line Interface (CLI) of the Call Server to display the pbxLink information.

LD 117 STAT SERV

The suite of STAT SERV (Statistic Services) commands enables a technician to display link-status information for Signaling Servers and Voice Gateway Media Cards 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.

STAT SERV status information includes the following:

- node ID
- host name
- ELAN IP address
- element role
- platform type
- connection ID
- enabled applications
- registered/unregistered endpoints, such as IP Phones and Voice Gateway Media Cards.
- information about the pbxLink and enabled applications

- Signaling Server resource count

The Signaling Server resource count aids in determining the number of virtual trunks that can be configured.

pbxLink information

The STAT SERV command provides the following pbxLink information:

- the time the pbxLink was last established
- the time the pbxLink was lost, if previously established
- the time the pbxLink last attempted to establish a connection, if the pbxLink failed to establish
- the Signaling Server resource count

Application information

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

Table 29 "Queried information in STAT SERV" (page 143) lists the applications and describes the information provided by those applications.

Table 29
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/busy Voice Gateway Channels
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 38 "Sample LD 117 STAT SERV output" (page 144) shows an example of LD 117 STAT SERV output.

Figure 38
Sample LD 117 STAT SERV output

```

=> stat serv

NODE HOSTNAME   ELANIP   LDR SRV  APPS PBXLINK
PBXLINK PBXLINK CONNECTID
ID           STATE
DATE  TIME
9090 host82   47.11.217.176 NO  SMC  LTPS  LINK UP
28/07/2004 17:51:31 200a4048
  Sets:[reg - 00000] [busy - 00000]
  VGWs:[reg - 00032] [busy - 00000]

9090 host9    47.11.217.177 YES SS  LTPS  LINK UP
28/07/2004 17:51:33 200a3f68
  VTRK
  Sets:[reg - 00003] [busy - 00000]
  VTRK:[reg - 00383] [busy - 00000]
  SIGNALLING SERVER CAPACITY (SSRC): 2048

9090 itgCard  47.11.217.2  NO  ITGP  LTPS  FAILED
28/07/2004 17:51:16 0

```

Table 30 "STAT SERV response fields and description" (page 144) lists the descriptions for the fields in the STAT SERV response.

Table 30
STAT SERV response fields and description

STAT SERV response field	Description
NODE ID	Identifies the related node. Value is a number from 0 to 9999.
HOSTNAME	Identifies the alias that the host has been given by the system. Value is a string.
ELANIP	Identifies the element IP connection to the Call Server. Value is an IP address.
LDR	Specifies if the element is the Leader for the related node. Value is YES or NO.

STAT SERV response field	Description
SRV	Specifies the element type. Values are: • 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: • LTPS • VTRK
PBXLINK STATE	Specifies the element current pbxLink state. Values are: • LINK UP • LOST • FAILED • INV CONN (element is connected, but its configuration is 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 pbxLink state last changed.
CONNECTED	Specifies the element connection ID.
Sets	Values are: • reg – the number of IP Phones registered to the element • busy – the number of IP Phones that are currently busy
VGWs	Values are: • reg – how many voice gateways (DSP resources) are configured on the element • busy – how many voice gateways (DSP resources) are active/busy on the element

STAT SERV response field	Description
VTRK	Values are: • reg – how many VTRK channels are configured on the element • busy – how many VTRK channels are active/busy on the element
SSRC	Signaling Server capacity

IP Phone support

The IP Line application supports the following IP Phones:

- IP Phone 2001
- IP Phone 2002 Phase I/ Phase II
- IP Phone 2004 Phase I/ Phase II
- IP Phone 2007
- IP Audio Conference Phone 2033
- IP Phone 1110
- IP Phone 1120E
- IP Phone 1140E
- IP Phone 1150E
- IP Softphone 2050
- Mobile Voice Client (MVC) 2050
- WLAN Handset 2210
- WLAN Handset 2211
- WLAN Handset 2212
- WLAN Handset 6120
- WLAN Handset 6140

For detailed information about IP Phones, see the following:

- *IP Phone 2001 User Guide (NN43115-102)*
- *IP Phone 2002 User Guide (NN43116-104)*
- *IP Phone 2004 User Guide (NN43117-102)*
- *IP Phone 2007 User Guide (NN43118-100)*
- *IP Audio Conference Phone 2033 User Guide (NN43111-100)*
- *IP Softphone 2050 User Guide (NN43119-101)*

- *Mobile Voice Client 2050 User Guide (NN43119-103)*
- *WLAN Handset 2210 User Guide (NN43150-110)*
- *WLAN Handset 2211 User Guide (NN43150-120)*
- *WLAN Handset 2212 User Guide (NN43150-130)*
- *WLAN Handset 6120/6140 User Guide (NN43150-100)*
- *IP Phone 1110 User Guide (NN43110-101)*
- *IP Phone 1120E User Guide (NN43112-103)*
- *IP Phone 1140E User Guide (NN43113-106)*
- *IP Phone 1150E User Guide (NN43114-100)*
- *Expansion Module for IP Phone 1100 Series User Guide (NN43130-101)*
- *WLAN IP Telephony Installation and Commissioning (NN43001-504)*
- *IP Phones Fundamentals (NN43001-368)*

Table 31 "IP Phone 2001" (page 147) describes the IP Phone 2001.

Table 31
IP Phone 2001

Feature	IP Phone 2001 characteristic
Display	
Display size and format	1 line display 24 characters
Information line	1 line – 24 characters
Dedicated date/time field	No
Context label field	No
Keys	
Context-sensitive soft keys	4 context-sensitive soft keys, soft-labeling 6 characters long
Self-labeled line/programmable feature keys	No
Other features	
DHCP support	Yes
Transducers	Handset (HD), speakerphone
Mute key	No
Navigation keys	Up and down

Feature	IP Phone 2001 characteristic
Voice codec support	G.711, G729A, G729AB, G.723.1
Firmware download	Automatic firmware version checking and download
3-port unmanaged Layer 2 switch for data and voice	No
Corporate Directory access	No
Unicode support	No

Table 32 "IP Phone 2002" (page 148) describes the IP Phone 2002.

Table 32
IP Phone 2002

Feature	IP Phone 2002 characteristic
Display	
Display size and format	1 line display 24 characters
Information line	1 line – 24 characters
Dedicated date/time field	No
Context label field	No
Keys	
Context-sensitive soft keys	4 context-sensitive soft keys, soft-labeling 6 characters long
Self-labeled line/programmable feature keys	4 self-labeled line/programmable feature keys 10 characters long
Other features	
DHCP support	Yes
Transducers	Headset (HS) / Handset (HD) / Handsfree (HF)
Mute key	Yes
Navigation keys	Up, down, left, and right
Voice codec support	G.711, G729A, G729AB, G.723.1
Firmware download	Automatic firmware version checking and download
3-port unmanaged Layer 2 switch for data and voice	Built-in

Feature	IP Phone 2002 characteristic
Corporate Directory access	Yes
Unicode support	No

Table 33 "IP Phone 2004" (page 149) describes the IP Phone 2004.

Table 33
IP Phone 2004

Feature	IP Phone 2004 characteristic
Display	
Display size and format	3 line display 24 characters on each line
Information line	3 lines – 24 characters on each line
Dedicated date/time field	Yes
Context label field	Yes
Keys	
Context-sensitive soft keys	4 context-sensitive soft keys, soft-labeling 7 characters long
Self-labeled line/programmable feature keys	6 self-labeled line/programmable feature keys 10 characters long
Other features	
DHCP support	Yes
Transducers	Headset (HS) / Handset (HD) / Handsfree (HF)
Mute key	Yes
Navigation keys	Up, down, left, and right
Voice codec support	G.711, G729A, G729AB, G.723.1
Firmware download	Automatic firmware version checking and download
3-port unmanaged Layer 2 switch for data and voice	Built-in Earlier models have an external switch.
Corporate Directory access	Yes
Unicode support	No

IP Phone Key Expansion Module

IP Line supports the Nortel IP Phone Key Expansion Module (KEM).

The IP Phone KEM is a hardware component that attaches to the IP Phone 2002 and IP Phone 2004 and provides additional line appearances and feature keys.

ATTENTION

The IP Phone KEM is not supported on the IP Phone 2001, IP Phone 2007, and IP Audio Conference Phone 2033.

Up to two IP Phone KEMs can be attached to an IP Phone 2002 or an IP Phone 2004. With two IP Phone KEMs attached, the IP Phone 2004 can have up to 60 lines/feature keys, while the IP Phone 2002 can have up to 52 lines/feature keys.

The IP Phone 2004 can also have up to 60 lines/feature keys using the shift key and one IP Phone KEM. With two IP Phone KEMs attached, the shift key does not affect the IP Phone KEMs because the maximum number of lines/feature keys is already available. The IP Phone 2002 does not support shift key functionality.

When an IP Phone KEM is installed on an IP Phone 2002 or IP Phone 2004, the controls on the IP Phone affect both the IP Phone itself and the IP Phone KEM.

The IP Phone KEM must be configured in LD 11 before it can be used.

For information about using the IP Phone KEM, see *IP Phone Key Expansion Module User Guide (NN43119-102)*.

[Table 34 "IP Phone 2007" \(page 150\)](#) describes the IP Phone 2007.

Table 34
IP Phone 2007

Feature	IP Phone 2007 characteristic
Display	

Feature	IP Phone 2007 characteristic
Display size and format	Color touch panel Stylus for clicking (no dragging) 2 display areas – application area and tools/navigation area 3 line display in each area 24 characters on each line
Dedicated date/time field	Yes
Context label field	Yes
Keys	
Context-sensitive soft keys	4 virtual context-sensitive soft keys, soft-labeling 7 characters long 2 actual soft keys, soft-labeling (located on either side of the Navigation key)
Self-labeled line/programmable feature keys	6 virtual self-labeled line/programmable feature keys , soft-labeling 10 characters long
Other features	
GUI screen	Supports Web-based (XML, HTML) applications through an external Applications Server
USB	Single USB port and driver support
DHCP support	Yes
Transducers	Headset (HS) / Handset (HD) / Handsfree (HF)
Mute key	Yes
Navigation keys	One key that rocks up, down, left, and right
Voice codec support	G.711, G729A, G729AB, G.723.1
Firmware download	Automatic firmware version checking and download
3-port unmanaged Layer 2 switch for data and voice	Built-in

Feature	IP Phone 2007 characteristic
Corporate Directory access	Yes
Unicode support	Yes

Table 35 "IP Audio Conference Phone 2033" (page 152) describes the IP Audio Conference Phone 2033.

Table 35
IP Audio Conference Phone 2033

Feature	IP Audio Conference Phone 2033 characteristic
Display	
Display size and format	1 line display 24 characters
Information line	1 line – 24 characters
Dedicated date/time field	No
Context label field	No
Keys	
Context-sensitive soft keys	3 context-sensitive soft keys which map to 4, soft-labeling 6 characters long
Self-labeled line/programmable feature keys	No
Other features	
DHCP support	Yes
Transducers	Handsfree (HF) – default
Mute key	Yes
Navigation keys	Up and down
Voice codec support	G.711, G729A, G729AB
Firmware download	Automatic firmware version checking and download
3-port unmanaged Layer 2 switch for data and voice	No
Corporate Directory access	No
Unicode support	No

Table 36 "WLAN Handset 2210/2211/2212 features" (page 153) lists the features of the WLAN Handsets 2210/2211/2212.

Table 36
WLAN Handset 2210/2211/2212 features

Feature	WLAN Handset 2210	WLAN Handset 2211	WLAN Handset 2212
Supported standard	802.11b (Wi-Fi) compatible	802.11b (Wi-Fi) compatible	802.11b (Wi-Fi) compatible
Soft keys	4 dynamically labeled soft keys	4 dynamically labeled soft keys	4 dynamically labeled soft keys
Feature support	Over 400 Nortel features	Over 400 Nortel features	Over 400 Nortel features
Alerting	Tactile	Tactile	Tactile
Line capacity	Maximum of 6 lines	Maximum of 6 lines	Maximum of 6 lines
Supported codecs	G.711 (A- and μ -law), G.729 AB	G.711 (A- and μ -law), G.729 AB	G.711 (A- and μ -law), G.729 AB
Addressing	DHCP or static IP	DHCP or static IP	DHCP or static IP
Battery capacity	4 hours talk, 70 hours standby	4 hours talk, 70 hours standby	4 hours talk, 70 hours standby
Security	WEP 40 bit and 128 bit encryption, WPA w/TKIP, WPA w/PSK	WEP 40 bit and 128 bit encryption, WPA w/TKIP, WPA w/PSK	WEP 40 bit and 128 bit encryption, WPA w/TKIP, WPA w/PSK
Jacks	headset jack	Headset jack	Headset jack
Transmit RF power	100 mW peak, <10 mW average	100 mW peak, <10 mW average	100 mW peak, <10 mW average
Dimensions	5.5" x 2.0" x 0.9"	5.5" x 2.2" x 1.0"	5.5" x 2.2" x 1.0"
Weight	4.2 ounces	6 ounces	6 ounces
Loudspeaker	No	Yes	Yes
Push-to-talk	No	8 independent push-to-talk channels	No
Unicode support	No	No	No
Built-in VPN client	No	No	Yes

Table 37 "WLAN Handset 6120/6140 features" (page 153) lists the features of the WLAN Handsets 6120/6140.

Table 37
WLAN Handset 6120/6140 features

Feature	WLAN Handset 6120	WLAN Handset 6140
Supported standards	802.11b/g/a	802.11b/g/a

Soft keys	4 dynamically labeled soft keys	4 dynamically labeled soft keys
Feature support	Over 400 supported features	Over 400 supported features
Alerting	Vibrate alert	Vibrate alert
Line capacity	Maximum of 6 lines	Maximum of 6 lines
Supported codecs	G.711 (A- and μ -law), G.729 AB, proprietary 24 kb/s ADPCM (SRP only)	G.711 (A- and μ -law), G.729 AB, proprietary 24 kb/s ADPCM (SRP only)
Addressing	DHCP or static IP	DHCP or static IP
Battery capacity	4 hours talk, 80 hours standby	4 hours talk, 80 hours standby
Security	Highest level of wireless security with support for WPA2, WPA, WEP, Cisco FSR and IPsec VPNs	Highest level of wireless security with support for WPA2, WPA, WEP, Cisco FSR and IPsec VPNs
Jacks	Headset jack	Headset jack
Transmit RF power	Maximum for North America is 100mW Maximum for other domains is 30mW	Maximum for North America is 100mW Maximum for other domains is 30mW
Dimensions	5.4" x 2.0" x 0.9"	5.7" x 2.0" x 0.9"
Weight	3.9 oz (with standard battery pack)	4.2 oz (with standard battery pack)
Loudspeaker	No	No
Push-to-talk	No	25 independent channels (includes one security channel)
Unicode support	No	No

Table 38 "IP Phone 1110" (page 154) lists the features for the IP Phone 1110

Table 38
IP Phone 1110

Feature	IP Phone 1110 characteristics
Display	
Display size and format	1 line display 24 characters
Information line	1 line – 24 characters
Dedicated date/time field	No
Context label field	No
Keys	

Feature	IP Phone 1110 characteristics
Context-sensitive soft keys	4 context-sensitive soft keys, soft-labeling 6 characters long
Self-labeled line/programmable feature keys	No
Other features	
Other	
GUI screen	Supports Web-based (XML, HTML) applications through an External Application Server (XAS)
USB	Single USB port and driver support
DHCP support	Yes
Transducers	Handset (HD), speakerphone
Mute key	Yes
Navigation keys	One key that rocks up, down, left, and right
Voice codec support	G.711, G729A, G729AB, G.723.1
Firmware download	Automatic firmware version checking and download
Integrated gigabit Ethernet switch	Supports LAN and PC 10/100 Mb/s Full Duplex mode
Corporate Directory access	No
Hearing Aid Compatibility	Yes
Unicode support	No

Table 39 "IP Phone 1120E features" (page 155) lists the features of the IP Phone 1120E.

Table 39
IP Phone 1120E features

Feature	Characteristics
Display	
Display size and format	Single line display in each area 24 characters on each line
Information line	1 line – 24 characters
Dedicated date/time field	No
Context label field	No
Keys	

Self-labeled line/programmable feature keys	4 virtual self-labeled line/programmable feature keys , soft-labeling 10 characters long
Context-sensitive soft keys	4 virtual context-sensitive soft keys, soft-labeling 7 characters long
Other	
GUI screen	Supports Web-based (XML, HTML) applications through an External Application Server (XAS)
USB	Single USB port and driver support
DHCP support	Yes
Transducers	Headset (HS) / Handset (HD) / Handsfree (HF)
Mute key	Yes
Headset jack	On/Off key
Navigation keys	One key that rocks up, down, left, and right
Voice codec support	G.711, G729A, G729AB, G.723.1
Firmware download	Automatic firmware version checking and download
Integrated gigabit Ethernet switch	Supports LAN and PC 10/100/1000 Mb/s Full Duplex mode
Corporate Directory access	Yes
Hearing Aid Compatibility	Yes
Unicode support	Yes

Table 40 "IP Phone 1140E features" (page 156) lists the features of the IP Phone 1140E.

Table 40
IP Phone 1140E features

Feature	Characteristics
Display	
Display size and format	3 line display 24 characters on each line
Information line	3 lines – 24 characters on each line
Keys	
Context-sensitive soft keys	4 context-sensitive soft keys, soft-labeling 7 characters long
Self-labeled line/programmable feature keys	6 self-labeled line/programmable feature keys 10 characters long

Other	
GUI screen	Supports Web-based (XML, HTML) applications through an External Application Server (XAS)
USB	Single USB port and driver support
DHCP support	Yes
Transducers	Headset (HS) / Handset (HD) / Handsfree (HF)
Mute key	Yes
Wireless headset support	Bluetooth wireless technology support
Headset jack	On/Off key
Navigation keys	One key that rocks up, down, left, and right
Voice codec support	G.711, G729A, G729AB, G.723.1
Firmware download	Automatic firmware version checking and download
Integrated gigabit Ethernet switch	Supports LAN and PC 10/100/1000 Mb/s Full Duplex mode
Corporate Directory access	Yes
Hearing Aid Compatibility	Yes
Unicode support	Yes

Table 41 "IP Phone 1150E features" (page 157) lists the features of the IP Phone 1150E.

Table 41
IP Phone 1150E features

Feature	Characteristics
Display	
Display size and format	3 line display 24 characters on each line
Information line	3 lines – 24 characters on each line
Keys	
Context-sensitive soft keys	4 context-sensitive soft keys, soft-labeling 7 characters long
Self-labeled line/programmable feature keys	6 self-labeled line/programmable feature keys 10 characters long
Other	
GUI screen	Supports Web-based (XML, HTML) applications through an External Application Server (XAS)

USB	Single USB port and driver support
DHCP support	Yes
Transducers	Headset (HS) / Handsfree (HF)
Mute key	Yes
Wireless headset support	Bluetooth wireless technology support
Navigation keys	One key that rocks up, down, left, and right
Voice codec support	G.711, G729A, G729AB, G.723.1
Firmware download	Automatic firmware version checking and download
Integrated gigabit Ethernet switch	Supports LAN and PC 10/100/1000 Mb/s Full Duplex mode
Corporate Directory access	Yes
Hearing Aid Compatibility	Yes
Unicode support	Yes

Expansion Module for IP Phone 1100 Series

IP Line supports the supports the Expansion Module for IP Phone 1100 Series (Expansion Module). The Expansion Module is supported on the IP Phone 1120E, IP Phone 1140E, and IP Phone 1150E.

Up to three Expansion Modules are supported on the IP Phones. With three Expansion Modules the IP Phones can have up to 54 additional self-labeled line/programmable feature keys. The IP Phone 1140E and IP Phone 1150E can also have up to 36 additional self-labeled line/programmable feature keys using the Shift key functionality with one Expansion Module. If more than one Expansion Module is connected, the Shift key functionality does not affect the Expansion Modules.

The IP Phone 1120E does not support Shift key functionality.

The Expansion Module has the following display characteristics:

- LCD display area—Each of the 18 physical keys on the Expansion Module has a 10-character display label beside the 18 self-labeled line/programmable feature keys. This label is set automatically, however, the user can edit the label using the controls on the IP Phone.
- adjustable display and contrast settings—Use the Contrast Adjustment option under the Telephone Options menu on the IP Phone to adjust the display and contrast settings. Any contrast changes you make on the IP Phone affect the Expansion Module. The Expansion Module and IP Phone do not have separate contrast adjustments.
- backlight—Whether the IP Phone is powered using local power or Power over Ethernet (PoE), the Expansion Module receives the same

backlight settings as the IP Phone. The backlight timer only turns off if the backlight timer is set.

The Expansion Module must be configured in LD 11 before it can be used.

For further information about the Expansion Module, see *Expansion Module for IP Phone 1100 Series User Guide (NN43130-101)* and *IP Phones Fundamentals (NN43001-368)*.

Element Manager support

Element Manager enables configuration of IP Line using a Web browser on CS 1000 systems.

Each Signaling Server hosts a Web server, Element Manager, that allows configuration, administration, and maintenance to be performed on the system components. Element Manager is a graphical Web interface that provides an alternative to the traditional CLI and overlays. The interface is available to users running a Web browser on a PC. No special client software is required.

The Element Manager Web server runs on each Signaling Server and the Signaling Server acts as a file server.

After a Web browser is opened and the IP address of the Signaling Server is entered, the Element Manager interface is displayed. Element Manager is then used to perform tasks such as configuring an IP Telephony Node, checking and uploading loadware and firmware files, and retrieving the CONFIG.INI and BOOTP.TAB configuration files from the Call Server. The Voice Gateway Media Cards are notified to FTP the files from the Call Server.

TM 3.1 Navigator incorporates links to each Element Manager Web server in a network.

BOOTP and CONFIG.INI

If the Voice Gateway Media Card is a Follower of a primary Signaling Server, it generates a BOOTP request to retrieve its network information. The request for IP address, node ID, and node IP is directed to a BOOTP server within its node. If the BOOTP request fails, the Voice Gateway Media Card uses the last configuration. This fallback configuration data is stored locally on the Voice Gateway Media Card. If the BOOTP request is successful, the Voice Gateway Media Card refreshes its current fallback configuration data.

If the Voice Gateway Media Card is located in a stand-alone IP Telephony node, and is designated as the Leader for its node, it provides BOOTP service to all other configured Voice Gateway Media Cards within its node. The Leader determines its own network information using a combination of locally stored static information and the bootp.tab file.

If the Voice Gateway Media Card is located in a stand-alone IP Telephony node, and is designated as a Follower, it generates a BOOTP request to retrieve its network information. The request for IP address, node ID, and node IP is directed to a BOOTP server within its node. If the BOOTP request fails, the Voice Gateway Media Card uses the last configuration. This fallback configuration data is stored locally on the Voice Gateway Media Card. If the BOOTP request is successful, the Voice Gateway Media Card refreshes its current fallback configuration data.

The Voice Gateway Media Card reads the contents of the CONFIG.INI file located on its disk for additional configuration parameters.

Call Statistics collection

IP Line enables statistics on the Quality of Service (QoS) of calls connected by the Call Server to be collected.

Commands in LD 32 and LD 117 print the number of IP Phones registered on a card, zone, node, or Signaling Server. Traffic printouts are available per zone at user-configurable intervals for the following:

- blocked calls
- bandwidth used
- call attempts and completions

Counting IP Phones

The commands to count registered IP Phones are available in LD 32 and LD 117.

Commands in LD 117 are as follows:

- ECNT FW <XX> <A> <BB> <FF> – count the number of IP Phones with specified firmware ID and, optionally, firmware version.
- ECNT MODL <MMMM> – count the number of IP Phones of the specified model>. If the MMMM parameter is omitted, the IP Phone Model Names and their associated mnemonics are listed.
- ECNT PEC <PEC> – count the number of IP Phones with a specified Product Engineering Code (PEC).

Previously, all ECNT commands were in LD 32. The following existing LD 32 ECNT commands are now duplicated in LD 117 to maintain a consistent interface. However, they continue to be maintained in LD 32 as well.

- ECNT CARD <Loop> <Shelf> <Card> <CustomerNumber>
- ECNT NODE <NodeNumber>
- ECNT SS <HostName>
- ECNT ZONE <ZoneNumber> <CustomerNumber>

Table 42 "LD 117 commands to count registered IP Phones" (page 161) describes these commands.

Table 42
LD 117 commands to count registered IP Phones

Command	Description
ECNT CARD L S C <customer>	Counts and prints the number of IP Phones registered for the specified virtual card. • If the <customer> parameter is specified, the count is specific to that customer. A card must be specified to enter a customer; otherwise, the count is across all customers. • If no parameters are entered, the count is printed for all zones. A partial TN can be entered for the card (L or L S) which then prints the count per that parameter. A customer cannot be specified in this case. Example: ECNT CARD 81 << Card 81 >> Number of Registered Ethersets: 5 Number of Unregistered Ethersets: 27
ECNT ZONE zoneNum <customer>	Counts and prints the number of IP Phones registered for the specified zone. • If <customer> parameter is specified, the count is specific to that customer. A zone must be specified to enter a customer; otherwise, the count is across all customers. • If no parameters are entered, the count is printed for all zones. • If an IP Phone is in VO login state and the Current Zone (CUR_ZONE) is different from the Configured Zone (CFG_ZONE), both zones are counted for the ECNT command. Example:

Command	Description
	ECNT ZONE 0 0 << Zone 0 Customer 0 >> Number of Registered Ethersets: 4 Number of Unregistered Ethersets: 17
ECNT NODE nodeNum	Counts and prints the number of IP Phones registered for the specified node. If the nodeNum parameter is not entered, the count is printed for all nodes. Example: ECNT NODE 8765 << Zone 8765 >> Number of Registered Ethersets: 3
ECNT SS <hostName>	Counts and prints the number of IP Phones registered for the specified Signaling Server. If hostName parameter is not entered, the count is printed for all Signaling Servers. Example: ECNT SS << Signaling Server: BVWAlphaFox IP 10.10.10.242>> Number of Register Ethersets: 1000 If the hostName variable contains an underscore (_), then an NPR001 error message is returned, as an underscore is considered to be an invalid character.
ECNT FW <XX> <A> <BB> <FF>	Prints the number of IP Phones with specified firmware ID and running specified firmware version. <XX> – firmware ID <A> – major version designator <BB> – minor version designator <FF> – filter to apply on firmware version; can be one of the following:

Command	Description
	= – equal to ~ – not equal to < – less than > – greater than Only the XX parameter is mandatory. ECNT FW <XX> <A> <BB> defaults to ECNT FW <XX> <A> <BB> = ECNT FW <XX> <A> counts all registered IP Phones with firmware ID equal to <XX> and major version designator equal to <A>. ECNT FW <XX> counts all registered IP Phones with firmware ID equal to <XX>. ECNT FW is equivalent to ECNT FW ALL; that is, the list containing firmware IDs and the quantity of IP Phones with this firmware ID is printed.
ECNT MODL <MMMM>	Prints the number of IP Phones of specified model. <MMMM> – specifies model name. If this parameter is omitted, then a list of the model names and associated mnemonics is printed.
ECNT PEC <PEC>	Prints the number of IP Phones with specified PEC, where: <PEC> – Product Engineering Code ECNT PEC is equivalent to ECNT PEC ALL; that is, the list containing the PECs and the quantity of IP Phones with this PEC is printed.

Error messages are printed when invalid data is entered for these commands. The messages include valuable information such as the correct ranges for the command parameters. See the following tables for the error messages:

- [Table 43 "ECNT Card command error messages" \(page 164\).](#)
- [Table 44 "ECNT Zone command error messages" \(page 164\).](#)
- [Table 45 "ECNT Node command error messages" \(page 165\).](#)
- [Table 46 "ECNT SS command error message" \(page 165\).](#)

Table 43
ECNT Card command error messages

Error	Error Message
Slot out of range error	Slot out of range. Range: [61 to 99]
Slot non-virtual loop error	Slot does not correspond to a virtual loop.
Slot not configured loop error	Slot corresponds to a virtual loop but it is not configured.
Customer out of range error	Customer out of range. Range: [0 to 31]
Customer not configured error	Customer does not exist.
Combination of invalid slot and invalid customer	Slot does not correspond to a virtual loop. Customer out of range. Range: [0 to 31]

Table 44
ECNT Zone command error messages

Error	Error Message
Zone out of range error	Zone out of range. Range: [0 to 255]
Zone not configured error	Zone not configured.
Customer out of range error	Customer out of range. Range: [0 to 31]
Customer not configured error	Customer does not exist.
Combination of invalid zone and invalid customer error	Zone not configured.

Error	Error Message
	Customer out of range. Range: [0 to 31]

Table 45
ECNT Node command error messages

Error	Error Message
Node out of range error	Node out of range. Range: [0 to 9999]
Node not configured error	Node not registered.

Table 46
ECNT SS command error message

Error	Error Message
SS not found in system error	Signaling Server <name> does not exist.

IP Phone Zone Traffic Report 16

A system traffic report, IP Phone Zone Traffic Report 16 in LD 2 is created on the system to print IP Phone data at the zone level. The data is printed for the following categories at the end of each collection period on a per-zone basis:

- Total inter/intra-zone calls made
- Total inter/intra zone calls blocked
- Percent average inter/intra zone bandwidth used
- Percent maximum inter/intra zone bandwidth used
- Total inter/intra zone bandwidth threshold exceeded count

The counters are reset after the data is printed.

The "Total inter/intra zone bandwidth threshold exceeded count" prints the number of times a user-configured bandwidth threshold was exceeded for the zone during the collection period. LD 2 commands that are related to setting the system threshold are used with a value defined for the bandwidth threshold.

Table 47
System threshold commands

Command	Description
TTHS TH tv	Prints the current system thresholds.
STHS TH tv -- TV	Sets the system thresholds.
A TH value of 5 is used for the zone bandwidth threshold. The system thresholds TV value is the percentage of the zone maximum bandwidth. The range values are 000 to 999, where 000 corresponds to 00.0% and 999 corresponds to 99.9%. The default is 90.0%.	

The following examples first set the system bandwidth to 75% and then print the actual value.

```
.STHS 5 750
.TTHS 5
```

[Table 48 "IP Phone Zone Traffic Report 16 intrazone data output" \(page 166\)](#) describes the intrazone IP Phone Zone Traffic Report 16 output data.

Table 48
IP Phone Zone Traffic Report 16 intrazone data output

Data	Description
cmi	intrazone calls made
cbi	intrazone calls blocked
pi	intrazone peak bandwidth (%)
ai	intrazone average bandwidth usage (%)
vi	intrazone bandwidth usage threshold violations
cmip	counts of measuring interval
cul	counts of unacceptable latency
cupl	counts of unacceptable packet loss
cuj	counts of unacceptable jitter samples
cur	counts of unacceptable R factor
cuerl	counts of unacceptable Echo Return Loss
cwl	counts of warning latency
cwj	counts of warning jitter

Data	Description
cwpl	counts of warning packet loss
cwr	counts of warning R factor
cwerl	counts of warning Echo Return Loss
ccms	Calls completed with media security
ccnms	Calls completed without media security
cfnp	Calls failed by near end policy
cffr	Calls failed by incoming release May not be due to security policy negotiation failure
cosr	Outgoing calls switched to RTP
cisr	Incoming call switched to RTP
cfnr	Calls failed due to lack of resources (SRTP-capable DSPs)

Table 49 "IP Phone Zone Traffic Report 16 interzone data output" (page 167) describes the interzone IP Phone Zone Traffic Report 16 output data.

Table 49
IP Phone Zone Traffic Report 16 interzone data output

Data	Description
cmo	interzone calls made
cbo	interzone calls blocked
po	interzone peak bandwidth (%)
ao	interzone average bandwidth usage (%)
vo	interzone bandwidth usage threshold violations
cmip	counts of interval measuring samples
cul	counts of unacceptable latency samples
cupl	counts of unacceptable packet loss
cuj	counts of unacceptable jitter samples
cur	counts of unacceptable R factor samples
cuerl	counts of unacceptable Echo Return Loss
cwl	counts of warning latency samples
cwj	counts of warning jitter samples
cwpl	counts of warning packet loss
cwr	counts of warning R factor samples
cwerl	counts of warning Echo Return Loss
ccms	Calls completed with media security

Data	Description
ccnms	Calls completed without media security
cfnp	Calls failed by near end policy
cfr	Calls failed by incoming release
cosr	Outgoing calls switched to RTP
cisr	Incoming call switched to RTP
cfnr	Calls failed due to lack of resources (SRTP-capable DSPs)

Figure 39
Example of the output from Traffic Report 16

```
LD 2
TFC000
.invs 16
0000 TFS016
ZONE 000
```

INTRAZONE	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
INTERZONE	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000

```
ZONE 001
```

INTRAZONE	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
INTERZONE	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000

```
ZONE 002
```

INTRAZONE	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
INTERZONE	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000

```
ZONE 003
```

INTRAZONE	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
INTERZONE	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000

```
ZONE 004
```

INTRAZONE	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
INTERZONE	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000

All other commands (SOPS, COPS, TOPS) function in the normal manner. [Table 50 "SOPS, COPS, TOPS commands" \(page 169\)](#) shows the SOPS, COPS, and TOPS commands:

Table 50
SOPS, COPS, TOPS commands

.tops 1 2 3 4 5 14	display the current system report list
.sops 1 2 3 4 5 14 -- 16	add report 16 to be printed
.tops 1 2 3 4 5 14 16	display system report list with report 16 added
.cops 1 2 3 4 5 14 16 -- 16	delete report 16
.tops 1 2 3 4 5 14	display system report list with report 16 deleted

Programmable line/DN feature keys (self-labeled)

Definition

The IP Phone user is able to program the label on the feature key. This label change is saved and then displayed on the feature key.

Availability

[Table 51 "Feature key availability on IP Phones" \(page 169\)](#) describes the feature key availability on the IP Phones.

Table 51
Feature key availability on IP Phones

Model	Number of feature keys	Number of feature keys using Shift key	Maximum label character length
IP Phone 2002	4	N/A	10
IP Phone 2004	6	12	10
IP Softphone 2050	6	12	10
MVC 2050	6	12	10
IP Phone 1120E	6	N/A	10
IP Phone 1140E	6	12	10
IP Phone 1150E	6	12	10

The IP Phone 2001, IP Audio Conference Phone 2033, and the IP Phone 1110 do not support feature keys.

The feature key labels for each IP Phones are stored in the Call Server database. When the Call Server performs an EDD, the feature key labels are saved to the database. The feature key label information is retrieved

from the file into memory during the sysload of the Call Server. When the system performs an INI or sysload, feature key label changes performed by users between the last EDD and the INI or sysload are lost.

When the IP Phone registers with the Call Server, the Call Server looks up the feature key label in the memory, based on the TN of the IP Phone. If the labels are found, they are sent to the IP Phone when the key map download occurs. If the labels are not found, the Call Server sends out the key number strings or key functions.

For more information about self-labeled line/programmable feature keys, see *IP Phones Fundamentals (NN43001-368)*.

Private Zone configuration

Private Zones are available for the CS 1000 systems.

Lack of DSP resources

DSP resources for each customer are placed in one common pool. A DSP channel is allocated to an IP-to-circuit-switched call based on a round-robin searching algorithm within the pool.

If an available resource cannot be found, the overflow tone is given. For most installations, this approach works because all IP Phone users share the IP Line DSP resources. The DSPs can be provisioned using a DSP-to-IP Phone ratio similar to trunk resources, because the DSPs are used only for circuit-switched access or conference calls.

When IP-to-PSTN calls are used, such as with ACD agents or other users who consistently are using trunk resources when making calls, it becomes difficult to provision the system in a way that guarantees an available DSP channel when these users need it. If the other users suddenly make a lot of conference calls or trunk calls, the DSP resources can deplete and as a result, calls cannot be made. This occurs because all DSP channels are in one pool.

DSP resources and Private Zones

IP Line provides the Private Zone Configuration feature for DSP configuration and allocation to the zone configuration. This feature enables the configuration of one or more gateway channels as a private resource. This guarantees DSP availability for critical or ACD agent IP Phone.

A zone can be configured as shared or private.

Shared Zone

The current default zone type is a Shared Zone. IP Phones configured in Shared Zones use DSP resources configured in shared zones. If all the gateway channels of the Shared Zones are used, the caller receives an overflow tone and the call is blocked.

Select gateway channels in the following order:

- Select a channel from the same zone as the zone where the IP Phone is configured.
- Select any available channel from the Shared Zones channels.

Private Zone

The Private Zone enables DSP channels configured in a Private Zone to be used only by the IP Phones that have also been configured for that Private Zone. If more DSP resources are required by these IP Phones than what are available in the zone, DSPs from other Shared Zones are used.

IP Phones configured in Shared Zones cannot use the Private Zones' channels.

Select the gateway channels in the following order:

- Select a channel from the same Private Zone as the zone where the IP Phone is configured.
- Select any available channel from the pool of Shared Zones channels.

LD 117

VGW channels and IP Phones are set as shared or private based on zone configuration. In LD 117, zone configuration can be set to either shared or private using the parameter <zoneResourceType>.

A zone is configured in LD 117 as follows:

```
NEW ZONE <zoneNumber> [<intraZoneBandwidth>
<intraZoneStrategy> <interZoneBandwidth> <interZoneStrategy>
<zoneResourceType>]
CHG ZONE <zoneNumber> [<intraZoneBandwidth>
<intraZoneStrategy> <interZoneBandwidth> <interZoneStrategy>
<zoneResourceType>]
```

By default, a zone is configured as shared (zoneResourceType=shared).

Example

The command to add a new zone, in this example zone 10, is as follows:

```
new zone 4 BQ 10000 BQ 10000 private
Zone 4 added. Total number of Zones = n
(where n is the total number of zones)
```

Site details

Use the **PRT ZONE** or **PRT ZONE ALL** command to see details for all configured zones. [Table 52 "Sample output from PRT ZONE or PRT ZONE ALL command" \(page 172\)](#) gives a sample output of the **PRT ZONE** or **PRT ZONE ALL** command.

Table 52
Sample output from PRT ZONE or PRT ZONE ALL command

			Intrazone				Interzone				
Zone	State	Type	Bandwidth (kb/s)	Strategy	Usage (%)	Peak (kb/s)	Bandwidth (kb/s)	Strategy	Usage (%)	Peak (kb/s)	HO/B RCH
0	ENL	SHARED	100000	BQ	0	0	100000	BQ	0	0	HO
1	ENL	SHARED	10000	BQ	0	0	10000	BQ	0	0	HO
4	ENL	PRIVATE	10000	BQ	0	0	10000	BQ	0	0	HO
10	ENL	SHARED	10000	BQ	0	0	10000	BQ	0	0	HO

Resource-sharing for Shared and Private Zones

If a resource-critical IP Phone is configured for a Private Zone, and there are not enough resources found within that zone, the search continues into the Shared Zones within the same customer for an available DSP channel.

However, if an IP Phone is configured in a Shared Zone, the Call Server limits its search to the pool of shared DSP channels. The search does not extend into the Private Zones' channels.

When configuring the allocation of shared versus private resources, consideration must be given to the number of private resources that are needed. Enough DSP resources must be configured to prevent the IP Phones configured in Shared Zones from running out of channels.

**WARNING**

The Call Server does not search for voice gateway channels in Private Zones when the IP Phone is configured in a Shared Zone. Only IP Phones configured in the same Private Zone can use the Private Zone voice gateway channels.

Because the voice gateway channels in the Private Zone are not accessible to IP Phones in the Shared Zone, ensure that only enough private channels are configured to cover the IP Phones in the Private Zone. Do not configure more channels than are required in the Private Zone as the Shared Zone IP Phones cannot access these channels.

Run-time configuration changes

IP Line enables most changes to be made without disabling or rebooting the Voice Gateway Media Cards. After adding configuration information for a new Voice Gateway Media Card and downloading the BOOTP file to the Leader, a new Voice Gateway Media Card can be added to an existing node without rebooting the other cards.

The following exceptions require a reboot:

- a role change; that is, changing a Leader to Follower or changing Follower to Leader
- changing the node IP subnet masks or gateway IP addresses requires a reboot of all cards in the node
- changing the AudioPort parameter in the "config.ini" file on the Voice Gateway Media Card requires a reboot of the card
- changing the IP address of a particular card so it can retrieve its new IP address information

Supported run-time changes

Therefore, IP Line supports only run-time changes for the following:

- changes to the CONFIG.INI file
- add card or delete card changes to the BOOTP.TAB file

Configuration changes have an effect only on new calls. Existing calls are not interrupted. However, there are exceptions:

- If the active Call Server ELAN link configuration data is changed (for example, a changed IP address), then active calls are released.

If the nonactive Call Server is changed (for example, survivable-side IP address), then the calls are not affected.

When the Call Server ELAN network interface is reinitialized to implement the configuration change, the IP Phones and gateway channels registrations are unregistered on the Call Server. The Call

Server releases the calls. When the link is reestablished, the LTPS synchronizes the call states and releases the active calls. Service is interrupted during this reestablishment period and the following are affected:

- New IP Phones cannot register.
- Registered IP Phones cannot establish new calls.
- The Voice Gateway Media Card faceplate displays S009.

After the ELAN link comes back up, the Line Terminal Proxy Server (LTPS) re-registers the IP Phones with the Call Server and all service is resumed.

- If the codec list is changed, the Voice Gateway Media Card DSPs might need to be reloaded. For instance, one DSP image contains G.711, FAX, and G.729A/G.729AB. The other DSP image contains G.711, FAX, and G.723.1. If the user has a node configured with the G.729AB codec and the user performs an administrative change to use G.723.1 (or vice versa), the DSPs must be reloaded.

After the CONFIG.INI file containing the administrative change is downloaded to a Voice Gateway Media Card, the card DSPs are reloaded as they become idle. For instance, if all DSPs are idle on the card, the new image is loaded to all of them at once. If one or more DSPs have active calls, the DSP is not reloaded until the active calls have been released. This can cause some DSPs to be reloaded later than others.

This functionality is supported by both Element Manager and TM 3.1.

Network wide Virtual Office

Network Wide Virtual Office is supported for the CS 1000 systems.

This feature enables a user to use any IP Phone within the network.

The Virtual Office feature provides a call service to travelling users who want to use a different physical IP Phone (other than the IP Phone they normally use). Users can log on to another IP Phone using their DN and preconfigured Station Control Password (SCPW).

After logged on, users have access to their DNs, autodial numbers, key layout, feature keys, and voice mail indication/access that are configured on their own home or office IP Phones. For example, if users go to another office or to a different location within the same office, they can log on to any available IP Phone and have all the features of their home/office IP Phone. When the user logs off the IP Phone, the features that were transferred to that IP Phone are removed.

Network Wide Virtual Office and the Network Routing Server

Network Wide Virtual Office is limited to a single Network Routing Server (NRS) zone. As long as Virtual Offices share the same NRS, a Virtual Office logon can redirect an IP Phone to any of the systems.

Requirements

A Signaling Server or stand-alone NRS is required in the network.

Supported IP Phones

Virtual Office is supported for the IP Phone 2001, IP Phone 2002, IP Phone 2004, IP Phone 2007, IP Audio Conference Phone 2033, IP Phone 1110, IP Phone 1120E, IP Phone 1140E, IP Phone 1150E, IP Softphone 2050, MVC 2050, and WLAN Handset 2210/2211/2212/6120/6140.

An IP Phone 2004, IP Softphone 2050, MVC 2050, IP Phone 2007, IP Phone 1140E, WLAN Handsets 2210/2212/2212/6120/6140 users can log on from an IP Phone 2002 and IP Phone 1120E under certain conditions. See ["Set type checking and blocking" \(page 186\)](#).

[Table 53 "Virtual Office logon from various IP Phones" \(page 175\)](#) shows which users can log on to particular IP Phones.

Table 53
Virtual Office logon from various IP Phones

IP Phone User	Virtual Office logon
An IP Phone 2001, IP Audio Conference Phone 2033, or IP Phone 1110 user...	...can Virtual Office log on from another IP Phone 2001, IP Audio Conference Phone 2033, IP Phone 1110, IP Phone 2002, IP Phone 2004, IP Phone 2007, IP Softphone 2050, MVC 2050, WLAN Handset /2211/2212/6120/6140, IP Phone 1120E, and IP Phone 1140E. See "Set type checking and blocking" (page 186) .
An IP Phone 2002 or IP Phone 1120E user...	...can Virtual Office log on from another IP Phone 2002, IP Phone 2004, IP Phone 2007, IP Softphone 2050, MVC 2050, WLAN Handset 2210/2211/2212/6120/6140, IP Phone 1120E, and IP Phone 1140E. ...can log on under certain conditions when they attempt a Virtual Office logon from an IP Phone 2001, IP Audio Conference Phone 2033, and IP Phone 1110. See "Set type checking and blocking" (page 186).

IP Phone User	Virtual Office logon
An IP Phone 2004, IP Phone 2007, IP Phone 1140E, or WLAN Handset 2210/2211/2212 user...	...can Virtual Office log on from another IP Phone 2004, IP Phone 2007, IP Softphone 2050, MVC 2050, WLAN Handset 2210/2211/2212/6120/6140, IP Phone 1120E, and IP Phone 1140E. ...can log on under certain conditions when they attempt a Virtual Office logon from an IP Phone 2001, IP Phone 2002, and IP Audio Conference Phone 2033. See "Set type checking and blocking" (page 186).
An IP Softphone 2050 or MVC 2050 user...	...can virtually log on from another IP Softphone 2050, MVC 2050, IP Phone 2004, IP Phone 2007, WLAN Handset 2210/2211/2212/6120/6140, IP Phone 1120E, and IP Phone 1140E. ...can log on under certain conditions when they attempt a Virtual Office logon from IP Phone 2002, IP Phone 1120E, and IP Phone 1140E. See "Set type checking and blocking" (page 186). Virtual logon for an IP Softphone 2050, and MVC 2050 user to an IP Phone 2001, IP Audio Conference Phone 2033, and IP Phone 1110. is blocked.
IP Phone 1150E user...	...can Virtual Office log on from an IP Phone 1150E only. Virtual Office log on for an IP Phone 1150E to any other IP Phone is blocked. The agent IP Phone must have a secondary (or private) DN assigned, which is then used as the VO User ID.

Virtual Office User Allowed (VOUA) and Virtual Office logon Allowed (VOLA) must be configured on the IP Phones as follows:

- The IP Phone where the user wants to virtually logon (destination) must have Virtual Office User Allowed (VOUA) configured.
- The IP Phone where the user wants to log on from (source) must have Virtual Office logon Allowed (VOLA) configured.

Failed password attempt

Three failed password attempts to log on using the Virtual Office feature locks the user out from Virtual Office logon at the Call Server for one hour. The Call Server lock can be removed by an administrator using an LD 32 command to disable and reenale that TN. See *Communication Server 1000M and Meridian 1 Large System Maintenance (NN43021-700)* or *Software Input Output Reference—Maintenance (NN43001-711)*.

Passwords and IP Phone Registration

An IP Phone registers using the TN (in its EEPROM). A valid user ID and password are used to determine the Home LTPS for the IP Phone during the Virtual Office connection. A Network Routing Server (NRS) is required if the Home LTPS is not the LTPS where the IP Phone is registered when the Virtual Office logon is initiated.

Virtual Office capabilities

Virtual Office provides the following capabilities:

1. A network-wide connection server (Network Routing Server [NRS]) is equipped to provide addressing information of call servers, based on a user DN.
2. A key sequence is entered at an IP Phone to initiate the logon sequence. Then the current network DN and a user-level password is entered. The password is the Station Control Password configured in LD 11. If a SCPW is not configured, the Virtual Office feature is blocked.
3. A user logs off when leaving the location.

For more detailed information about Virtual Office, see *IP Phones Fundamentals (NN43001-368)*.

Bandwidth Management for Network wide Virtual Office

Bandwidth is calculated for IP Users who are using the Virtual Office feature to log on to their home IP Phones from different Call Servers within the network.

When an IP User moves from the home location to a location that has another Call Server, and performs a Virtual Office log on from his home Call Server, the IP Phone used for Virtual Office registration obtains the following:

- DN number associated with the user ID
- TN parameters including the configured bandwidth zone

The zone information is saved in the Current Zone field. All features that depend on configured zone information receive the correct bandwidth calculations. Configured Zone and Current Zone fields replace the current Bandwidth Zone field. The Configured Zone field stores the configured zone number. This value only changes if the zone is reconfigured. The Current Zone field stores the current zone number. This value changes with each Virtual Office log on.

The zone information is saved in the Current Zone field. All features that depend on configured zone information receive the correct bandwidth calculations.

Requirements

The Bandwidth Management for Network wide Virtual Office feature requires the following:

- IP Client cookies must be supported on the IP Phones
- CS 1000 Release 5.0 software
- Virtual Office package 382
- Virtual Office Enhancement (VOE) package 387
- Network Connection Server (NCS)

For more information about the Bandwidth Management for Network wide Virtual Office feature, see *Branch Office Installation and Commissioning (NN43001-314)*.

Branch Office and Media Gateway 1000B

The Media Gateway 1000B (MG 1000B) provides a means of extending CS 1000 Release 5.0 features to one or more remotely-located branch offices using the Branch Office feature. A branch office is a remote location in the network where IP Phones, PSTN access, and TDM telephones are located.

Definition

Branch Office is a feature set of the equipment and software that a secondary location needs to centralize the call processing of its IP-based communications network. The Call Server at the main office provides the call processing for the IP Phones in both the main office and the MG 1000B in the branch office location. The MG 1000B in the branch office location provides access to the local PSTN.

Connections

The MG 1000B is connected to the main office over virtual trunks on a WAN or LAN. IP Phone calls and IP network connections are controlled by, and come from, the main office. If the main office fails to function, or a network outage occurs, the CP PM Call Server in the MG 1000B provides service to the IP Phones located in the branch office location. The IP Phones then survive an outage between the MG 1000B and the main office.

Components

The basic hardware of an MG 1000B includes the CP PM Call Server and the Signaling Server. The Media Gateway provides access to the local PSTN for users in the branch office location. It also provides support for analog devices such as fax machines or telephones in the branch office location.

For detailed information about MG 1000B, see *Branch Office Installation and Commissioning (NN43001-314)*.

802.1Q support

The following IP Phones support 802.1Q:

- IP Phone 2001
- IP Phone 2002
- IP Phone 2004
- IP Phone 2007
- IP Audio Conference Phone 2033
- IP Phone 1110
- IP Phone 1120E
- IP Phone 1140E
- IP Phone 1150E

The IP Softphone 2050 supports 802.1Q through the PC operating system. This support enables the definition of virtual LANs (VLANs) within a single LAN. This improves bandwidth management, limits the impact of broadcast and multicast messages, and simplifies VLAN configuration and packet prioritization. A higher level of security between network segments can be achieved.

Configuration of 802.1Q on IP Phones

The 802.1Q support for the IP Phones is configured and controlled using the IP Phone user interface or DHCP. The DHCP approach eliminates the need to manually configure the VLAN ID during the installation.

To configure 802.1Q, configure the following:

- p bits
- VLAN ID

Configure the p bits

By default, the 3-bit field p bits are set to 110b (6), which is the value recommended by Nortel. The p bit value can be changed using either TM or Element Manager. Two fields in TM 3.1 and Element Manager are used to set the p bits:

1. A check box that, when selected, means the priority bits must be set to the value specified by the 802.1Q priority bit value field. If the check box is unselected, the IP Phone sends out the default priority of 6.
2. A 802.1Q priority bit value field. This field sets the value that the IP Phones sends out. The range is 0 to 7.

Configure the VOICE and DATA VLAN ID

The VOICE VLAN ID and DATA VLAN ID fields can be specified on a per interface basis and are global settings. This means that all voice packets transmitted by the IP Phone have the same VOICE VLAN ID and all data packets have the same DATA VLAN ID. Though only one network interface exists on the IP Phone, the IP Phone has two internal IDs: one for voice traffic and one for data traffic. The IP Phone firmware can detect and route the voice and data traffic.

If a DATA VLAN is enabled, the IP Phone adds the DATA VLAN ID to untagged traffic. However, if the traffic arriving on the PC port is already tagged, the frame passes through unchanged.

The VLAN ID is specified as follows:

- The default VLAN ID is 000 (hex).
- The VOICE and DATA VLAN ID can be specified during a manual configuration of the IP Phone using the IP Phone keypad, or automatically retrieved using DHCP (automatic VLAN discovery).
- In the case of the VOICE VLAN ID, the VOICE VLAN ID can also be configured by the DHCP parameter when using the Automatic VLAN ID configuration using DHCP approach.

For more information about manual or automatic IP Phone configuration, see *IP Phones Fundamentals (NN43001-368)*.

The following describes the IP Phone support for 802.1Q.

Step	Action
1	If 802.1Q is disabled, standard Ethernet frames are transmitted.
2	If 802.1Q is enabled, all frames transmitted by the Ethernet driver have the 802.1Q tag bytes inserted between the source MAC address and the protocol type field. The tag protocol identifier field contains 8100 (hex) and the CFI bit is set to 0.
3	When 802.1Q is enabled, separate voice and data VLANs can be configured. Each VLAN has its own ID and priority on the IP Phone. Voice packets have the priority bits of all frames set to 6 (octal) and the VOICE VLAN ID is set to 000 (hex) by default. Data packets have the priority bits of all frames set to 0 and the DATA VLAN ID is set to 000 (hex) by default. The GUI and TPS configured values override these values.
4	The IP Phone Ethernet driver receives any Ethernet frame destined for it, regardless of whether 802.1Q is enabled or the received frame is an 802.1Q tagged frame.

The only exception is any 802.1Q tagged frame with CFI = 1. In this case, the frame is discarded.

- 5 The IP Phone Ethernet driver strips the 802.1Q tag information from the frame before passing it on to the IP stack.
- 6 The IP Phone Ethernet driver filters the packets by the VLAN tag and MAC address. Tagged traffic is prioritized and routed based on the priority bits.

—End—

DHCP requirements

Some implementation requirements of the Automatic VLAN Discovery using DHCP are:

1. A DHCP server IP address pool must exist for each subnet (also VLANs). This is standard DHCP operation. The requirement is the same for PCs or IP Phones.
2. A DHCP server should not exist in more than one VLAN at one time (one subnet for each VLAN), unless the link to the DHCP server is tagged and the DHCP server can recognize this. With an untagged link to the DHCP server, traffic could originate on one VLAN and end up on the other VLAN. In this case, the VLAN using DHCP feature does not work.
3. Voice and data subnets must be separate if the three-port switch with VLANs is being used.
4. A Layer 3 switch (or router) with a relay agent must be used because traffic from the voice VLAN to the data VLAN must be routed. Presumably, the DHCP server is on the data VLAN. Without a relay agent, a DHCP server must exist on each subnet.
5. At least two IP address pools are used on the DHCP server – one for the Voice VLAN/subnet and another for the Data VLAN/subnet. Additional pools can be added as required as long as one IP address pool per subnet and VLAN is used. A relay agent is required if it is a PC-only network.

Control of the IP Phone 802.1Q

The 802.1Q header in the outgoing packets from the IP Phones is enabled by one of the following:

- If the IP Phone VLAN GUI response is set to 1, then the 802.1Q functionality is enabled. All packets from the IP Phone have the 802.1Q header as part of the Ethernet frame.

- If the IP Phone VLAN GUI response is set to 2, then the 802.1Q functionality is enabled after the DHCP response is received with the VLAN ID.
- If the TM or Element Manager configuration enables the use of the p bits, after downloaded to the IP Phone, the 802.1Q functionality is enabled.

802.1Q and the Voice Gateway Media Cards

The Voice Gateway Media Cards cannot send the 802.1Q header because the card operating system does not support it. The switch ports connecting the Voice Gateway Media Card TLAN network interface should be configured for untagged operation so if a 802.1Q header is present, it is stripped before a packet is passed to the card.

The configuration in TM 3.1 and Element Manager is for the control of the priority bits in the 802.1Q header sent by the IP Phones only.

Three-port switch support

The IP Phone three-port switch does not interpret the 802.1Q header. Instead, the three-port switch allows the packets to pass through unmodified. Packet priority is achieved on a per-port basis. IP Phone port traffic has a higher priority than traffic for the Ethernet port to which the PC is connected.

An IP Phone can receive broadcast frames from a PC data VLAN. Any broadcast storm packets from the data network are seen by the IP Phone. However, this type of traffic does not adversely affect the IP Phone.

Data Path Capture tool

IP Line contains the Data Path Capture tool, a built-in utility used to capture audio information. This tool helps debug audio-related gateway problems and allows after-the-fact analysis of what the user heard.

The Data Path Capture process is controlled by a set of CLI commands. For further information, see [Table 101 "Data Path Capture Tool commands" \(page 434\)](#).

IP Phone firmware

See the ReadmeFirst documentation to determine the IP Phone minimum firmware (F/W) versions supported by IP Line.

CS 1000 systems

Default location of firmware files

For CS 1000 system configurations, the default storage location for the firmware files is on the Signaling Server in the /u/fw directory. The firmware file is downloaded to this directory, the file is selected in Element Manager, and the Transmit button is clicked.

Graceful Disable

The DISI command in LD 32 can be used to disable the Voice Gateway Media Card gateway channels when they become idle. This command removes gateway call traffic from a Voice Gateway Media Card; however, it does not remove the IP Phones registered to the Voice Gateway Media Card. Even after the gateway channels are disabled, all IP Phones registered to the card are impacted when the card is unplugged or reset. Also, if a Voice Gateway Media Card or Signaling Server is the node Master when it is removed, the IP Phone registration service is interrupted until the next election occurs.

To overcome these problems, the Graceful TPS enhancement provides a card-level CLI command that disables the LTPS service on the Voice Gateway Media Card or Signaling Server.

The Graceful TPS command:

- prevents new IP Phones from registering
- soft-resets any idle, registered IP Phones

Because the LTPS does not accept new registrations, the IP Phones register with another card LTPS after the reset. Eventually, all IP Phones are registered with other TPSs and the card can be removed without impact to any users.

Operation of the LTPS DISI

The Graceful TPS Disable is controlled from the CLI of the card. When the disiTPS command is executed on the card LTPS, the following occurs:

- The card does not accept any new registration requests.
- The card soft-resets all registered IP Phones that are in the idle state and redirects the IP Phones to the node Master.
- The card soft resets the remaining busy registered IP Phones after they release their active call.
- If the card is node Master, an election is held to transfer the mastership. This occurs only on the Voice Gateway Media Card. The Signaling Server node mastership is not transferred.

ATTENTION

When only the `disiTPS` command is entered on a Signaling Server and the mastership remains with that Signaling Server, then IP Phones can re-register to both Voice Gateway Media Cards and another Signaling Server in the node.

To ensure that the IP Phones re-register only to the secondary Signaling Server, Nortel recommends that the command `disableServices` be used on the Signaling Server instead of `disiTPS`. Using the `disiTPS` command alone on the on the Signaling Server is not recommended.

Alternatively, the `vtrkShutdown` command followed by the `disiTPS` can be entered.

Feature operation of the Voice Gateway DISI

The Voice Gateway can also be disabled from the CLI of a Voice Gateway Media Card. When the `disiVGW` command is executed, the following happens on that card Voice Gateway:

- Idle gateway channels are unregistered.
- A busy gateway channel is unregistered when it becomes idle.

ATTENTION

Care should be taken with this command to avoid a potential problem when calls are placed on hold. When an IP Phone has a call on hold, the voice gateway channel on the card is idle; however, it is still reserved in the Call Server. If the voice gateway is still disabled when the call is taken off hold, the call does not have a speech path.

Recommendation

Nortel recommends that the LD 32 DISI command be used for disabling the gateway channels.

Hardware watchdog timer

A hardware watchdog timer is enabled on the Voice Gateway Media Cards. This functionality adds further robustness to the existing exception handler and maintenance task audits.

The hardware watchdog timer handles scenarios such as the following:

- the CPU failing
- the code running and not triggering an exception
- resetting the card and bringing it back to normal operation

The timer runs on the Voice Gateway Media Cards processors. The card main processor is polled every 20 seconds. If three pollings are missed, then the card is reset. This gives the main processor 60 seconds to respond, covering most normal operating conditions.

A reset reason is logged and saved when a card resets. The reset reason is displayed as a message during the start-up sequence and appears in the SYSLOG file.

The following are examples of reset reasons:

- JAN 04 12:17:45 tXA: Info Last Reset Reason: Reboot command issued Output after card reset using the CLI command `cardReboot`.
- JAN 04 12:17:45 tXA: Info Last Reset Reason: Watchdog Timer Expired Output after card reset due to watchdog timer expiration.
- JAN 04 12:17:45 tXA: Info Last Reset Reason: Manual reset Output after card reset due to either the faceplate reset button press or a power cycle to the card.
- JAN 04 12:17:45 tXA: Info Last Reset Reason: Unknown Output after card reset due either the card F/W not supporting the reset reason or a corruption of the reset reason code.

The last reset reason can also be displayed at any time by entering the CLI command `lastResetReason`.

Codecs

Codec refers to the voice coding and compression algorithm used by the DSPs on the Voice Gateway Media Card. Different codecs provide different levels of voice quality and compression properties. The specific codecs and the order in which they are used are configured on the LTPS and CS 1000.

[Table 54 "Supported codecs" \(page 185\)](#) shows which codecs are supported on the systems.

Table 54
Supported codecs

Codec	Payload size
G.711 a-law, G.711 mu-law, NOVA	10, 20, and 30 ms
G.729A	10, 20, 30, 40, and 50 ms
G.729AB	10, 20, 30, 40, and 50 ms
G.723.1 ¹	30 ms
T.38 ²	supported for fax calls on gateway channels
G.711 Clear Channel ²	supported for fax calls on gateway channels

The G.723.1 codec has bit rates of 5.3 kb/s and 6.3 kb/s. In IP Line, the G.723.1 codec can only be configured with a 5.3 kb/s bit rate; however, the system accepts both G.723.1 5.3 kb/s and 6.4 kb/s from the far-end.

T.38 is the preferred codec type for fax calls over virtual trunks. However, the G.711 Clear Channel codec is used if the far-end does not support the T.38 codec.

For detailed information about codecs, see ["Codecs" \(page 205\)](#).

Set type checking and blocking

If the registration is a regular request (not a Virtual Office logon), the Call Server checks the configured TN type against the actual IP Phone type.

When the LTPS attempts to register the IP Phone with the Call Server, the following occurs:

- If the TN has Flexible Registration Denied (FRD) CLS set, the Call Server checks the IP Phone type against the TN type. If the types do not match registration is rejected and registration in the Emulation Mode is blocked.
- If the TN has Flexible Registration Allowed (default) CLS set, the Call Server checks the IP Phone type against the TN type. If the types are compatible, the TN is converted and the IP Phone registers.
- If the TN has Flexible Registration on Upgrade CLS set, the Call Server checks the IP Phone type against the Virtual TN (VTN) type. If the types are compatible, the TN is converted and the IP Phone registers. After the TN is converted, the Flexible Registration CLS is set to FRD and registration in Emulation Mode is blocked.

However, if the registration request is a virtual logon, this check is not performed. All IP Phones are allowed to be registered onto any IP TN type when the logon is through Virtual Office.

Special checking on the self-labeled line/programmable feature keys is performed when an IP Phone 2004, IP Phone 2007, IP Softphone 2050, IP Phone 1120E, or IP Phone 1140E user logs in from an IP Phone 2002, or when an IP Phone 2002, IP Phone 2004, IP Phone 2007, IP Softphone 2050, MVC 2050, IP Phone 1120E, or IP Phone 1140E user logs in from an IP Phone 2001, IP Audio Conference Phone 2033, or IP Phone 1110.

Special checking is required to prevent a user from logging in from an IP Phone that cannot display an incoming call because the IP Phone used to log on does not have the self-labeled line/programmable feature keys to display the incoming call. If the logon was allowed to occur, the IP Phone could ring without providing the user a way to answer the call. The configuration of the logging-in user is examined for self-labeled line/programmable feature key types that receive incoming calls. If self-labeled line/programmable feature key types appear on any keys not present on the type of IP Phone being used for the logon, the logon is blocked.

The logon from an IP Phone 2002 is blocked for users configured for Automatic Call Distribution (ACD).

IP Phone 2002 logon restrictions

Because the IP Phone 2002 and IP Phone 1120E support only four feature keys, a restricted VO logon is applied to IP Phone 2004, IP Phone 2007, IP Softphone 2050, and IP Phone 1140E TNs when they log on using an IP Phone 2002, or IP Phone 1120E. When the IP Phone 2004, IP Phone 2007, IP Softphone 2050, or IP Phone 1140E user logs in from an IP Phone 2002, or IP Phone 1120E, the logon is blocked if the user configuration has one of the following:

- key 0 defined as ACD
- any key from key 4 to key 15 defined as AAK, CWT, DIG, DPU, GPU, ICF, MCN, MCR, MSB, PVN, PVR, SCR or SCN

IP Phone 2001, IP Audio Conference Phone 2033, and IP Phone 1110 logon restrictions

Because the IP Phone 2001, IP Audio Conference Phone 2033, and IP Phone 1110 do not support any feature keys, a restricted VO logon is applied to IP Phone 2002, IP Phone 2004, IP Phone 2007, IP Softphone 2050, IP Phone 1120E, and IP Phone 1140E TNs when they log on using an IP Phone 2001, IP Audio Conference Phone 2033, or IP Phone 1110. When an IP Phone 2002, IP Phone 2004, IP Phone 2007, IP Softphone 2050, IP Phone 1120E, or IP Phone 1140E user logs on from an IP Phone 2001, IP Audio Conference Phone 2033, or IP Phone 1110, the logon is blocked if the user configuration has one of the following:

- key 0 defined as ACD
- any other key (from key 1 to key 15) defined as AAK, CWT, DIG, DPU, GPU, ICF, MCN, MCR, MSB, PVN, PVR, SCR or SCN.

Enhanced Redundancy for IP Line nodes

The Enhanced Redundancy for IP Line nodes feature relaxes the checking performed by a node on the Node ID that is presented by a registering IP Phone. Under the circumstances described in this section, an IP Phone with a 3-digit Node ID can register to a node that is configured with a 4-digit Node ID. To enable the registration to be successful, the 3-digit Node ID must match the first 3 digits of the node 4-digit Node ID.

This feature enhances the IP Phone survivability in the case of network outages or equipment failure, as it allows an IP Phone to register to more than one node on a system. By configuring the IP Phone S1 and S2 Connect Server IP addresses to the node addressees of two different nodes, and properly configuring the Node IDs, the IP Phone is able to register to another secondary node if it cannot register to the primary node.

The rules are as follows:

- if the Node ID on the system has 3 digits or less, the Node ID from the IP Phone must match exactly
- if the Node ID on the system has 4 digits and:
 - the Node ID from the IP Phone has fewer than 3 digits, reject the registration
 - the Node ID from the IP Phone has 4 digits, the Node ID must match exactly
 - if the Node ID from the IP Phone has 3 digits and they match the first 3 digits of the node 4 digit Node ID (left to right), then allow the IP Phone to register. If the first three digits do not match, reject the registration.

Up to 10 nodes can be configured on a system (3-digit Node ID base + 0-9 for the fourth digit). The IP Phones are distributed among the nodes by programming different S1 and S2 IP addresses into the IP Phones. The IP Phones register to the primary Connect Server (the S1 IP address) if possible.

If a network outage or equipment failure prevents the registration to the primary Connect Server, the IP Phone can register to a secondary Connect Server (the S2 IP address). This feature enables a node registered IP Phones to spread across the spare IP Phone registration capacity of the other nodes in the system in the event of a network outage or equipment failure.

Example:

For example, the installer configures two nodes on a system with Node IDs 3431 and 3432. An IP Phone configured with Node ID 343 can register with either node.

If the IP Phone presented one of the following Node IDs, it would be rejected for registration

- 3
- 34
- 3433

The TN must still match before the IP Phone is allowed to register.

If the customer does not want to use the Enhanced Redundancy for IP Line Nodes feature, programming 2- or 4-digit Node IDs retains the exact match requirement.

Personal Directory, Callers List, and Redial List

Contents

This section contains the following topics:

- ["Introduction" \(page 189\)](#)
- ["Personal Directory" \(page 191\)](#)
- ["Callers List" \(page 192\)](#)
- ["Redial List" \(page 194\)](#)
- ["IP Phone Application Server configuration and administration" \(page 195\)](#)
- ["IP Phone Application Server database maintenance" \(page 198\)](#)
- ["Call Server configuration" \(page 202\)](#)
- ["Password administration" \(page 203\)](#)

Introduction

Personal Directory, Callers List, and Redial List are supported on the IP Phone 2002, IP Phone 2004, IP Phone 2007, IP Softphone 2050, Mobile Voice Client (MVC) 2050, IP Phone 1120E, IP Phone 1140E, IP Phone 1150E, WLAN Handset 2210, WLAN Handset 2211, WLAN Handset 2212, WLAN Handset 6120, and WLAN Handset 6140. Personal Directory, Callers List, and Redial List are not supported on the IP Phone 2001, IP Audio Conference Phone 2033, and IP Phone 1110.

An IP Phone must register to a Signaling Server to access the Personal Directory, Callers List, and Redial List features. The IP Phone Application Server ELAN network interface IP address must be configured. See ["IP Phone Application Server configuration and administration" \(page 195\)](#).

ATTENTION

Calling Party Name Display (CPND) must be configured as a Class of Service (CLS) on the system to enable Personal Directory, Callers List, and Redial List.

Personal Directory is controlled by the user, who can enter or copy names to their personal directory, delete entries, or delete the entire list. Personal Directory is not a call log feature.

Callers List and Redial List are call log features. The content of these lists is generated during call processing. CPND must be configured as a CLS to generate the names in the logs. Content cannot be changed; however, a user can delete or, in some cases, copy entries or lists.

[Table 55 "Comparison of Personal Directory with Callers List and Redial List" \(page 190\)](#) compares the Personal Directory with the Callers List and Redial List features.

Table 55
Comparison of Personal Directory with Callers List and Redial List

Operation	Personal Directory	Callers List and Redial List
Displays date and time of transaction	No	Yes
Modify entry	Yes	No
Dial from the list	Yes	Yes
Delete entry	Yes	Yes
Content view mode (The IP Phone 2004, IP Phone 2007, IP Phone 1140E, IP Phone 1150E, WLAN Handsets 2210/2211/2212/6120/6140 display name and DN simultaneously. The IP Phone 2002 and IP Phone 1120E display either the name or DN. They cannot display the name and DN simultaneously.)	Yes	Yes
Delete list	Yes	Yes
Edit and dial (Temporarily modify an entry and dial out. Does not modify record in database.)	No	Yes
Access through soft keys	Yes	Yes
Maximum number of entries	100	20 (Redial List) 100 (Callers List)

Virtual Office

Personal Directory, Callers List, and Redial List are available when using Virtual Office (VO). Data is stored on the Signaling Server, not on the IP Phone. This means when a user logs on using Virtual Office or logs on in a branch office in Normal Mode, they can always access their stored names and numbers.

Media Gateway 1000B

Personal Directory, Callers List, and Redial List are supported in a branch office configuration when the Media Gateway (MG) 1000B in the branch office location is in Normal Mode. Personal Directory, Callers List, and Redial List are not available in Local Mode, as the entries are stored on the main office Signaling Server.

User key for Personal Directory, Callers List, and Redial List

An IP Phone Private Network Identifier (PNI) + Home Location Code (HLOC) + primary DN (PDN) are used as the lookup key for the IP Phone Personal Directory, Callers List, and Redial List data.

For the HLOC, if a CLID table entry exists (CLID = yes in LD 15) for the Primary DN (PDN) or the first non-ACD key DN, the CLID table HLOC is used. When no CLID entry exists, the HLOC defined in LD 15 Network Data section is used (it might be 0 if HLOC is not configured).

The PNI ensures the HLOC + PDN is unique across customers on a system if the system is multi-customer.

Because the user PDN and HLOC are used, then to identify a specific user, a user primary DN and HLOC must be unique to the network to support their own specific Personal Directory, Callers List, and Redial List. If using Multiple Appearance DN (MADN) for a group of users and it is necessary to provide users with their own Personal Directory, Callers List, and Redial List, do not configure the Primary DN (PDN) as MADN.

If the MADN is used as the PDN for a group of users, this results in a shared Personal Directory, Callers List, and Redial List. This means that a call arriving on any IP Phone sharing the PDN MADN appears in the Callers List. Calls to a secondary DN on another IP Phone in the shared group appear in the Callers List for all IP Phones, even though the call did not ring on the other IP Phone.

Personal Directory

Personal Directory supports the following features:

- maximum entries = 100
- maximum characters in name = 24

- maximum characters in DN = 31
- multiple actions:
 - add new entry
 - edit entry
 - delete entry
 - delete contents of directory
 - copy an entry from Personal Directory to Personal Directory
 - copy an entry from Corporate Directory to Personal Directory
 - dial the DN of an entry
 - name search
- password protection to control access to Personal Directory
- one minute time-out

Callers List

Callers List supports the following features:

- maximum entries = 100
- maximum characters in name = 24
- maximum characters in DN = 31
- multiple actions:
 - dial the DN of an entry
 - edit the entry
 - copy the entry
 - delete the entry
- sorted by the time the call is logged
- contains caller name, DN, time of last call occurrence, and how many times the caller calls this user
- Idle Display option: displays and counts all calls or only unanswered calls
- displays caller name (Redial List only displays the caller DN)
- after the 100 entry limit is reached, the newest entry overwrites the oldest entry
- one minute time-out

Call log options

Use Call log options to configure the following preferences on the IP Phone:

- if the Callers List logs all incoming calls or only unanswered calls
- if Idle Set Display indicates when new calls have been logged to the Callers List
- if a name stored in the Personal Directory that is associated with the incoming call DN is displayed instead of the name transmitted by the Call Server
- the three area codes that should be displayed after the DN, rather than before it (for example, local area codes)

Follow the steps in [Procedure 6 "Accessing the call log options" \(page 193\)](#) to access the call log options for the IP Phone.

Procedure 6

Accessing the call log options

Step	Action
1	Press the IP Phone Services key. The Telephone Options menu displays.
2	From the Telephone Options menu, select Call Log Options .
3	Select the desired options.
—End—	

[Table 56 "Call log options" \(page 193\)](#) summarizes the call log options.

Table 56
Call log options

Call log option	Description	Default value
Log all/unanswered incoming calls	Configures the Callers List to log all incoming calls or only the unanswered incoming calls.	Log all calls
New Call Indication	When New Call Indication is turned on, a message is displayed on the IP Phone to inform the user of a new incoming call. If not configured, nothing is displayed.	On

Call log option	Description	Default value
Preferred Name Match	Configures whether the caller name displayed is the CPND from the Call Server or the name associated with the DN stored in the Personal Directory	CPND from the Call Server is displayed
Area code set-up	Configures how the incoming DN is displayed. If the area code of the incoming call matches a specified area code, the DN is displayed in the configured manner (for example, the area code may be displayed after the DN)	No area code
Name display format	Configures the format of the name display of the incoming call on the IP Phone. There are two choices: <first name> <last name> <last name> <first name>	<first name> <last name>

The IP Phone 2002 does not display the New Call Indication on the idle screen at the same time as the date and time. Instead, the New Call Indication alternates with the date and time display.

Redial List

Redial List supports the following features:

- maximum entries = 20
- maximum characters in a name = 24
- maximum characters in a DN = 31
- contains name, DN, and the time the last call to that DN occurred in each entry
- the newest entry overwrites the oldest entry after the 20-entry limit is reached
- sort by the time the call is logged
- multiple actions:

- dial the DN of an entry
 - edit the entry
 - copy the entry
 - delete the entry
 - delete contents of a list
- one minute time-out

IP Phone Application Server configuration and administration

The IP Phone Application Server runs on the Signaling Server. If less than 1000 users are supported, then the IP Phone Application Server can run on the same Signaling Server as Element Manager. If more than 1000 users are supported, then the IP Phone Application Server must run on a separate Signaling Server (preferably a Follower) with no colocated applications. Therefore, it is necessary to configure in Element Manager the ELAN network interface IP address of the specific Signaling Server where the IP Phone Application Server is installed.

The IP Phone Application Server can be shared across multiple IP Telephony nodes on the same Call Server.

Configure the IP Phone Application Server and remote backup

If the IP Phone Application Server must support more than 1000 users, see ["Configure IP Phone Application Server on a separate Signaling Server" \(page 197\)](#).

The IP Phone Application Server and remote backup configuration are configured in Element Manager by clicking (in the navigator) **IP Network > Personal Directories**.

Because a backup and restore of the IP Phone Application Server database can be performed, it is necessary to configure information to support the backup/restore functionality. See [Figure 40 "Personal Directories Server Configuration window" \(page 196\)](#).

The following parameters are configured:

- ELAN network interface IP address of the IP Phone Application Server where the database is located
- checkbox to turn on or off the remote backup functionality
- IP address of the server where the backup is saved
- path, file name, user ID, and password to support the backup/restore functionality

Figure 40
Personal Directories Server Configuration window

NORTEL CS 1000 ELEMENT MANAGER

Managing: **192.167.100.3**
 System » IP Network » Personal Directories » Server Configuration

Server Configuration

Server Configuration

Server IP Address: 192.167.100.4

Backup Configuration

Perform scheduled remote backup: ☒

Remote backup time of day(hh:mm): 0:0

Remote backup IP address: 47.11.22.11

Remote backup path: /auto/ethernet

Remote backup file name: ipldb.db

Remote backup userid: etherset

Remote backup password: ••••••••

Submit Cancel

Table 57 "Sample IP Phone Application Server configuration" (page 196) provides a sample IP Phone Application Server configuration.

Table 57
Sample IP Phone Application Server configuration

Data field name	Example	Description
Server Configuration		
Server IP Address	92.168.10.12	IP address of the database server (for example, the Leader Signaling Server ELAN network interface IP address)
Backup Configuration		
Perform scheduled remote backup	Checkbox is selected	Select checkbox to enable scheduled remote backups.
Remote backup time of day (hh:mm)	00:00	the time of day to perform the backup (default is 00:00 midnight)

Data field name	Example	Description
Remote backup IP address	47.11.22.11	remote backup server IP address
Remote backup path	/auto/etherset	remote path where the backup file is saved
Remote backup file name	ipldb.db	file name of the backup file
Remote backup userid	etherset	logon name for the remote backup
Remote backup password	etherset	password for remote backup

The Personal Directory, Callers List, and Redial List features are not available to the user if the IP Phones lose contact with the Signaling Server. The IP Phones then register with the Voice Gateway Media Card but the features only become available again when contact with the Signaling Server is reestablished.

In a node composed of Voice Gateway Media Cards and Signaling Server, IP Phones only register to the Voice Gateway Media Cards when the Signaling Server are not present due to a failure condition. Five minutes after a node election is completed, each Voice Gateway Media Card with IP Phones registered to it checks to see if a Signaling Server is present in the node. If a Signaling Server is present, any idle IP Phones that are found are reset (server-switched) back to S1 (Server 1) so they can re-register to the Signaling Server. If an IP Phone is busy, a one-minute timer is started. Every one minute, the process comes back to check for idle IP Phones and idle phones are reset. This checking continues until no IP Phones remain registered to the Voice Gateway Media Cards.

Configure IP Phone Application Server on a separate Signaling Server

If the IP Phone Application Server must support more than 1000 users, follow the steps in [Procedure 7 "Configuring the IP Phone Application Server on a separate Signaling Server" \(page 197\)](#) to configure the IP Phone Application Server on a separate Signaling Server.

Procedure 7

Configuring the IP Phone Application Server on a separate Signaling Server

Step	Action
1	In the Element Manager navigator, click IP Network > Nodes: Servers, Media Cards to configure a new node. The Node Configuration window appears.
2	Enter a unique Node ID in the New Node field. Click the to Add button.

The **Edit** window appears.

- 3 Configure the IP addresses and subnet masks for the Signaling Server.
- 4 Click **Save and Transfer**.
- 5 Configure the IP Phone Application Server using the ELAN network interface IP address of the new Signaling Server.

In the navigator, click **IP Network > Personal Directories** . The Personal Directories window appears.

- 6 Click **Server Configuration**.
- 7 Configure the backup parameters for Personal Directory, Callers List, and Redial List and click **Submit**.
See [Table 57 "Sample IP Phone Application Server configuration" \(page 196\)](#).
- 8 Reboot the Signaling Server that was configured as the IP Phone Application Server.
- 9 When the Signaling Server comes back online, reset all the IP Phones by performing **isetResetAll** on every LTPS in the system. See [Table 95 "Reset commands" \(page 429\)](#).

—End—

Alarms

If the IP Phone Application Server is not installed on the primary Signaling Server, and the other Signaling Server cannot contact the IP Phone Application Server, then an SNMP alarm is raised. The alarm indicates that the Personal Directory, Callers List, and Redial List are not available. If this occurs, the other Signaling Server track the Signaling Server where the IP Phone Application Server resides. When contact with the IP Phone Application Server is made, Personal Directory, Callers List, and Redial List access resumes.

IP Phone Application Server database maintenance

All IP Phone Application Server database maintenance is performed in Element Manager.

Configure a daily backup to occur at a scheduled time.

Database recovery can be performed for the entire database of the IP Phone Application Server or for one user entries.

IP Phone Application Server database backup

Follow the steps in [Procedure 8 "Backing up the IP Phone Application Server database server manually"](#) (page 199) to perform a manual backup of the IP Phone Application Server database.

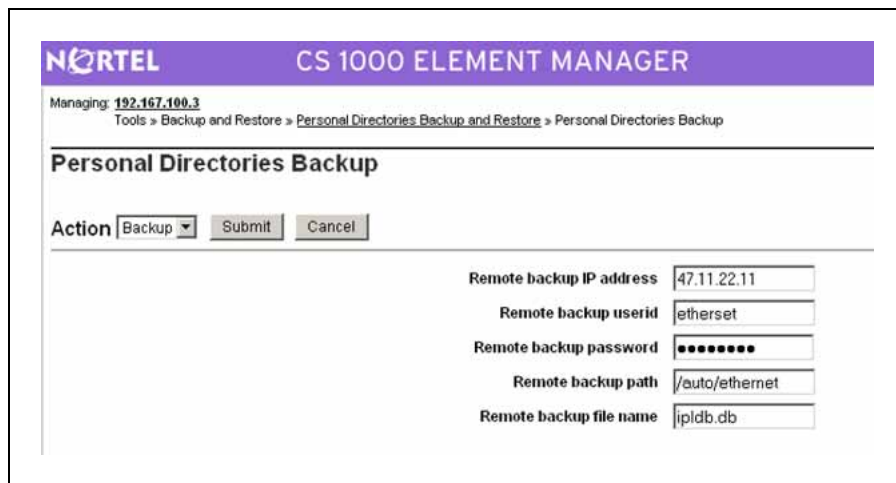
A scheduled backup of the database can also be configured. See ["Configure the IP Phone Application Server and remote backup"](#) (page 195).

Procedure 8

Backing up the IP Phone Application Server database server manually

Step	Action
1	In the Element Manager navigator, click Tools > Backup and Restore > Personal Directories . The Personal Directories Backup and Restore window appears.
2	Click Personal Directories Backup . The Personal Directories Backup window appears. See Figure 41 "Personal Directories Backup window" (page 199).

Figure 41
Personal Directories Backup window



- Enter the data for the **Remote backup IP address**, **Remote backup userid**, **Remote backup password**, **Remote backup path**, and **Remote backup file name** fields.
- Click **Submit**.

—End—

Full database recovery

Follow the steps in [Procedure 9 "Performing a full database recovery"](#) (page 200) to perform a full database backup for the IP Phone Application Server.

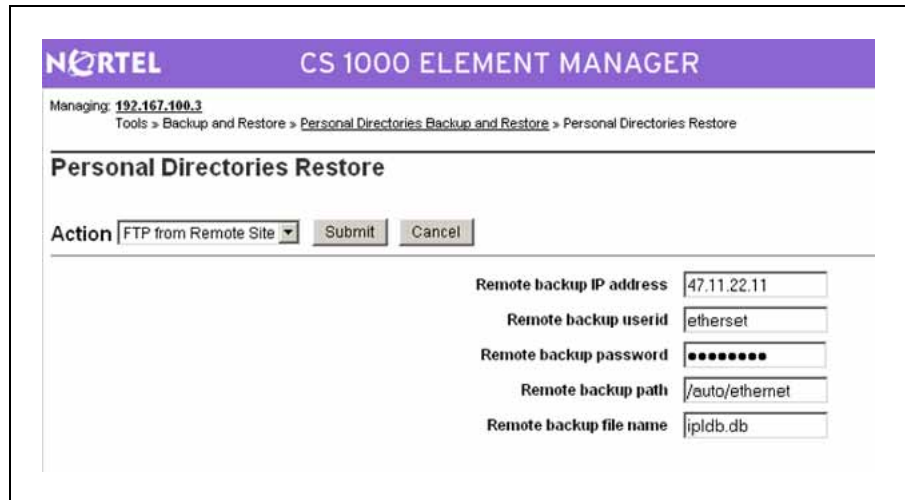
Procedure 9

Performing a full database recovery

Step	Action

1	Click Tools > Backup and Restore > Personal Directories . The Personal Directories Backup and Restore window appears.
2	Click Personal Directories Restore . The Personal Directories Restore window appears. See Figure 42 "Personal Directories Restore window" (page 200).

Figure 42
Personal Directories Restore window



3	From the Action drop-down list, select FTP from Remote Site if the backup is saved on a remote server. If the backup is already saved locally on the server, go to Step 8.
4	Enter the data for the Remote backup IP address , Remote backup userid , Remote backup password , Remote backup path , and Remote backup file name fields.
5	Click Submit .
6	Click OK . After the file is transferred by FTP to the local drive, an information window appears indicating successful file transfer.
7	Click OK .

The file is transferred to the server but the database is not yet restored.

8 From the Action drop-down list, select **Restore All Users**.

9 Click **Submit**.

10 Click **OK**.

The data for all users is restored and the existing data in the Personal Directories database is overwritten.

—End—

ATTENTION

The length of time to restore a database depends on the amount of records.

Selective database recovery for a single user

Follow the steps in [Procedure 10 "Performing a selective database recovery" \(page 201\)](#) to perform a database recovery for a single user. The procedure cannot be performed unless there is a valid backup file.

Procedure 10

Performing a selective database recovery

Step	Action
1	Click Tools > Backup and Restore > Personal Directories . The Personal Directories Backup and Restore window appears.
2	Click Personal Directories Restore . The Personal Directories Restore window appears.
3	From the Action drop-down list, select Restore Single User . The Personal Directories Restore window for a single user opens. See Figure 43 "Personal Directories Restore for a single user window" (page 202) .

Figure 43
Personal Directories Restore for a single user window

- 4 Enter the **Customer Number** and **Directory Number (DN)** of the user.
- 5 Select the check box(es) of the data that is to be restored.
- 6 Click **Submit**.

—End—

Fault clearance

The recovery of the database clears any faults.

Recommendation

Nortel recommends that the IP Phone Application Server is installed on a dedicated Signaling Server to ensure that database operations do not affect call processing.

Call Server configuration

To provide password protection for an IP Phone user Personal Directory, Callers List, and Redial List, Station Control Password (SCPW) must be configured on the Call Server. If SCPW is not configured, password administration on the IP Phone cannot be accessed.

In LD 15 and in Element Manager, a new prompt, DFLT_SCPW, has been added to the Flexible Feature Code (FFC) parameters for the Call Server. When DFLT_SCPW is set to YES, the system assigns a default password (the primary DN) to IP Phone users when an IP Phone is added or changed in LD 11.

ATTENTION

System administrators must ensure that users change the default password on the IP Phone to control access, as the default password is the same on all IP Phones when DFLT_SCPW is set to YES.

The new prompt DFLT_SCPW and the existing prompt Station Control Password Length (SCPL) are prompted only if FFC package 139 is enabled.

The SCPL is also defined in LD 15 Flexible Feature Code (FFC) configuration parameters and in Element Manager. If the SCPL length is changed, the change takes effect only after a data dump and then a sysload of the Call Server. The SCPL is changed to the new length during the sysload. If the length is increased, then 0 is inserted at the beginning of the SCPW to conform to the new length. If the password length is reduced, then the leading digits are removed during the sysload.

Password administration

The Station Control Password (SCPW) controls access to the user private Personal Directory, Callers List, and Redial List information.

When the IP Phone first registers to the system after it is created, by default the password protection is turned off. If a default password is defined for the user, the user can enable or disable password protection and change the password. The changed password is updated on the Call Server and can be viewed in LD 20. Other applications that use this password, such as Virtual Office and Remote Call Forward, are affected by the password change.

Initial password

When an IP Phone first registers with the system, by default the password protection is turned off. SCPW must be initially configured for each user. If no SCPW has been defined, password protection for the IP Phone cannot be enabled. The prompt DFLT_SCPW in LD 15 specifies that a default SCPW is assigned to an IP Phone user when an IP Phone is added or changed in LD 11. See [Table 58 "LD 15 – Enable a default SCPW."](#) (page 203).

Table 58
LD 15 Enable a default SCPW

Prompt	Response	Description
REQ:	CHG	Change existing data.
TYPE:	FFC	Change Flexible Feature Code parameters.
CUST		Customer number.
	0 to 99	Range for Large System and CS 1000E system.
	0 to 31	Range for CS 1000M Small System and Media Gateway 1000B.

Prompt	Response	Description
...		
FFCS	(NO) YES	Change Flexible Feature Code end-of dialing indicator.
ADLD	(0) to 20	Auto Dial Delay (in seconds).
DFLT_SCPW	(NO) YES	Default Station Control Password.
		NO = disable Default Station Control Password (default).
		When DFLT_SCPW = YES, the system automatically assigns an SCPW when a new IP Phone 2002, IP Phone 2004, or IP Softphone 2050 is created.
		An SCPW is not automatically assigned to an existing IP Phone unless that IP Phone is given a service change.

Password guessing protection

A password retry counter tracks how many incorrect password entries are made. If the IP Phone password verification fails three times in one hour, the user is locked out for one hour. This means that the Personal Directory, Callers List, and Redial List cannot be accessed and password administration cannot be performed. A message displays on the IP Phone to indicate that access is locked.

After one hour, the retry counter is reset and access is unlocked. The retry counter also resets when the password is entered correctly.

The administrator can reset the counter and unlock the access either in Element Manager or in LD 32.

If a user is locked out from using their SCPW to access their Personal Directory, Callers List, and Redial List, they also are blocked from access to their Virtual Office logon, because VO uses the same SCPW. Conversely, a user who is locked out from the VO logon is also locked out from accessing their Personal Directory, Callers List, and Redial List.

Forgotten password

If the user forgets their IP Phone password, the administrator can reset the retry counter and change the user password in Element Manager. After the administrator changes the password, the lock is released automatically.

Codecs

Contents

This section contains the following topics:

- ["Introduction" \(page 205\)](#)
- ["Codec configuration" \(page 207\)](#)
- ["Codec registration" \(page 209\)](#)
- ["Codec negotiation" \(page 212\)](#)
- ["Codec selection" \(page 215\)](#)

Introduction

The IP Phones and Voice Gateway Media Cards support different codecs and codec parameters with different compression rates and audio quality. The CS 1000 system selects the appropriate codecs based on user-configurable parameters.

For instance, an IP Phone-to-IP Phone call in the same zone within a LAN can be set up using G.711 at 64 kb/s. For an IP Phone-to-IP Phone call over a WAN, the call can be set up using G.729A or G.729AB at 8 kb/s. These data rates and the Voice Gateway Channel Server on the Voice Gateway Media Card are for the voice stream only. Packet overhead is not included.

Predefined codec table

The Line Terminal Proxy Server (LTPS) and the Voice Gateway Channel Server on the Voice Gateway Media Card have a predefined table of codec option sets that can be supported.

The first entry in the table has the highest quality audio (BQ = Best Quality) and requires the largest amount of bandwidth. The last entry requires the least amount of bandwidth (BB = Best Bandwidth) with lower voice quality.

When the Call Server sets up a Call Server connection between an IP Phone-to-IP Phone or IP Phone-to-Voice Gateway Channel Server, the predefined table determines which codec it selects for that connection. This information is provided to the system as part of the IP Phone registration sequence.

For more information about the registration sequence, see *Converging the Data Network with VoIP Fundamentals (NN43001-260)*.

Codec selection

The systems use this information to set up a speech path and select a codec that both endpoints support. As part of zone management, the system further selects the codec based on whether it is trying to optimize quality (BQ) or bandwidth usage (BB).



CAUTION

When voice compression codecs are used, voice quality is impaired if end-to-end calls include multiple compressions.

Codec refers to the voice coding and compression algorithm used by the DSPs on the Voice Gateway Media Card. Different codecs provide different levels of voice quality and compression properties. The specific codecs, and the order in which they are used, are configured in the LTPS and on the system.

Table 59 "Supported codecs" (page 206) shows which codecs are supported on the CS 1000 system.

Table 59
Supported codecs

Codec	Payload size
G.711 a-law, G.711 mu-law, NOVA	10, 20, and 30 ms
G.729A	10, 20, 30, 40, and 50 ms
G.729AB	10, 20, 30, 40, and 50 ms
G.723.1 ¹	30 ms
The G.723.1 codec has bit rates of 5.3 kb/s and 6.3 kb/s. The G.723.1 codec can only be configured with a 5.3 kb/s bit rate; however, the system accepts both G.723.1 5.3 kb/s and 6.3 kb/s from the far end. T.38 is the preferred codec type for fax calls over virtual trunks. However, the G.711 Clear Channel codec is used if the far end does not support the T.38 codec.	

Codec	Payload size
T.38 ²	supported for fax calls on gateway channels
G.711 Clear Channel ²	supported for fax calls on gateway channels
The G.723.1 codec has bit rates of 5.3 kb/s and 6.3 kb/s. The G.723.1 codec can only be configured with a 5.3 kb/s bit rate; however, the system accepts both G.723.1 5.3 kb/s and 6.3 kb/s from the far end. T.38 is the preferred codec type for fax calls over virtual trunks. However, the G.711 Clear Channel codec is used if the far end does not support the T.38 codec.	

The MVC 2050 supports only the G.711 codec with 30 ms payload.

If there are multiple nodes on a system and the same codec is selected on more than one node, ensure that each node has the same voice payload size configured for the codec.

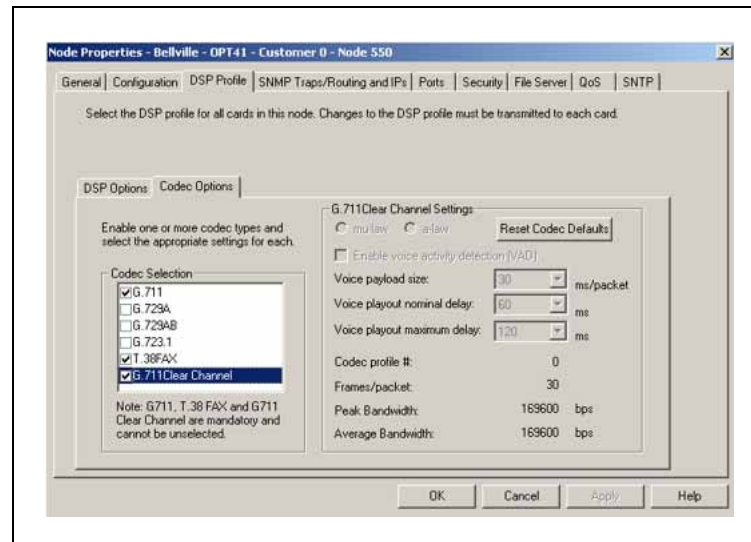
Codec configuration

Configure the codec in the DSP Profile sections of TM 3.1 and Element Manager.

Codec selection in TM 3.1

Figure 44 "Codec list on TM 3.1" (page 208) shows the list of codecs available on the DSP Profile tab within TM 3.1 IP Line application. The Codec Options sub-tab presents a table of different sets of codec options identified by a codec setting index number. There is a list of up to 32 codec settings for G.711, G.729A, and G.729AB. The lesser codec setting index corresponds to BQ (Best Quality) in LD 117 zone configuration. The greater codec setting index corresponds to BB (Best Bandwidth). For more information, see *Converging the Data Network with VoIP Fundamentals (NN43001-260)*.

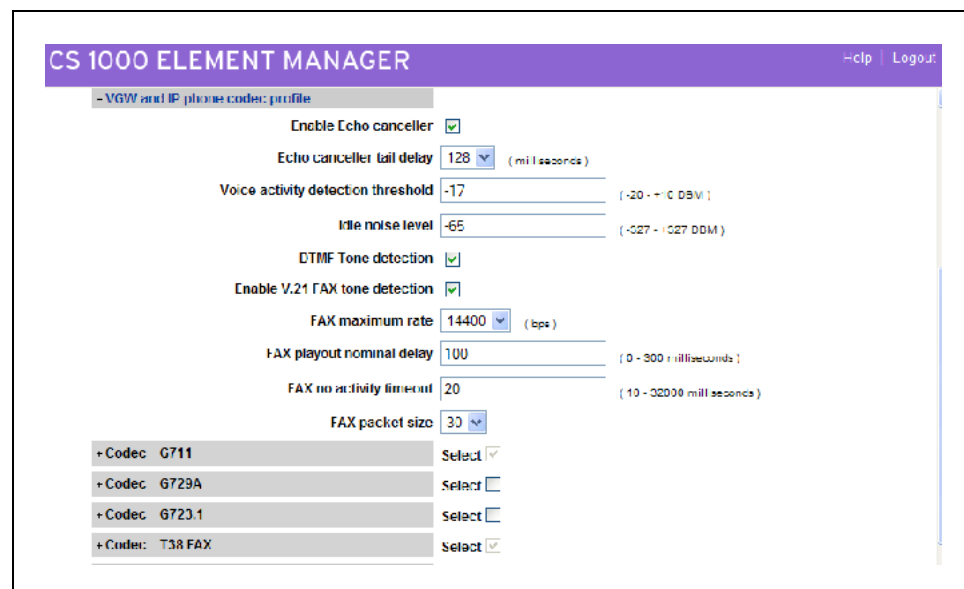
Figure 44
Codec list on TM 3.1



Codec selection in Element Manager

Figure 45 "Codec list in Element Manager" (page 208) shows the list of codec types that are displayed in Element Manager.

Figure 45
Codec list in Element Manager



The G.711 and T.38 Fax codecs are automatically selected and cannot be unselected. Even though these codecs cannot be unselected, the payload size and the jitter buffer for G.711 can be changed. For G.711 Clear Channel, only the jitter buffer can be changed.

Select any two, any one, or none of the G.729A, and G.723.1 codecs. If the G.729A codec is selected, the payload size and the jitter buffer settings can be changed. If the G.723.1 codec is selected, only the jitter buffer can be changed, as the only supported payload size is 30 msec.

For codec configuration in Element Manager, see "[Configure Voice Gateway Profile data](#)" (page 270).

Codec registration

After the configuration of codecs is complete, the IP Phones and DSPs have to register the configured codecs with the Call Server.

Codec registration for IP Phones

The IP Phones always register both the G.711 a-law and mu-law codecs, as well as all codec configured by the user. The codecs that can be configured by the user are G.729A, G.729AB, and G.723.1.

The minimum number of codecs registered for an IP Phone is two: G.711 a-law and G.711 mu-law (G.711 is always configured).

The maximum number of codecs registered for an IP Phone is five: G.711 a-law, G.711 mu-law, G.729A, G.729AB, and G.723.1.

ATTENTION

IP Phones do not register the fax codecs (T.38 and G.711 Clear Channel).

Example 1

A user configures a G.711 mu-law codec (with a 30 msec payload) and a G.723.1 codec (with a 30 msec payload).

The following three codecs are actually registered:

1. G.711 mu-law (30 msec)
2. G.711 a-law (30 msec)
3. G.723.1 (30 msec)

Example 2

A user configures four codecs:

1. G.711 a-law codec with a 10 msec payload
2. G.729A codec with 50 msec payload
3. G.729AB codec with 30 msec payload
4. G.723.1 codec with a 30 msec payload

The following five codecs are actually registered:

1. G.711 a-law (10 msec)
2. G.711 mu-law (10 msec)
3. G.729A (50 msec)
4. G.729AB (30 msec)
5. G.723.1 (30 msec)

Codec registration for DSPs

DSPs register the following codecs:

- Both G.711 a-law and G.711 mu-law codecs are always registered.
- Both fax codecs (T.38 and G.711 Clear Channel) are always registered.
- One best bandwidth (BB) codec, if at least one of G.729A, G.729AB, or G.723.1 codecs is configured. The BB codec is based on the codec type. The order of preference for choosing the BB codec is G.729AB, G.729A, and then G.723.1.

ATTENTION

When G.723.1 codec is configured on the Media Card 32-port cards, the number of channels is reduced to 24. This is a limitation of the DSP software. The unused channels are not registered, therefore the Call Server software does not access them.

Minimum codecs

The minimum number of codecs registered for DSPs is four:

- G.711 a-law
- G.711 mu-law
- T.38
- G.711 Clear Channel

Maximum codecs

The maximum number of codecs registered for DSPs is six:

- G.711 a-law
- G.711 mu-law
- T.38
- G.711 Clear Channel
- one of G.729AB and/or G.729A, or G.723.1

Example 1

A user configures four codecs:

1. G.711 a-law codec with a 10 msec payload
2. G.729A codec with 50 msec payload
3. G.729AB codec with 30 msec payload
4. G.723.1 codec with a 30 msec payload

The following six codecs are actually registered:

1. G.711 a-law (10 msec)
2. G.711 mu-law (10 msec)
3. G.729AB (30 msec)
4. G.729A (50 msec)
5. T.38
6. G.711 Clear Channel

The G.729AB codec is selected, as it is the first in the order of preference of the BB codecs. The G.723.1 codec does not get registered.

Example 2

A user configures three codecs:

1. G.711 mu-law codec with a 20 msec payload
2. G.729A codec with 30 msec payload
3. G.723.1 codec with a 30 msec payload

The following five codecs are actually registered:

1. G.711 mu-law (20 msec)
2. G.711 a-law (20 msec)
3. G.729A (30 msec)
4. T.38
5. G.711 Clear Channel

The G.729A codec is selected, as it precedes the G.723.1 codec in the order of preference of the best bandwidth codecs.

Voice Gateway codec registration

The Voice Gateway registers codecs for the gateway channels as follows:

- G.711 a-law and G.711 mu-law are always registered.

- T.38 and G.711 Clear Channel fax codecs are always registered. G.711 Clear Channel is used for IP Trunk connections to Business Communication Manager (BCM), which does not support T.38 fax.
- A minimum of two codecs are registered if only G.711 was configured.
- A maximum of four codecs can be registered - the G.711 a-law and mu-law for BQ codec, and some BB codecs (defined by the following rules).
 - If the G.729A codec is configured, only the G.729A codec is registered with the Call Server.
 - If the G.729AB codec is configured, the G.729A codec and the G.729AB codec are registered with the Call Server.
 - If the G.723 codec is configured, the G.723 codec is registered with the Call Server.

Example 1

G.711 a-law, G.729A, G.729AB, and G.723.1 are configured.
The Voice Gateway registers G.711 a-law, G.711 mu-law, G.729A, and G.729AB.

Example 2

G.711 mu-law, G.729A, and G.723.1 are configured.
The Voice Gateway registers G.711 a-law, G.711 mu-law, and G.729A.

Example 3

G.711 mu-law and G.723.1 are configured.
The Voice Gateway registers G.711 a-law, G.711 mu-law, and G.723.1.

Codec negotiation

For every virtual trunk call, a common codec must be selected for the call. This is known as codec negotiation. Codec negotiation for virtual trunk calls is performed through the H.323 FastStart and Terminal Capability Set (TCS) messages.

For a call setup with the FastStart procedure, the originating node sends its codec list in the FastStart element in the SETUP message to the terminating node. For a call setup using the SlowStart procedure or for a call modification (media redirection), each node sends its codec list in the TCS message to the other node.

Codec sorting

Before sending a codec list in FastStart and TCS messages, the codec list must be sorted according to the BB or BQ policy. This is determined by the following:

- the zone configuration of the IP Phone/DSP involved in the call
- the zone configuration of the virtual trunk used for the call

Codec sorting methods

There are two methods for sorting the codec list:

1. BQ sorting – the codec list is sorted so that the first codec in the list is the best BQ codec, the second codec is the second best BQ codec in the list, and so on.
2. BB sorting – the codec list is sorted so that the first codec in the list is the best BB codec, the second codec is the second best BB codec in the list, and so on.

[Table 60 "BQ and BB codec sorting lists" \(page 213\)](#) shows the codec list sorting order for the BQ and BB codecs. To know if a codec is BQ (as compared to another codec), see the lists in columns 1 and 2. To determine if a codec is BB (as compared to another codec), see the lists in columns 3 and 4. The BQ or BB codec is listed at the top of the column.

Table 60
BQ and BB codec sorting lists

Best Quality (BQ) sorting		Best Bandwidth (BB) sorting	
For mu-law systems	For a-law systems	For mu-law systems	For a-law systems
G.71_mu_law_10msec	G.711_a_law_10msec	G.729AB_50msec	G.729AB_50msec
G.711_mu_law_20msec	G.711_a_law_20msec	G.729AB_40msec	G.729AB_40msec
G.711_mu_law_30msec	G.711_a_law_30msec	G.729AB_30msec	G.729AB_30msec
G.711_a_law_10msec	G.711_mu_law_10msec	G.729AB_20msec	G.729AB_20msec
G.711_a_law_20msec	G.711_mu_law_20msec	G.729AB_10msec	G.729AB_10msec
G.711_a_law_30msec	G.711_mu_law_30msec	G.729A_50msec	G.729AB_10msec
G.729A_10msec	G.729A_10msec	G.729A_40msec	G.729A_50msec
G.729A_20msec	G.729A_20msec	G.729A_30msec	

Best Quality (BQ) sorting		Best Bandwidth (BB) sorting	
For mu-law systems	For a-law systems	For mu-law systems	For a-law systems
G.729A_30msec	G.729A_30msec	G.729A_20msec	G.729A_40msec
G.729A_40msec	G.729A_40msec	G.729A_10msec	G.729A_30msec
G.729A_50msec	G.729A_50msec	G.723.1_5.3kb/s_30ms	G.729A_20msec
G.729AB_10msec	G.729AB_10msec	G.723.1_6.4kb/s_30ms	G.729A_10msec
G.729AB_20msec	G.729AB_20msec	G.711_mu_law_30msec	G.723.1_5.3kb/s_30ms
G.729AB_30msec	G.729AB_30msec	G.711_mu_law_20msec	G.723.1_6.4kb/s_30ms
G.729AB_40msec	G.729AB_40msec	G.711_mu_law_10msec	G.711_a_law_30msec
G.729AB_50msec	G.729AB_50msec	G.711_a_law_30msec	G.711_a_law_20msec
G.723.1_5.3kb/s_30ms	G.723.1_5.3kb/s_30ms	G.711_a_law_20msec	G.711_mu_law_30msec
G.723.1_6.4kb/s_30ms	G.723.1_6.4kb/s_30ms	G.711_a_law_10msec	G.711_mu_law_20msec
T.38	T.38	T.38	G.711_mu_law_10msec
G.711CC	G.711CC	G.711CC	T.38
			G.711CC

Codec selection

For every virtual trunk call, a codec must be selected before the media path is opened.

When a call setup with the FastStart procedure is used, the terminating node selects a common codec and sends the selected codec to the originating node. For a call modification (media redirection) or for a call setup using the SlowStart procedure, the codec selection occurs on both nodes. Each node has two codec lists: its own list and the far-end list. To select the same codec on both nodes, it is essential to use the same codec selection algorithm on both nodes.

For the codec selection, both the near- and far-end codec lists are retrieved:

- The far-end list is not modified because it is already sorted when it is received (in FastStart or TCS message).
- The near-end list is sorted and then expanded to include lower payloads, the same way it is done before sending the codec list in FastStart message.

The following conditions are met before codec selection occurs:

- There are two codec lists:
 - The near-end list is the codec list of the local unit.
 - The far-end list is the codec list received from the far end.
- Each codec list can contain more than one payload size for a given codec type. The codec list depends on the codec configuration.
- Each codec list is sorted by order of preference. The first codec in the near-end list is the near-end most preferred codec and the first codec in far-end list is the far end most preferred codec, and so on.

After the above conditions are met, a codec selection algorithm is used to select the codec to be used for a call. There are two different codec selection algorithms:

1. H.323 Master/Slave algorithm
2. Best Bandwidth codec Selection algorithm

H.323 Master/Slave algorithm

The codec selection algorithm proposed by the H.323 standard involves a Master/Slave negotiation, initiated each time two nodes exchange their capabilities (TCS message). The Master/Slave information decides that one node is Master and the other node is Slave. The outcome of the

Master/Slave negotiation is not known in advance, it is a random result: one node could be Master then Slave (or Slave then Master) during the same call.

- The Master node uses its own codec list as the preferred one. From the far-end list, it finds the common codec.

The Master gets the first codec in its own list (Codec1). The Master then checks the far-end list to see if Codec1 is a common codec (that is, is Codec1 also listed in the far-end list). If Codec1 is common to both lists, Codec1 becomes the selected codec. Otherwise, the Master obtains the second codec from its own list and repeats the search in the far-end list, and so on.

- The Slave node uses the far-end list as the preferred list. The Slave selects a codec from the far-end list and then searches in its own list to find the common codec.

The issues caused by the Master/Slave algorithm are due to the random nature of the Master/Slave information. The codec that is selected and used during a virtual trunk call cannot be pre-determined. This can make bandwidth usage calculations and bandwidth management difficult.

Known issues include:

- After an on-hold and off-hold scenario (that triggers Master/Slave negotiation), the codec used for the restored call can be different than the codec used before the call was placed on hold. The Master/Slave information could have been changed when the call was on hold.
- Because the terminating end of a call is always the Master, a call from Telephone1 (Node1) to Telephone2 (Node2) can use a different codec than a call from Telephone2 (Node2) to Telephone1 (Node1).
- For tandem calls, the Master/Slave information is not relevant. That is, the Master/Slave information is designed to be used only between two nodes, not among three or more nodes. The Master/Slave algorithm makes the codec selection for tandem calls more complex and inefficient.

To solve the issues, another codec selection algorithm was needed. This algorithm is called the Best Bandwidth codec Selection algorithm and is not based on the unpredictable Master/Slave information.

The Best Bandwidth codec Selection algorithm is used for virtual trunk calls between Nortel equipment, because any change to the Master/Slave algorithm implies a change to the H.323 standard. The H.323 Master/Slave algorithm is used when there is a virtual trunk call between Nortel equipment and third-party equipment.

Best Bandwidth Codec Selection algorithm

The Best Bandwidth Codec Selection algorithm was implemented to solve the issues caused by the H.323 Master/Slave algorithm. The Best Bandwidth Codec Selection algorithm selects one common codec based on two codec lists. With this algorithm, every time the selection is done using the same two lists, the selected codec is always the same.

The "Best Bandwidth" codec selection is based on the codec type only; it does not take into account the fact that some codecs, while generally using less bandwidth, consume more bandwidth than others at certain payload sizes.

- The Best Bandwidth Codec Selection algorithm finds the first codec in the near-end list that is also in far-end list (codec is the same type and has the same payload size). Call the selected codec C1.
- Find the first codec in the far-end list that is also in the near-end list (same type, same payload size). Call this codec C2.
- The C1 and C2 codec that is selected is considered to be the BB codec type. To determine which codec type is Best Bandwidth, the following rules are used:
 - a G.729AB codec is considered BB compared to G.729A, G.723.1, G.711_mu-Law, and G.711_a-Law codecs
 - a G.729A codec is considered BB compared to G.723.1, G.711_mu-Law, and G.711_a-Law codecs
 - a G.723.1 codec is considered BB compared to a G.711_mu-Law and G.711_a-Law codec
 - a G.711_mu-Law codec is considered BB compared to a G.711_a-Law codec

Table 61 "Best Bandwidth codec Selection between any two codecs types" (page 217) shows the codec that would be selected between any two codecs. For example, if the two codecs are the G.729A and G.723.1, the selected codec is the G.729A.

Table 61
Best Bandwidth codec Selection between any two codecs types

Codec type	G.711_a-Law	G.711_mu-Law	G.729A	G.729AB	G.723.1
G.711_a-Law	G.711_a-Law	G.711_muLaw	G.729A	G.729AB	G.723.1
G.711_mu-Law	G.711_mu-Law	G.711_mu-Law	G.729A	G.729AB	G.723.1
G.729A	G.729A	G.729A	G.729A	G.729AB	G.729A
G.729AB	G.729AB	G.729AB	G.729A B	G.729AB	G.729AB
G.723.1	G.723.1	G.723.1	G.729A	G.729AB	G.723.1

Installation and configuration summary

Contents

This section contains the following topics:

- ["Introduction" \(page 219\)](#)
- ["Before you begin" \(page 219\)](#)
- ["Installation summary" \(page 219\)](#)
- ["Voice Gateway Media Card installation summary sheet" \(page 222\)](#)

Introduction

This chapter provides a summary of the procedures required to install a new IP Telephony node, add cards to the node, install the cards, transmit data to the cards, and install the IP Phones. It also includes information about what is required before beginning the installation procedures.

Read ["Codecs" \(page 205\)](#) before installing an IP Telephony node.

Before you begin

Ensure that the CS 1000 system is running CS 1000 Release 5.0 software.

Installation summary

Use the following summary of steps as a reference guide to install and configure an IP Telephony node and Voice Gateway Media Cards on a system. This summary is intended to serve as a pointer to the more detailed procedures contained in other chapters and to provide a sequential flow to the steps involved in the overall installation procedure.

Complete all installation and configuration steps before transmitting data to the Voice Gateway Media Cards.

Procedure 11**Preinstallation and configuration steps**

Step	Action
1	Complete the Voice Gateway Media Card installation summary sheet. See Table 62 "Voice Gateway Media Card installation summary sheet" (page 223) .
2	Complete the IP Phone configuration data summary sheet. See Table 63 "IP Phone configuration data summary sheet" (page 223) .
3	Install the hardware components: - Install the Voice Gateway Media Card. See Procedure 12 "Installing the ITG-P 24-port line card" (page 229) for installing the ITG-P 24-port line cards and Procedure 14 "Installing the Media Card" (page 232) for installing the Media Card 32-port cards. - Cable the Voice Gateway Media Cards: - Install the ELAN subnet, TLAN subnet, serial interface cable for the ITG-P 24-port line card. See Procedure 16 "Installing the NTMF94EA ELAN, TLAN, serial interface cable" (page 238). - Install the Shielded 50-pin to Serial/ELAN/TLAN Adapter for the Media Card 32-port cards. See Procedure 17 "Installing the Shielded 50-pin to Serial/ELAN/TLAN Adapter onto the Media Card" (page 240).
4	Configure IP Line data on the system: - Configure the IP address for the ELAN network interface. See Procedure 18 "Configuring the ELAN network interface IP address for the active ELNK" (page 242). - Configure VoIP bandwidth management zones. See "Configure VoIP bandwidth management zones (LD 117)" (page 243). - Configure IP Line physical TNs. See "Configure physical TNs (LD 14)" (page 246). - Configure virtual superloops. See "Configure virtual superloops for IP Phones" (page 248). - For information about mapping virtual superloops on a Small System, see "Small Systems" (page 249). - Configure IP Phone features. See "Configure IP Phone features in LD 11" (page 250).
5	Configure IP Line data using Element Manager:

- a. Manually add an IP Telephony node. See ["Manually add an IP Telephony node"](#) (page 265).
 - b. Configure SNMP traps and community strings access for security. See ["Configuring SNMP trap destinations and community strings"](#) (page 268).
 - c. Configure DiffServ CodePoint (DSCP) data, 802.1Q support, and NAT support. See ["Configure Quality of Service"](#) (page 274).
 - d. Configure Call Server ELAN network interface (Active ELNK) IP address, TLAN Voice port (RTP UDP port), and the routing tables on the Voice Gateway Media Card. See ["Configure ELAN IP address, TLAN voice port, and routes"](#) (page 276).
 - e. Configure file server access. See ["Configure file server access"](#) (page 280).
 - f. Configure the loss plan. See ["Configure loss and level plan"](#) (page 281).
 - g. Configure Voice Gateway Media Card properties. See ["Add card and configure the card properties of the Voice Gateway Media Card"](#) (page 283).
- 6 Submit and transfer the node information to the Call Server. See ["Submit and transfer the node information"](#) (page 285).
- 7 Transmit Voice Gateway Media Card configuration data to the Voice Gateway Media Cards:
- a. Set Leader IP Address. See [Procedure 33 "Configuring the Leader IP address for a second or subsequent node"](#) (page 288).
 - b. Transmit node and card properties to the Leader. See [Procedure 34 "Transmitting node properties to Leader"](#) (page 290).
- 8 Upgrade the card software and IP Phone firmware:
- a. Verify card software version. See ["Determine Voice Gateway Media Card software version"](#) (page 294).
 - b. Verify card firmware release. See ["Determine the IP Phone firmware version"](#) (page 295).
 - c. Download software and firmware files from the Nortel Web site. See ["Download the current loadware and IP Phone firmware"](#) (page 297).
 - d. Upload the software and firmware files to the file server. See ["Upload the loadware and firmware files to the file server"](#) (page 298).

- e. Upgrade the software on the Voice Gateway Media Card. See ["Upgrade the Voice Gateway Media Card loadware" \(page 299\)](#).
 - f. Reboot the card. See ["Reboot the Voice Gateway Media Card" \(page 300\)](#).
 - g. Upgrade the firmware on the card. See ["Upgrade the IP Phone firmware" \(page 302\)](#).
- 9** Configure TM alarm notification feature to receive IP Line SNMP traps.
- 10** Assemble and install an IP Phone. See *IP Phones Fundamentals (NN43001-368)*.
- 11** Configure the IP Phone Installer Passwords (see ["IP Phone Installer Password" \(page 320\)](#)).
- a. Enable and set the administrative IP Phone Installer Password. See [Procedure 45 "Configuring the Administrative IP Phone Installer Password" \(page 328\)](#).
 - b. If needed, enable and set a temporary IP Phone Installer Password. See [Procedure 46 "Configuring the temporary IP Phone Installer Password" \(page 330\)](#).

—End—

Voice Gateway Media Card installation summary sheet

Nortel recommends that a Voice Gateway Media Card installation summary sheet (see [Table 62 "Voice Gateway Media Card installation summary sheet" \(page 223\)](#)) be filled out as the line cards are unpacked, inventoried, and provisioned. IP address information is usually supplied by the IP Network Administrator.

To complete the installation summary sheet, the following information is required:

- MAC address. This is the ELAN network interface MAC address on the Voice Gateway Media Card faceplate sticker (for example, 00:60:38:01:12:77).
- ELAN network interface IP address, used to perform management through TM and to communicate with the system
- TLAN Node IP address for the IP Telephony node
- TLAN network interface IP address on each card
- IP address of the active ELNK Ethernet network interface on the system core

Nortel recommends that an IP Phone configuration data summary sheet (see [Table 63 "IP Phone configuration data summary sheet" \(page 223\)](#)) be filled out as the IP Phones are installed and configured.

Table 62
Voice Gateway Media Card installation summary sheet

Site _____ CS 1000 system _____ CS 1000 customer _____ Node ID (Number) _____ TLAN Node IP address _____ CS 1000 active ELNK IP address _____ TLAN gateway (router) IP address _____ TLAN subnet mask _____ ELAN gateway (router) IP address _____ ELAN subnet mask _____				
TN	ELAN Management MAC address	ELAN Management IP address	TLAN (Voice) Card IP address	Card role
				Leader
				Follower (TM: Leader1)
				Follower
				Follower
				Follower
				Follower
				Follower
				Follower
				Follower
				Follower
				Follower
				Follower

Table 63
IP Phone configuration data summary sheet

No DHCP								
IP			Partial DHCP					
						Full DHCP		
			Connect Server IP	Node #	V TN	DN	User	User
Sub-net	Gateway IP							

address	mask	address	address*				Name	Location
*Connect Server IP address is the Node IP address of the IP Telephony node.								

Installation and initial configuration of an IP Telephony node

Contents

This section contains the following topics:

- ["Introduction" \(page 225\)](#)
- ["Equipment considerations" \(page 226\)](#)
- ["Install the hardware components" \(page 226\)](#)
- ["Initial configuration of IP Line data" \(page 241\)](#)
- ["Node election rules" \(page 257\)](#)

Introduction

This chapter explains how to install and perform the initial configuration of new IP Telephony nodes, Voice Gateway Media Cards (ITG-P 24-port, Media Card line cards), and associated cables.

Before installing an IP Telephony node, see *Converging the Data Network with VoIP Fundamentals (NN43001-260)* for information about IP network engineering guidelines.

ATTENTION

The maximum number of Voice Gateway Media Cards that can be installed in each node is 30. When more than 30 Voice Gateway Media Cards are needed on a single CS 1000 system, then multiple nodes must be used. The maximum number of Signaling Servers and Voice Gateway Media Cards that can be combined within a node is 35.

Installation and configuration procedures

The following is a list of procedures in this chapter:

- [Procedure 12 "Installing the ITG-P 24-port line card" \(page 229\)](#)
- [Procedure 13 "Installing the CompactFlash card on the Media Card" \(page 231\)](#)

- Procedure 14 "Installing the Media Card" (page 232)
- Procedure 15 "Replacing the existing I/O Panel Filter Connector" (page 234)
- Procedure 16 "Installing the NTMF94EA ELAN, TLAN, serial interface cable" (page 238)
- Procedure 17 "Installing the Shielded 50-pin to Serial/ELAN/TLAN Adapter onto the Media Card" (page 240)
- Procedure 18 "Configuring the ELAN network interface IP address for the active ELNK" (page 242)

Equipment considerations

This section lists the required and optional equipment that can be used to install, configure, and maintain the Voice Gateway Media Cards and IP Phone products.

Required equipment

The required equipment includes the following:

- a PC to manage IP Line, with the Internet Explorer 6.0.2600 (or later) to run Element Manager for CS 1000 systems
- local TTY or terminal in a switch room (this is required for Leader configuration)
- two shielded CAT 5 Ethernet cables to connect the Voice Gateway Media Card to an external switch (recommended) or hub equipment
- 10/100BaseT network interface (optional autosensing) to support TLAN and 10BaseT ELAN network interface connections
- 10/100BaseT network interface (optional autosensing) in each location where an IP Phone resides
- serial cables

Optional equipment

The optional equipment includes the following:

- a server configured with Dynamic Host Configuration Protocol (DHCP); for example, a Nortel NetID server
- an external modem router to enable remote dial-up connection to the ELAN subnet for technical support (Nortel RM356 modem router is recommended)

Install the hardware components

The Media Card 32-port cards and the ITG-P 24-port line card use IP Line software.

For Media Card 32-port card installation instructions, see [Procedure 14 "Installing the Media Card" \(page 232\)](#). For ITG-P 24-port line card installation instructions, see ["Installing and cabling the ITG-P 24-port line card" \(page 228\)](#).

ATTENTION

The ITG-P 24-port card is not supported in the Media Gateway 1000E of the CS 1000E system.

Voice Gateway Media Card

The Media Card 32-port card, MC 32S card, and ITG-P 24-port card running IP Line software are known as Voice Gateway Media Cards.

Summary of installation steps

The following table summarizes the steps for installing each Voice Gateway Media Card.

Table 64
Installation summary

Step	ITG-P 24-port line card	Media Card line cards
Determine card slot.	See "Identify the IPE card slots on a CS 1000M or Meridian 1" (page 228)	See "Identify the IPE card slots on a CS 1000M or Meridian 1" (page 228)
Unpack the card.	Remove all contents from the packaging box.	Remove all contents from the packaging box.
Install the CompactFlash Card.	Not applicable.	Procedure 13 "Installing the CompactFlash card on the Media Card" (page 231)
Install the Voice Gateway Media Cards.	Procedure 12 "Installing the ITG-P 24-port line card" (page 229)	Procedure 14 "Installing the Media Card" (page 232)
Install NTCW84JA ITG-specific I/O Panel Filter Connector for Option 51C/61C/81/81C.	Procedure 15 "Replacing the existing I/O Panel Filter Connector" (page 234)	Procedure 15 "Replacing the existing I/O Panel Filter Connector" (page 234)
Install the NTMF94EA ELAN, TLAN, RS-232 Serial Maintenance I/O interface cable.	Procedure 16 "Installing the NTMF94EA ELAN, TLAN, serial interface cable" (page 238)	Not applicable.
Install the A0852632 Shielded 50-pin to Serial/ELAN/TLAN Adapter.	Not applicable.	Procedure 17 "Installing the Shielded 50-pin to Serial/ELAN/TLAN Adapter onto the Media Card" (page 240)

Step	ITG-P 24-port line card	Media Card line cards
Configure card as a Leader or Follower.	In Element Manager: Procedure 33 "Configuring the Leader IP address for a second or subsequent node" (page 288) (Leader) Procedure 35 "Configuring the Follower cards" (page 292) (Follower) .	In Element Manager: Procedure 33 "Configuring the Leader IP address for a second or subsequent node" (page 288) (Leader) Procedure 35 "Configuring the Follower cards" (page 292) (Follower) .
Add the card and configure the card properties	In Element Manager: Procedure 31 "Adding card and configuring Voice Gateway Media Card properties" (page 283)	In Element Manager: Procedure 31 "Adding card and configuring Voice Gateway Media Card properties" (page 283)
Transmit/Transfer properties	In Element Manager: Procedure 34 "Transmitting node properties to Leader" (page 290)	In Element Manager: Procedure 34 "Transmitting node properties to Leader" (page 290)

Identify the IPE card slots on a CS 1000M

Depending on the module that is used, the ITG-P 24-port line card must be installed in a specific slot. Use [Table 65 "Voice Gateway Media Card installation by module type" \(page 228\)](#) to identify the IPE card slots selected for the Voice Gateway Media Card.

Table 65
Voice Gateway Media Card installation by module type

CS 1000M modules	ITG-P 24-port line card slots
NT8D37BA/EC IPE module	All available IPE card slots
NT8D37AA/DC IPE module	0, 4, 8, and 12

EMC restriction must be considered when installing the Voice Gateway Media Cards.

Installing and cabling the ITG-P 24-port line card

Each ITG-P 24-port line card requires two slots in the CS 1000. Only the left slot of the card connects to the IPE backplane and I/O panel.

A maximum of eight ITG-P 24-port line cards can be installed in an IPE shelf in a Large System. The ITG-P 24-port line card can occupy any two adjacent slots in an IPE shelf, with the left slot of the card plugging into slots 0 to 6 and 8 to 15. The left slot of an ITG-P 24-port line card cannot be plugged into slot 7, because the XPEC card is situated between slots 7 and 8.

To enable a module to hold the maximum number of ITG-P 24-port line cards, install each card with the left slot of the card inserted into an even-numbered slot.



CAUTION

CAUTION WITH ESD DEVICES

Wear an ElectroStatic Discharge Strap (ESDS) when handling ITG-P 24-port and Media Card line cards. As an additional safety measure, handle all cards by the edges, and when possible, with the loosened packaging material still around the component.



WARNING

The CAT5 Ethernet cable between the ITG-P 24-port line card TLAN network interface and the Layer 2 switch must have a length of 50 meters or less for proper operation of the TLAN network interface

To install an ITG-P 24-port line card, follow the steps in [Procedure 12 "Installing the ITG-P 24-port line card" \(page 229\)](#).

Procedure 12

Installing the ITG-P 24-port line card

Step	Action
1	For each ITG-P 24-port line card in the node, identify the IPE card slot selected for the ITG-P 24-port line card. Use the information from the "Voice Gateway Media Card installation summary sheet" (page 222) , and Table 65 "Voice Gateway Media Card installation by module type" (page 228) . Even though the ITG-P 24-port line card is a two-slot card, only the left slot is counted for the card slot number. For example, for an ITG-P 24-port line card installed in slots 2 and 3, the slot number is 2.
2	Remove any existing I/O panel cabling associated with any card previously installed in the selected card slot.
3	Insert the ITG-P 24-port line card into the card guides and gently push it until it makes contact with the backplane connector. Hook the locking devices. The red LED on the card faceplate remains lit until the card is configured and enabled in the software, at which point the LED turns off.

The faceplate display window displays start-up self-test results (T:xx) and status messages. A display "F:XX" indicates a failure of the self-test. It is normal for the ITG-P 24-port line card to display "F:10" during the start-up self-test. F:10 indicates that the self-test did not find a Security Device. The ITG-P 24-port line card does not have a security device.

Some failures indicate that the card must be replaced. See [Table 82 "ITG-P 24-port line card faceplate maintenance display codes" \(page 402\)](#) for a list of the ITG-P 24-port line card display codes.

—End—

Installing and cabling the Media Card 32-port card

The Media Card 32-port line card is the successor of the ITG-P 24-port line card. It increases the packet processing power of the ITG-P 24-port line card, increases the channel density from 24 to 32 ports, and reduces the slot usage from a dual slot to a single IPE slot. The Media Card 32-port card requires only one slot in the IPE shelf.



CAUTION CAUTION WITH ESDS DEVICES

Wear an ElectroStatic Discharge strap when handling Media Card line cards. As an additional safety measure, handle all cards by the edges, and when possible, with the loosened packaging material still around the component

CompactFlash installation

The Media Card package contains the following items:

- Media Card
- CompactFlash card
- retaining pin

The CompactFlash card must be installed on the Media Card before installing the Media Card in the system. Follow the steps in [Procedure 13 "Installing the CompactFlash card on the Media Card" \(page 231\)](#) to install the CompactFlash card.

If it is necessary to remove the CompactFlash card, follow the steps outlined in [Procedure 71 "Removing the CompactFlash" \(page 456\)](#).

Procedure 13**Installing the CompactFlash card on the Media Card****Step Action**

- 1 Remove the Media Card and CompactFlash card from the packaging.

**CAUTION****CAUTION WITH ESDS DEVICES**

Observe the necessary precautions for handling ESD-sensitive devices. Wear a properly connected antistatic wrist strap while removing the cards from the packaging and work on a static-dissipating surface.

- 2 Locate the CompactFlash card socket in the lower left-hand corner of the Media Card. See [Figure 46 "CompactFlash card socket on Media Card" \(page 231\)](#).

Figure 46**CompactFlash card socket on Media Card**

- 3 Position the CompactFlash card with the label facing up, the metal clip pulled up, and contact pins toward the socket as shown in [Figure 47 "Position the CompactFlash in socket" \(page 232\)](#).

Figure 47
Position the CompactFlash in socket



- 4 Insert the CompactFlash card in the socket.
Ensure force is applied equally at both ends of the CompactFlash when pushing it in.
- 5 Gently insert the CompactFlash card, so that it is fully in contact with the connectors on the drive.
- 6 Push the metal clip down so that the CompactFlash card is locked in.

—End—

Install the Media Card

To install a Media Card, follow the steps in [Procedure 14 "Installing the Media Card"](#) (page 232).

Procedure 14 Installing the Media Card

Step	Action
1	For each Media Card in the node, identify the IPE card slot selected for the Media Card.

Use the information from the ["Voice Gateway Media Card installation summary sheet"](#) (page 222), and Table 66 "Media Card installation by module type" (page 233).

Table 66
Media Card installation by module type

CS 1000 Modules	Media Card
NT8D37BA/EC IPE modules	All available IPE card slots
NT8D37AA/DC IPE modules	0, 4, 8, and 12

- 2 Remove any existing I/O panel cabling associated with any card previously installed in the selected card slot.
- 3 Insert the Media Card into the card guides and gently push it until it makes contact with the backplane connector. Hook the locking devices.

The red LED on the faceplate remains lit until the card is configured and enabled in the software, at which point the LED turns off.

The card faceplate display window displays start-up self-test results (T:xx) and status messages. A display "F:xx" indicates a failure of the self-test. Some failures indicate that the card must be replaced.

See ["Transfer node configuration from Element Manager to the Voice Gateway Media Cards"](#) (page 286). See Table 83 "Media Card faceplate maintenance display codes" (page 403) for a listing of the Media Card display codes.

—End—

Installing the NTCW84JA ITG-specific I/O Panel filter connector for a Large System

For Large Systems, the standard IPE module I/O filtering is provided by the 50-Pin filter connectors mounted in the I/O Panel on the back of the IPE shelf. The filter connector attaches externally to the MDF cables and internally to the NT8D81AA Backplane to the I/O Panel ribbon cable assembly.

For 100BaseTX TLAN operation, the standard I/O filter connector must be replaced with the NTCW84JA ITG Line-specific I/O filter connector for the following:

- the leftmost of the two card slots occupied by the ITG-P 24-port line card
- the slot occupied by the Media Card

For Small Systems, the standard I/O filter connector already supports 100BaseTX TLAN operation.

To replace an existing I/O Panel Filter Connector, follow the steps in [Procedure 15 "Replacing the existing I/O Panel Filter Connector" \(page 234\)](#).

The NTCW84JA ITG-specific Filter Connector is not required on Small Systems.



CAUTION

For Large systems manufactured between 1998-1999 and shipped in North America, the IPE modules have the NT8D81BA Backplane to I/O Panel ribbon cable assembly with a non-removable filter connector. The NT8D81BA is compatible with a 10BaseT operation of the TLAN network interface, but if a 100BaseT operation of the TLAN network interface is required, order the NT8D81AA Backplane to I/O Panel ribbon cable assembly to replace it. Do not install the NTCW84JA ITG-specific filter connector onto the existing non-removable filter connector.

Replace existing I/O panel filter connector

The standard I/O filter connector is shielded metal with a black plastic insert connector. The NTCW84JA connector uses yellow warning labels to indicate EMC filtering modifications and which MDF connection points can support 100BaseT connections.

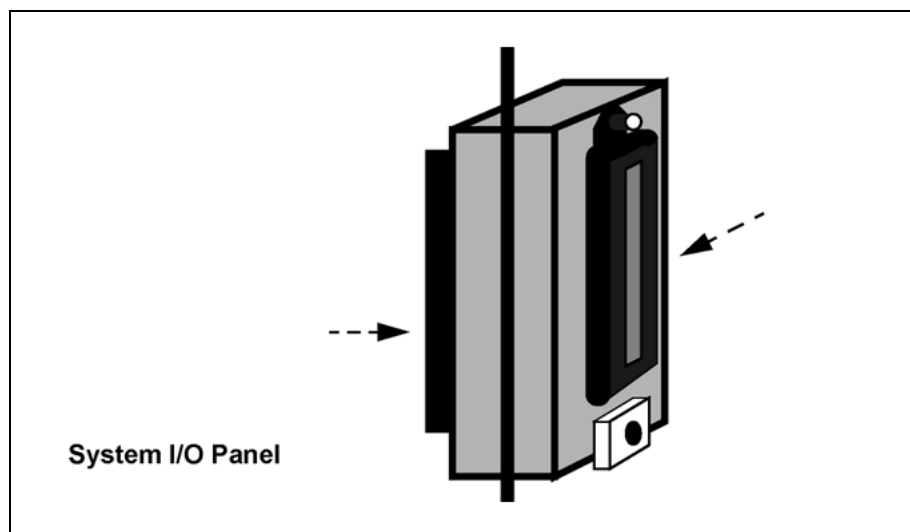
Procedure 15

Replacing the existing I/O Panel Filter Connector

Step	Action
1	Before any of the following steps, remove the ITG pack, or any other IPE pack, from the IPE shelf card slot corresponding to the I/O Panel connector to be removed.
ATTENTION Make sure to use the I/O Panel Filter Connector which corresponds to the left slot number of the ITG-P card.	
2	Remove the NT8D81AA Backplane to I/O Panel ribbon cable assembly, that is connected to the Backplane side of the existing block, by releasing the latching pins on the filter block and pulling the NT8D81AA cable away.
3	Unscrew the existing filter connector from the I/O panel. There is one screw on the lower front of the connector and one screw on the upper back of the connector. Remove the connector.

- 4 Reposition the new NTCW84JA filter connector in the now vacant I/O panel opening. See [Figure 48 "NTCW84JA 50 pin ITG-specific I/O Panel filter connector for Large Systems"](#) (page 235).

Figure 48
NTCW84JA 50 pin ITG-specific I/O Panel filter connector for Large Systems



- 5 Attach the new NTCW84JA ITG-specific filter connector to the I/O panel by securely fastening the top back screw and the bottom front screw.
- 6 Reconnect the NT8D81AA cable and secure it in place by snapping shut the locking latches provided on the NTCW84JA connector.

—End—

Incorrect configuration problems

TLAN network interface operation problems can arise from the standard I/O filter connector in IPE modules on Large Systems. Some problem scenarios and their respective solutions are outlined in [Table 67 "I/O filter connector"](#) (page 235).

Table 67
I/O filter connector

Scenario	Solution
The installer forgets to replace the standard IPE module I/O filter connector with the provided Voice Gateway Media Card/ITG-specific filter connector that removes filtering from pairs 23 and 24.	Correctly install the Voice Gateway Media Card/ITG-specific filter connector by replacing the standard IPE Module I/O filter connector.

Scenario	Solution
The installer installs the Voice Gateway Media Card/ITG-specific filter connector on top of the standard IPE module I/O filter connector.	Correctly install the Voice Gateway Media Card/ITG-specific filter connector by replacing the standard IPE Module I/O filter connector.
The installer encounters an IPE module that is equipped with standard filter connectors molded onto the backplane I/O ribbon cable assemblies. The installer does not replace the IPE module backplane I/O ribbon cable assemblies with the ones that have interchangeable I/O filter connectors.	Order new IPE Module Backplane I/O ribbon cable assemblies that have interchangeable I/O filter connectors if it becomes necessary to use one of the IPE Modules with molded-on I/O filter connectors.
The UTP cabling from the TLAN network interface to the Layer 2 switch does not meet the UTP CAT5 termination and impedance uniformity standards.	Always ensure that UTP cabling from the TLAN network interface to the Layer 2 switch is CAT5-compliant.

Voice Gateway Media Card ELAN and TLAN network interfaces CS 1000M system

The ELAN and TLAN network interfaces are provided by one of the following:

- NTMF94EA ELAN, TLAN, RS-232 Serial Maintenance I/O interface cable (see [Figure 49 "NTMF94EA ELAN, TLAN, and RS-232 Serial Maintenance I/O cable" \(page 237\)](#))
- A0852632 Shielded 50-pin to Serial/ELAN/TLAN Adapter (see [Figure 50 "Shielded 50-pin to Serial/ELAN/TLAN Adapter" \(page 239\)](#))

The ITG-P 24-port line card uses the NTMF94EA ELAN, TLAN, RS-232 Serial Maintenance I/O interface cable.

The Media Card uses the A0852632 Shielded 50-pin to Serial/ELAN/TLAN Adapter.

The ELAN network interface supports 10BaseT operation and the TLAN network interface supports 10/100BaseT operation. To support the 100BaseT operation on Large Systems, the TLAN network interface requires specialized I/O panel mounting connectors. These replace the standard connectors provided on the system.

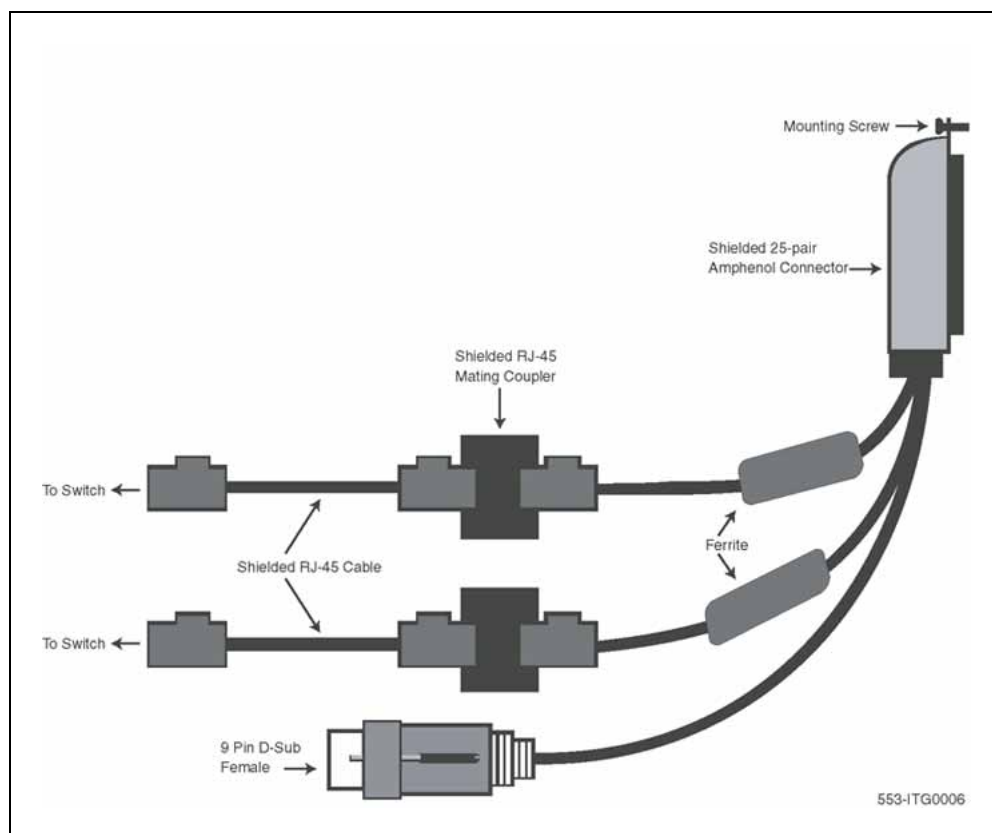
Cables and connectors for the ELAN and TLAN network interface functions include the following:

- the NTCW84JA I/O panel filter block
- NTMF94EA ELAN, TLAN, RS-232 Serial Maintenance I/O interface cable
- A0852632 Shielded 50-pin to Serial/ELAN/TLAN Adapter. Standard shielded, CAT5 LAN cables (<100 meters) are recommended to attach the LAN ports to the local network.

Install the NTMF94EA ELAN, TLAN, RS-232 Serial Maintenance I/O interface cable

The NTMF94EA cable provides the ELAN, TLAN and serial interface for the ITG-P 24-port line card. See [Appendix "I/O, maintenance, and extender cable description" \(page 493\)](#) for pinouts and technical specifications on the NTMF94EA cable.

Figure 49
NTMF94EA ELAN, TLAN, and RS-232 Serial Maintenance I/O cable



To install the NTMF94EA ELAN, TLAN, serial interface cable, complete the steps in [Procedure 16 "Installing the NTMF94EA ELAN, TLAN, serial interface cable" \(page 238\)](#).



WARNING

Plug all Voice Gateway Media Card ELAN network interfaces belonging to the same node into the same ELAN hub or Layer 2 switch port group.

Procedure 16**Installing the NTMF94EA ELAN, TLAN, serial interface cable**

Step	Action
1	On Large Systems, connect the NTMF94EA ELAN, TLAN, and RS-232 Serial Maintenance I/O cable to the I/O panel connector for the left hand card slot. For Small Systems, connect the cable to the I/O connector in the cabinet that corresponds to the IP Line card slot (see Figure 106 "NTMF94EA ELAN, TLAN and RS-232 serial maintenance I/O cable" (page 494)).
2	Connect a shielded CAT5 Ethernet cable from the customer TLAN Layer 2 or Layer 3 switch port to the RJ-45 port labeled "TLAN".
3	Connect a shielded CAT5 Ethernet cable from the customer ELAN Layer 2 or Layer 3 switch port to the RJ-45 port labeled "ELAN".
4	Install the NTAG81CA serial cable into the faceplate Maintenance port. This connection is used to configure the IP address for Leader 0. If required, use the NTAG81BA maintenance extender cable. Alternatively, for a permanent connection to the maintenance port, use the DB9 female connector on the NTMF94BA breakout cable to connect a modem (using a null modem) or directly to a local TTY terminal.

**WARNING**

The serial maintenance ports presented at the faceplate and at the backplane are identical. Do not connect a terminal to both access points simultaneously. This results in incorrect and unpredictable operation of the Voice Gateway Media Card.

The switch LEDs and the faceplate link LEDs light when the card is connected to the WAN/LAN through the TLAN network interface.

See *Converging the Data Network with VoIP Fundamentals* (NN43001-260) for more information about engineering and connecting the LAN/WAN.

—End—

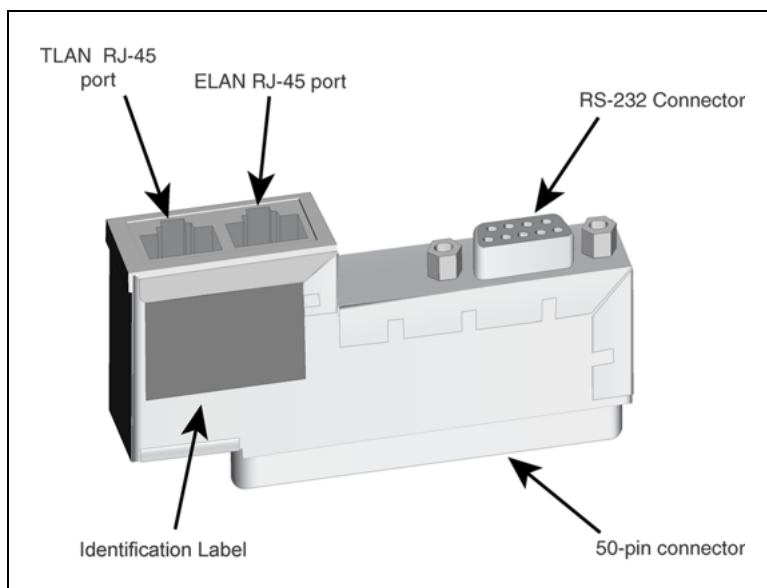
Install the Shielded 50-pin to Serial/ELAN/TLAN Adapter

The Media Card can support a single connector solution for access to the TLAN and ELAN network interfaces. This connector (see [Figure 50 "Shielded 50-pin to Serial/ELAN/TLAN Adapter" \(page 239\)](#)) is called the A0852632 Shielded 50-pin to Serial/ELAN/TLAN Adapter. It replaces the single NTMF94EA ELAN, TLAN, RS-232 Serial Maintenance I/O interface cable ('octopus' cable).

The adapter breaks out the signals from the I/O connector to the following:

- ELAN network interface
- TLAN network interface
- one RS-232 (local console) port

Figure 50
Shielded 50-pin to Serial/ELAN/TLAN Adapter



On Large Systems, the NT8D81AA cable is used to bring all 24 Tip and Ring pairs to the I/O panel. The NTCW84JA I/O panel mounting block must be installed on Large Systems before the A0852632 Shielded 50-pin to Serial/ELAN/TLAN Adapter is installed. See [Figure 50 "Shielded 50-pin to Serial/ELAN/TLAN Adapter" \(page 239\)](#).

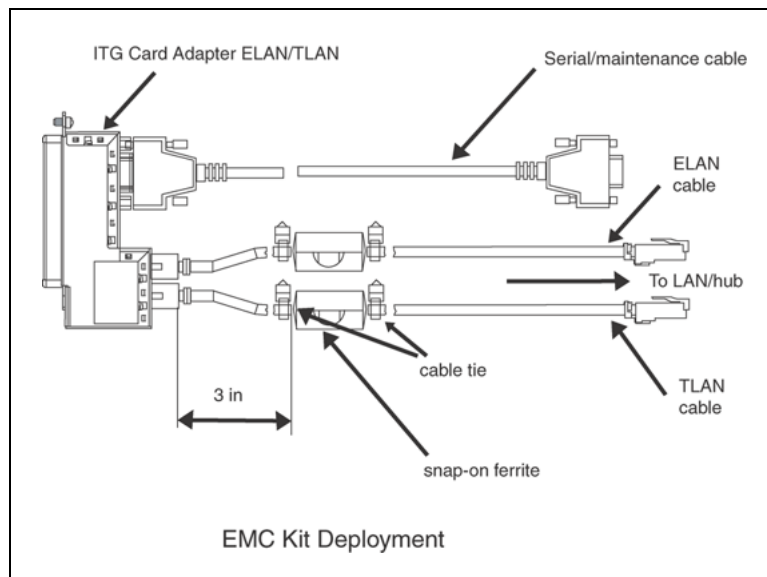
To ensure proper connection, install the adapter securely; otherwise, connectivity could be lost.

EMC Shielding Kit

An ITG EMC shielding kit (NTVQ83AA) must be installed on the ELAN and TLAN network interface cables to meet regulatory requirements at the installation site. As shown in [Figure 51 "ITG EMC Shielding Kit Deployment"](#)

(page 240), a ferrite must be placed on both the ELAN and TLAN network interface CAT5 Ethernet cables during installation. Cable ties are then placed to retain the ferrites in the correct position. This applies to Small Systems and Large Systems.

Figure 51
ITG EMC Shielding Kit Deployment



Follow the steps in [Procedure 17 "Installing the Shielded 50-pin to Serial/ELAN/TLAN Adapter onto the Media Card"](#) (page 240) to install the ITG EMC shielding kit (NTVQ83AA) on the ELAN and TLAN network interface cables.

Procedure 17

Installing the Shielded 50-pin to Serial/ELAN/TLAN Adapter onto the Media Card

Step	Action
1	Install the Shielded 50-pin to Serial/ELAN/TLAN Adapter into the card connector (1, 2, 3, or 4) where the Media Card is located.
2	Connect a shielded Cat 5 cable from the customer TLAN switch equipment to the port labeled "TLAN".
3	Connect a shielded Category 5 cable from the customer ELAN hub or switch equipment to the port labeled "ELAN".
4	Install the NTAG81CA serial cable into the faceplate Maintenance port.

—End—

Initial configuration of MC 32S card

The MC 32S card is shipped from the factory with a blank compact flash card. When the card first powers-up, it boots from a Gold Control and Signaling Processor (CSP) image. The Gold CSP image is a scaled-down version due to size restrictions on the on-board compact flash card. You must format the compact flash card and install the full CSP software before the MC 32S card functions to its full capability.

The software for the MC 32S card consists of five files, which are located in a zip file and stored on the Signaling Server. All Gold versions of firmware are loaded on the MC 32S when the card is shipped from the factory.

Configuring the Leader and Follower on the MC 32S

When the MC 32S card is configured as a Leader, the card obtains its IP address from NVRAM and not from the bootp server. The Leader card becomes a bootp server for any Follower cards present on the node. The Leader card also has an impact during an election of the node Master. During an election, a card programmed as the Leader card wins an election over a card programmed as a Follower card.

The Master of the node is determined by a TPS election. Whenever a new card comes on line or goes offline in a node, an election is held. The Master of the node also becomes the bootp server. The bootp server responds to bootp requests from the Follower cards and provides the cards with their IP configuration.

For information about configuring the MC 32S card using Element Manager, see ["Configuration of IP Telephony nodes using Element Manager" \(page 259\)](#)

Initial configuration of IP Line data

Before beginning the configuration:

- Ensure the system is running CS 1000 Release 5.0 software.
- Verify the License system limit in LD 22. The License system limit must have sufficient unused units to support the number of IP Phones to be installed. For more information, see *Software Input Output Reference—Maintenance (NN43001-711)*.
- Expand the License limit, if necessary, by ordering additional Licenses. See ["Licenses" \(page 42\)](#) for more information.

Summary of procedures

1. "Configure IP address for the system active ELNK Ethernet network interface (LD 117)" (page 242).
2. "Configure VoIP bandwidth management zones (LD 117)" (page 243).
3. "Configure physical TNs (LD 14)" (page 246).
4. "Configure virtual superloops for IP Phones" (page 248).
5. "Configure IP Phone features in LD 11" (page 250).

Configure IP address for the system active ELNK Ethernet network interface (LD 117)

To configure the Call Server ELAN network interface IP address (active ELNK), follow the steps in [Procedure 18 "Configuring the ELAN network interface IP address for the active ELNK"](#) (page 242).

Procedure 18

Configuring the ELAN network interface IP address for the active ELNK

Step	Action
1	Go to LD 117.
2	Create host entries with the IP address on the ELAN subnet by entering one of the following commands: NEW HOST PRIMARY_IP xx.xx.xx.xx NEW HOST SECONDARY_IP xx.xx.xx.xx (for Large Systems only)
3	Assign the host entry IP address to active and inactive ELNK interfaces on the ELAN subnet by entering one of the following commands: CHG ELNK ACTIVE PRIMARY_IP CHG ELNK INACTIVE SECONDARY_IP (for Dual CPU only)
4	Verify the IP address for the Ethernet network interface by entering the following command: PRT ELNK .
5	Enter the following command: Update DBS .
6	Go to LD 137. Check the status of the Ethernet network interface by entering the command: STAT ELNK . If the ELNK network interface is disabled, enable it by entering: ENL ELNK .

—End—

Configure VoIP bandwidth management zones (LD 117)

Up to 256 zones can be defined in LD 117. The Call Server uses the zones for VoIP bandwidth management. For more information, see *Converging the Data Network with VoIP Fundamentals (NN43001-260)*.

The term Intrazone means within the same zone. Interzone means between two different zones.

Table 68 "LD 117 bandwidth management zone configuration" (page 243) lists the zone parameters as follows:

- p1 – total bandwidth (kb/s) available for Intrazone calls
- p2 – defines the codec for Intrazone calls (that is, preserve voice quality or preserve bandwidth). BQ provides the best voice quality but uses the most bandwidth. BB uses the least amount of bandwidth but reduces voice quality.
- p3 – total bandwidth available for Interzone calls
- p4 – preferred strategy for the choice of the codec for Interzone calls
- p5 – zone resource type. The type is either shared or private.

For information about Private Zone configuration, see "Private Zone configuration" (page 170).

LD 117 also includes the DIS and ENL commands to disable or enable a zone. When a zone is created, its default state is enabled.



CAUTION

Zone 0 must be configured in LD 117 first before other zones are configured or all calls associated with zone 0 are blocked.

Table 68
LD 117 bandwidth management zone configuration

Command	Description
NEW ZONE xxx p1 p2 p3 p4 p5	Create a new zone, where: xxx = zone number = (0) – 255. p1 = Intrazone available bandwidth = 0 – (10 000) – 10 0000 (kb/s) p2 = Intrazone preferred strategy = (BQ – Best Quality) or BB – Best Bandwidth

Command	Description
	p3 = Interzone available bandwidth = 0 – (10 000) – 10 0000 (kb/s) p4 = Interzone preferred strategy = BQ for Best Quality or BB for Best Bandwidth p5 = Zone resource type = (shared) or private
New ZONE xxx	Create a new zone with default values for the parameters: p1 = 10 000 (kb/s) p2 = BQ p3 = 10 000 (kb/s) p4 = BQ p5 = shared
CHG ZONE xxx p1 p2 p3 p4 p5	Change parameters of a zone. All parameters must be reentered, even those that are unchanged.
OUT ZONE xxx	Remove a zone.
DIS ZONE xxx	Disable a zone. When a zone is disabled, no new calls are established inside, from, or toward this zone.
ENL ZONE xxx	Enable a zone.
PRT ZONE xxx	Print zone and bandwidth information, where xxx specifies a zone. If no zone is specified, information for all zones is printed. PRT ZONE ALL also prints information for all zones.
PRT ZONE ALL	

Element Manager for Zone Configuration

Optionally, zones can be configured for CS 1000 systems using Element Manager instead of LD 117.

To view Element Manager for zone configuration, follow the steps in [Procedure 20 "Using Element Manager to configure Voice Gateway channels" \(page 246\)](#):

Procedure 19

Viewing Element Manager for Zone Configuration

Step	Action
1	Launch and log into Element Manager. See Procedure 23 "Launching Element Manager" (page 263) .
2	In the navigator, click IP Network > Zones .

The **Zones** window appears. See [Figure 52 "Zone List"](#) (page 245).

Figure 52
Zone List

- 3 Under **Configuration**, click the **to Add** button to add a new zone.

The **Zone Basic Property and Bandwidth Management** window appears. See [Figure 53 "Zone Basic Property and Bandwidth Management window"](#) (page 245).

Figure 53
Zone Basic Property and Bandwidth Management window

—End—

Configure physical TNs (LD 14)

Use LD 14 to define the physical TNs for the Voice Gateway Media Card.

See [Table 69 "Configure physical TNs in LD 14" \(page 246\)](#) for a list of the prompts and responses in LD 14.

Table 69
Configure physical TNs in LD 14

Prompt	Response	Description
REQ	NEW CHG OUT	Create the Voice Gateway channels on a line card. Change configuration data for a Voice Gateway channel. Delete the Voice Gateway channels on a line card.
TYPE	VGW	Voice Gateway
TN	l s c u	TN of the first ITG Physical TN Where l = loop, s = shelf, c = card, u = unit.
DES	aa.....a	Description for gateway channel. Identify the channel using the card TLAN network interface IP address or MAC address.
XTRK	aaa	ITGP – ITG-P 24-port card MC32 – Media Card 32-port card MC 32S -ITG-PM 32-port card
ZONE	0 – 255	Zone number to which this ITG Physical TN belongs. Verify that the zone exists in LD 117.
CUST	xx	Customer number as defined in LD 15.

Using Element Manager for Voice Gateway channels

Alternatively, for CS 1000 systems, configure the Voice Gateway channels using Element Manager instead of using LD 14.

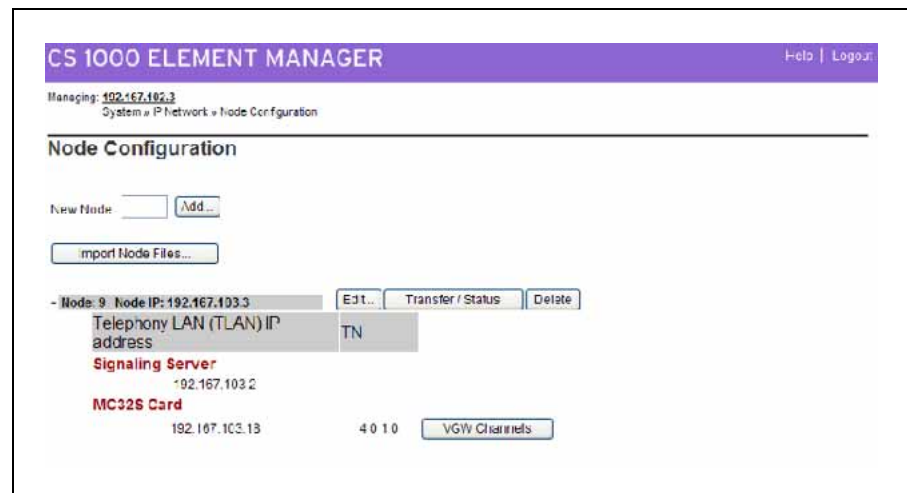
To use Element Manager to configure Voice Gateway channels, follow the steps in [Procedure 20 "Using Element Manager to configure Voice Gateway channels" \(page 246\)](#).

Procedure 20**Using Element Manager to configure Voice Gateway channels****Step Action**

- 1 Launch and log into Element Manager. See [Procedure 23 "Launching Element Manager" \(page 263\)](#) for details.

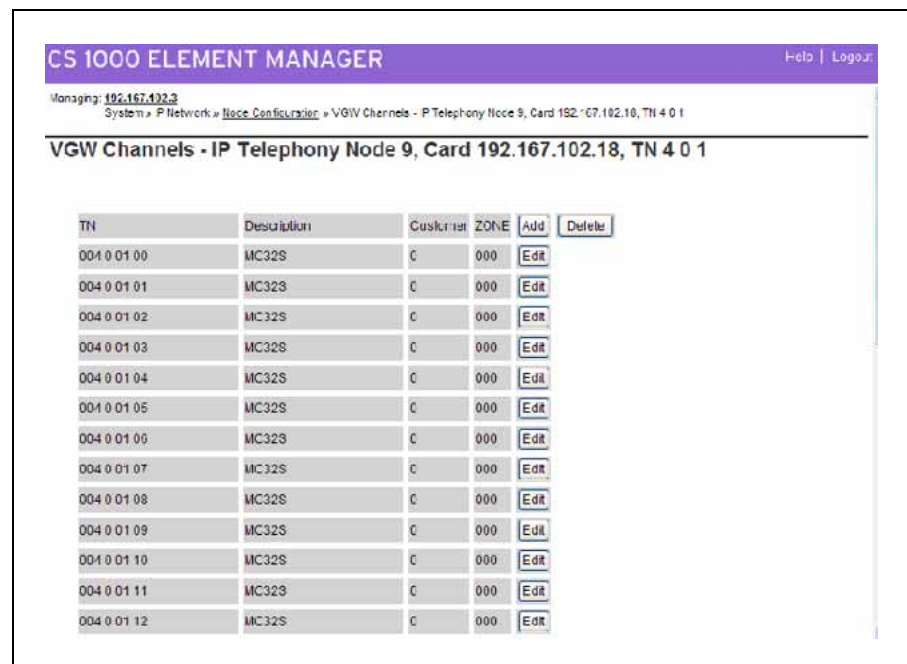
- 2 In the navigator, click **IP Network > Nodes: Servers, Media Cards**.
The **Node Configuration** window appears.

Figure 54
Node Configuration window



- 3 Expand a node by clicking the plus sign (+) to the left of the node.
- 4 Click the **VGW Channels** button next to the card to be configured.
The **VGW Channels** window appears.

Figure 55
VGW Channels window



- 5 To add new gateway channels, click the **Add** button at the top in the **VGW Channels** window.

The **Add VGW Channels** window appears. The Add VGW Channels window is the equivalent to LD 14 NEW command
- 6 To edit a specific Voice Gateway channel, click the **Edit** button to the right of the channel in the VGW Channels window.

The **Edit VGW channel** window appears.

The Edit VGW channel window is equivalent to LD 14 CHG command that enables the changing of the DES and ZONE parameters of the channel.
- 7 To delete a Voice Gateway channel, click the **Delete** button in the Gateway Channel summary window.

The **Delete VGW channels** for the Voice Gateway channel opens.
- 8 Select a gateway channel from the drop-down list box and click **Delete**. The Delete VGW channels window is the equivalent of LD 14 OUT command.

—End—

Configure virtual superloops for IP Phones

One or more virtual superloops must be configured to support IP Phone Virtual TNs (VTNs) in LD 97 or in Element Manager. To create the virtual superloop in Element Manager, click **System > Superloops** in the Element Manager navigator.

Large Systems and CS 1000E

In Large Systems and CS 1000E, virtual superloops contend for the same range of loops with phantom, standard and remote superloops, digital trunk loops, and all service loops. Virtual superloops can reside in physically-equipped network groups or in virtual network groups.

Group maximums

Without FIBN, Package 365, there is a maximum of five network groups available, 0 to 4. With Package 365, there are a maximum of eight network groups, 0 to 7.

For normal traffic engineering, provision up to 1024 VTNs on a single virtual superloop for a Large System/CS 1000E. For non-blocking, do not exceed 120 VTNs on a single virtual superloop for a Large System/CS 1000E.

Nortel recommends that virtual superloops are configured starting in the highest non-physically equipped group available. [Table 70 "LD 97 – Virtual superloop configuration for Large Systems/CS 1000E" \(page 249\)](#) lists the prompts and responses required to configure virtual superloops in LD 97.

Table 70
LD 97 Virtual superloop configuration for Large Systems/CS 1000E

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	SUPL	Superloop
SUPL	Vxxx	V represents a virtual superloop and xxx is the number of the virtual superloop where: - xxx = 0 to 156 and multiple of four for a Large System without FIBN package 365 - xxx = 0 to 252 and multiple of four for a Large System with FIBN package 365

Small Systems

In Small Systems, virtual superloops contend for the same range of superloops, 96 to 112, with phantom superloops.

A maximum of 1000 VTNs can be configured on a CS 1000M system, CS 1000M Cabinet, and CS 1000M Chassis system.

In a Small System, mapping virtual superloops to virtual cards is the same as mapping phantom superloops to phantom cards. See [Table 71 "Virtual superloop/virtual card mapping for Small Systems" \(page 249\)](#).

Table 71
Virtual superloop/virtual card mapping for Small Systems

SUPL	Card
96	61 to 64, 81 to 84
100	65 to 68, 85 to 88
104	69 to 72, 89 to 92
108	73 to 76, 93 to 96
112	77 to 80, 97 to 100

Configuring virtual superloops in Element Manager

To configure a virtual superloop in Element Manager, follow the steps in [Procedure 21 "Configuring a virtual Superloop in Element Manager" \(page 250\)](#).

Procedure 21**Configuring a virtual Superloop in Element Manager****Step Action**

- 1 In the Element manager navigator, click **System > Core Equipment > Superloops**.

The **Superloops** window appears. See [Figure 56 "Configuring a virtual superloop in Element Manager"](#) (page 250).

Figure 56**Configuring a virtual superloop in Element Manager**

- 2 Select the superloop number from the **Choose a Superloop Number** drop-down list.
- 3 Select **Virtual** from the **type** drop-down list.
- 4 Click **to Add**.

—End—

Configure IP Phone features in LD 11

The existing License header that is printed at the start of LD 11 includes the new License limit for the IP Phone. See [Table 63 "IP Phone configuration data summary sheet"](#) (page 223).

Table 72**LD 11 Configure an IP Phone**

Prompt	Response	Description
REQ :	NEW, CHG, CHGTYP, PRT, OUT, CPY, MOV	New, Change, Change TN type, Print, Out, Copy, Move
TYPE		For IP Phone 2001, IP Phone 2002, IP Phone 2004,

Prompt	Response	Description
:	2001P2, 2002P1, 2002P2, 2004P1, 2004P2, 2033, 2007, 2050PC, 2050MC, 1110, 1120, 1140, 1150, 2210, 2211, 2212, 6120, 6140	IP Audio Conference Phone 2033, IP Phone 2007, IP Softphone 2050, Mobile Voice Client 2050, IP Phone 1110, IP Phone 1120E, IP Phone 1140E, IP Phone 1150E, and WLAN Handsets 2210/2212/2212/6120/6140. The system accepts this response if it is equipped with packages 88 and 170. The IP Phones are also restricted by the IP Phone License setting.
TN	l s c u	Where l = loop, s = shelf, c = card, u = unit. Enter loop (virtual loop), shelf, card, and unit (terminal number), where unit = 0 to 31.
DES	a...z	ODAS telephone designator
CUST	xx	Customer number as defined in LD 15.
ZONE	0 to 255	Zone number to which this IP Phone belongs. Verify that the zone number exists in LD 117.
CLS	ADD	ADD - Automatic Digit Display, default for IP Phone. For a complete list of responses, see <i>Software Input Output Administration (NN43001-611)</i> .
KEY	xx aaa yy zz...zz	IP Phone function key assignments where: xx = keys 0 to 5 (and 6 to 11 using the Shift key) for IP Phone 2004, IP Phone 2007, IP Phone 1140E, IP Phone 1150E, WLAN Handsets 2210/2211/2212/6120 xx = keys 0 to 3 for the IP Phone 2002, and IP Phone 1120E These keys are self-labeled physical keys that can be programmed with any feature. For the WLAN Handset 2210/2211/2212/6120, the keys are self-labeled virtual keys that can be programmed with any feature. xx = 0 for the IP Phone 2001, IP Audio Conference Phone 2033, and IP Phone 1110; any other key number entered returns an error message. aaa = key name or function

Prompt	Response	Description
		yyy, zzz = additional information required for the key. Keys 16 to 26 are reserved for dedicated IP Phone context-sensitive soft keys. Table 74 "LD 11 IP Phone dedicated context-sensitive soft key assignment" (page 256) lists the dedicated IP Phone key name values (aaa). Other key name values can be found in <i>Software Input Output Administration (NN43001-611)</i>

Configure the IP Phone Key Expansion Module

Configure the optional IP Phone Key Expansion Module (KEM) in LD 11.

The IP Phone KEM is supported on the IP Phone 2002 and IP Phone 2004 *only*.

Table 73
LD 11 Configure the IP Phone KEM

Prompt	Response	Description
REQ	NEW	Add new data.
:	CHG	Change existing data.
TYPE	2002P1, 2002P2,	IP Phone 2002 (Phase I and Phase II)
:	2004P1, 2004P2	IP Phone 2004 (Phase I and Phase II)
...		
ZONE	0 to 255	Zone number to which the IP Phone 2002 or IP Phone 2004 belongs.
KEM	(0) -2	Number of attached IP Phone KEMs
		Up to two IP Phone KEMs can be attached to an IP Phone. Pressing <CR> without entering a number leaves the value unchanged.
...		
KEY	xx aaa yyyy (cccc or D) zz..z	

Prompt	Response	Description
		IP Phone function key assignments The following key assignments determine calling options and features available to a telephone. Note that KEY is prompted until just a carriage return <CR> is entered. Where: xx = key number For IP Phone 2002, where: xx = 0 to 31, when KEM = 0 xx = 0 to 55, when KEM = 1 xx = 0 to 79, when KEM = 2 For IP Phone 2004, where: xx = 0 to 31, when KEM = 0 xx = 0 to 79, when KEM = 1 xx = 0 to 79, when KEM = 2 Type xx = NUL to remove a key function or feature. aaa = key name or function yyyy = additional information required for the key zz..z = additional information required for the key aaa The cccc or D entry deals specifically with the Calling Line Identification feature, where: cccc = CLID table entry of (0)-N, where N = the value entered at the SIZE prompt in LD 15 minus 1. You can enter a CLID table entry if aaa = ACD, HOT d, HOT L, MCN, MCR, PVN, PVR, SCN, or SCR. D = the character "D". When the character "D" is entered, the system searches the DN keys from key 0 and up, to find a DN key with a CLID table entry. The CLID associated with the found DN key will then be used. The position of the (cccc or D) field varies depending on the key name or function.

Prompt	Response	Description
PAGEOFST	<Page> <KeyOffset>	Automatically calculates the IP Phone KEM key based on the entered values. This prompt enables the system administrator to enter a Page number of 0 or 1 and a Key Offset number from 0 to 23. Once entered, the KEY prompt is prompted with the appropriate KEY value filled in. Enter <CR> to terminate data entry. Applies to an IP Phone 2004 with KEM = 1, and where <CR> was entered at the KEY prompt. This does not apply to an IP Phone 2002. When values are entered for Page and KeyOffset, the KEY xx prompt displays, followed by PAGEOFST prompt. This loop continues until no values (<CR> only) are entered at the PAGEOFST prompt.
KEY xx		Edit the IP Phone KEM key number specified by PAGEOFST, where: xx = the number of the key (for example, KEY 36)
KEMOFST	<KEM> <KeyOffset>	Enter <CR> to keep the current setting. Automatically calculates the IP Phone KEM key based on the entered values. This prompt enables the system administrator to enter a KEM number of 1 or 2 and a Key Offset number from 0 to 23. Once entered, the KEY prompt is prompted with the appropriate KEY value filled in. Enter <CR> to terminate data entry. When values are entered for KEM and KeyOffset, the KEY xx prompt displays, followed by KEMOFST prompt. This loop continues until no values (<CR> only) are entered at the KEMOFST prompt. This applies an IP Phone 2002 if <CR> was entered at the KEY prompt, and an IP Phone 2004 with KEM = 2, and where <CR> was entered at the KEY prompt.
KEY xx		Edit the IP Phone KEM key number specified by KEMOFST, where: xx = the number of the key (for example, KEY 36) Enter <CR> to keep the current setting.

Configure the Expansion Module for IP Phone 1100 Series

Configure the optional Expansion Module for IP Phone 1100 Series (Expansion Module) in LD 11.

The Expansion Module is supported on the IP Phone 1120E, IP Phone 1140E, and IP Phone 1150E.

Prompt	Response	Description
REQ	NEW/CHG	Add new or change existing data.
TYPE	1120, 1140, 1150	For IP Phone 1120E, IP Phone 1140E, and IP Phone 1150E
...	...	...
KEM	(0) - 3/ <CR>	Number of attached Expansion Modules (0). Up to three Expansion Modules are supported.
...	...	...
CLS	KEM3	KEM3 CLS is defined.
KEY	0 - <see text>/ <CR>	Key number range expanded to support number of Expansion Modules specified by KEM prompt. The range on the IP Phone is as follows:
		xx = key number For IP Phone 1120E, where: xx = 0 to 31 when KEM = 0 xx = 0 to 49 when KEM = 1 xx = 0 to 67 when KEM = 2 xx = 0 to 85 when KEM = 3 For IP Phone 1140E and IP Phone 1150E, where: xx = 0 to 31 when KEM = 0 xx = 0 to 67 when KEM = 1 xx = 0 to 67 when KEM = 2 xx = 0 to 85 when KEM = 3
PAGEOFST	<Page> <KeyOff-set> <CR>	You are prompted for PAGEOFST if an IP Phone 1140E or an IP Phone 1150 is attached, if one Expansion Module is specified at the KEM prompt, and if <CR> is entered at the KEY prompt. This prompt enables you to enter a Page number of 0, or 1, and a Key Offset number from 0 to 17. Once entered, the KEY is prompted with the appropriate KEY value filled in. <CR> ends the input.

KEY <key>	<keys conf data>	<key> is the key number for the Page + Key Offset entered at PAGEOFST. Enter the key's configuration <CR> or just <CR>.
KEMOFST	<KEM> <Key-Off-set>/ <CR>	You are prompted for KEMOFST if an IP Phone 1120E is attached and if one, two, or three Expansion Modules are specified at the KEM prompt, and if <CR> is entered for KEY prompt. This prompt enables you to enter a KEM number of 1, 2, or 3 and a KEY Offset number from 0 to 17. Once entered, the KEY prompt is prompted with the appropriate KEY value filled in. <CR> ends the input.
KEY <key>	<keys conf data>	<key> is the key number for the KEM + Key Offset entered at KEYOFST. Enter the key's configuration <CR> or just <CR>.

IP Phone dedicated context-sensitive soft keys

Table 74 "LD 11 IP Phone dedicated context-sensitive soft key assignment" (page 256) describes the features that can be assigned to dedicated context-sensitive soft keys 17 to 26 on the IP Phone 2001, IP Phone 2002, IP Phone 2004, IP Phone 2007, IP Phone Audio Conference 2033, IP Phone 1110, IP Softphone 2050, MVC 2050, IP Phone 1120E, IP Phone 1140E, IP Phone 1150E, and WLAN Handsets 2210/2211/2212/6120. Remove unused feature keys by configuring the dedicated context-sensitive soft keys to NUL. Some features depend on the given Class of Service.

If an attempt is made to configure anything other than the permitted response, the system generates an error code. For related error messages, see *Software Input Output Reference—System Messages (NN43001-712)*.

Table 74

LD 11 IP Phone dedicated context-sensitive soft key assignment

IP Phone key number	Responses Allowed
Key 16	MWK, NUL MWK – Message Waiting key
Key 17	TRN, NUL TRN – Call Transfer key

IP Phone key number	Responses Allowed
Key 18	AO3, AO6, NUL AO3 – 3-party conference key AO6 – 6-party conference key
Key 19	CFW, NUL CFW – Call Forward key
Key 20	RGA, NUL RGA – Ring Again key
Key 21	PRK, NUL PRK – Call Park key
Key 22	RNP, NUL RNP – Ringing Number pickup key
Key 23	SCU, SSU, SCC, SSC, NUL SCU – Speed Call User SSU – System Speed Call User SCC – Speed Call Controller SSC – System Speed Call Controller
Key 24	PRS, NUL PRS – Privacy Release key
Key 25	CHG, NUL CHG – Charge Account key
Key 26	CPN, NUL CPN – Calling Party Number key

Node election rules

A Signaling Server with Virtual Trunks configured wins an election because it registers on the NRS with an IP node. Because the IP node could be provided to a Branch Office system during redirection to normal mode or to another CS 1000 peer system during Network wide Virtual Office logon, the TPS application must be enabled on the Signaling Server which is running the VTRK application.

The rules for the node election process are as follows:

1. A Signaling Server wins over any Voice Gateway Media Cards.
2. A Leader card always wins over a Follower card.
3. Media Card 32-port card wins over an ITG-P card but the Media Card 32S card *always* wins over an ITG-P card.
4. Within each class (Leader/Follower), the card with the longest uptime wins.
5. In the event of a tie in uptime length, the card with the lowest IP address wins.

The precedence of the rules is from 1 (highest) to 5 (lowest).

Configuration of IP Telephony nodes using Element Manager

Contents

This section contains the following topics:

- "Introduction" (page 259)
- "Configure IP Line data using Element Manager" (page 260)
- "Transfer node configuration from Element Manager to the Voice Gateway Media Cards" (page 286)
- "Upgrade the Voice Gateway Media Card software and IP Phone firmware" (page 293)
- "Assemble and install an IP Phone" (page 307)
- "Change the default IPL> CLI Shell password" (page 307)
- "Configure the IP Phone Installer Passwords" (page 307)
- "Import node configuration from an existing node" (page 307)

Introduction

This chapter explains how to configure IP Telephony nodes and Voice Gateway Media Cards using Element Manager. Element Manager is accessed using a PC with Internet Explorer 6.0.2600 (or later). The PC must be connected to a LAN that has access to the Signaling Server Node IP address, either directly or routed through the network.

The ELAN subnet IP address might be required, instead of the Node IP address, to access the Element Manager logon window in secure environments.

This chapter also provides instruction for transmitting files to Voice Gateway Media Cards, upgrading card software, and upgrading IP Phone firmware.

Read the information about IP network engineering guidelines in *Converging the Data Network with VoIP Fundamentals (NN43001-260)* before installing an IP Telephony node.

Upgrade the ITG-P 24-port line cards to IP Line

CS 1000 systems require the ITG-P 24-port line cards to be running IP Line.



WARNING

In CS 1000 systems, TM 3.1 is required to upgrade an ITG-P 24-port line card running IP Line 2.2 (or earlier) to IP Line. After the card software is upgraded to IP Line using TM 3.1, configuration, administration, and maintenance tasks can be performed using Element Manager.

See ITG-P 24-port card upgrades in *Communication Server 1000E Upgrade—CS 1000M Cabinet to CS 1000E (NN43041-466)* or *Communication Server 1000E Upgrade—CS 1000M Chassis to CS 1000E (NN43041-467)* for the procedure to upgrade an ITG-P 24-port line card to IP Line software.

Configure IP Line data using Element Manager

Element Manager can be used to manually add and configure an IP Telephony node on CS 1000 systems. Multiple nodes can be configured and managed from Element Manager.

Node definition

A node is defined as a collection of Signaling Servers and Voice Gateway Media Cards. Each node in the network has a unique Node ID. This Node ID is an integer value. A node has only one Primary Signaling Server or Leader Voice Gateway Media Card. All the other Signaling Servers and Voice Gateway Media Cards are defined as Followers.

All IP addresses and subnet mask data must be in dotted decimal format. Convert subnet mask data from Classless Inter-Domain (CIDR) format. for more information, see [Appendix "Subnet Mask Conversion from CIDR to Dotted Decimal Format" \(page 507\)](#).

See [Table 62 "Voice Gateway Media Card installation summary sheet" \(page 223\)](#) for IP addresses and information required in this procedure.

The following sections discuss how to configure IP Line using Element Manager. The following three sections found in the IP Telephony section of Element Manager are not covered in this NTP:

- SNTP (see *IP Peer Networking Installation and Commissioning (NN43001-313)*)
- NRS (see *IP Peer Networking Installation and Commissioning (NN43001-313)*)

- Signaling Server (see *Signaling Server Installation and Commissioning (NN43001-312)*)

Internet Explorer browser configuration

Element Manager requires Microsoft Internet Explorer 6.0.2600 (or later). Element Manager is not supported on the Netscape Navigator browser. The PC should be a PIII with a 500 MHz processor (at minimum).

ATTENTION

Internet Explorer caching interferes with the Element Manager application, in that users cannot see real-time changes as they occur. For this reason, Internet Explorer caching must be turned off.

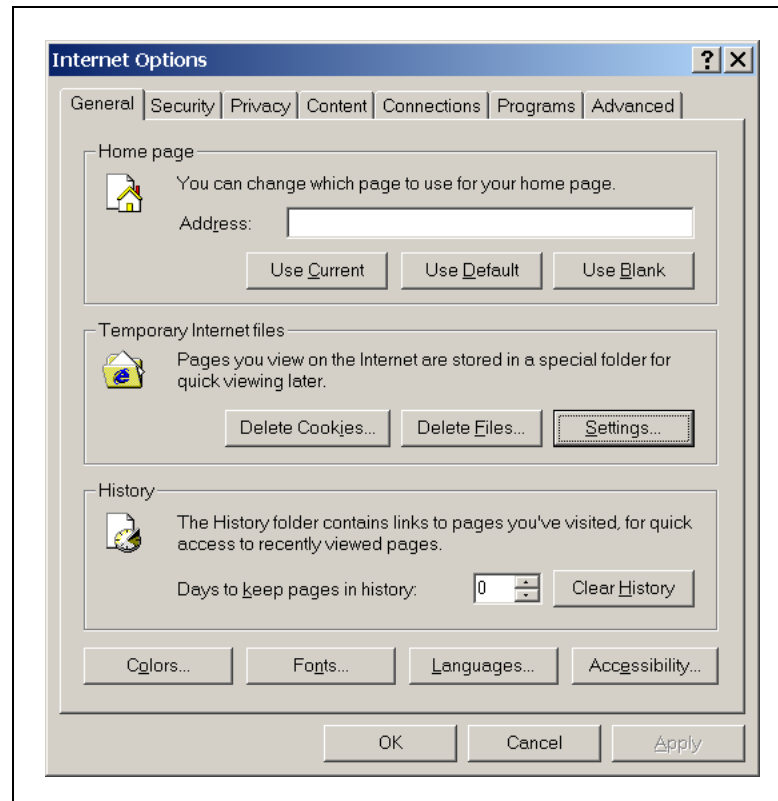
Follow the steps in [Procedure 22 "Turning off browser caching in Internet Explorer" \(page 261\)](#) to prevent caching of Web pages by Internet Explorer.

Procedure 22

Turning off browser caching in Internet Explorer

Step	Action
1	Launch Internet Explorer.
2	Click Tools > Internet Options . The Internet Options window appears. See Figure 57 "Internet Explorer – Internet Options" (page 262) .

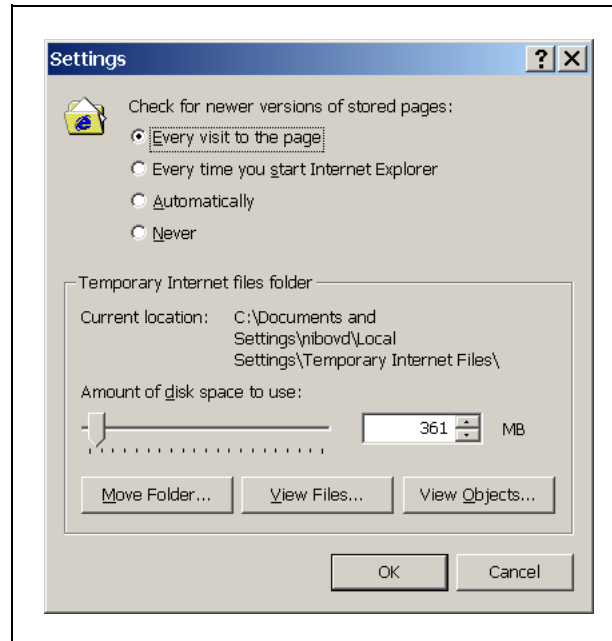
Figure 57
Internet Options window



- 3 On the **General** tab, under the **Temporary Internet files** section, click the **Settings** button.

The Settings window appears. See [Figure 58 "Temporary Internet files Settings window"](#) (page 263).

Figure 58
Temporary Internet files Settings window



- 4 Click the **Every visit to the page** radio button.
 This checks for new versions of stored pages on every visit to the Web page.
- 5 Click **OK** in the Settings window.
- 6 Click **OK** in the Internet Options window.

—End—

Launch Element Manager

Follow the steps in [Procedure 23 "Launching Element Manager" \(page 263\)](#) to launch Element Manager.

Procedure 23

Launching Element Manager

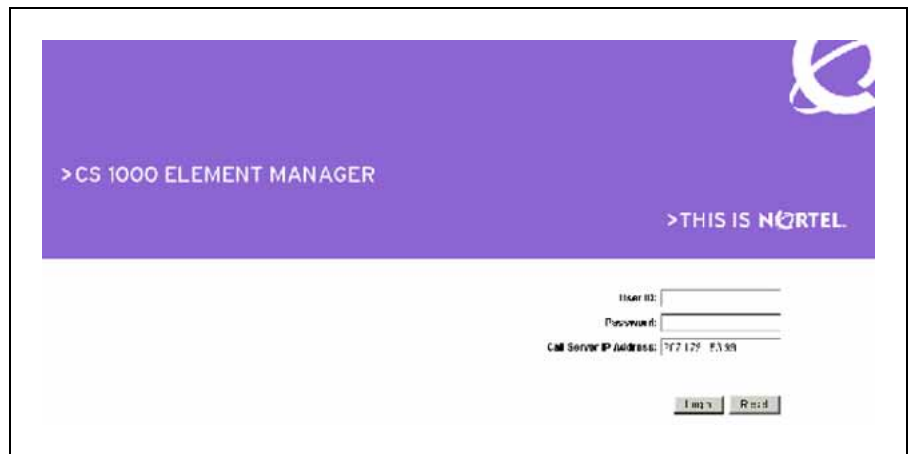
Step	Action

1	Open Internet Explorer.
2	Enter the Signaling Server Node IP address in the Address Bar (url line) of the browser window. Click Go or press Enter on the keyboard.

The ELAN network interface IP address might be required, instead of the Node IP address, to access the Element Manager logon window in secure environments.

- 3 Element Manager opens and the **logon** window appears.
See [Figure 59 "Element Manager Login window" \(page 264\)](#).
 - a. Enter the **User ID** and **Password** of the Call Server.
 - b. Enter the IP address of the Call Server in the **Call Server IP** field.
 - c. Click the **logon** button.

Figure 59
Element Manager logon window



The **Home - System Overview** window appears.

The Element Manager navigator is located on the left side of the Element Manager browser window.

To log out of Element Manager, click **Logout** in the upper right-hand corner of the window.

When working in the **IP Network > Node: Servers, Media Cards** window, Element Manager times out after a period of inactivity. Users are prompted with a warning five minutes before Element Manager times out. If the user clicks OK within the warning time out period, the timer is reset. If the user does not respond, the session is cancelled and the user is forced to logon again. Any data that was modified, but not submitted, is lost.

—End—

Summary of procedures

The following is the summary of the steps required to configure a node and a Voice Gateway Media Card using Element Manager:

1. "Manually add an IP Telephony node" (page 265)
2. "Configuring SNMP trap destinations and community strings" (page 268)
3. "Configure Voice Gateway Profile data" (page 270)
4. "Configure Quality of Service" (page 274)
5. "Configure ELAN IP address, TLAN voice port, and routes" (page 276)
6. "Configure file server access" (page 280)
7. "Configure loss and level plan" (page 281)
8. "Add card and configure the card properties of the Voice Gateway Media Card" (page 283)
9. "Submit and transfer the node information" (page 285)

Manually add an IP Telephony node

Follow the steps in [Procedure 24 "Adding an IP Telephony node manually" \(page 265\)](#) to add an IP Telephony node using Element Manager.

Procedure 24

Adding an IP Telephony node manually

Step	Action
1	To manually add a new IP Telephony node, click IP Network > Node: Servers, Media Cards in the navigator. The Node Configuration window appears. See Figure 60 "Adding a new node" (page 265).

Figure 60
Adding a new node



If this is the first node to be added, the **"No nodes are configured"** message is displayed. There are two options: **"New Node to Add"** or **"Import Node Files"**.

The **Node Configuration** window shows a list of all the configured nodes. To expand a node and view its elements, click the plus sign (+) to the left of the Node name.

The Node Configuration window includes five buttons:

- **to Add** – used to add a new IP Telephony node. Enter an unused Node ID and then click **to Add**.
- **Import Node Files** – imports the configuration files from an existing node.
- **Edit** – retrieves the node information from the Call Server and returns the information to the Edit window. The node information can then be changed.
- **Transfer/Status** – used to transfer/obtain the status on the requested changes to the node. The node then obtains its information (CONFIG.INI and BOOT.P files) from the Call Server.

If any element within the Node fails to transfer either BOOTP or CONFIG files, the **Transfer/Status** button is highlighted in red. If the transfer status of the node elements is unavailable, the **Transfer/Status** button is highlighted in yellow.

- **Delete** – This button is used to delete the selected node and its information from the Call Server.

2 Enter the new Node ID in the **New Node** text box.

The Node ID can be one to four digits in length. When defining the node number, determine if the Enhanced Redundancy for IP Line Nodes functionality is required (see ["Enhanced Redundancy for IP Line nodes" \(page 187\)](#)). If it is required, factor the requirement into the node number assignment process.



CAUTION

The Voice Gateway Media Cards identify themselves with a node using the node number or node ID. If there are multiple IP Telephony nodes sharing the same TLAN subnet, each node must have a unique ID. Each system on the TLAN subnet must have a unique node ID assigned to the Voice Gateway Media Cards on the system.

The Node ID field corresponds to the Node ID field in the IP Phone configuration. Write down the node number, which is used during the IP Phone configuration.

3 Click to **Add**.

The **Edit** window appears. See Figure 61 "Editing a node " (page 267).

Figure 61
Editing a node

The Edit window includes three different buttons:

- **Save and Transfer** – saves and transfers changes to the Call Server and returns the users to the Node Configuration window.
- **Cancel** – discards changes made to the IP Telephony node and returns the users to the Node Configuration window.
- **Add** – associated with specific sections of the IP Telephony node properties. The user can add new cards and Signaling Servers.

- 4** Click the plus sign (+) to the left of the node name to display the node information, if it is not already expanded.
- a. **Node ID:** The node ID entered on the previous page appears.
 - b. **Voice LAN (TLAN) Node IP address:** Enter the Voice LAN (TLAN) Node IP address in dotted decimal format. The Voice LAN Node IP address is on the TLAN subnet. The Node IP

address is the IP address used by the IP Phones to communicate with the Voice Gateway Media Cards on the TLAN subnet. If a Voice Gateway Media Card becomes the primary (Leader) during an election, it assigns itself the Node IP address.

ATTENTION

An asterisk (*) indicates that a field is a required/mandatory field.

- c. **Embedded LAN (ELAN) gateway IP address:** Enter the Embedded LAN (ELAN) subnet gateway IP address in dotted decimal format. This is the IP address of the gateway of the subnet to which the Voice Gateway Media Card belongs. Also, this is the IP address of the router interface on the ELAN subnet, if present. If there is no Embedded LAN subnet gateway, enter 0.0.0.0.
- d. **Embedded LAN (ELAN) subnet mask:** Enter the Embedded LAN (ELAN) subnet mask address in dotted decimal format. This is the subnet mask that is used along with the ELAN subnet IP address to identify to which subnet the Voice Gateway Media Card belongs.
- e. **Voice LAN (TLAN) subnet mask:** Enter the Voice LAN (TLAN) subnet mask address in dotted decimal format. This is the subnet mask that is used along with the TLAN IP address, to identify the subnet to which the Voice Gateway Media Card belongs.

ATTENTION

Do not click **Save and Transfer** until all the node information has been entered. If the Submit button is clicked prematurely, the Node Configuration window reappears. If **Save and Transfer** was clicked prematurely, click the **Edit** button to return to the Node Edit window and continue the configuration.

—End—

SNMP configuration

For more information about SNMP, see *Communication Server 1000 Fault Management—SNMP (NN43001-519)*.

Configuring SNMP trap destinations and community strings

IP Line introduces single point configuration for SNMP traps. To configure the SNMP trap destinations, and community strings for the Call Server, Signaling Server, Voice Gateway Media Cards, and Media Gateway Controller in Element Manager, follow the steps in [Procedure 25 "Configuring SNMP trap destinations" \(page 269\)](#).

ATTENTION

It is necessary to perform a datadump to save the configuration information permanently whether the parameters are configured in Element Manager or in LD 117.

Procedure 25**Configuring SNMP trap destinations****Step Action**

- 1 In the Element Manager navigator, click **System > Alarms > SNMP**. The **SNMP Configuration** window appears. See [Figure 62 "SNMP configuration window"](#) (page 269).

Figure 62
SNMP configuration window

- 2 In the **Trap Source** section, enter the following parameters:
 - **Navigation Site Name**
 - **Navigation System Name**

These parameters are used during trap generation.

- 3 In the **MIB-2 System Group Parameters** section, enter the appropriate parameters from the system administrator:
 - **System Contact**

- **System Location-**
- **System Name**

4 In the **Community** section, enter the following parameters for system management community strings for access to the Management Information Base (MIB) and trap generation, and administrator community strings for access to the MIB views.

- **System Management Read**
- **System Management Write**
- **Trap community**
- **Administrator Group**

The SNMP community strings control access to the IP Telephony node. Element Manager uses the community strings to refresh the Voice Gateway Media Card status and to control the transmitting and retrieving of configuration data files for database synchronization.

5 In the **Trap Destinations** section, enter the IP address of the trap destination. SNMP traps are sent to the IP address entered. A maximum of 8 IP addresses can be configured.

6 Click **Save**.

The parameters are automatically synchronized to the Call Server, Signaling Server, Voice Gateway Media Cards, and Media Gateway Controller.

After the parameters are synchronized, the associated host route entries are added to the routing table automatically. If a trap destination is removed, the corresponding routing table entry is removed as a result.

—End—

Configure Voice Gateway Profile data

Follow the steps in [Procedure 26 "Configuring DSP Profile data" \(page 270\)](#) to configure the Voice Gateway Profile data.

Procedure 26

Configuring DSP Profile data

Step	Action

1	In the Edit window, click VGW and IP Phone codec profile .

The **VGW and IP phone codec profile** information expands. See Figure 63 "VGW and IP phone codec profile window" (page 271).

The **VGW and IP phone codec profile** area includes VGW information and a list of codecs.

Figure 63
VGW and IP phone codec profile window

The screenshot shows the 'CS 1000 ELEMENT MANAGER' interface with a 'Help | Logout' link in the top right. The main title is '- VGW and IP phone codec profile'. The settings are as follows:

- Enable Echo canceller:** ☒
- Echo canceller tail delay:** 128 (milliseconds)
- Voice activity detection threshold:** -17 (range: -20 to +10 DBM)
- Idle noise level:** 65 (range: -327 to +327 DBM)
- DTMF Tone detection:** ☒
- Enable V.21 FAX tone detection:** ☒
- FAX maximum rate:** 14400 (bps)
- FAX playout nominal delay:** 100 (range: 0 to 200 milliseconds)
- FAX no activity timeout:** 20 (range: 10 to 32000 milliseconds)
- FAX packet size:** 30

Below the settings is a list of codecs with 'Select' buttons:

+ Codec: G711	Select ☒
+ Codec: G729A	Select ☐
+ Codec: G723.1	Select ☐
+ Codec: 138 FAX	Select ☒

- 2 Under **VGW and IP phone codec profile**, leave the values at their default settings unless directed to change them by Nortel Field Support.
 - a. **Enable Echo canceller:** The echo canceller is enabled by default. Do not uncheck this box. Never disable echo canceller unless directed by Nortel Field Support.
 - b. **Echo canceller tail delay:** Select the maximum value available. The default value is 128ms. Never reduce the echo canceller value unless directed by Nortel Field Support.
 - c. **Voice activity detection threshold:** The default value is -17db. The range is -20db to +10db.
 - d. **Idle noise level:** The default value is -65db. The range is -327db to +327db.
 - e. **DTMF Tone detection:** Ensure this is checked to enable DTMF tone detection. This is enabled by default.
 - f. **Enable V.21 FAX tone detection:** Ensure this is checked to enable V.21 FAX tone detection. This is enabled by default.
 - g. **FAX maximum rate:** The FAX maximum rate is one of the following values: 2400, 4800, 7200, 9600, 12 000, or 14 400. The default value is 14400 bps.

- h. **FAX playout nominal delay:** The default value is 100 ms. The range is 0ms to 300ms.
- i. **FAX no activity timeout:** The default value is 20 seconds. The range is 10 seconds to 32000 seconds.
- j. **FAX packet size:** Select the desired FAX packet size. The default value is 30 bytes. The range is 20 to 48 bytes.

To select a codec, scroll through the list, and click the corresponding **Select** check box. A maximum of four codecs can be selected.

Recommendation

Nortel recommends that the system be configured with both G.711 and G.729A if there is a possibility that an IP Softphone 2050 could be configured with the "I use a modem to connect to the network" check box checked. If the node does not have G.729A and/or G.723 configured, IP Softphone 2050 users with that checkbox selected will have calls blocked.

This does not apply to the MVC 2050 as it only supports G.711 capability; there is no dial-up capability.

For more information, see *IP Phones Fundamentals (NN43001-368)*.

The codec list contains four codec settings for G.711, G.729A, C.723.1, and T.38 FAX for the Voice Gateway Media Card.

- 3** The G.711, G711 Clear Channel, and T.38 FAX codecs are selected by default, and these selections cannot be cleared. However, the following changes can be made:

- The payload size, jitter buffer setting, and companding law for the G.711 codec can be changed. The default is G.711 mu-law.
- Only the jitter buffer can be changed for the G.711 Clear Channel codec.

Up to three additional codecs can be optionally selected: G.729A, G.729AB, and/or G.723.1 codecs.

- If the G.729A or G.729AB codec are selected, the payload and jitter buffer can be changed. The payload defaults are the maximum supported payload.
- If the G.723.1 codec is selected, only the jitter buffer can be changed. The payload size of 30 msec is the only supported payload.

The supported G.723.1 codec has bit rates of 5.3 kb/s and 6.3 kb/s.

- 4 Expand the selected **Codec**. See [Figure 64 "Selected Codec" \(page 273\)](#).

Figure 64
Selected Codec

The screenshot shows the 'CS 1000 ELEMENT MANAGER' interface. It lists three codecs: G711, G729A, and G723.1. The G723.1 codec is selected. For each codec, the following settings are visible:

- Codec Name:** G711, G729A, or G723.1
- Voice payload size:** 20 (ms/frame) for G711 and G729A; 30 for G723.1
- Voice playout (jitter buffer) nominal delay:** 40 for G711 and G729A; 60 for G723.1
- Voice playout (jitter buffer) maximum delay:** 80 for G711 and G729A; 120 for G723.1

A note below each section states: 'Modifications may cause changes to maximum delay settings'.

Element Manager enables some jitter buffer adjustments on the browser side. The following are the jitter buffer adjustments that are made in Element Manager:

- A change of payload resets the Nominal Voice Playout (NVP) and Maximum Voice Playout (MVP) values to the default recommended values:

$$\text{NVP} = 2 * \text{payload}$$

$$\text{MVP} = \text{NVP} + 2 * \text{payload}$$
- A change of NVP value changes the MVP value to the default ($\text{MVP} = \text{NVP} + 2 * \text{payload}$) and changes the values listed in the MVP pull down list so the minimum value listed does not violate the requirement of $\text{NVP} + 2 * \text{payload}$.
- The MVP value can be changed. The pull-down values range from the minimum recommended value (see above) to the maximum allowed value for the selected codec type.

- 5 Configure the following values for the codec:
 - a. **Codec Name:** The codec name is based on the selected codec.
 - b. **Voice payload size (ms/frame):** The payload size is determined by the selected codec.

For each codec type, the payload is defaulted to the maximum supported: 30 msec for G.711 (a-law and mu-law), 50 msec for G.729A, 50 msec for G.729AB, and 30 msec for the G.723.1.

If a system has multiple nodes and the same codec is selected on more than one node, ensure that each node has the same voice payload size configured for the codec.

- c. **Voice playout (jitter buffer) nominal delay:** Set the nominal value to the highest setting that the device allows. The range is 20 to 200 ms and is dependent on the codec. Changing this value can cause the automatic adjustment of the other settings for this codec. For more information, see *Converging the Data Network with VoIP Fundamentals (NN43001-260)*.
- d. **Voice playout (jitter buffer) maximum delay:** The maximum delay has a range of 60 to 500 ms and is dependent on the codec. Changing this value can cause the automatic adjustment of the other settings for this codec.
- e. **VAD:** Select this check box to enable Voice Activity Detection. Because CS 1000 Release 5.0 does not support VAD for G723.1codec, Element Manager does not support configuration of VAD for G723.1.

- 6 Repeat step 5 for each of the selected codecs.

—End—

Configure Quality of Service

The Quality of Service (QoS) section includes the settings for the following:

- DiffServ CodePoint (DSCP)
- 802.1Q support

Follow the steps in [Procedure 27 "Configuring QoS" \(page 274\)](#) to configure QoS.

Procedure 27 Configuring QoS

Step	Action
1	In the Edit window, click the plus sign (+) to the left of QoS . See Figure 65 "QoS window " (page 275) .

Figure 65
QoS window

- 2 The Differentiated Service (DiffServ) CodePoint (DSCP) value determines the priorities of the management and voice packets in the IP Line network. The range for both management and voice packet DiffServ is 0 to 63 inclusive.

The DiffServ value can be configured, if required, to obtain better QoS over the IP data network (LAN/WAN).

The value entered depends on the policy in the customer data network.

ATTENTION

Do not change DiffServ from the default values unless instructed by the IP network administrator.

Only modify the Control packets priority and Voice packets priority values as and when directed by the IP network administrator.

The recommended configuration values are as follows:

- a. **Diffserv CodePoint (DSCP) Control packets:** A value of 40 - Class Selector 5 (CS5). The range is 0 to 63. This configures the priority of the signaling messaging.
 - b. **Diffserv CodePoint (DSCP) Voice packets:** A value of 46 Control DSCP - Expedited Forwarding (EF). The range is 0 to 63.
- 3** 802.1Q enables Virtual LANs (VLANs) to be defined within a single LAN. This improves bandwidth management and limits the impact of broadcast storms and multicast messages.
 - a. **Enable 802.1Q support:** 802.1Q support is disabled by default.
 - b. **802.1Q Bits value (802.1p):** The priority field is a 3-bit value, with a default value of 6. The range is 0 to 7. A value of 6 is recommended by Nortel. The p bits within the 802.1Q standard enables packet prioritization at Layer 2, improving network throughput for IP Telephony data.

—End—

Configure ELAN IP address, TLAN voice port, and routes

The LAN configuration section is used for configuring the Call Server ELAN IP address (Active ELNK), TLAN voice port, and routes.

This information is applicable only to Small Systems.

Procedure 28

Configuring the Call Server ELAN network interface IP address (Active ELNK), TLAN voice port, and routes

Step	Action

1	In the Edit window, click the plus sign (+) to the left of LAN Configuration .

See [Figure 66 "LAN configuration window" \(page 277\)](#).

Figure 66
LAN configuration window

CS 1000 ELEMENT MANAGER Help | Logout

Managing: 192.167.102.3
System » IP Network » Node Configuration » IP Telephony Node » Edit

Edit

Save and Transfer Cancel

- + IP Telephony Node
- + VGW and IP phone codec profile
- + QoS
- LAN configuration
- Embedded LAN (ELAN) configuration

Call server IP address: 192.167.102.3

Unistern Signaling port: 15000

Broadcast port: 15001 (1024 - 86656)

Telephony LAN (TLAN) configuration

Unistern Signaling port: 5000

RTP/RTCP Starting port: 5200 (1024 - 65535)

Embedded LAN (ELAN) Router: Adc

Host Table: Adn

DNS Servers

Primary DNS Server IP address: 10.10.10.10

Alternate DNS Server1 IP address: 10.10.10.10

Alternate DNS Server2 IP address: 10.10.10.10

2 Enter the following **Embedded LAN (ELAN) configuration** settings:

- Call Server IP address:** This is the IP address of the Call Server on the ELAN subnet. Enter the Call Server ELAN network interface IP address (Active ELNK).

The Call Server ELAN network interface IP address must correspond to the Active ELNK IP address configured in LD 117. The IP address must be in the same subnet as the ELAN subnet for the IP Line node.

- Survivable Media Gateway IP address:** This address is configured for survivability. It is the IP address of the Survivable Media Gateway on the ELAN subnet.

The Survivable Media Gateway IP address must correspond to the Active ELNK IP address. If configured, all Voice Gateway Media Cards in the same node should be in the same Survivable Cabinet.

The Survivable Media Gateway associated with the Primary Signaling Server IP Telephony node is called the Alternate Call Server. It is normally located in the same equipment rack with the Call Server and Signaling Server; therefore, it is normally connected to the same ELAN subnet as the Call Server and the Primary Signaling Server IP Telephony node. The Alternate Call

Server Media Gateway should be equipped with sufficient trunk cards, Voice Gateway Media Cards, and centralized CallPilot, so that it provides a large degree of survivability in case of Call Server equipment failure for IP Phone users who normally register through the Signaling Server.

- c. **Signaling port:** The default value is 15 000. The range is 1024 to 65 535.
- d. **Broadcast port:** The default value is 15 001. The range is 1024 to 65 535.

3 Under Voice LAN (TLAN) configuration:

- a. **Signaling port:** The default value is 5000. The range is 1024 to 65 535. The TLAN Signaling occurs on UDP ports 7300, 4100, 5100, and 5000.
- b. **Voice port:** Change the Voice port only as instructed by the IP network administrator to improve QoS for the IP Phones. For example, if RTP Header compression is used to reduce voice bandwidth on narrow band WAN links, then the TLAN voice port range needs to be set to 16384 or higher. The exact range is provided by the system administrator. The TLAN Voice port range is 1024 to 65535. The default Voice ports are 5200 to 5295.



CAUTION

Do not set the Voice port to a value that is already used for signaling (4100, 5000, 5100, 7300).

The Voice port defines the first port in a range spanning the gateway channels on the card; this means a Voice port value of 5200 reserves the following:

- ports 5200 to 5263 on the Media Card 32-port line card, and MC 32S
- and 5200 to 5247 on the ITG-P 24-port line card.

If this value is changed from the default, verify that the selected Voice port value does not intrude into one of the reserved Signaling port values.

- 4** Click the **Add** button to the right of **Embedded LAN (ELAN) Routes** if entries must be made to the card routing table. The Routes information expands.

See [Figure 67 "Embedded LAN \(ELAN\) Routes"](#) (page 279).

Figure 67
Embedded LAN (ELAN) Routes

The screenshot shows the 'CS 1000 ELEMENT MANAGER' interface. The 'Embedded LAN (ELAN) configuration' section includes fields for 'Call server IP address' (192.167.102.3), 'Unistim Signaling port' (15000), and 'Broadcast port' (15001). The 'Telephony LAN (TLAN) configuration' section includes 'Unistim Signaling port' (5000) and 'RTP/RTCP Starting port' (5200). The 'Embedded LAN (ELAN) Routes' section has an 'Add' button. Below it, there is a table with two columns: 'IP address' and 'Subnet mask'. There are two rows of input fields for these values, each with a 'Remove' button.

In the **Routes** section, enter the **IP address** and **Subnet mask** for any host that is not on the ELAN subnet but requires access to the Voice Gateway Media Card across the ELAN subnet. A Telnet session for maintenance from a remote PC is an example of when this would be needed. The address of the remote PC would be added in the Route list.

The default route on the card causes packets destined for unknown subnets to be sent out on the TLAN network interface. Packets from an external host arrive on the ELAN network interface and responses are sent on the TLAN network interface. This process can cause one-way communication if the TLAN subnet is not routed to the ELAN subnet. It is necessary to add an entry in the Route list to correct the routing so that response packets are sent on the ELAN subnet. Each entry creates a route entry in the card route table that directs packets out the ELAN network interface. See [Figure 68 "Specifying additional ELAN routes"](#) (page 280).

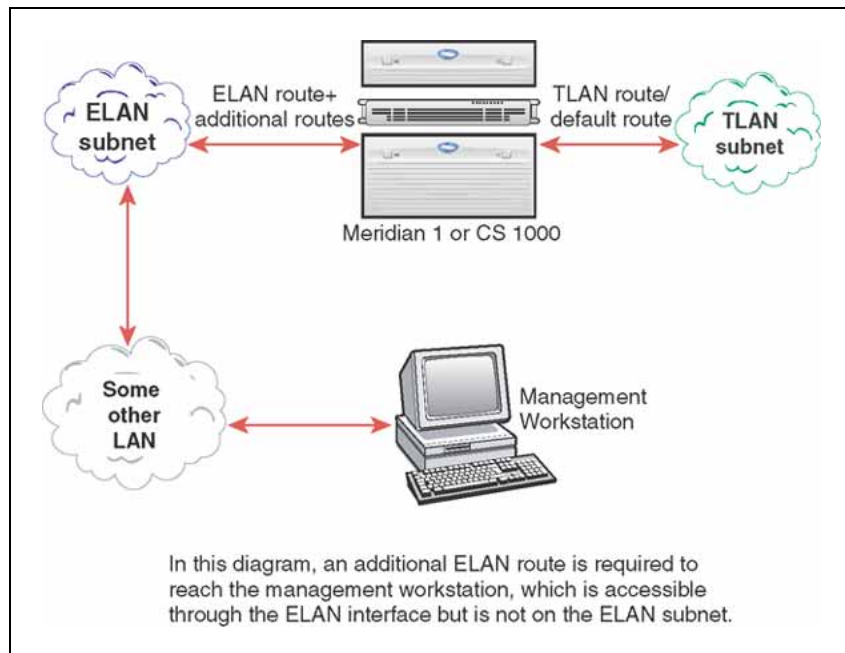


CAUTION

Use caution when assigning card routing table entries. Do not include the IP address of an IP Phone. Otherwise, voice traffic to these IP Phones is incorrectly routed through the ELAN subnet and ELAN subnet gateway. To avoid including the wrong IP address, Nortel recommends that Host IDs are defined for the card routing table entries.

- 5 To add additional routes, click the **Add** button again and enter the route information. Repeat this step for each route to be added.

Figure 68
Specifying additional ELAN routes



—End—

Configure file server access

Firmware files for the IP Phones are stored on a Signaling Server. Each time a Follower Signaling Server powers up or reboots, IP Phone firmware files are retrieved from the Master Signaling Server. You can configure the Master Signaling Server to retrieve the IP Phone firmware files from an external FTP site server during bootup. All files, which match xNN.fw naming convention are retrieved and registered. For more information, see ["Enhanced UNiStim Firmware Download for IP Phones"](#) (page 79).

To configure the file server, follow the steps in [Procedure 29 "Configuring access to the file server"](#) (page 280).

Procedure 29

Configuring access to the file server

Step	Action

1	In the Edit window, click the plus sign (+) to the left of Firmware . See Figure 69 "Firmware configuration" (page 281).

Figure 69
Firmware configuration

CS 1000 ELEMENT MANAGER Help | Logout

Managing: 192.167.102.3
System > IP Network > Node Configuration > IP Telephony > Node ID 9 > Edit

Edit

- IP Telephony Node

Node ID 9

telephony LAN (ILAN) Node IP address: 192.167.102.3

Embedded LAN (FI LAN) gateway IP address: 192.167.102.1

Embedded LAN (CLAN) subnet mask: 255.255.255.0

Voice LAN (TLAN) subnet mask: 255.255.255.0

+ VGW and IP phone codec profile

+ QoS

+ LAN configuration

+ SNMP

+ Virtual Trunk Network Health Monitor configuration

+ H323 GW Settings

- Firmware

Firmware download server IP address: 192.167.102.3

Firmware file path: download/firmware

User ID:

Password:

- 2 Specify the parameters needed to connect to the file server:
 - a. **Firmware download server IP address:** Enter the IP address of the file server where the firmware is downloaded.
 - b. **Firmware file path:** Enter the path for the location of the firmware files.
 - c. **User ID:** Enter the User ID that is required to access the file server.
 - d. **Password:** Enter the Password that is required to access the file server.

—End—

Configure loss and level plan

The loss and level plan determines parameters, such as transmission gain, that vary from country to country.

Dynamic Loss Plan

A Dynamic Loss Plan has been implemented to define the gateway loss value per endpoint connection type. The loss plan adjusts the Voice Gateway Media Card gateway channel loss for each call by sending pad values to the card. Loss plan values are now configured through LD 73.

Default values

The default values in the system are for the North American loss plan.

Non-North American countries

Installation of IP Line in any other country requires setting the pad values in Table 15 to that country loss plan. If the system is installed in other countries, the GPRI package (International 1.5/2.0 Mb/s Gateway package 167) must be used, and the NTP-specified values must be entered in LD 73. At the PDCA prompt, enter Table 15.

See *Transmission Parameters Reference (NN43001-282)* for more information.

United Kingdom

In addition, when a system is installed in the UK, the CLI command **UKLossPlanSet** is entered at the CLI of one card in each node. This adjusts the loss plan of the IP Phones to the higher transmit levels required in the UK. Follow the steps in [Procedure 30 "Setting the loss plan for the UK" \(page 282\)](#) to set the loss plan for the UK.

Procedure 30

Setting the loss plan for the UK

Step	Action
1	Telnet to the card, connect to the maintenance port, or use TM 3.1 or Element Manager to access the Voice Gateway Media Card.
2	Log into the IPL> , or oam> shell.
3	At the prompt, enter the command UKLossPlanSet .
4	Press <CR>.
5	Exit from the logon session.

—End—

After the **UKLossPlanSet** command is entered, the loss plan adjustment is transmitted by that card to all other cards in the node. The loss plan is then adjusted on any registered IP Phones, and on other IP Phones as they register.

To clear the loss plan adjustment, use the command **UKLossPlanClr**.

See "IP Phone Loss Plan (UK) commands" (page 440) for more information about these and other loss plan commands.

Add card and configure the card properties of the Voice Gateway Media Card

If the network administrator provides IP addresses and subnet masks in CIDR format, for example, "10.1.1.10/24", convert the subnet mask to dotted decimal format. See [Appendix "Subnet Mask Conversion from CIDR to Dotted Decimal Format" \(page 507\)](#).

In the Cards section, cards can be added, changed, or removed in the node one at a time.



WARNING

Every node must have a Leader. Exercise caution when removing the Leader card. If the Leader card is deleted, a new Leader must be configured immediately.

Follow the steps in [Procedure 31 "Adding card and configuring Voice Gateway Media Card properties" \(page 283\)](#) to add a new Voice Gateway Media Card and configure its properties, or to configure the properties of an existing Voice Gateway Media Card.

Procedure 31

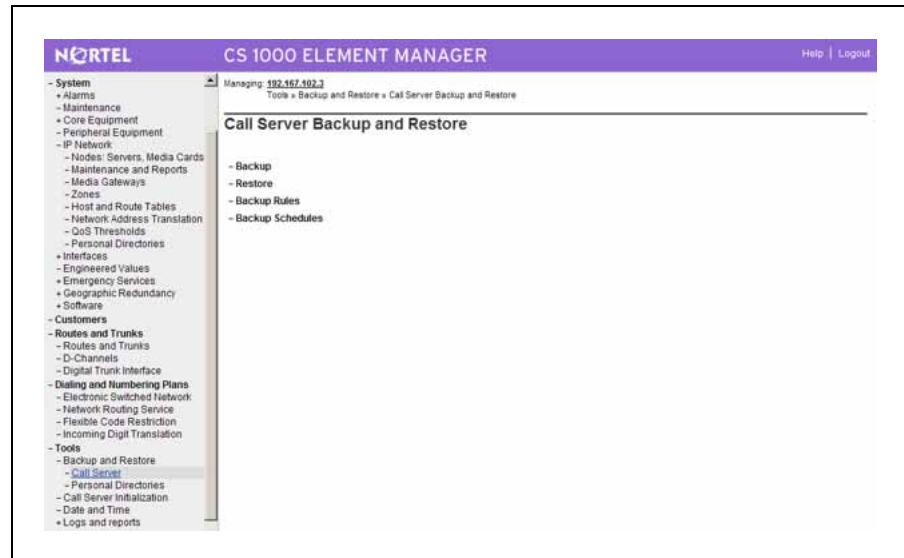
Adding a card and configuring Voice Gateway Media Card properties

Step	Action

1	In the Edit window, click the plus sign (+) to the left of Cards and then click the Add button.

See [Figure 70 "Cards configuration " \(page 284\)](#).

Figure 70
Cards configuration



- 2 Enter the **Card Properties** data for Leader 0 and Follower cards. The fields with asterisks are required fields:
- Role:** The role is assigned based on the information that Element Manager reads from the card configuration. This is a read-only field.
 - Embedded LAN (ELAN) IP address:** This is the ELAN network interface IP address for the card. Element Manager and the system use this IP address to communicate with the card.
 - Embedded LAN (ELAN) MAC address:** This is the motherboard Ethernet address from the [Table 62 "Voice Gateway Media Card installation summary sheet"](#) (page 223).
 - Telephony LAN (TLAN) IP address:** This is the TLAN network interface IP address for the card.
 - Voice LAN (TLAN) gateway IP address:** This is the IP address of the router interface on the TLAN subnet.
 - Hostname:** This is the Host name.
 - Card TN:** Enter the card slot number from 1 to 50.
 - Card processor type:** Choose either Pentium or Media Card from the drop-down list. Select Pentium if using the ITG-P 24-port line card (dual-slot card). Select Media Card if using the Media Card 32-port or MC 32S card (single slot).
 - H323 ID:** The H323 ID within IP Line is for the Virtual Office/ Media Gateway 1000B feature. Keep the H323 ID the same for all the elements within one node.

- j. **Enable set TPS:** Select the check box.
- 3 To add additional cards to the node, click the **Add** button again and enter the new card information. Repeat this step for each card that is being added to the node.
New cards appear under the Cards menu as they are added.
- 4 To edit the properties of an existing Voice Gateway Media Card, click the plus sign (+) to the left of the card to be edited to display the card properties and make the desired changes.

—End—

Submit and transfer the node information

To submit node changes and transfer the changes to the Call Server, follow the steps in [Procedure 32 "Submitting and transferring the node information" \(page 285\)](#).

Procedure 32

Submitting and transferring the node information

Step	Action
1	Click Save and Transfer when all the node information is configured in the Edit window. Clicking Save and Transfer saves and transfers the data to the Call Server and to all the node elements. There is a Save and Transfer button at both the top and bottom of the Edit window. The Edit window closes, and the Node Configuration window appears with the new node added. Save and Transfer can be clicked after each section is configured in the Edit window. However, each time Save and Transfer is clicked, the Edit window closes and the Node Configuration window is displayed. To continue the node configuration, click the Edit button to return to the Edit window. If Cancel is clicked, all information that has been configured is discarded. The Edit window closes and the Node Configuration window appears.
2	Click the Transfer/Status button for the node. The Transfer confirmation dialog box opens.
3	Click OK to confirm the transfer.

After a few seconds, the **Transfer Progress** window appears and displays each of the Voice Gateway Media Cards in the node.

The Voice Gateway Media Cards retrieve the CONFIG.INI and BOOTP.TAB files from the Call Server. A check mark is added to each field as the card receives its CONFIG.INI and BOOTP.TAB files.

- 4 When the transfer is complete, click **OK** in the **Transfer Successful** dialog box.
- If the transfer is successful for a card, the Status column displays "Complete" and a check mark is displayed.
 - If the transfer is unsuccessful, the Status column displays "Fail". A failed transfer can be caused by several situations, including the following:
 - improper cabling. Check cable connections.
 - improper card configuration. Ensure all information is configured correctly.
 - the Voice Gateway Media Card running an older version of the software than the Signaling Server. Verify the software version on the Voice Gateway Media Card and upgrade the software if necessary. See ["Upgrade the Voice Gateway Media Card software and IP Phone firmware"](#) (page 293).

—End—

Transfer node configuration from Element Manager to the Voice Gateway Media Cards

Before beginning the node configuration transfer, ensure the following:

- The Voice Gateway Media Cards and cables have been installed.
- The ELAN and TLAN network interfaces of all cards have access to the IP network.
- To enable access to Element Manager through a Web browser, a network PC must be able to access the node Signaling Server, either directly or remotely.

The IP Telephony node and card properties are configured using Element Manager. The configuration data is saved to the Call Server and then transferred to the Voice Gateway Media Cards.

Saving the configuration

The configuration data is saved when the **Save and Transfer** button in the **Edit** window is clicked. The files are saved to the Call Server. After the data is saved, the configuration must be transferred to the Voice Gateway Media Card. When **Transfer/Status** in the **Edit** window is clicked, Element Manager instructs each card where to retrieve the files using FTP. The Voice Gateway Media Card then retrieves the CONFIG.INI and BOOTP.TAB files.

Transferring the configuration - main node

For a Signaling Server node, the process to transfer the node configuration to the cards consists of the following steps:

1. Transmit the node properties. See [Procedure 34 "Transmitting node properties to Leader" \(page 290\)](#).
2. Configure the Follower card. See [Procedure 35 "Configuring the Follower cards" \(page 292\)](#).

The following sequence of steps are applicable only to nodes that do not use the Signaling Server as the Leader; that is, a second (or subsequent) node is being configured on the system – not the main node. The Signaling Server must be properly configured to use Element Manager, so that the steps of setting and rebooting the Leader are not needed. The Signaling Server requires a reboot only if the Signaling Server IP address information has been changed, such as the node IP address or Signaling Server TLAN network interface IP address. The Voice Gateway Media Cards require a reboot only if the card network interface IP address information has changed.

Transferring the configuration - second node

For a second (or subsequent) node, the process to transfer the node configuration to the cards consists of the following steps:

1. Configure the Leader IP address. See [Procedure 33 "Configuring the Leader IP address for a second or subsequent node" \(page 288\)](#).
2. Transmit the node properties. [Procedure 34 "Transmitting node properties to Leader" \(page 290\)](#).
3. Configure the Follower card. See [Procedure 35 "Configuring the Follower cards" \(page 292\)](#).

Configuring the Leader network interface IP address

Follow the steps in [Procedure 33 "Configuring the Leader IP address for a second or subsequent node" \(page 288\)](#) to configure the network interface IP address of the Leader Voice Gateway Media Card.

Procedure 33**Configuring the Leader IP address for a second or subsequent node****Step Action**

- 1** Access the IPL> or oam> CLI by connecting the COM port of a PC to the RS-232 serial maintenance port on the faceplate of the Leader Voice Gateway Media Card with an NTAG81CA PC Maintenance cable.

If required, use an NTAG81BA Maintenance Extender cable between the PC Maintenance cable and the PC.

Alternatively, connect the NTAG81BA Maintenance Extender cable to the female DB-9 connector of the NTMF94EA ELAN, TLAN RS-232 Ports cable for a more permanent connection to the Voice Gateway Media Card serial maintenance port.

ATTENTION

Never connect two terminals to the faceplate and I/O panel breakout cable serial maintenance port connectors at the same time.

- 2** Use the following communication parameters for the TTY terminal emulation on the PC:
- 9600 baud
 - 8 bits
 - no parity
 - one stop bit
- 3** Observe the Leader card faceplate maintenance display window.
- When the display reads "T:20", the card begins to send BootP requests on the ELAN subnet. A series of dots is printed on the TTY.
- 4** Type +++ to escape from the BootP request.
- 5** At the logon prompt, enter the user ID and password to access the IPL> or oam> CLI:
- If the card is a new card (out of the box), then the user ID is **itgadmin** and the password is **itgadmin**.
 - If the card has been previously connected to the Call Server, then the user ID and password are the PWD1 of the Call Server.
 - If the user ID and password are forgotten, see [Procedure 47 "Resetting the user name and password to default" \(page 332\)](#) to reset the IPL> or oam> CLI Shell username and password.

- 6 When the maintenance window displays "T:21", log into the IPL> or oam> CLI. At the prompt, enter the **setLeader** command to configure the Leader Embedded LAN (ELAN) network interface IP address, Embedded LAN gateway IP address and the Embedded LAN subnet mask:

```
setLeader "xx.xx.xx.xx", "yy.yy.yy.yy", "zz.zz.zz.zz"
```

The three parameters must each be enclosed in double quotation marks. There must be a space after the command and before the first parameter. Put commas and no spaces between the following parameters:

- "xx.xx.xx.xx" = IP address
Enter the same IP address that was entered in the **Embedded LAN IP address** field for **Leader** in the **Cards** menu of the **Edit** window.
- "yy.yy.yy.yy" = Gateway IP address.
Enter the same IP address that was entered in the **Embedded LAN gateway IP address** field in the **Node** menu of the **Edit** window. If there is none, enter the following: "0.0.0.0"
- "zz.zz.zz.zz" = Management LAN subnet mask.
Enter the same address that was entered in the **Embedded LAN subnet mask** field **Node** menu of the **Edit** window.

This step assumes that the new IP Telephony node has already been configured in Element Manager.

- 7 Reboot the Leader Voice Gateway Media Card.

At the IPL> or oam> prompt, enter: **cardReset**, or press the **Reset** button on the faceplate of the Leader Voice Gateway Media Card.



WARNING

Do not use a pencil to reset the Voice Gateway Media Card. The graphite carbon can create an electrical short circuit on the board.

- 8 Check the maintenance display for T:22 to confirm a successful reboot.
- 9 Log into Element Manager.
- 10 In the Element Manager navigator, click **IP Network > Nodes: Servers, Media Cards**.

The **Node Configuration** window appears.

- 11 Click **Transfer/Status** to check the status of the Voice Gateway Media Card.
The **Transfer/Status** window is displayed.
- 12 If the card role is not correct, verify LAN connections and IP configuration.

—End—

Transmit node properties

To transmit the node properties to the Leader, follow the steps in [Procedure 34 "Transmitting node properties to Leader" \(page 290\)](#).

Procedure 34

Transmitting node properties to Leader

Step	Action
1	If changes are made to the node or card configuration data, ensure the data is saved to the Call Server by clicking the Save and Transfer button in the Edit window. A confirmation dialog box opens.
2	Click OK to confirm the save of the node data. The Edit window closes, and the Node Configuration window appears.
3	In the Node Configuration window, click the Transfer/Status button associated with the node. The Transfer/Status window appears.
4	Select the Leader card check box.
5	Click Transfer to Selected Elements. A transfer confirmation dialog box is displayed.
6	Click OK. Element Manager notifies the Leader and the Voice Gateway Media Cards, which then retrieve the CONFIG.INI and BOOTP.TAB files from the Call Server. The Transfer Progress window appears and displays each of the Voice Gateway Media Cards in the node. The Voice Gateway Media Cards retrieve the CONFIG.INI and BOOTP.TAB files from the Call Server.

- 7 When the transfer is complete, click **OK** in the **Transfer Successful** dialog box.

If the transfer is successful for a card, the Status column displays **Complete**. If the transfer is unsuccessful, the Status column displays **Fail**.

- 8 Reset the Leader card in the following situations:
- if the Leader card is a new card (out of the box)
 - if the Leader card is a card that is being configured for the first time as a Leader card
 - if the Leader card IP address has changed
- a. In the navigator, click **IP Network > Maintenance and Reports**.
The **Node Maintenance and Reports** window appears.
- b. Expand the node by clicking the plus sign (+) to the left of the associated node.
- c. Click the **Reset** button for the Leader card.

ATTENTION

If any of the Signaling Server IP address information is changed, the Signaling Server must be rebooted.

Alternatively, restart the card by entering the **cardReset** command at the **IPL>** or **oam>** prompt or by pushing the Reset button on the card faceplate.



WARNING

Do not use a pencil to reset the Voice Gateway Media Card. The graphite carbon can create an electrical short circuit on the board.

—End—

Configure the Follower cards

To configure a Follower card, follow the steps in [Procedure 35 "Configuring the Follower cards" \(page 292\)](#).

Procedure 35
Configuring the Follower cards

Step	Action
1	Check the displays on the card faceplate. - After successfully rebooting, the Leader card is now fully configured with the node properties of the node. The card enters a state of "active Leader". The card faceplate display shows Lxxx, where xxx = the number of IP Phones registered with the LTPS on the Leader card. L000 shows that no IP Phones are registered. - The Follower cards receive their BOOTP configuration information from the Leader card. The Follower card faceplate display shows Fxxx, where xxx = the number of IP Phones registered with the Follower card LTPS. F000 shows that no IP Phones are registered.
2	Reboot the Follower card if the card faceplate does not display FXXX or F000.
3	After all the Follower cards have the correct display on their faceplates, log into Element Manager.
4	Select IP Network > Nodes: Servers, Media Cards . The Node Configuration window appears.
5	Click the Transfer/Status button associated with the node. The Transfer/Status window appears.
6	Select the desired Follower card.
7	Click Transfer to Selected Elements .
8	Click OK to confirm the transfer. The Transfer Progress window appears and displays each of the Voice Gateway Media Cards in the node. The Voice Gateway Media Cards retrieve the CONFIG.INI and BOOTP.TAB files from the Call Server.
9	When the transfer is complete, click OK in the Transfer Successful dialog box. If the transfer is successful for a card, the Status column displays Complete. If the transfer is unsuccessful, the Status column displays Fail .

- 10 If the Follower card is a new card (never used before), reboot the card.

—End—

Upgrade the Voice Gateway Media Card software and IP Phone firmware



WARNING

Before beginning the upgrade, ensure that a PWD1 user name and password has been configured on the Call Server. If there is no PWD1 user name and password, configure them in LD 17. This is necessary to enable logon to the Signaling Server and Voice Gateway Media Cards.

Before beginning, ensure that the following software is installed on the PC:

- Software to extract zipped files (WinZip or equivalent)
- Microsoft Internet Explorer version 6.02 (or later). NetScape Navigator is not supported.

Upgrade procedure steps

The following steps are required to upgrade the Voice Gateway Media Card loadware and IP Phone firmware:

1. Determine the version of the software currently installed on the Voice Gateway Media Card. See ["Determine Voice Gateway Media Card software version" \(page 294\)](#).
2. Determine the version of the IP Phone firmware. See [Procedure 36 "Determining the IP Phone firmware version" \(page 295\)](#).
3. Obtain the latest software from the Signaling Server installation CD. See ["Download the current loadware and IP Phone firmware" \(page 297\)](#).
4. Upload the software and firmware files using the File Upload system utility in Element Manager. See [Procedure 39 "Uploading loadware and firmware files" \(page 298\)](#).
5. Upgrade the Voice Gateway Media Card software. See [Procedure 40 "Upgrading the card loadware" \(page 299\)](#).
6. Restart the Voice Gateway Media Card. See [Procedure 41 "Rebooting the Voice Gateway Media Card" \(page 300\)](#).
7. Upgrade and distribute IP Phones firmware on the Voice Gateway Media Card. See [Procedure 43 "Upgrading the IP Phone firmware" \(page 302\)](#).

Upgrade options

After the Voice Gateway Media Card loadware and IP Phone firmware is verified, there are three upgrade options:

1. Upgrade the Voice Gateway Media Card software only. It may only be necessary to upgrade the Voice Gateway Media Card software. This option is used most frequently; however, verify if an IP Phone firmware upgrade is also required.
2. Upgrade both the Voice Gateway Media Card software and the IP Phone firmware.

Defer restarting the cards until the end of the firmware upgrade. If the IP Phones are registered to the Signaling Server, rebooting the Voice Gateway Media Card does not affect the IP Phones as long as they are not using a gateway channel on the rebooted card. However, if the IP Phones are registered to the Voice Gateway Media Card, resetting the card causes the IP Phone to reboot and re-register.

3. Upgrade only the IP Phone firmware.

In this case, restart all the IP Phones instead of the Voice Gateway Media Cards. To do this, select a single test IP Phone and reset the firmware only on that test IP Phone before completing the procedure on all IP Phones. If the upgrade works properly, use the `umsUpgradeAll` command to complete the upgrade on all the IP Phones.

For more information, see ["Enhanced UNISTim Firmware Download for IP Phones" \(page 79\)](#).

IP Phone firmware requirements

The IP Phone 2001, IP Phone 2002, IP Phone 2004, IP Phone 2007, IP Audio Conference Phone 2033, IP Phone 1110, IP Phone 1120E, IP Phone 1140E, and IP Phone 1150E firmware can be upgraded in the field.

UFTP

IP Phones use UNISTim File Transfer Protocol (UFTP) to transfer the firmware; therefore, the customer network must support UFTP. The customer' network must open UDP port 5105.

If the firmware cannot be transferred due to firewall restrictions (such as when the IP Phone is behind a firewall that has port 5105 blocked), then upgrade the IP Phone with the current firmware version before distributing the telephone.

Determine Voice Gateway Media Card software version

To determine the version of software on the Voice Gateway Media Card, log in to the Signaling Server. At the command line, enter `swVersionShow`.

swVersionShow example

```

oam> swVersionShow Installed Image:  IPL IPL-5.00.08
(MC32S) - Wed Feb 14 19:23:27 EST 2007
Additional Modules:
mainos.sym
BOOTCODE: MGCB5.00
MSP: DSP2AA05
FPGA: MGCFV007
oam>

```

Determine the IP Phone firmware version

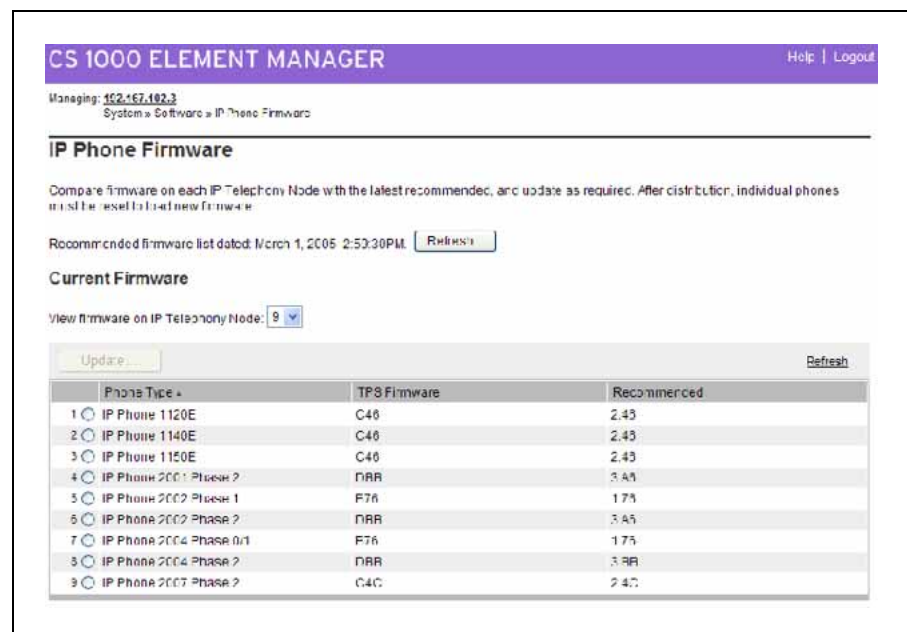
To determine the version of IP Phone firmware on the Voice Gateway Media Card, follow the steps in [Procedure 36 "Determining the IP Phone firmware version" \(page 295\)](#).

Procedure 36**Determining the IP Phone firmware version****Step Action**

- 1 In the Element Manager navigator, click **Software > IP Phone Firmware**.

The **IP Phone Firmware** window appears. See [Figure 71 "IP Phone Firmware window" \(page 295\)](#).

Figure 71
IP Phone Firmware window



The current local firmware versions are displayed in the **TPS Firmware** column. This column changes based on the Node selected.

The recommended firmware versions are displayed in the Recommended column.

—End—

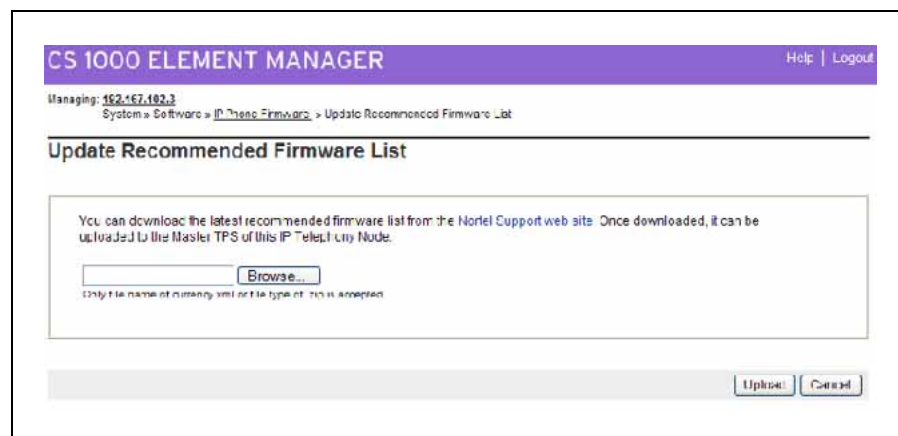
Procedure 37

Updating Recommended Firmware List

Step	Action

1	To check for firmware list updates, click Refresh. The Update Recommended Firmware List window appears. See Figure 72 "Update Recommended Firmware List window" (page 296).

Figure 72
Update Recommended Firmware List window



2	Click the Nortel Support Web site link to obtain the latest firmware file list.
3	Click Save .
4	Click Browse to locate the firmware file list on the PC.
5	Click Upload to upload the firmware file list to the Master TPS of the selected IP Telephony node.

—End—

Download the current loadware and IP Phone firmware

To check for the latest loadware and IP Phone firmware releases on the Nortel Customer Support Web site, follow the steps in [Procedure 38](#) "Downloading loadware and firmware from the Nortel web site" (page 297).

Procedure 38

Downloading loadware and firmware from the Nortel Web site

Step	Action
1	Check the Nortel Customer Support Web site for the latest IP Line loadware and IP Phone firmware releases. The IP Line loadware and IP Phone firmware files are contained in the SSE-5.00.xx Signaling Server CD Image file in the "CS 1000" product list on the Nortel Web site. The file contains: - The IPL500xx.p2, IPL500xx.sa and mc32s loadware files. The IPL500xx.p2 file is the IP Line application for the ITG-P 24-port card, IPL500xx.sa is the IP Line application for the Media Card, and .mc32s is the IP Line application for the Media Card 32S card. - IP Phone firmware files for the IP Phone 2001, IP Phone 2002, IP Phone 2004, IP Audio Conference Phone 2033, IP Phone 2007, IP Phone 1110, IP Phone 1120E, IP Phone 1140E, and IP Phone 1150E. For example, 0602Bxx.BIN (Phase I IP Phone 2004), 0603Bxx.BIN (Phase I IP Phone 2002), and 0604Dnn.BIN (Phase II IP Phone 2001, IP Phone 2002, and IP Phone 2004) firmware files. - A readme.txt file. The readme.txt file explains important considerations for installing the new loadware and firmware versions. The readme file also includes identifying information for the loadware and firmware files such as the date and time, size and checksum.
2	Compare the latest loadware and firmware versions available to the loadware and firmware versions currently installed on the Voice Gateway Media Card and the IP Phones.
3	If more recent files are available, download the SSE-5.00.xx Signaling Server CD Image file.

—End—

Upload the loadware and firmware files to the Signaling Server

The next step is to upload the files from the Element Manager PC to the file server. The **Centralized File Upload** window enables loadware and firmware to be uploaded and stored on the Signaling Server. These files can then be downloaded to the IP Phones and the Voice Gateway Media Cards using the firmware and loadware upgrade functions available from the Software Upgrade menu. The Signaling Server can be used as a central distribution point to load and activate loadware, firmware and patches. To upload the files, follow the step in [Procedure 39 "Uploading loadware and firmware files"](#) (page 298).

For patches, Element Manager does not need to upload to Signaling Server first. The Signaling Server obtains the patch file from the Element Manager PC directly.

Procedure 39

Uploading loadware and firmware files

Step	Action
1	In the Element Manager navigator, click Software > File Upload . The File Upload window appears. See Figure 73 "Centralized File Upload window" (page 298).

Figure 73
Centralized File Upload window

Delete	File Name	Type	Create Time
☐	IPL50008.p2	ITG Pentium workfile	WED FEB 14 22:15:50 2007
☐	IPL50008.sa	Voice Gateway Media Card workfile	WED FEB 14 22:15:52 2007
☐	IPL50008.mc32s	MC32S workfile	WED FEB 14 22:15:54 2007
☐	0602B75.bin	IC004	WED FEB 14 21:27:22 2007
☐	0603B75.bin	IC002	WED FEB 14 21:27:22 2007
☐	0604D3E.bin	IC00x Phase2	WED FEB 14 21:27:22 2007
☐	0621C4C.bin	IC00x Phase2	WED FEB 14 21:27:22 2007

LW/FW file name

Click a button to invoke a command.

2 Click **Browse**.

The **Choose File** window appears. In the Choose File window, select the path and file to upload. Alternatively, enter the path and file name for the file to be uploaded.

Only one loadware or firmware file can be uploaded at a time.

Once selected, the path and file name appear in the text box to the left of the Browse button.

3 Click File Upload.

The file appears in the list at the top of the window when it is uploaded.

To delete older versions of the firmware and loadware files, select the check box associated with the older file and click the **Delete** button located at the top of the column of check boxes.

—End—

Upgrade the Voice Gateway Media Card loadware

After the files are uploaded to the file server, the Voice Gateway Media Cards must be upgraded to the newest loadware version. To upgrade the card loadware, follow the steps in [Procedure 40 "Upgrading the card loadware" \(page 299\)](#).

Procedure 40

Upgrading the card loadware

Step	Action
1	In the Element Manager navigator, click Software > Voice Gateway Media Card. The Voice Gateway Media Card (VGMC) Loadware Upgrade window appears.
2	Expand the node by clicking the plus sign (+) to the left of the node.
3	Select the card to upgrade by selecting the check box to the left of the card information. Element Manager supports upgrading the software on up to four cards at the same time.
4	In the lower part of the window, click the radio button of the most current software version. If the card receiving the upgrade is an ITG-P 24-port line card, select the radio button next to the most current version of the ITG-P 24-port line card software. If the card receiving the upgrade is a Media Card 32S card, select the radio button next to the most current version of the Media Card 32S card software.
5	Click Loadware Upgrade at the bottom left of the window.

- A confirmation dialog box appears.
- 6 Click **OK** to confirm the card upgrade.
The upgrade begins.
The **Loadware Upgrade Progress** window appears.
The status of the upgrade is shown for each of the cards selected to receive the loadware upgrade. This status of the upgrade can be Work in progress, Upgrading, Fail, or Finished.
 - 7 Click **OK**.
 - 8 Repeat steps 3 to 7 to upgrade the other card.

—End—

Reboot the Voice Gateway Media Card

Follow the steps in [Procedure 41 "Rebooting the Voice Gateway Media Card" \(page 300\)](#) to reboot a Voice Gateway Media Card.

Procedure 41

Rebooting the Voice Gateway Media Card

Step	Action
1	Disable the Voice Gateway Media Card.
2	Click the Element Manager navigator, click IP Network > Maintenance and Reports . The Node Maintenance and Reports window appears.
3	To expand the node containing the card to be rebooted, click the plus sign (+) to the left of the node.
4	Click the Voice Gateway Media Card associated Reset button to reboot the card. The cards remain in the "Disabled" state after the upgrade, so a "Reset" command can be used. The cards can also be reset by using a pointed object to press the Reset button on the card faceplate.
5	Click the card Status button in the Node Maintenance and Reports window to verify the status of the Voice Gateway Media Card.
6	Use the LD 32 ENLC command to re-enable the Voice Gateway Media Cards.

- 7 Repeat these steps for each Voice Gateway Media Card that received the software upgrade.

—End—

Re-enable the Voice Gateway Media Card

Follow the steps in [Procedure 42 "Re-enabling the Voice Gateway Media Card"](#) (page 301) to re-enable the Voice Gateway Media Card.

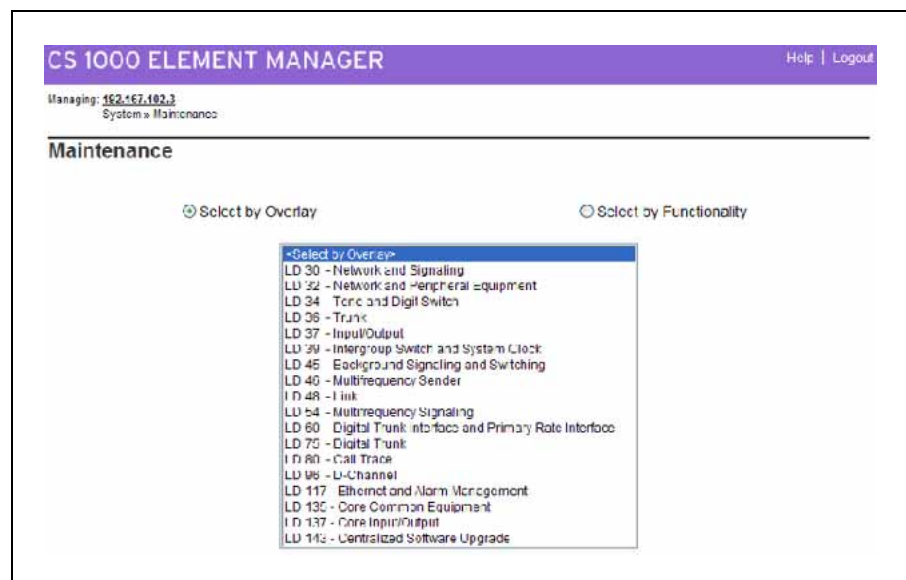
Procedure 42

Re-enabling the Voice Gateway Media Card

Step	Action

1	In the Element Manager navigator, click System > Maintenance . The Maintenance window appears. See Figure 74 "Maintenance window" (page 301).

Figure 74
Maintenance window



2	From the Select by Overlay drop-down list, select LD 32 - Network and Peripheral Equipment . The Network and Peripheral Diagnostics window appears.
3	From the Card Commands drop-down list, select ENLC - Enable and reset card .
4	Under Command Parameters , enter card# .

- 5 Click **Submit**.
- 6 Repeat Steps 3 to 5 for each Voice Gateway Media Card to be re-enabled.

—End—

Upgrade the IP Phone firmware

When the IP Line loadware has been upgraded on the Signaling Server, determine if an IP Phone firmware upgrade is also required. If an upgrade is required, the Signaling Server must be upgraded to the newest IP Phone firmware version.

The firmware upgrade process is enhanced in CS 1000 Release 5.0 to be IP Telephony Node specific.

ATTENTION

A firmware download does not occur with IP Phones performing a Virtual Office logon or Media Gateway 1000B (MG 1000B) logon to a remote system. No firmware upgrade takes place during a Virtual Office logon or MG 1000B user registration with the LTPS. The registration is allowed because the IP Phone firmware version must be 1.33 or later to perform a Virtual Office logon or MG 1000B user registration.

The **umsUpgradeAll** command has no impact on Virtual Office logon IP Phones. These IP Phones are not reset. If the Virtual Office logon is on the same Call Server, then the IP Phone firmware is upgraded after the user logs out. If the Virtual Office logon is between different Call Servers, then the IP Phone just registers back to its home LTPS and follows the normal firmware rules for regular registration.

When the **umsUpgradeAll** command is executed, MG 1000B user IP Phones that are on active calls are flagged. After the IP Phones become idle, the IP Phones are switched by the Call Server back to the MG 1000B for the firmware upgrade.

Follow the steps in [Procedure 43 "Upgrading the IP Phone firmware" \(page 302\)](#) to upgrade IP Phone firmware.

Procedure 43

Upgrading the IP Phone firmware

Step	Action
1	In the Element Manager navigator, click Software > IP Phone Firmware. The IP Phone Firmware window appears. See Figure 75 "IP Phone Firmware window" (page 303).

Figure 75
IP Phone Firmware window

CS 1000 ELEMENT MANAGER Help | Logout

Managing: 102.167.102.3
System » Software » IP Phone Firmware

IP Phone Firmware

Compare firmware on each IP Telephony Node with the latest recommended, and update as required. After distribution, individual phones must be reset to load new firmware.

Recommended firmware list dated: March 1, 2005 2:53:30 PM. [Refresh](#)

Current Firmware

View firmware on IP Telephony Node:

[Update](#) [Refresh](#)

	Phone Type	TPS Firmware	Recommended
1	☐ IP Phone 1120E	C46	2.43
2	☐ IP Phone 1140E	C46	2.43
3	☐ IP Phone 1150E	C46	2.43
4	☐ IP Phone 2001 Phase 2	0000	3.05
5	☐ IP Phone 2002 Phase 1	F76	1.75
6	☐ IP Phone 2002 Phase 2	0000	3.05
7	☐ IP Phone 2004 Phase 0/1	F76	1.75
8	☐ IP Phone 2004 Phase 2	0000	3.05
9	☐ IP Phone 2007 Phase 2	C4C	2.40

- 2 Select the IP Telephony Node from the drop-down list to view the firmware present on the Master Terminal Proxy Server (TPS) of each Telephony Node configured on the Call Server.

- 3 Select the radio button of the IP Phone type to update the firmware for the current IP Telephony node.

The phones listed in the Phone Type column are the phones listed in the Currency file.

- 4 Click **Update**.

The Update Phone Firmware opens for the selected IP Phone type. See [Figure 76 "Update Phone Firmware window" \(page 304\)](#).

Figure 76
Update Phone Firmware window

CS 1000 ELEMENT MANAGER Help | Logout

Managing: 192.167.102.3
 System » Software » IP Phone Firmware » Update Phone Firmware: IP Phone 1120E, IP Telephony Node 9

Update Phone Firmware: IP Phone 1120E, IP Telephony Node 9

Select Firmware File: C46

If the recommended file is not present, you can download it from the [Nortel Support web site](#).

Browse... Upload

Only file type of .zip or .bin is accepted.

Selected Firmware Details

Version: C46

Firmware ID: 0x24

Supported Phones: IP Phone 1120E

The following elements will receive the selected firmware:

Element	IP Address	Type	Status
1 CS1000C_FIV	192.167.102.4	Signaling Server	Not Started

Refresh

- 5 Click the Nortel Support Web site link to download the Currency file from the Nortel Web site.
 - 6 Click **Save**.
 - 7 Click **Browse** to locate the Currency file on the PC.
 - 8 Click **Upload** to upload the Currency file to the Master TPS of the selected IP Telephony node.
- A list of elements from which Element Manager is launched appears.
- 9 Click **Update** to distribute the firmware to the listed elements.
- The IP Phones continue to run the old firmware until each IP Phone re-registers with the Signaling Server containing the new IP Phone firmware.
- 10 Repeat the preceding steps for all the card that have to be upgraded.
- Commands are available from the IPL> or oam> command line to upgrade a single IP Phone immediately, all IP Phones immediately, or schedule all IP Phones to be upgraded at a later time. Before doing this, verify that the Signaling Server has the correct IP Phone firmware version.
- 11 Select an IP Phone for test purposes.

- 12 Telnet to the Signaling Server and then log into the IPL> or oam> command line, and enter the following:

```
isetReset "xxx.xxx.xxx.xxx"
```

where
xxx.xxx.xxx.xxx is the IP Address of the selected IP Phone.
- 13 Monitor the display on the test IP Phone. As the IP Phone upgrades the firmware, note the IP Address of the Signaling Server from which the IP Phone is receiving its upgrade.
- 14 Press the **Services** key (key with globe with arrow pointing East and West. The Services key enables access to the **Telephone Options** list.
 - a. Press **Select** to select Telephone Options.
 - b. Use the **Navigation** keys to scroll to **Set Info**.
 - c. Press the **Select** soft key, then press the **Navigation** keys until it displays **FW Version**. Select the appropriate firmware on the Signaling Server.
- 15 Lift the handset of the IP Phone and make a call to verify the IP Phone works.
- 16 Enable and schedule Firmware Download Maintenance Mode to ensure that the Signaling Server utilize its processing power for the firmware upgrade. For more information, see ["Enhanced UNiStim Firmware Download for IP Phones" \(page 79\)](#).
- 17 Before proceeding, ensure the time on the Signaling Server is configured correctly. Telnet to the Signaling Server and log in. At the IPL> or oam> command line, enter the following:

```
umsUpgradeAll "hh:mm/p"
```

hh:mm/p specifies the time when the upgrade will occur, a represents a.m., and p represents p.m. The time is in Standard format.

For example, umsUpgradeAll "11:30a" or umsUpgradeAll "2:45p".

At the time specified, all the IP Phones registered to the Signaling Server go out of service. This can take several minutes.

Upon completion of the firmware upgrade, the IP Phones are brought back online as they complete their firmware upgrade.

**CAUTION**

If the **umsUpgradeAll** command is used without the time parameter, all IP Phones registered on cards that are logged into are immediately taken out of service. Use the time parameter with the command to prevent this from happening.

After the test IP Phone is working, the **umsUpgradeAll** command does not require the time parameter. However, if the time parameter is not used, the command immediately resets all the IP Phones currently registered on the Signaling Server.

To schedule a specific reset time for the IP Phones, instead of resetting them immediately, check the time on all the Voice Gateway Media Cards. Reset the time, if necessary, to ensure all Voice Gateway Media Cards have the same time, and then issue the **umsUpgradeAll "hh:mm/p"**, where "hh:mm/p" represents the time the upgrade is scheduled to occur.

- 18 At the prompt, verify the IP Phones for are upgraded by entering the following:

`isetShow`
- 19 Inspect the list to ensure all IP Phones have the correct firmware version.
- 20 For any IP Phones that did not upgrade successfully, try one of the following (in order):
 - Use the **isetReset "IP Address"** command.
 - Enter the following combination of key strokes at the telephone console: **release, mute, up, down, up, down, up, mute, 9, release.**
 - Power the telephone off and then on again.

If the upgrade was unsuccessful on any of the IP Phones, the cause is probably due to one of the following:

- The Signaling Server did not upgrade its software successfully.
- An IP Phone firmware version was unable to be upgraded by the Signaling Server in the normal manner.
- The **umsUpgradeAll** command has not been issued.

If the upgrade was unsuccessful, redo the appropriate procedure. If the upgrade is still unsuccessful, contact a technical support representative for further assistance.

—End—

For additional information about configuring the IP Phones, see *IP Phones Fundamentals* (NN43001-368).

Assemble and install an IP Phone

To assemble and install an IP Phone, see *IP Phones Fundamentals* (NN43001-368)..

Change the default IPL CLI Shell password

The IPL> Command Line Interface (CLI) is password-protected to control Telnet access and access to the local maintenance port. The same user name and password also controls FTP access to the Voice Gateway Media Card. The IPL> CLI has a default user name of `itgadmin` and a default password of `itgadmin`.

The default user name and password must be changed as a preventative security measure. See ["IPL> CLI Shell user name and password" \(page 317\)](#) and [Procedure 45 "Configuring the Administrative IP Phone Installer Password" \(page 328\)](#).

Configure the IP Phone Installer Passwords

The IP Phone Installer Password, used when changing the TN on the telephone, controls registration with a virtual line TN on the Call Server. See ["IP Phone Installer Password" \(page 320\)](#) for more information about the IP Phone Installer Passwords.

To enable and set the administrative IP Phone Installer Password, see [Procedure 45 "Configuring the Administrative IP Phone Installer Password" \(page 328\)](#).

If required, enable and configure a temporary IP Phone Installer Password. See [Procedure 46 "Configuring the temporary IP Phone Installer Password" \(page 330\)](#).

Element Manager can also be used to configure the IP Phone Installer Passwords. See ["Setting the IP Phone Installer Password" \(page 377\)](#).

Import node configuration from an existing node

It is possible to import a node and its configuration data from an existing node into Element Manager.

For example, if Node 151 exists, but does not exist on the Call Server, then Node 151 can be imported into Element Manager. Once imported, the node configuration data can be updated and edited.

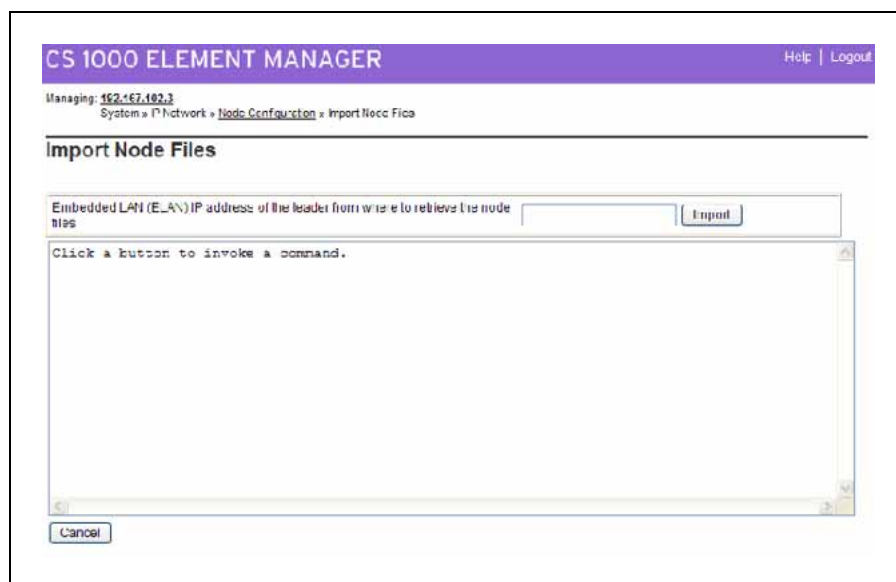
Procedure 44

Importing node files

Step	Action

1	In the Element Manager navigator, click IP Network > Nodes: Servers, Media Cards . The Node Configuration window appears.
2	Click Import Node Files . The Import Node Files window appears. See Figure 77 "Import Node Files window" (page 308).

Figure 77
Import Node Files window



3	Enter the Embedded LAN (ELAN) network interface IP address of the Leader card in the text box. This address is used to retrieve the node files.
4	Click the Import button. If the node already exists on the Call Server, a message appears indicating that the node already exists on the Call Server.

If the node does not exist, Element Manager tries to write the configuration to the Call Server. If it succeeds, a message indicating the import was successful appears. If Element Manager cannot write the configuration to the Call Server, a fail reason appears in the text area of the Import Node Files window.

A message box also appears. In the message box, click the **OK** button to proceed to the **Node Summary** window. The node information can then be viewed and, if necessary, edited.

If the node import is not successful, an error message appears in the text box area.

—End—

IP Line administration

Contents

This section contains the following topics:

- "Introduction" (page 311)
- "IP Line feature administration" (page 312)
- "Password security" (page 317)
- "IP configuration commands" (page 333)
- "TLAN network interface configuration commands" (page 333)
- "Display the number of DSPs" (page 334)
- "Display IP Telephony node properties" (page 334)
- "Display Voice Gateway Media Card parameters" (page 335)
- "Packet loss monitor" (page 338)
- "Transfer files using the CLI" (page 338)
- "Download the IP Line error log" (page 340)
- "Reset the Operational Measurements file" (page 340)

Introduction

This chapter explains how to administer IP Line and the Voice Gateway Media Cards on the CS 1000 system.

Administration procedures include activities such as monitoring the system status, operational reports, performing upgrades, changing configuration, and adding, changing, and removing cards. Administration does not include engineering, provisioning, initial installation and configuration, maintenance, or troubleshooting.

The Voice Gateway Media Card provides four administration interfaces:

- Telephony Manager (TM) 3.1

TM IP Line application provides a GUI to the Voice Gateway Media Card. TM 3.1 is used to provide OM reports.

- Element Manager

Element Manager is a Web server that provides a GUI using the Internet Explorer 6.0.2600 (or later) Web browser. Element Manager is used to Telnet to the card, install and upgrade software and firmware, configure alarm event reporting, view and update card property and configuration data, add new cards to a node, schedule reports, and other related tasks.

- IPL> and oam> Command Line Interface (CLI)

Use the CLI to display card and node status, change passwords, check channel states, and other card information. The CLI is also used for expert level support and debug. The prompt for the CLI on the ITG-24 port line card and Media Card 32-port is IPL>. The prompt for the CLI on the Media Card 32S is oam>. Access the CLI through a direct serial connection to the I/O panel serial port, the Maint Port on the faceplate, or through a Telnet session. Use a VT-100 terminal emulation program set to 9600 baud, 8 bits, no parity, one stop bit.

- Overlays

IP Line feature administration

Corporate Directory

LD 11 accepts Class of Service (CLS) CRPA/CRPD for IP Phones.

Table 75

Corporate Directory: LD 11 configuration

Prompt	Response	Description
REQ	NEW CHG	Add new data or change existing data.
TYPE:	2001P2, 2002P1, 2002P2, 2004P1, 2004P2, 2050PC, 2050MC, 2033, 2007, 1110, 1120, 1140, 1150, 2210, 2211, 2212, 6120, 6140	Enter terminal type.
TN	1 s	Enter IP Phone TN.
...	...	...
CLS	CRPA CRPD	Enable/Disable the Corporate Directory feature for this TN. Corporate Directory is not supported on the IP Phone 2001, IP Audio Conference Phone 2033, and IP Phone 1110.

The Call Server service change does not affect Corporate Directory immediately. If an IP Phone is in Corporate Directory mode, and there is a service change to configure CLS as CPRD, then the current display and key handling should not be affected. The changed CLS occurs only when the user quits the Corporate Directory application and enters again.

For more information about the operation of the Corporate Directory feature, see *Telephony Manager 3.1 System Administration (NN43050-601)*.

Private Zone configuration

DSP channels and IP Phones are set as Shared or Private based on zone configuration. This is accomplished through the parameter `zoneResourceType` in the zone configuration commands in LD 117.

The `<zoneResourceType>` parameter specifies the zone to be either shared or private.

A zone is configured in LD 117 as follows:

```
NEW ZONE <zoneNumber> [<intraZoneBandwidth>
<intraZoneStrategy> <interZoneBandwidth> <interZoneStrategy>
<zoneResourceType>]
CHG ZONE <zoneNumber> [<intraZoneBandwidth>
<intraZoneStrategy> <interZoneBandwidth> <interZoneStrategy>
<zoneResourceType>]
```

By default, a zone is configured as Shared (`zoneResourceType=shared`).

Virtual Office

The IP Phone Virtual Office feature uses the Station Control Password (SCPW) feature. The SCPW password can be maintained either through LD 11 administration or by the user if Flexible Feature Code (FFC) code access is configured. If the SCPW is not configured for a TN registering by means of the Virtual Office feature, the logon is rejected. An appropriate error message is displayed to alert the user that a password must be configured.

Enable the SCPW in the Customer Data Block (CDB) by configuring the length of the SCPW (`scpl`). The SCPW must be at least four digits.

To logon using Virtual Office, the TN associated with the current IP Phone registration must be configured with the CLS VOLA (Virtual Office logon Allowed). The TN associated with the User ID for the logon must be configured with the CLS VOUA (Virtual Office User Allowed).

Two CLSs restrict Virtual Office usage. The two classes of services are:

- VOLA/VOLD – defines whether this TN (physical IP Phone) allows/disallows a Virtual Office logon option.
- VOUA/VOUD – defines if a specific remote user can log onto this TN (allows/disallows a particular user to logon using Virtual Office).

Table 76 "LD 11 Virtual Office Login for IP Phones" (page 314) shows the CLS for LD 11.

Table 76
LD 11 Virtual Office logon for IP Phones

Prompt	Responses	Description
REQ:	NEW CHG	Add new data or change existing data.
TYPE:	2001P2, 2002P1, 2002P2, 2004P1, 2004P2, 2050PC, 2050MC, 2033, 2007, 1110, 1120, 1140, 1150, 2210, 2211, 2212, 6120, 6140	Enter terminal type. The system accepts this response if it is equipped with packages 88 and 170. The IP Phone 2001, IP Audio Conference Phone 2033, IP Phone 1110, IP Phone 2002, IP Softphone 2050, and MVC 2050 are also restricted by the IP Phone License setting.
CUST	xx	Customer number as defined in LD 15
BUID	<user id>	Dialable DN, main office user ID
MOTN	l s c u	Enter X to delete. Main Office Terminal Number Where l = loop, s = shelf, c = card, u = unit. Accept default for Media Gateway 1000B, or Small System Main Office
...	...	...
CLS	(VOLA) VOLD	Virtual Office logon operation is allowed/denied on this TN
CLS	(VOLA) VOUD	Allow/Disallow Virtual Office user on this TN using other IP Phone

Emergency Services Access while logged in to Virtual Office

If 911 is dialed while logged into Virtual Office, the LTPS re-directs the 911 call to the local area 911 service (PSAP), not the remote Call Server 911 service. [Table 77 "e911 process for IP Phones logged in to Virtual Office" \(page 315\)](#) describes the process.

Table 77
e911 process for IP Phones logged in to Virtual Office

Step	Description
1	The LTPS aborts the call on the remote Call Server.
2	The LTPS displays <i>Emergency Call</i> on the IP Phone.
3	The LTPS logs the IP Phone out of Virtual Office.
4	The LTPS reconnects to the local Call Server.
5	The LTPS restarts the 911 call, thus reaching the correct PSAP. The extra processing adds 5 seconds to the call setup time.
6	After the emergency call ends, the IP Phone remains registered to the Home LTPS as a normal telephone, in case the PSAP makes a call back to the originator of the emergency call. After the IP Phone is redirected to its Home Site, it is not allowed to initiate a new operation for five minutes. This prevents the user from accidentally dialing the emergency DN and hanging up. In this case, the emergency response personnel might call back to confirm the accidental call (and thus confirm that there is no emergency). If the IP Phone were allowed to immediately resume a Virtual Office logon to another site, it could not receive the call back. If the local TN has another IP Phone Virtual Office logged into it when it comes back, the non-emergency IP Phone is pre-empted. If this occurs, ESxxxx messages are generated on the system TTY.

Emergency Services Access while logged out of Virtual Office

If 911 is dialed while logged out of Virtual Office, the LTPS redirects the 911 call to the local area 911 service (PSAP), not the remote Call Server 911 service. The Call Server is provisioned with Emergency Service Access Terminal Numbers (ESTN). The ESTN is used to register the IP Phone with

the Call Server. The logged out IP Phone can make ESA calls only. See [Table 78 "e911 process for IP Phones while logged out of Virtual Office" \(page 316\)](#).

Table 78
e911 process for IP Phones while logged out of Virtual Office

Step	Description
1	The LTPS aborts the call on the remote Call Server.
2	The LTPS displays <i>Emergency Call Only</i> on the IP Phone.
3	The LTPS registers the IP Phone to the Call Server when the IP Phone goes off-hook, or when the Primary DN key, Handsfree key, or Headset key (IP Phone 1150E) are pressed. The Call Server allocates an ESTN. and maps the ESTN key to the logged out IP Phone Primary DN. A 60-second timer is created for the logged out IP Phone which has an ESTN allocated. If the ESA number is not dialed before the time expires, the ESTN is released and the IP Phones returns to the original logged out state. The user must re-initiate the call.
4	The LTPS starts the ESA call, thus reaching the correct PSAP. The timer is reset to a preconfigured period of time (default 20 minutes) in case the PSAP makes a call back to the originator of the emergency call.
5	When the timer expires, the LTPS unregisters the IP Phone from the Call Server. The IP Phone returns to the original logged out state and the IP Phone ESTN becomes available for other ESA calls from any other logged out IP Phone.

Configuration

The Emergency Services Access (ESA) feature must be configured on all nodes participating in Virtual Office logons. ESTN range must be specified in LD 24, and then configured in LD 11.

For more information, see *Emergency Services Access Fundamentals (NN43001-613)* and *Branch Office Installation and Commissioning (NN43001-314)*.

802.1Q

The 802.1Q support for IP Phones is configured and controlled using the telephone user interface or DHCP. The DHCP approach eliminates the requirement to manually set the VLAN ID as part of the installation. The configuration is composed of two items: setting the "p" bits and setting the VLAN ID.

TM 3.1 and Element Manager have two fields for setting 802.1Q support:

- Enable 802.1Q support: A check box that, when checked, sets the priority bits to the value specified by the next item. If the check box is unchecked, the IP Phone sends out the default priority of 6.

- 802.1Q Bits value (802.1p): A 802.1Q priority bit value field that sets the value the IP Phone sent out in the priority field. The range is 0 to 7.

Password security

The following password security features should be configured to work with the IP Line application:

1. SNMP community strings
2. IPL> or oam> CLI Shell password
3. Call Server Level 1 Password (PWD1)
4. IP Phone Installer Password

The SNMP community strings are configured for the entire system. IPL> and oam> CLI Shell passwords and the Call Server Level 1 Password (PWD1) operate at the card level. The IP Phone Installer Password works at the node level.

- The SNMP community strings are configured centrally on the Call Server and synchronized to all devices, including the Voice Gateway Media Cards.
- The IPL> and oam> CLI Shell password is synchronized with the PWD1.
- The Level 1 Passwords (PWD1) is set at the Call Server and is sent to all Voice Gateway Media Cards in the node.
- The IP Phone Installer Password is first applied to one Voice Gateway Media Card in the node, and then is applied to all the Voice Gateway Media Cards in the node.

SNMP community strings

SNMP community strings are required to access the Voice Gateway Media Card.

Element Manager is used to configure the community strings for CS 1000 systems.

CLI Shell user name and password

The Command Line Interface (CLI) is password-protected to control Telnet access and access to the local maintenance port. The same user name and password also controls FTP access to the Voice Gateway Media Cards.

logon banner

The IP Line logon banner information includes the IP Line Voice Gateway Media Card loadware version, ELAN network interface IP address, card type, firmware version, current time and date, system name, system location, and system contact.

The following information is an example of the logon banner displayed on the Media Card:

```
logon:
Password
Welcome to the IP Line command line.
Software Version: IPL-5.00.01
Management IP: 47.11.216.216
Host Type: Media Card
Firmware Version: ITG Firmware RIs 5.7
SysName: ITG Line
SysLocation: TN 10 0
SysContact: designer
OS Time: Date (04/03/2005) Time (09:07:43)
Use "logout" to logout.
Idle session timeout = 20 minutes.
IPL>
```

Password guessing protection

Password guessing protection helps to block a hacker from attempting to log into the Voice Gateway Media Card shell by making repeated attempts to guess the shell user ID and password.

The password guessing protection is applicable to either a tip session (direct maintenance port-connected TTY session) or a Telnet session.

The password guessing protection feature is described as follows:

- There is a logon failure threshold of 3 and a lockout period of 10 minutes. This is not user-configurable.
- Password guessing protection is enabled by default when the card starts the first time. The protection can be disabled and re-enabled at the VxWorks shell. Entering the `shelllogonProtectSet 0` command disables the protection and `shelllogonProtectSet 1` enables it.
- When the logon failure threshold is exceeded (by 3 consecutive failed logon attempts), the system raises an "ITG1038" critical alarm. This alarm is sent to indicate the card logon has been locked due to too many incorrect password entries.

Alarm value = ITG alarm 38

perceivedSeverity = Critical

probableCause = Unauthorized maximum access attempts

Alarm text = IPL logon protection (logon locked)

When the 10 minute timer expires for the lockout period, the system raises an "ITG5038" cleared alarm. The clear message is sent after the lockout period expires.

perceivedSeverity = Cleared

probableCause = Unauthorized maximum access attempts
Alarm text = IPL logon protection (logon available)

- There is no online indication or warning during the failed logon attempt lockout state. Everything appears the same to the user trying to logon. The user is not informed that logon blocking has been activated. The logon is ignored for 10 minutes.

Both the critical and cleared alarms are sent as SNMP traps to the system administrator. For security reasons, these two alarms do not call the syslog function as the other itgAlarms do, so no syslog message is displayed on the console or written in the syslog file.

- On the Voice Gateway Media Card, the faceplate displays GO38 (ITG1038) when the ITG1038 alarm is received, because it is a critical alarm. The ITG5038 clears GO38 from the faceplate when the 10 minute timer expires.

Node password synchronization

The BOOTP.TAB, CONFIG.INI, and IP Phone firmware files must be the same on all cards in the system. The cards that can be in the system are the ITG-P 24-port line card, the Media Card 32-port line card MC 32S card, and the Signaling Server. To maintain a consistent configuration within the system, files are transferred from Leader 0 to the Follower cards using FTP.

In order for the FTP process to work correctly, all the cards in a node must be synchronized with the same user ID and password. After the Voice Gateway Media Cards are synchronized with the Call Server, the user logon is synchronized with the Call Server PWD1. The cards can then only be accessed by using the Call Server Level 1 Password (PWD1) user ID and password.

A card uses its user ID and password when it tries to access another card to FTP files. The FTP fails unless all the cards have the same user ID and password, due to failed user authentication. Therefore, a unique user ID and password should be used within one system. Because most applications (except the NRS) communicate directly with the Call Server, the Call Server Level 1 PWD1 user ID and password is the unique password among all platforms.

Level 1 Password (PWD1)

The minimum password length on the Call Server is four characters. The minimum password on the Voice Gateway Media Card and the Signaling Server is eight characters.

For example, if the Call Server PWD1 is "0000", it is padded to the right with the four space characters to become "0000 ". This is done automatically by the software. It is not necessary to manually add the spaces.

Password Updates

The Call Server PWD1 user ID and password is sent to all Voice Gateway Media Cards at the following times:

- when the Voice Gateway Media Cards initially establish a connection with the Call Server across the ELAN subnet
- when an EDD operation is performed on the Call Server

After the PWD1 information is downloaded from the Call Server, it is saved in the Voice Gateway Media Card NVRAM. If a Voice Gateway Media Card has not yet established a link with the ELAN subnet, the user ID and password that are currently stored in the card NVRAM are used to log in. The user ID and password might not match the PWD1 on the Call Server because the Call Server has not yet downloaded the current PWD1 to the Voice Gateway Media Card. After the ELAN subnet connection is established, the user ID and password are synchronized on all Voice Gateway Media Cards, and the new user ID and password are saved in the card NVRAM.

Because all Voice Gateway Media Cards automatically receive the user ID and password from the Call Server, the password can be changed in a single location, the Call Server CLI. This eliminates the need to change the password on every card in the node (just change the password once on the Call Server). When the password is changed at the Call Server, the password is automatically sent to all the Voice Gateway Media Cards.

A user can change the user ID and password logon on any card using the `shellPasswordSet` CLI command. However, updates from the Call Server overwrite the card user ID and password in the NVRAM.

If the PWD1 is changed and an EDD operation is not performed, the cards can contain a mixture of old and new passwords. This could happen if a new card is plugged in, an existing card reboots or loses and reestablishes its ELAN subnet connection. Nortel recommends that an EDD be performed when the PWD1 password is changed on the Call Server. Performing an EDD ensures that all cards have the new PWD1 user ID and password.

For more information about the PWD1 Level 1 password, see the *LD 17 Gate Opener PWD (Password)* section in *Software Input Output Administration (NN43001-611)*.

IP Phone Installer Password

An IP Phone displays the node ID and Terminal Number (TN) of the IP Phone for 5 seconds as the IP Phone boots up. Password protection controls who can change the TN on the IP Phone. The IP Phone Installer Password protection controls registration with a virtual line TN on the Call Server.

The IP Phone Installer Password can also be configured using the CLI commands in Element Manager. See ["Setting the IP Phone Installer Password" \(page 377\)](#).

For further information about password protection support on an IP Phone, see *IP Phones Fundamentals (NN43001-368)*.

Administrator IP Phone Installer Password

This feature adds basic IP Phone Installer Password protection on the IP Phones to control registration with a virtual line TN on the Call Server. This feature does not provide a user password or a Station Control Password for IP Phones.

IP Phone 2004, IP Phone 2007, IP Phone 1140E, IP Phone 1150E, WLAN Handset 2210/2211/2212/6120/6140

When the password is configured, the IP Phone screen shows:

1. The four digit Node ID and a Password prompt instead of the Node ID and TN fields. For example, see [Figure 80 "IP Phone 2004/ IP Phone 2007 registration with password checking" \(page 325\)](#) and [Figure 78 "IP Phone 2004/IP Phone 2007 registration with no password checking" \(page 323\)](#).
2. When the user enters the password, an asterisk (*) is displayed for each digit entered. The password is not shown.
3. After the Node ID and Password are entered, the user presses OK. If the password passes the Connect Server authentication, a screen is displayed with the TN field. For example, (see [Figure 80 "IP Phone 2004/ IP Phone 2007 registration with password checking" \(page 325\)](#)).

IP Phone 2001, IP Phone 2002, and IP Audio Conference Phone 2033, IP Phone 1110, and IP Phone 1120E

When the password is configured, the IP Phone screen shows:

- The four digit Node ID screen is displayed first. For example, see [Figure 81 "IP Phone 2001/IP Phone 2002/IP Audio Conference Phone 2033 registration with password checking" \(page 325\)\)](#).
- The user is then prompted with the Password screen instead of the TN field screen. For example, see [Figure 81 "IP Phone 2001/IP Phone 2002/IP Audio Conference Phone 2033 registration with password checking" \(page 325\)](#) and [Figure 79 "IP Phone 2001/IP Phone 2002/IP Audio Conference Phone 2033 registration with no password checking" \(page 323\)](#).
- When the user enters the password, an asterisk (*) is displayed for each digit entered. The password is not shown.

- After the Password is entered, the user presses OK. If the password passes the Connect Server authentication, a screen is displayed with the TN field. For example, see [Figure 81 "IP Phone 2001/IP Phone 2002/IP Audio Conference Phone 2033 registration with password checking"](#) (page 325).

If the Node ID and Password are not entered, the registration continues after 5 seconds and the TN is not displayed.

If an invalid Node ID password is entered, the Node ID and Password screen is displayed again. This screen is re-displayed a maximum of two times, giving the technician a total of three chances to enter the password. After three failed attempts, the registration continues as if there were no password entries. Reboot the IP Phone and try again if more tries are needed.

If a zero length (null) password is entered, then the Node ID, TN, and Password screens are not displayed on the IP Phone during the registration process. This provides the most security as it prevents any entry of passwords or TNs from the IP Phone.

Temporary IP Phone Installer Password

A Temporary IP Phone Installer Password can be configured, which provides temporary user access to the TN for configuration.

A temporary password removes the need to distribute the Node password and then change the password afterwards. The temporary password is automatically deleted after it has been used the defined number of times or when the duration expires, whichever comes first.

The following are examples of situations where the Temporary IP Phone Installer Password can be used:

- A department is installing an IP Softphone 2050. The technician creates a temporary password, sets an appropriate number of uses (such as allowing two logons for each IP Softphone 2050 in case a problem occurs the first time) and sets the duration to expire by the end of the weekend. The password access automatically ends before Monday morning (or sooner if the number of uses expires).
- A telecommuter needs to install an IP Phone. The technician provides the temporary password that expires the next day or after two uses. When the IP Phone Installer Password protection is enabled, the Set TN is not displayed as part of the Set Info submenu of the Telephone Option menu. The IP Phone TN can be retrieved on the core CPU through the LD 20 PRT DNB and LD 32 IDU, or LD 80 TRAC, PDT>, or LDB>**rlmShow**. It can also be found on the Voice Gateway Media Card through IPL> or oam>**isetShowByIP**.

Registration screens with TN password feature

The following screens show the existing TN entry screen that appears when the IP Phone registers:

- [Figure 78 "IP Phone 2004/IP Phone 2007 registration with no password checking" \(page 323\)](#) shows an example of the display the screen on the IP Phone 2004/IP Phone 2007 if password protection is disabled or not configured. This also applies to IP Phone 1140E, IP Phone 1150E, and WLAN Handset 2210/2211/2212/6120/6140.
- [Figure 79 "IP Phone 2001/IP Phone 2002/IP Audio Conference Phone 2033 registration with no password checking" \(page 323\)](#) displays the screen on the IP Phone 2001/IP Phone 2002/ IP Audio Conference Phone 2033 if password protection is disabled or not configured. This also applies to IP Phone 1120E and IP Phone 1110.

Figure 78
IP Phone 2004/IP Phone 2007 registration with no password checking

Page 1:

Node: _ _ _ _			
TN: _ _ _ _ . _ _ _ . _ _ _			
OK	BKSpace	Clear	Cancel

Figure 79
IP Phone 2001/IP Phone 2002/IP Audio Conference Phone 2033 registration with no password checking

Page 1:

Node: _ _ _ _			
OK	BKSpace	Clear	Cancel

Page 2:

TN: _ _ _ _ . _ _ _ . _ _ _			
OK	BKSpace	Clear	Cancel

When the TN password protection feature is configured with a non-zero length password and is enabled:

- [Figure 80 "IP Phone 2004/ IP Phone 2007 registration with password checking" \(page 325\)](#) shows the IP Phone 2004 /IP Phone 2007 TN entry screens. This also applies to IP Phone 1140E, IP Phone 1150E, and WLAN Handset 2210/2211/2212/6120/6140.
 - [Figure 80 "IP Phone 2004/ IP Phone 2007 registration with password checking" \(page 325\)](#) displays the Node ID and Password. Note the Password entry input field is blank (underscores are not displayed). Therefore, the maximum length of the password is not disclosed. This also applies to IP Phone 1140E, IP Phone 1150E, and WLAN Handset 2210/2211/2212/6120/6140.
 - If the correct password is entered, the TN is displayed.
- [Figure 81 "IP Phone 2001/IP Phone 2002/IP Audio Conference Phone 2033 registration with password checking" \(page 325\)](#) shows the IP Phone 2001/IP Phone 2002/IP Audio Conference Phone 2033 TN entry screens. This also applies to IP Phone 1120E and IP Phone 1110.
 - [Figure 81 "IP Phone 2001/IP Phone 2002/IP Audio Conference Phone 2033 registration with password checking" \(page 325\)](#) displays the Node ID. The Node ID is entered and the user presses OK. This also applies to IP Phone 1120E and IP Phone 1110.
 - [Figure 81 "IP Phone 2001/IP Phone 2002/IP Audio Conference Phone 2033 registration with password checking" \(page 325\)](#) displays the Password entry window. Note the Password entry input field is blank (underscores are not displayed). Therefore, the maximum length of the password is not disclosed. This also applies to IP Phone 1120E and IP Phone 1110.
 - If the correct password is entered, the TN is displayed.

Figure 80
IP Phone 2004/ IP Phone 2007 registration with password checking

Page 1:

Node: _ _ _ _
Password:
OK BKSpace Clear Cancel

Page 2:

TN: _ _ _ . _ _ _ . _ _ _ . _ _ _
OK BKSpace Clear Cancel

Figure 81
IP Phone 2001/IP Phone 2002/IP Audio Conference Phone 2033 registration with password checking

Page 1:

Node: _ _ _ _
OK BKSpace Clear Cancel

Page 2:

Password:
OK BKSpace Clear Cancel

Page 3:

TN: _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
OK BKSpace Clear Cancel

IP Line CLI commands for password control

The IP Phone Installer Passwords are configured on any Voice Gateway Media Card in the node. The IP Phone Installer Password is configured and administered using a set of six IPL> CLI or oam> commands:

- nodePwdSet "password"

- `nodePwdShow`
- `nodeTempPwdSet "temppwd", uses, <time>`
- `nodeTempPwdClear`
- `nodePwdEnable`
- `nodePwdDisable`

The commands begin with `node` as they work at the node level. For detailed information about these commands, see [Table 99 "IP Phone Installer Password commands" \(page 431\)](#).

When an IP Telephony node is first installed, the IP Phone Installer Password is not defined or enabled by default. To prevent users from inadvertently re-configuring the Node ID and TN on their IP Phones, enable the IP Phone Installer Password after the IP Phone is initially installed and the system is in service.

Password security controls access to an IP Phone TN for the purpose of registering to a different virtual line TN on the Call Server after the IP Phones have been installed. A password is not encrypted by the IP Phone or the Voice Gateway Media Card.

By default, when a node is initially installed, the administrative password and the temporary password are not defined, and the password feature is disabled.

The `nodePwdSet "password"` command configures and enables the password. When the password is enabled and configured, the screen on the IP Phone displays the four digit Node ID and a Password prompt, instead of the Node ID and TN fields.

**WARNING**

The `nodePwdSet` command with no "password" parameter enables the administrator password and sets a null (zero-length) password.

Enabling the administrator password and setting a null password makes it impossible to install the IP Phones because the Node ID and TN prompts are not displayed on the telephone screen.

Always specify the password parameter when issuing the `nodePwdSet` command. This password parameter is 6 to 14 digits. The valid characters are 0 to 9, *, and #.

If the **nodePwDEnable** command is entered before the password is set using the **nodePwDSet** command, the password is also enabled with a null (zero-length) password and as a result, the password and TN prompts are also never displayed on the IP Phones.

The administrator normally uses the Administrative IP Phone Installer Password if it is necessary to install a new telephone or change the configuration (node ID and TN) of an existing telephone.

If an IP Phone cannot be installed because a prompt for a node ID and TN does not appear, log into a Voice Gateway Media Card and check the status of the password using the **nodePwDShow** command.

ATTENTION

The administrator can create a temporary IP Phone Installer Password for experienced users who are delegated to install IP Phones. If a null administrator password is set and a temporary password is created, the temporary password overrides the null administrator password.

To suppress all password prompting to reconfigure the Node ID and TN, clear the temporary password using the **nodeTempPwDClear** command. Also, configure the administrative password to a null password using the **nodePwDSet** command with no "password" parameter specified.

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

Configure the IP Phone Installer Passwords

The IP Phone Installer Passwords are configured on one Voice Gateway Media Card or on the Signaling Server in the node. The passwords are then applied to all cards in the node.

If the IP Phone Installer Password is configured on the Signaling Server, or on the Voice Gateway Media Card with which, for example, an IP Phone 2004 is registered, the IP Phone's **Telephone Options > Diagnostics** submenu is locked and the **Set Info** submenu does not display the **Set IP Information** or **Ethernet Information** options.

Administrative IP Phone Installer Password

The Administrative IP Phone Installer Password is used by the administrator to install a new IP Phone or change the configuration (node ID and TN) of an existing IP Phone.

To configure the Administrative IP Phone Installer Password, follow the steps in [Procedure 45 "Configuring the Administrative IP Phone Installer Password" \(page 328\)](#).

Procedure 45**Configuring the Administrative IP Phone Installer Password****Step Action**

- 1 Connect to any Voice Gateway Media Card in the node.
- 2 logon to the IPL> or oam> CLI and type the **nodePwdShow** command. This command displays the settings of the IP Phone Installer (node) password.

If in the default state, the IP Phone Installer Password has never been set. The **nodePwdShow** command displays the following:

```

NodeID PwdEna  Pwd      TmpPwd  Uses      Timeout
=====
123      No              0d 0h 0m 0s

```

where

NodeID – the IP Phone Installer Password configuration applies to all Voice Gateway Media Cards on the same TLAN that belong to this Node ID.

PwdEna – by default the cards should be in disabled state (PwdEna=No). The PwdEna setting specifies the enabled (Yes) or disabled (No) state of the IP Phone Installer Password.

Pwd – this is the Administrator IP Phone Installer Password. In the default state, the Administrator password is null (zero-length).

TmpPwd – this is the temporary IP Phone Installer Password. In the default state, the temporary password is null.

Uses – the Uses parameter applies to the temporary IP Phone Installer Password. In the default state, this setting is null. If the card is not in the default state, the Uses parameter is a numeric value from 0 –1000. This number specifies the remaining number of uses for the temporary password. If zero is entered for the Uses parameter when setting the temporary password, the Time parameter is mandatory. When the Time parameter is in effect, the password expiration is based on time instead of the number of uses.

Timeout – the Timeout heading corresponds to the Time parameter of the temporary IP Phone Installer Password. In the default state, the Time is null. If the card is not in the default state, this setting specifies the duration in hours in which the temporary password is valid. The range is 0 – 240 hours (which is a maximum of 10 days). The number specified under Timeout indicates the remaining time to expire of the temporary password. The Time parameter is optional if the Uses parameter is non-zero. The Time parameter is mandatory if the Uses parameter is set to zero.

If both the Uses and Time parameters are entered, the password expires based on whichever happens first; that is, the number of Uses is reduced to zero or the Time has expired. If both the Uses and Time parameters are entered and are set to zero, it is the same as not configuring the temporary password.

3 Configure the Administrator IP Phone Installer Password.

The `nodePwdSet <"password">` command enables and configures the administrator password. The `<password>` parameter can be null, or 6 to 14 digits in length. The valid characters are 0 to 9, *, and #. This command can be entered at any time. The new password entered simply overwrites the previous password.

Configure the password, first with a null password and then with a password specified.

4 Type `nodePwdSet` at the `IPL>` prompt.

Note that no password parameter is specified.

Type `nodePwdShow` to see the following:

```

NodeID PwdEna  Pwd      TmpPwd  Uses    Timeout
=====
123      No                0d 0h 0m 0s

```

PwdEna – the password is now enabled (PwdEna=Yes).

Pwd – if no `<"password">` parameter specified, the administrator password is null. IP Phones cannot be installed when the password is null. A null password causes the node ID and Password screen to be skipped during restart.



WARNING

The `nodePwdSet` command, with no parameter, by default enables the administrator password and sets a null (zero-length) password.

IP Phones cannot be installed if the administrator password is enabled and set to null.

Always specify the password parameter to install IP Phones.

5 Type `nodePwdSet <"password">` at the `IPL>` or `oam>` prompt, where the password parameter is 6 to 14 digits in length.

The valid character are 0-9 * #. For this example, use "1234567" as the password.

6 Type `nodePwdShow` to see the following:

```

      NodeID  PwdEna   Pwd      TmpPwd
Uses  Timeout  =====  =====  =====
=====  =====  =====  123      No
1234567
                        od 0h 0m 0s

```

PwdEna – the administrator password is enabled (PwdEna=Yes).

Pwd – the administrator password, 1234567, is displayed.

Always specify the <password> parameter when entering the **nodePwdSet** command.

The **nodePwdEnable** and **nodePwdDisable** commands enable and disable the administrative IP Phone Installer Password, respectively.

—End—

Temporary IP Phone Installer Password

A temporary IP Phone Installer Password can be configured. This enables temporary user access to the TN for configuration. A temporary password removes the need to distribute the administrative (node) password and then the need to change it afterwards. If there is a null administrator password configured and a temporary password is created, the temporary password overrides the null administrative password.

The syntax for temporary IP Phone Installer Password specifies:

- the password
- the number of times that the password can be entered
- the time that the password is valid

To configure a temporary IP Phone Installer Password, follow the steps in [Procedure 46 "Configuring the temporary IP Phone Installer Password" \(page 330\)](#).

Procedure 46

Configuring the temporary IP Phone Installer Password

Step	Action
1	Type nodeTempPwdSet <"password">, <uses>, <time> at the IPL> or oam> prompt, where "password" is the temporary password string 6 to 14 digits in length, uses is the value from 0 to 1000, and time is between 0 and 240 hours. For example, nodeTempPwdSet "987654", 15, 3
2	Type nodePwdShow to see the following:

NodeID	PwdEna	Pwd	TmpPwd	Uses
Timeout	=====	=====	=====	=====
=====	=====	123	No	1234567
987654	15	0d 0h 0m 0s		

The temporary password is automatically deleted after it has been used the defined number of times (Uses) or when the duration expires (Timeout), whichever comes first. However, to delete the temporary password before the number of uses or time has expired, type the **nodeTempPwdClear** command at the IPL> or oam prompt.

- 3** Type **nodePwdShow** to verify that the temporary password has been deleted.:

NodeID	PwdEna	Pwd	TmpPwd
Uses Timeout	=====	=====	=====
=====	=====	=====	123 No
1234567		0d 0h 0m 0s	

—End—

Default user name and password

The IPL> CLI has a default user name of **admin1** and a default password of **0000**. The default user name and password must be changed as a preventative security measure. The **shellPasswordSet** command changes the IP Line username and password. But because the password is synchronized with the Call Server, Nortel recommends you change the PWD1 password.

Reset the CLI Shell user name and password

If the authorized system management personnel do not have the current IPL> CLI Shell user name and password, reset the user name and password to the default (admin1 and 0000).

To reset the IPL> CLI shell user name and password, follow the steps in [Procedure 47 "Resetting the user name and password to default" \(page 332\)](#). This procedure requires a connection to the local maintenance port on the Voice Gateway Media Card and also requires rebooting the card, which interrupts services.

Procedure 47**Resetting the user name and password to default****Step Action**

- 1 Connect a terminal to the Maintenance port (labeled Maint) either directly or through a dial-up modem. The terminal communication parameters must be as follows:
 - 9600bps
 - 8 data bits
 - no parity
 - 1 stop bit
- 2 Press the **Enter** key on the keyboard.
The **logon:** prompt is displayed.
- 3 Reboot the card by pressing the **RESET** button on the faceplate of the card with a pointed object, such as a ball-point pen.

**WARNING**

Do not use a pencil to reset the Voice Gateway Media Card. The graphite carbon can create an electrical short circuit on the board.

- 4 Start up messages are displayed on the terminal. Type **jk1** on the terminal keyboard when the prompt is displayed.

jk1 runs from BIOS or boot ROM which is printed early in the bootup process. There is only a six second window at the prompt to enter **jk1**. If the prompt is missed, restart the card and repeat the above step.
- 5 After the card has booted from BIOS or boot ROM, a CLI prompt such as the BIOS> appears. Enter the following command:

shellPasswordNvramClear at the prompt.
- 6 Type **reboot** at the prompt to reboot the card.
- 7 Wait for the card to completely reboot into the IP Line application. The password synchronization feature changes the password on the card automatically.

—End—

IP configuration commands

Table 79 "IP configuration commands" (page 333) describes the IP configuration commands.

Table 79
IP configuration commands

IP configuration command	Function
setLeader	Performs all the necessary actions to make a Leader. Sets IP address, gateway, subnet mask, boot method to static, and Leader bit in NVRAM.
clearLeader	Clears the Leader info in NVRAM and sets the boot method to use BOOTP, thus, making the card a Follower.
NVRIPShow	Prints the values of the IP parameters that reside in NVRAM.

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

TLAN network interface configuration commands

autonegotiate mode can be disabled if the ports on some data network switches and routers are manually configured. For example, configuring a port for 100BaseT full-duplex can disable autonegotiation on the signaling link.

The Voice Gateway Media Card and the IP Phone default to half-duplex mode when no autonegotiation signaling occurs. The result is that the Voice Gateway Media Card and the IP Phone operate in half-duplex mode, while the switch is in full-duplex mode. Communication continues, but random packet loss can occur which affects the correct operation and voice quality.

ATTENTION

Configure ports for autonegotiation, autosense.

Configure the speed and duplex setting of the TLAN network interface using the following commands:

- **tLanSpeedSet speed** – this command configures the speed of the TLAN network interface. By default, the network interface autonegotiates to the highest speed supported by the switch. If the switch is 10/100BaseT, the network interface negotiates to 100BaseT. Use this command to debug Ethernet speed-related problems by forcing the network interface to 10BaseT operation immediately. The duplex mode setting is saved in NVRAM and read at start-up. The parameter speed is set to the following:

10 – disables autonegotiation and sets speed to 10 Mb/s
10100 – enables autonegotiation

- **tLanDuplexSet duplexMode** – this command immediately configures the duplex mode of the TLAN network interface while operating when autonegotiate is disabled and speed has been fixed to 10 Mb/s (or 10BaseT mode). The duplex mode is saved in NVRAM and read at start-up. The parameter duplexMode is set to the following:
 - 0 – enables full-duplex mode
 - 1 – enables half-duplex mode

If the autonegotiation is disabled, and the speed and duplex mode are forced using the CLI commands, Nortel recommends that half-duplex mode be used to inter-operate with the far end when the far end is set to autonegotiate.

If the duplex mode is configured as full-duplex, the far end must be configured as full-duplex and autonegotiate must be turned off.

Half-duplex mode works with either half-duplex or autonegotiate at the far end. However, full-duplex at the near end only operates with full-duplex at the far end.

For the IP Line application, half-duplex has ample bandwidth for a Voice Gateway Media Card even with 24 busy channels, VAD disabled, and G.711 codec with 10 Mb/s voice payload size.

Display the number of DSPs

The **DSPNumShow** command displays the number of DSPs on the Voice Gateway Media Card.

At the IPL> or the oam> prompt, type: **DSPNumShow**.

Display IP Telephony node properties

The **IPInfoShow** command displays information about an IP Telephony node.

At the IPL> or oam> prompt, type: **IPInfoShow**

The following IP Telephony node information is displayed on the TTY:

- IP addresses for the ELAN and TLAN subnets
- default router for the ELAN and TLAN subnets
- subnet mask for the ELAN and TLAN subnets
- IP routing table

- IP configuration of the card (which is related to the IP configuration of the node)

The IPInfoShow command displays information similar to the following:

```
Maintenance Interface = lnIsa0
Maintenance IP address = 47.103.220.199
Maintenance subnet mask = 255.255.255.224
Voice Interface = lnPci1
Voice IP address = 47.103.247.221
Voice subnet mask = 255.255.255.0
```

ROUTE NET TABLE

destination	gateway	flags	Ref cnt	Use	Interface
0.0.0.0	47.103.247.1	3	7	5800883	lnPci1
47.103.220.192	47.103.220.199	101	0	0	lnIsa0
47.103.247.0	47.103.247.221	101	0	0	lnPci1
47.103.247.0	47.103.247.221	101	0	0	lnPci1

ROUTE HOST TABLE

destination	gateway	flags	Ref cnt	Use	Interface
127.0.0.1	127.0.0.1	5	0	0	lo0

value = 77 = 0x4d = 'M'

Display Voice Gateway Media Card parameters

The following commands provide information about a Voice Gateway Media Card:

- itgCardShow
- ifShow
- serialNumShow
- firmwareVersionShow
- swVersionShow
- electShow (not available on the MC 32S card)
- tpsShow (not available on the MC 32S card)

itgCardShow

The **itgCardShow** command displays information about a Voice Gateway Media Card.

At the IPL> or oam> prompt, type: **itgCardShow**

The **itgCardShow** command displays information similar to the following:

```
Index : 1
Type : EXUT
Role : Leader
Node : 123
Leader IP : 47.103.247.220
Card IP : 47.103.247.221
Card TN : 44 0 10
Card State : ENBL
Uptime : 1 days, 19 hours, 43 mins, 11 secs (157391 secs)
Codecs : G711Ulaw(default), G711Alaw, G729AB
lnPci stat : 100 Mb/s (Carrier OK)
value = 1 = 0x1
```

electShow

The **electShow** command shows information to help a technician quickly become familiar with the current state of the node. The command displays a list of cards in the node and information about each card. This includes showing all registered followers to a leader.

The output has two sections:

- cards currently registered
- cards that are in the BOOTP.TAB configuration but not yet registered

Registered cards

The following information is displayed for each card currently registered:

- platform
- TN
- ELAN network interface MAC
- TLAN network interface IP Address
- ELAN network interface IP Address
- how long it has been registered
- how many IP Phones are registered to the card
- number of Time Outs

Unregistered cards

The following information is displayed for each card currently not yet registered based on BOOTP.TAB:

- platform
- TN
- ELAN network interface MAC
- TLAN network interface IP Address
- ELAN network interface IP Address

Example

The following is an example of the output on a Signaling Server:

```
oam> electShow
Node ID : 678
Node Master : Yes
Up Time : 1 days, 3 hours, 1 mins, 58 secs
TN : 00 00
Host Type : ISP 1100
IP TLAN : 47.11.215.55
IP ELAN : 47.11.216.139
Election Duration : 15
Wait for Result time : 35
Master Broadcast period : 30
===== master tps =====
Host Type TN TLAN IP Addr
ISP 1100 00 00 47.11.215.55
Next timeout : 3 sec
AutoAnnounce : 1
Timer duration : 60 (Next timeout in 17 sec)
===== all tps =====
Num TN Host Type ELAN MAC TLAN IP Addr ELAN IP Addr Up Time
NumOfSets TimeOut
001 00 00 ISP 1100 00:02:B3:C5:50:C2 47.11.215.55
47.11.216.139 001 03:01:58 5 0
002 03 00 ITG-P 00:60:38:8E:71:5C 47.11.215.37 47.11.217.157
006 05:30:13 0 0
===== Cards in node configuration that are not
registered =====
Num TN Host Type ELAN MAC TLAN IP Addr ELAN IP Addr
001 7 0 SMC 00:60:38:BD:C1:C1 47.11.215.54 47.11.216.49
value = 27886252 = 0x1a982ac
```

When all cards configured in a node are registered, the last part of the output displays the following:

```
===== All cards in node configuration are
registered =====
```

tpsShow

The following is an example of the output from the tpsShow command for an ITG-P 24-port line card.

```
IPL> tpsShow
Node ID : 0
Is master : 1
Up time : 4 days, 2 hours, 40 mins, 53 secs (355253 secs)
TN : 03-00
Platform : ITG Pentium
TPS Service : Yes
IP TLAN : 192.168.1.140
IP ELAN : 192.168.1.14
ELAN Link : Up
Sets Connected: 4
Sets Reserved : 0
value = 18 = 0x12
```

Packet loss monitor

Monitor audio packet loss using the following commands:

- **vgwPLLog 0|1|2** – enables the packet loss monitor. Packet loss is measured in the receive direction and the two halves of a call are monitored and logged independently. This command is not available on the MC 32S card.
 - A value of zero (0) disables packet loss logging.
 - A value of one (1 – default) logs a message if packet loss during the course of the call exceeds the threshold set with the **itgPLThreshold** command.
 - A value of two (2) indicates that log messages are printed as packet loss is detected during the call. A message is printed each time packet loss is detected indicating how many packets were lost at that moment.
- **itgPLThreshold xxx** – this command sets the packet loss logging and alarm threshold, where xxx is a number between 1 and 1000, and represents the threshold in 0.1% increments. Packet loss which exceeds the threshold generates an SNMP trap and writes a message to the log file if logging is enabled. The default value is 10 (1%).

Transfer files using the CLI

A number of special file transfer commands are available to Put/Get files from the IPL> CLI or oam> CLI. These commands are normally used as part of an expert support procedure if TM or Element Manager is not available.

These commands, listed in [Table 80 "File transfer" \(page 339\)](#), are from the perspective of the Voice Gateway Media Card. If *Get* is part of the command, the file is transferred from the TM PC to the Voice Gateway Media Card. If *Put* is part of the command, the file is transferred from the Voice Gateway Media Card to the external FTP Server.

These commands, list in are from the perspective of the MC 32S card.

To transfer a file, enter one of the commands listed in [Table 80 "File transfer" \(page 339\)](#) at the IPL> CLI or [Table 81 "File transfer for the MC 32S card" \(page 339\)](#) at the oam> prompt, depending on what type of file transfer is to occur.

[Table 80 "File transfer" \(page 339\)](#) lists the commands, which can be entered at the IPL> CLI. [Table 81 "File transfer for the MC 32S card" \(page 339\)](#) lists the commands, which can be entered at the oam> prompt.

Table 80
File transfer

Command	Parameters
swDownload	<hostname> <username> <password> <directory path> <file name>
configFileGet	<hostname> <username> <password> <directory path> <file name>
bootPFileGet	<hostname> <username> <password> <directory path> <file name>
hostFileGet	<hostname> <username> <password> <directory path> <file name> <ITGfile name> <listener>
bootPFilePut	<hostname> <username> <password> <directory path> <file name>
currOMFilePut	<hostname> <username> <password> <directory path> <file name>
prevOMFilePut	<hostname> <username> <password> <directory path> <file name>
logFilePut	<hostname> <username> <password> <directory path> <file name>
configFilePut	<hostname> <username> <password> <directory path> <file name>
hostFilePut	<hostname> <username> <password> <directory path> <file name> <ITGfile name>
firmwareFileGet	<hostname> <username> <password> <directory path> <file name>
firmwareFilePut	<hostname> <username> <password> <directory path> <file name>

Table 81
File transfer for the MC 32S card

swDownload	swDownload [host user passwd dir file name]
configFileGet	spcPkgconfigFileGet [host user passwd hostDirPath hostfile name]
bootPFileGet	bootPFileGet [host user passwd hostDirPath hostfile name]

hostFileGet	hostFileGet [ftype listener host user passwd hostDirPath hostfile name localDirPath localfile name]
bootPFilePut	bootPFilePut [host user passwd hostDirPath hostfile name]
currOMFilePut	omFilePut [host user passwd hostDirPath hostfile name]
prevOMFilePut	prevOMFilePut [host user passwd hostDirPath hostfile name]
hostFilePut	hostFilePut [ftype listener host user passwd hostDirPath hostfile name localDirPath localfile name]

These commands are case-sensitive. The parameters following the command must each be enclosed in quotation marks, and there must be a comma and no spaces between the parameters. For a complete description of these commands, see [Table 93 "File Transfer commands" \(page 424\)](#).

Hostname refers to any of the following:

- the IP address of the FTP host
- the Voice Gateway Media Card itself (use loopback address 127.0.0.1)
- another Voice Gateway Media Card

Download the IP Line error log

The IP Line error log contains error conditions as well as normal events. Some error conditions can be severe enough to raise an alarm through SNMP traps.

Use the **LogFilePut** command to download an IP Line error log.

Reset the Operational Measurements file

Reset the Operational Measurements (OM) file if incorrect statistics might have been collected.

At the IPL> or oam> prompt, type: **resetOM**.

The resetOM command resets all operational measurement parameters that have been collected since the last log dump. The statistics start from zero.

IP Line administration using Element Manager

Contents

This section contains the following topics:

- ["Introduction" \(page 311\)](#)
- ["Element Manager administration procedures" \(page 341\)](#)
- ["Backup and restore data" \(page 352\)](#)
- ["Update IP Telephony node properties" \(page 355\)](#)
- ["Update other node properties" \(page 374\)](#)
- ["Telnet to a Voice Gateway Media Card using Virtual Terminal" \(page 374\)](#)
- ["Check the Voice Gateway Channels" \(page 376\)](#)
- ["Setting the IP Phone Installer Password" \(page 377\)](#)

Introduction

This chapter explains how to administer IP Line and the Voice Gateway Media Card on CS 1000 systems using Element Manager.

Element Manager administration procedures

This section describes the administration procedures that can be performed using Element Manager.

Turn off browser caching

Internet Explorer caching interferes with the Element Manager application, in that users cannot see real-time changes as they occur. For this reason, Nortel recommends that Internet Explorer caching be turned off prior to using Element Manager.

Follow the steps outlined in [Procedure 22 "Turning off browser caching in Internet Explorer" \(page 261\)](#) to prevent caching of Web windows by the Internet Explorer browser.

IP Line Operational Measurement report scheduling and generation

Operational Measurement (OM) reports provide important statistical and traffic information and feedback to the system administrator to better engineer the system. The information stored in the OM file applies only to the calls routed over the IP network by way of IP Line. OM reports give a quantitative view of system performance, such as jitter.

A single Voice Gateway Media Card Operational Measurements file can be viewed directly from Element Manager. This OM report is a view of the LTPS and Voice Gateway channel activity on that specific card. Use this procedure to view the individual card information for each Voice Gateway Media Card in the node.

The Voice Gateway Media Card OM file contains the following information:

- the number of incoming and outgoing calls
- the number of call attempts
- the number of calls completed
- the total holding time for voice calls

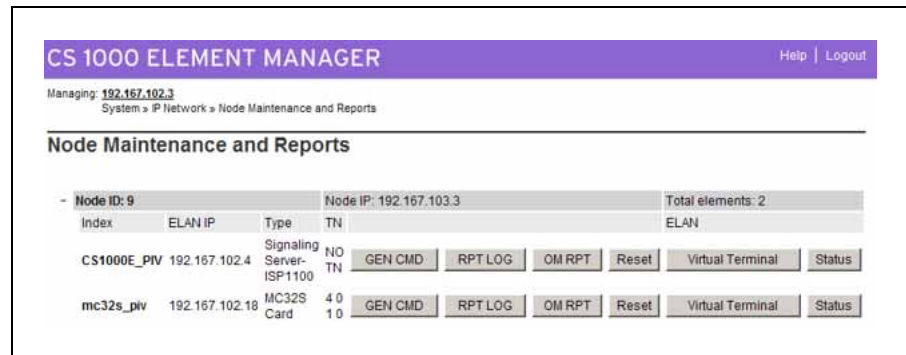
To view a single Voice Gateway Media Card OM file directly from Element Manager, follow the steps in [Procedure 48 "Retrieving the current OM file from the Voice Gateway Media Card using Element Manager" \(page 342\)](#).

Procedure 48

Retrieving the current OM file from the Voice Gateway Media Card using Element Manager

Step	Action
1	In the Element Manager navigator, click IP Network > Maintenance and Reports . The Node Maintenance and Reports window appears.
2	Expand the node containing the Voice Gateway Media Card by clicking the plus sign (+) to the left of the Node ID. See Figure 82 "Node Maintenance and Reports window" (page 343) .

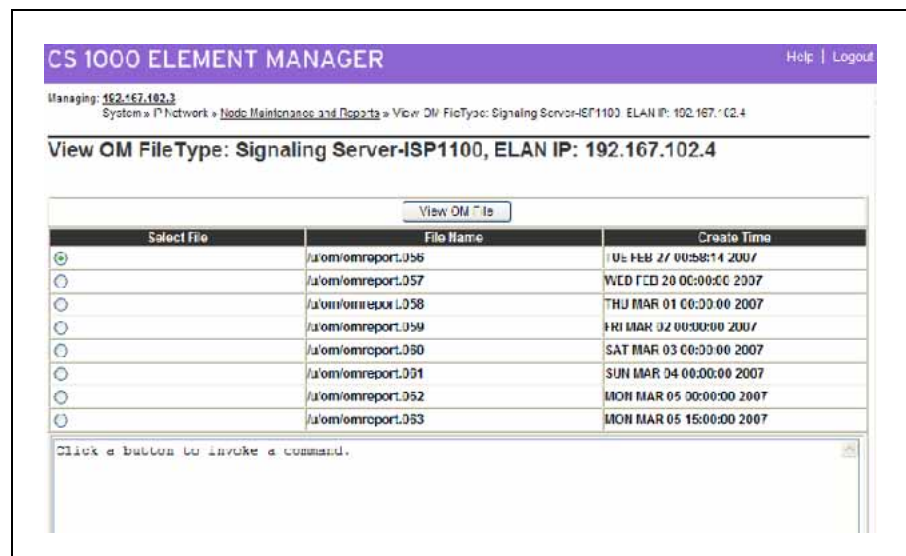
Figure 82
Node Maintenance and Reports window



- 3 Click the **OM RPT** button associated with the Voice Gateway Media Card.

The **View OM File** window appears. See [Figure 83 "View OM File window"](#) (page 343).

Figure 83
View OM File window



The eight most recent OM Report files are displayed in chronological order for that Voice Gateway Media Card.

- 4 To view a OM file, click the radio button for the file to be viewed and then click **View OM File**.

The OM report data appears at the bottom of the window.

—End—

Collection period

The file contains collection period information for each hour of the day that the card was running.

The collection periods start with the hour from midnight to 1:00 am. As each hour passes, a collection period is added to the OM file; therefore, there is a maximum of 24 collection periods each day.

Output

The OM report output tracks the statistics for each IP Phone type.

Data is first output for the IP Phones followed by the data for the gateway channels.

Output example

An example of a single hour OM report is as follows:

```
collection_time : 11/7/2006 2:00
2004Reg_Att: 0
2004Reg_Fail: 0
2004Unreg_Att: 0
2004Aud_Setup: 0
2004Jitter_Avg: 0.0
2004Jitter_Max: 0
2004Latency_Avg: 0.0
2004Latency_Max: 0
2004Pkt_Lost: 0.00
2004Listen_RFactor: 0.0
2004Voice_Time: 0 mins 0 secs
2002Reg_Att: 0
2002Reg_Fail: 0
2002Unreg_Att: 0
2002Aud_Setup: 0
2002Jitter_Avg: 0.0
2002Jitter_Max: 0
2002Latency_Avg: 0.0
2002Latency_Max: 0
2002Pkt_Lost: 0.00
2002Listen_RFactor: 0.0
2002Voice_Time: 0 mins 0 secs
2001Reg_Att: 0
2001Reg_Fail: 0
2001Unreg_Att: 0
2001Aud_Setup: 0
2001Jitter_Avg: 0.0
2001Jitter_Max: 0
2001Latency_Avg: 0.0
2001Latency_Max: 0
2001Pkt_Lost: 0.00
2001Listen_RFactor: 0.0
```

2001Voice_Time: 0 mins 0 secs
1150Reg_Att: 0
1150Unreg_Att: 0
1150Aud_Setup: 0
1150Jitter_Avg: 0.0
1150Jitter_Max: 0
1150Latency_Avg: 0.0
1150Latency_Max: 0
1150Pkt_Lost: 0.00
1150Listen_RFactor: 0.0
1150Voice_Time: 0 mins 0 secs
1130Reg_Att: 0
1130Reg_Fail: 0
1130Unreg_Att: 0
1130Aud_Setup: 0
1130Jitter_Avg: 0.0
1130Jitter_Max: 0
1130Latency_Avg: 0.0
1130Latency_Max: 0
1130Pkt_Lost: 0.00
1130Listen_RFactor: 0.0
1130Voice_Time: 0 mins 0 secs
2004P2Reg_Att: 0
2004P2Reg_Fail: 0
2004P2Unreg_Att: 0
2004P2Aud_Setup: 0
2004P2Jitter_Avg: 0.0
2004P2Jitter_Max: 0
2004P2Latency_Avg: 0.0
2004P2Latency_Max: 0
2004P2Pkt_Lost: 0.00
2004P2Listen_RFactor: 0.0
2004P2Voice_Time: 0 mins 0 secs
2002P2Reg_Att: 0
2002P2Reg_Fail: 0
2002P2Unreg_Att: 0
2002P2Aud_Setup: 0
2002P2Jitter_Avg: 0.0
2002P2Jitter_Max: 0
2002P2Latency_Avg: 0.0
2002P2Latency_Max: 0
2002P2Pkt_Lost: 0.00
2002P2Listen_RFactor: 0.0
2002P2Voice_Time: 0 mins 0 secs
2033Reg_Att: 0
2033Reg_Fail: 0
2033Unreg_Att: 0
2033Aud_Setup: 0
2033Jitter_Avg: 0.0
2033Jitter_Max: 0

```
2033Latency_Avg: 0.0
2033Latency_Max: 0
2033Pkt_Lost: 0.00
2033Listen_RFactor: 0.0
2033Voice_Time: 0 mins 0 secs
2050Reg_Att: 0
2050Reg_Fail: 0
2050Unreg_Att: 0
2050Aud_Setup: 0
2050Jitter_Avg: 0.0
2050Jitter_Max: 0
2050Latency_Avg: 0.0
2050Latency_Max: 0
2050Pkt_Lost: 0.00
2050Voice_Time: 0 mins 0 secs
2210Reg_Att: 0
2210Reg_Fail: 0
2210Unreg_Att: 0
2210Aud_Setup: 0
2210Jitter_Avg: 0.0
2210Jitter_Max: 0
2210Latency_Avg: 0.0
2210Latency_Max: 0
2210Pkt_Lost: 0.00
2210Listen_RFactor: 0.0
2210Voice_Time: 0 mins 0 secs
1120Reg_Att: 0
1120Reg_Fail: 0
1120Unreg_Att: 0
1120Aud_Setup: 0
1120Jitter_Avg: 0.0
1120Jitter_Max: 0
1120Latency_Avg: 0.0
1120Latency_Max: 0
1120Pkt_Lost: 0.00
1120Listen_RFactor: 0.0
1120Voice_Time: 0 mins 0 secs
1110Reg_Att: 0
1110Reg_Fail: 0
1110Unreg_Att: 0
1110Aud_Setup: 0
1110Jitter_Avg: 0.0
1110Jitter_Max: 0
1110Latency_Avg: 0.0
1110Latency_Max: 0
1110Pkt_Lost: 0.00
1110Listen_RFactor: 0.0
1110Voice_Time: 0 mins 0 secs
2050MCReg_Att: 0
2050MCReg_Fail: 0
```

2050MCUnreg_Att: 0
2050MCAud_Setup: 0
2050MCJitter_Avg: 0.0
2050MCJitter_Max: 0
2050MCLatency_Avg: 0.0
2050MCLatency_Max: 0
2050MCPkt_Lost: 0.00
2050MCVoice_Time: 0 mins 0 secs
2211Reg_Att: 0
2211Reg_Fail: 0
2210Unreg_Att: 0
2211Aud_Setup: 0
2211Jitter_Avg: 0.0
2211Jitter_Max: 0
2211Latency_Avg: 0.0
2211Latency_Max: 0
2211Pkt_Lost: 0.00
2211Listen_RFactor: 0.0
2211Voice_Time: 0 mins 0 secs
1160Reg_Att: 0
1160Reg_Fail: 0
1160Unreg_Att: 0
1160Aud_Setup: 0
1160Jitter_Avg: 0.0
1160Jitter_Max: 0
1160Latency_Avg: 0.0
1160Latency_Max: 0
1160Pkt_Lost: 0.00
1160Listen_RFactor: 0.0
1160Voice_Time: 0 mins 0 secs
2212Reg_Att: 0
2212Reg_Fail: 0
2212Unreg_Att: 0
2212Aud_Setup: 0
2212Jitter_Avg: 0.0
2212Jitter_Max: 0
2212Latency_Avg: 0.0
2212Latency_Max: 0
2212Pkt_Lost: 0.00
2212Listen_RFactor: 0.0
2212Voice_Time: 0 mins 0 secs
2007Reg_Att: 0
2007Reg_Fail: 0
2007Unreg_Att: 0
2007Aud_Setup: 0
2007Jitter_Avg: 0.0
2007Jitter_Max: 0
2007Latency_Avg: 0.0
2007Latency_Max: 0
2007Pkt_Lost: 0.00

```
2007Listen_RFactor: 0.0
2007Voice_Time: 0 mins 0 secs
1140Reg_Att: 0
1140Reg_Fail: 0
1140Unreg_Att: 0
1140Aud_Setup: 0
1140Jitter_Avg: 0.0
1140Jitter_Max: 0
1140Latency_Avg: 0.0
1140Latency_Max: 0
1140Pkt_Lost: 0.00
1140Listen_RFactor: 0.0
1140Voice_Time: 0 mins 0 secs
1175Reg_Att: 0
1175Reg_Fail: 0
1175Unreg_Att: 0
1175Aud_Setup: 0
1175Jitter_Avg: 0.0
1175Jitter_Max: 0
1175Latency_Avg: 0.0
1175Latency_Max: 0
1175Pkt_Lost: 0.00
1175Listen_RFactor: 0.0
1175Voice_Time: 0 mins 0 secs
ChanAud_Setup: 0
ChanJitter_Avg: 0.0
ChanJitter_Max: 0
ChanPkt_Lost: 0.00
ChanVoice_Time: 0 mins 0 secs
H323VtrkInVoCallAttempt: 0
H323VtrkInVoCallComp: 0
H323VtrkOutVoCallAttempt: 0
H323VtrkOutVoCallComp: 0
H323VtrkTotalVoiceTime: 0 mins 0 secs
H323VtrkInFaxCallAttempt: 0
H323VtrkInFaxCallComp: 0
H323VtrkOutFaxCallAttempt: 0
H323VtrkOutFaxCallComp: 0
H323VtrkFallBack: 0
H323VtrkQoSFallBack: 0
H323VtrkATPMFallBack: 0
H323VtrkRelCompFallBack: 0
SIPVtrkInVoCallAttempt: 0
SIPVtrkInVoCallComp: 0
SIPVtrkOutVoCallAttempt: 0
SIPVtrkOutVoCallComp: 0
SIPVtrkTotalVoiceTime: 0 mins 0 secs
SIPVtrkInFaxCallAttempt: 0
SIPVtrkInFaxCallComp: 0
SIPVtrkOutFaxCallAttempt: 0
```


SIPVtrkOutFaxCallComp: 0
SIPVtrkFallBack: 0
SIPVtrkQoSFallBack: 0
SIPVtrkATPMFallBack: 0
SIPVtrkRelCompFallBack: 0
SIPVtrkTLSAuthenticationFailure: 0
SIPVtrkTLSIncomingAttempt: 0
SIPVtrkTLSIncomingComp: 0
SIPVtrkTLSIncomingFailure: 0
SIPVtrkTLSOutgoingAttempt: 0
SIPVtrkTLSOutgoingComp: 0
SIPVtrkTLSOutgoingFailure: 0
OutTotalH323OvlCallCount: 0
OutSuccessH323OvlCallCount: 0
OutOvl2EnblocCallCount: 0
InTotalH323OvlCallCount: 0
InSuccessH323OvlCallCount: 0
TotalARQGenerated: 0
TotalARJRcvd: 0
TotalACFRcvd: 0
H323NrsGatekeeperReq: 0
H323NrsGatekeeperConf: 0
H323NrsGatekeeperRej: 0
H323NrsRegistrationReq: 144
H323NrsRegistrationConf: 144
H323NrsRegistrationRej: 0
H323NrsUnregistrationReqRecd: 0
H323NrsUnregistrationConfSent: 0
H323NrsUnregistrationRejSent: 0
H323NrsAdmissionReq: 0
H323NrsAdmissionConf: 0
H323NrsAdmissionRej: 0
H323NrsLocationReqRecd: 0
H323NrsLocationConfSent: 0
H323NrsLocationRejSent: 0
H323NrsBandwidthReqRecd: 0
H323NrsBandwidthConfSent: 0
H323NrsBandwidthRejSent: 0
H323NrsDisengageReq: 0
H323NrsDisengageConf: 0
H323NrsDisengageRej: 0
SIPNrsRoutingAttempts: 0
SIPNrsRoutingSuccesses: 0
SIPNrsRoutingFailures: 0
SIPNrsRegistrationAttempts: 138
SIPNrsRegistrationSuccesses: 138
SIPNrsRegistrationFailures: 0
SIPCTITotalSoftClientlogonAttempts: 0
SIPCTITotalSoftClientlogonSuccesses: 0
SIPCTITotalAnswerCallRequests: 0

```
SIPCTITotalAnswerCallSuccesses: 0
SIPCTITotalClearConnectionRequests: 0
SIPCTITotalClearConnectionSuccesses: 0
SIPCTITotalConsultationCallRequests: 0
SIPCTITotalConsultationCallSuccesses: 0
SIPCTITotalDeflectCallRequests: 0
SIPCTITotalDeflectCallSuccesses: 0
SIPCTITotalHoldCallRequests: 0
SIPCTITotalHoldCallSuccesses: 0
SIPCTITotalMakeCallRequests: 0
SIPCTITotalMakeCallSuccesses: 0
SIPCTITotalRetrieveCallRequests: 0
SIPCTITotalRetrieveCallSuccesses: 0
SIPCTITotalSingleStepTransferRequests: 0
SIPCTITotalSingleStepTransferSuccesses: 0
SIPCTITotalTransferCallRequests: 0
SIPCTITotalTransferCallSuccesses: 0
SIPCTITotalMonitorStartRequests: 0
SIPCTITotalMonitorStartSuccesses: 0
SIPCTITotalMonitorStopRequests: 0
SIPCTITotalMonitorStopSuccesses: 0
SIPCTITotalConferenceCallRequests: 0
SIPCTITotalConferenceCallSuccesses: 0
SIPCTITotalSetForwardingRequests: 0
SIPCTITotalSetForwardingSuccesses: 0
SIPCTITotalGetForwardingRequests: 0
SIPCTITotalGetForwardingSuccesses: 0
SIPCTITotalSessionTerminated: 0
```

Each collection period provides the following information:

- The date and time for the collection period hour.
- LTPS information for IP Phones that are registered to the LTPS on the Voice Gateway Media Card during that hour. During normal operation, the LTPS values for the Voice Gateway Media Card can be zeros as the IP Phones normally register to the LTPS on the Signaling Server.
- Voice Gateway channel information accumulated during the hour. The Voice Gateway data is prefixed by *Chan*.
- Notes indicating whether the machine has been rebooted during the hour.
- Virtual Trunk statistics display only for a Signaling Server that has been running the VTRK H.323 Signaling Server in the last hour.

The OM file relates to the omreport.xxx file on the Voice Gateway Media Card, where xxx indicates the numbers of days since December 31.

In general, no relationship exists between the IP Phones registered on a Voice Gateway Media Card and the Voice Gateway channels on the card (if two or more cards are used) in the node. If only one Voice Gateway Media Card is used (with multiple IP Phones), a partial correlation might exist between the IP Phones and the card information. However, even with only one Voice Gateway Media Card, there still is not a 100% correlation, as an IP Phone can still call another IP Phone without involving the Voice Gateway channels.

Element Manager supports the ability to view OM files only. TM can optionally be used to support other Operational Measurements tasks such as scheduling reports, generating reports, opening reports, and viewing reports.

See ["Operational Measurement report scheduling and generation" \(page 382\)](#) for more information.

View IP Line log files

Element Manager uses RPC to transfer the sysfile from the Voice Gateway Media Card to the PC. The error log file displays error information, including error date/time, the originating module (IP Telephony node), and specific error data.

To view error conditions that are abnormal events, but not severe enough to raise an alarm, follow the steps in [Procedure 49 "Viewing IP Line log files" \(page 351\)](#).

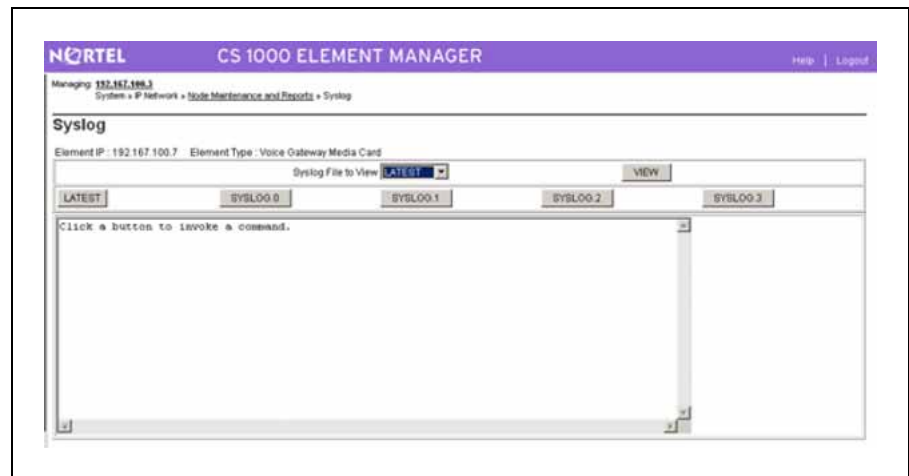
Procedure 49

Viewing IP Line log files

Step	Action
1	In the Element Manager navigator, click IP Network > Maintenance and Reports . The Node Maintenance and Reports window appears.
2	Expand the node containing the Voice Gateway Media Card by clicking the plus sign (+) to the left of the Node ID.
3	Click the SYS LOG button associated with the Voice Gateway Media Card. The Syslog window appears. See Figure 84 "Syslog window" (page 352) . The Syslog window has five buttons to view the log files: The LATEST button displays the most recent syslog information for the Voice Gateway Media Card.

- There are four SYSLOG.# buttons; one for each of the four syslog files on the Voice Gateway Media Card.

Figure 84
Syslog window



From the **Syslog File to View** drop-down list, select **LATEST** to view the most current syslog information that was written to the Voice Gateway Media Card and click **View**

Alternatively, click the **Latest** button. As well, **SYSLOG.0**, **SYSLOG.1**, **SYSLOG.2**, and **SYSLOG.3** can be selected from the drop-down list and viewed by clicking **View**. Alternatively, click the **SYSLOG.0**, **SYSLOG.1**, **SYSLOG.2**, or **SYSLOG.3** button to view the associated syslog file. The syslog file data is displayed in the window below the buttons. The data can be error messages or information messages. For each message, the date, timestamp, and the task that is printing the message is displayed.

—End—

Backup and restore data

All data is stored on the Call Server. Element Manager accesses the data for the elements being maintained. Element Manager does not store data.

There is no Element Manager-specific data that needs to be backed up. All data is retrieved from the Call Server and elements.

The c:/u/db/node directory is populated on the Call Server when the node configuration is saved. The BOOTP.TAB and CONFIG.INI files are saved in this directory as c:/u/db/node/nodexxxx.btp and c:/u/db/node/nodexxxx.cfg where xxxx is the node ID:

- nodexxxx.btp is the BOOTP.TAB file

- nodexxxx.cfg is the CONFIG.INI.

If a node is removed, the associated files are also removed. For every node that is created, a nodeyyyy.btp and nodeyyyy.cfg file are created in the C:/u/db/node directory.



WARNING

Do not manually edit or delete the node files. Manually editing or deleting these files can cause corruption of Element Manager.

Backup

The Backup command invokes the Equipment Data Dump (EDD) operation on the Call Server to back up all Call Server data. Within Element Manager, the **Call Server Backup** function invokes a data dump and writes the Call Server data to the primary and internal backup drives.

The backup includes all Call Server data as well as the BOOTP.TAB and CONFIG.INI files for each node configured in the system. These files are stored on the Call Server for the IP Telephony nodes configured in the system.

This Backup function can also be performed on the Call Server by entering the **EDD** CLI command using LD 43.

During the Backup function, the BOOTP.TAB and CONFIG.INI files of all registered nodes are copied so that they can be restored in case of system failure.

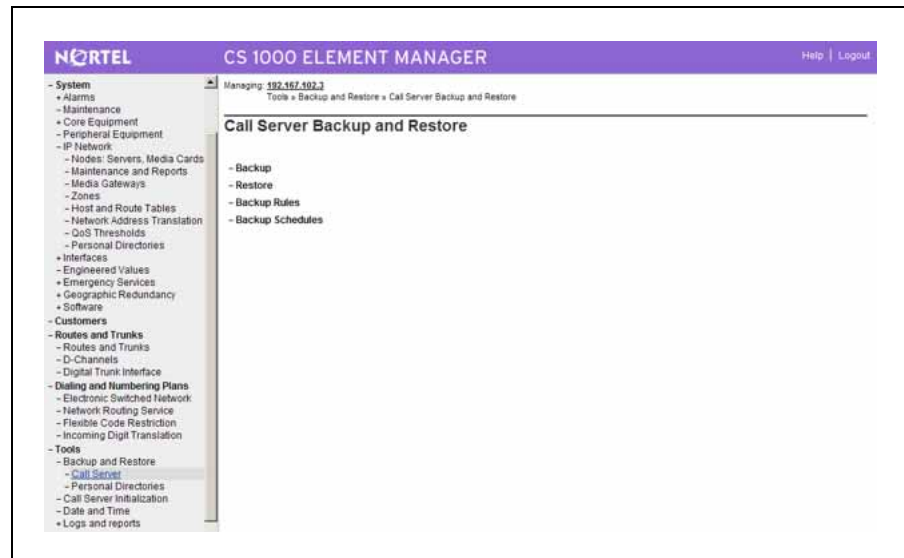
Follow the steps in [Procedure 50 "Backing up the Call Server data" \(page 353\)](#) to back up the Call Server.

Procedure 50

Backing up the Call Server data

Step	Action
1	In the Element Manager navigator, click Tools > Backup and Restore > Call Server Backup and Restore . See Figure 85 "Call Server Backup and Restore window" (page 354) .

Figure 85
Call Server Backup and Restore window



- 2 Click **Backup**.

The **Call Server Backup** window appears. See Figure 86 "Call Server Backup window" (page 354).

Figure 86
Call Server Backup window



- 3 Select **Backup** from the **Action** drop-down list.
- 4 Click the **Submit** button or click **Cancel** to cancel the backup.
- The window displays messages indicating "Backup in progress. Please wait..."
- 5 Click **OK** in the EDD complete dialog box.
- The Backup function then displays information in a tabular form indicating the actions that were performed.

—End—

Restore the backed up files

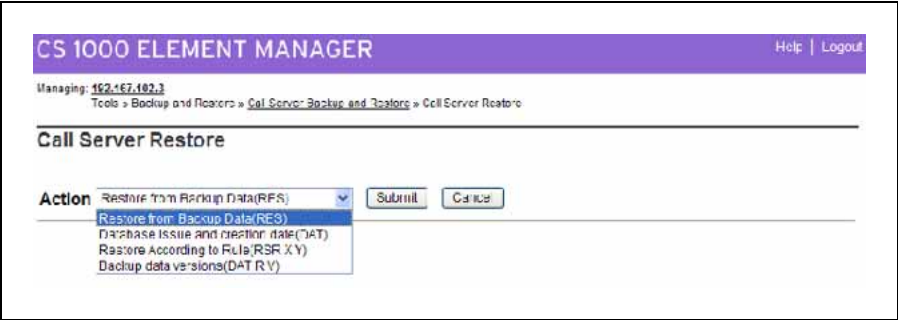
The Call Server Restore function restores the backed up files from the internal backup device to the primary device. The Restore function performs the same task as the `RIB` CLI command in LD 43.

To restore the Call Server data, follow the steps in [Procedure 51 "Restoring the Call Server data" \(page 355\)](#).

Procedure 51
Restoring the Call Server data

Step	Action
1	In the Element Manager navigator, click Tools > Backup and Restore > Call Server . The Call Server Backup and Restore window appears.
2	Click Restore . The Call Server Restore window appears. See Figure 87 "Call Server Restore window" (page 355) .

Figure 87
Call Server Restore window



3	Select Restore from Backup Data (RES) from the Action drop-down list.
4	Click the Submit button. If the Restore is successful, the message "Restore was done successfully" is displayed.

—End—

Update IP Telephony node properties

To update the node properties of a Voice Gateway Media Card, follow the steps in [Procedure 52 "Updating the IP Telephony node properties" \(page 356\)](#).

Procedure 52**Updating the IP Telephony node properties****Step Action**

- 1 In the Element Manager navigator, click **IP Networks > Nodes: Servers, Media Cards**.
The **Node Configuration** window appears.
- 2 Click the **Edit** button associated with the node to be updated.
The **Edit** window appears. See [Figure 88 "Edit window"](#) (page 356).

Figure 88
Edit window

The screenshot shows the 'Edit' window in the CS 1000 ELEMENT MANAGER. The window title is 'CS 1000 ELEMENT MANAGER' with a 'Help' link and a user profile 'logoul'. The breadcrumb trail is 'Managing: 192.167.102.3 System > IP Network > Node Configuration > IP Telephony: Node ID 9 > Edit'. The main heading is 'Edit'. Below it are 'Save and Transfer' and 'Cancel' buttons. The configuration is for 'Node ID 9'. The 'IP Telephony Node' section includes the following fields:

- Telephony LAN (T1 AN) Node IP address: 192.167.103.3
- Embedded LAN (ELAN) gateway IP address: 192.167.102.1
- Embedded LAN (ELAN) subnet mask: 255.255.255.0
- Voice LAN (T1 AN) subnet mask: 255.255.255.0

Below these fields is a list of expandable sections:

- + VGV and IP phone codec profile
- + CoS
- + LAN configuration
- + SNTP
- + Virtual Trunk Network Health Monitor configuration
- + H323 GV Settings
- + Firmware
- + SIP GV Settings
- + SIP URI Map
- + SIP CD Services

- 3 Perform all required updates to the parameters in the appropriate sections.

If Voice Gateway Media Cards are added to, deleted from, or replaced in the node or a Voice Gateway Media Card is changed, then use one of the following procedures:

- ["Add a Voice Gateway Media Card to the node"](#) (page 357)
- ["Delete a Follower Voice Gateway Media Card from the node"](#) (page 362)
- ["Change the IP addresses of an IP Telephony node in Element Manager"](#) (page 365)

- See the Maintenance chapter for the procedures to replace a Voice Gateway Media Card. See ["Replace a Leader Voice Gateway Media Card" \(page 460\)](#).

—End—

Add a Voice Gateway Media Card to the node

To add a Voice Gateway Media Card to the node, follow the steps in [Procedure 53 "Adding a Voice Gateway Media Card to the node" \(page 357\)](#).

Procedure 53

Adding a Voice Gateway Media Card to the node

Step	Action
1	Choose a card slot for the new card. Note the TN.
2	Configure IPTN in LD 14 at the Call Server.
3	Install the I/O cables for connection to the ELAN and TLAN network interfaces on the selected card slot.
4	In the Element Manager navigator, click IP Network > Nodes: Servers, Media Cards . The Node Configuration window appears.
5	Click the Edit button for the node that is receiving the new Voice Gateway Media Card. The Edit window appears.
6	Click the Add button to the right of the Cards section.
7	Observe that the Cards section expands. See Figure 89 "Add Card window " (page 358) .

Figure 89
Add Card window

CS 1000 ELEMENT MANAGER Help | Logout

- Cards

- Card 192.167.102.18 Properties

Role: Follower

Embedded LAN (ELAN) IP address: 192.167.102.18

Embedded LAN (ELAN) MAC address: 00:17:65:f9:f9:fd

Telephony LAN (TLAN) IP address: 192.167.103.18

Voice LAN (TLAN) gateway IP address: 192.167.103.1

Hostname: mc300s_priv

Card TN: 401

Card processor type: MC32S Card

Telephony LAN (TLAN) DSP IP address: 192.167.103.19

H323 ID: CS1000E_PRIV

Enable Line TPS: ☒

If Telephony LAN(TLAN) IP address and Telephony LAN(TLAN) gateway IP address are not in the same subnet as Telephony LAN(TLAN) Node IP address when Line TPS is enabled, then the TPS application will not run.

Primary Call Server IP address: 192.167.102.3

Alternate Call Server1 IP address: 0.0.0.0

Alternate Call Server2 IP address: 0.0.0.0

+ Signaling Servers

- 8 Enter the **Card Properties** data:
- Role:** Element Manager reads the role from the card configuration.
 - Embedded LAN (ELAN) IP address:** This is the ELAN network interface IP address for the card. Element Manager and the system use this IP address to communicate with the card.
 - Embedded LAN (ELAN) MAC address:** This is the Ethernet address from the [Table 62 "Voice Gateway Media Card installation summary sheet"](#) (page 223).
 - Telephony LAN (TLAN) IP address:** This is the TLAN network interface IP address for the card.
 - Voice LAN gateway (TLAN) IP address:** This is the IP address of the router interface on the TLAN subnet.
 - Hostname**
 - Card TN:** Enter the card slot number between 1 – 50.
 - Card processor type:** Choose either Pentium or Media Card from the drop-down list. Select Pentium if using the ITG-P 24-port line card (dual-slot card), or select Media Card if using the Media Card single-slot card.

- i. **H323 ID:** The H323 ID in IP Line is for the Virtual Office/ MG 1000B feature. Keep the H323 ID the same for all the elements within one node.
 - j. **Enable Line TPS** check box: Select this check box.
 - k. Add **Primary Call Server IP address**. Add **Alternate Call Server1 IP address** and **Alternate Call Server2 IP address**, if applicable.
- 9** To add additional cards to the node, click the **Add** button again and enter the new card information. Repeat this step for each card to be added to the node.
- Observe that new cards appear under the Cards section as they are added.
- 10** Click the **Save and Transfer** button after the card have been added and configured.
- Clicking the **Save and Transfer** button saves the data to the Call Server.
- 11** Click **OK** to confirm.
- The **Save and Transfer** button can be clicked after each card is configured in the **Edit** window. However, each time the **Save and Transfer** button is clicked, the **Edit** window closes and the **Node Configuration** window is displayed. To continue the node configuration, click the **Edit** button to return to the **Edit** window.
- If the **Cancel** button is clicked, all information that has been configured is discarded. The **Edit** window closes and the **Node Configuration** window appears.
- The **Edit** window closes, and the **Node Configuration** window appears.
- 12** Click the **Transfer/Status** button associated with the node where the new card was added.
- 13** Click **OK** to confirm the transfer.
- The **Transfer Progress** window appears and displays each of the Voice Gateway Media Card in the node.
- The Voice Gateway Media Card retrieve the CONFIG.INI and BOOTP.TAB files from the Call Server. A check mark is added to each field as the card receives its CONFIG.INI and BOOTP.TAB files.
- 14** When the transfer is complete, click **OK** in the **Progress Check Complete** dialog box.

- If the transfer is successful for a card, the Status column displays "Complete".
- If the transfer is unsuccessful, the Status column displays "Fail".

15 Insert the new card.

The card boots and obtains its IP configuration from the node master. This process takes several minutes.

The Maintenance faceplate display shows an alarm of T:21 or S009.

- T:21 is displayed if the card is new and there is no CONFIG.INI file.
- S009 is displayed if the card has been used before and has a CONFIG.INI file that contains an IP address for the Call Server that is no longer correct.

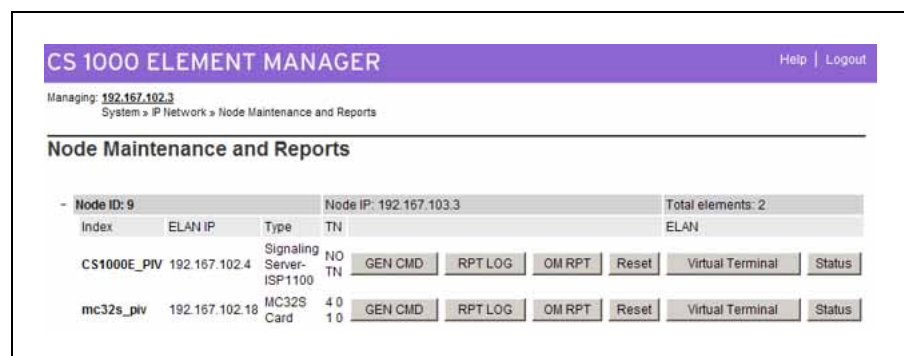
16 In the Element Manager navigator, click **IP Network > Maintenance and Reports**.

The **Node Maintenance and Reports** window appears.

17 Expand the node containing the Voice Gateway Media Card by clicking the plus sign (+) to the left of the Node ID.

18 Click the **GEN CMD** button associated with the Voice Gateway Media Card. See [Figure 90 "Voice Gateway Media Card and GEN CMD button"](#) (page 360).

Figure 90
Voice Gateway Media Card and GEN CMD button



The **General Commands** window appears.

19 From the Group drop-down list, select **Misc**.

20 From the **Command** drop-down list, click the **cardRoleShow** command.

If the card role is not a Follower as expected, Telnet to the card IPL> or oam> CLI using Virtual Terminal, and enter the **clearLeader** command to remove the clearLeader flag.

- 21 In the Element Manager navigator, click **IP Network > Nodes: Servers, Media Cards**.
The **Node Configuration** window appears.
- 22 Click the **Transfer/Status** button for the node.
This action downloads the node information to the card.
- 23 In the Element Manager navigator, click **IP Network > Maintenance and Reports**.
The **Node Maintenance and Reports** window appears.
- 24 Expand the node containing the new card that were added by clicking the plus sign (+) to the left of the Node ID.
- 25 Click the **Status** button for each Voice Gateway Media Card that was added.

The card status displays as "Enabled" or "Disabled". If the status message of "Web3003: Destination IP address cannot be reached; initial RPC failure" is displayed, then verify the network connection and the proper configuration of the network equipment.
- 26 Verify that all the new Voice Gateway Media Cards in the node have a signaling link to the Call Server.
- 27 In the Element Manager navigator, click **IP Network > Maintenance and Reports**.
The **Node Maintenance and Reports** window appears.
- 28 Expand the node containing the Voice Gateway Media Card by clicking the plus sign (+) to the left of the Node ID.
- 29 Click the **GEN CMD** button associated with the Voice Gateway Media Card.
- 30 In the **Group** drop-down list, select **pbxLink**.
- 31 From the **Command** drop-down list, select **pbxLinkShow**.
- 32 Click **RUN**.

The output appears in the window below.

The **pbxLinkShow** command can also be entered at the IPL > or oam> command line. Telnet to each Voice Gateway Media Card and log in. Enter the **pbxLinkShow** command at the IPL > or oam> prompt. Alternatively, look at the display on the card faceplate and ensure it is not displaying an alarm.

- 33 In the **Group** drop-down list of the General Commands window, select **Misc**.

- 34 In the Command drop-down list, select **cardRoleShow** and click **RUN**.

If the card role is not Follower as expected, Telnet to the card IPL > or oam> CLI and enter the **clearLeader** command to remove the clearLeader flag.

- 35 Verify the card software and firmware version on the new card and, if necessary, upgrade the software and the firmware. Use the procedures outlined in the section "[Upgrade the Voice Gateway Media Card software and IP Phone firmware](#)" (page 293).

—End—

Delete a Follower Voice Gateway Media Card from the node

To delete a Voice Gateway Media Card from the node, follow the steps in [Procedure 54 "Deleting a follower Voice Gateway Media Card from the node"](#) (page 362).

Procedure 54

Deleting a follower Voice Gateway Media Card from the node

Step	Action
1	In the Element Manager navigator, click IP Network > Nodes: Servers, Media Cards . The Node Configuration window appears.
2	Click the Edit button for the node containing the Voice Gateway Media Card to be deleted. The Edit window appears.
3	Expand the Cards section by clicking the plus sign (+) to the left of Cards .
4	Confirm the card to be deleted and then click the Remove button for that card.
5	Confirm the deletion by clicking OK .

- 6 Click **Save and Transfer** to save the node change.
The **Edit** window closes, and the **Node Configuration** window appears.
- 7 Click the **Transfer/Status** button associated with the node containing the card that was removed.
- 8 Click **OK** to confirm the transfer.
The **Transfer Progress window** opens and the changes are transferred to the Call Server.
- 9 Click **OK** in the **Progress Check Complete** dialog box.
- 10 Remove the Voice Gateway Media Card.

**CAUTION****CAUTION WITH ESDS DEVICES**

Follow antistatic procedures and place the Voice Gateway Media Card in an appropriate antistatic package.

- 11 Remove the Voice Gateway Media Card configuration data from the Call Server.
 - a. Identify the TN of the Voice Gateway Media Card.
 - b. In LD 20, enter the **L TN** (List Terminal Number) command where TYPE = VGW, to list the TNs on the Voice Gateway Media Card TN. This returns a list of units equipped on the card. Verify the number of units that are equipped on the card. Note the first unit equipped on the card.
 - c. In LD 14, use the **Out n** command, where n equals the number of units that are equipped on the card.
- 12 At the TN prompt, enter the TN for the first unit that was equipped on the card. As the units are deleted, verify that the intended units are outed.

—End—

Delete the Leader Voice Gateway Media Card from the node

In the usual system configuration, the Signaling Server is the Leader of the node. However, if a second or subsequent node is configured on the system, then a Voice Gateway Media Card is configured as the Leader for that node.

If the Leader card for a second or subsequent node (that is, the card in Element Manager that displays the card role as Leader) is deleted, then another card in the node must be selected and the `setLeader` command must be issued on that card. A node must have a Leader card for it to operate correctly when the node is powered up.

The role of a card can be viewed in Element Manager; however, it cannot be changed there. Element Manager displays the card role based on the `setLeader` status of the card.

Follow the steps in the [Procedure 55 "Deleting the Leader Voice Gateway Media Card" \(page 364\)](#) to first select a new Leader card and then to delete the current Leader Voice Gateway Media Card.

Procedure 55

Deleting the Leader Voice Gateway Media Card

Step	Action
1	In the Element Manager navigator, click IP Network > Maintenance and Reports . The Node Maintenance and Reports window appears.
2	Expand the node containing the Voice Gateway Media Card that becomes the new Leader by clicking the plus sign (+) to the left of the Node ID.
3	Select a card in the node to become the new Leader.
4	Click the Virtual Terminal button to the right of the card and log into the card.
5	Enter the <code>setLeader</code> command. The card becomes the new Leader.
6	Remove the "old" Leader card from the Media Gateway.
7	Reboot the new Leader card. Wait for the card to come up as the Leader.
8	Click IP Network > Nodes: Servers, Media cards .
9	On the Node Configuration window, click Edit for the node.
10	In the Edit window, click the Remove button for the "old" Leader card that was removed.
11	Click OK to confirm the deletion of the card.
12	Click Save and Transfer .

- 13 In the **Node Configuration** window, click the **Transfer/Status** button associated with the node containing the new Leader card and the deleted Leader card.

—End—

Change the IP addresses of an IP Telephony node in Element Manager

Before changing any IP address, understand "Codecs" (page 205), and consult with the system administrator.

To change the IP address of an IP Telephony node, follow the steps in Procedure 56 "Changing the IP addresses of an IP Telephony node in Element Manager" (page 365).

Procedure 56

Changing the IP addresses of an IP Telephony node in Element Manager

Step	Action
1	In the Element manager navigator, click IP Network > Nodes: Servers, Media Cards . The Node Configuration window appears.
2	Click the Edit button for the node that is having the IP address changes. The Edit window appears.
3	Expand the Node section, if it is not already expanded, by clicking the plus sign (+) to the left of the Node ID.

Figure 91
Edit window

The screenshot shows the 'Edit' window in the CS 1000 Element Manager. The breadcrumb trail is: Managing: 192.167.102.3 > System > IP Network > Node Configuration > IP Telephony Node ID 9 > Edit. The window title is 'Edit'. There are two buttons at the top: 'Save and Transfer' and 'Cancel'. Below them is a section titled '- IP Telephony Node'. Under this section, 'Node ID 9' is displayed. There are four input fields with their respective labels: 'Telephone LAN (TI AN) Node IP address' with value '192.167.103.3', 'Embedded LAN (ELAN) gateway IP address' with value '192.167.102.1', 'Embedded LAN (ELAN) subnet mask' with value '255.255.255.0', and 'Voice LAN (TI AN) subnet mask' with value '255.255.255.0'.

- a. **Node ID:** The Node ID appears automatically.

- b. **Telephony LAN (TLAN) Node IP address:** Enter the Voice LAN (TLAN) Node IP address in dotted decimal format. The Voice LAN Node IP address is on the TLAN subnet. The Node IP address is the IP address used by the IP Phones to communicate with the Voice Gateway Media Cards on the TLAN subnet. If a Voice Gateway Media Card becomes the primary card (Leader) during an election, it assigns itself the Node IP address.
 - If the node IP address is changed, this affects the configuration of the Connect Server IP address in the DHCP Server for the IP Phones.
 - If the IP Phones are using partial DHCP mode, manually reconfigure the IP address of each IP Phone.
- c. **Embedded LAN (ELAN) gateway IP address:** Enter the Embedded LAN (ELAN) gateway IP address in dotted decimal format. This is the IP address of the gateway of the subnet to which the Voice Gateway Media Card belongs. This is the IP address of the router interface on the ELAN subnet, if present. If the subnet does not have a Embedded LAN gateway, enter 0.0.0.0.
 - When a Embedded LAN gateway is added to the ELAN subnet, it must restrict access so that only authorized traffic is permitted on the ELAN subnet.
 - The router must disable the BootP relay agent for the ELAN network interface.
 - The router must block all broadcast and multicast traffic from the ELAN subnet and enable only proper access (that is, only authorized traffic and users coming through the ELAN gateway).
- d. **Embedded LAN (ELAN) subnet mask:** Enter the Embedded LAN subnet mask address in dotted decimal format. This is the subnet mask that is used along with the ELAN network interface IP address to identify to which subnet the Voice Gateway Media Card belongs. When changing these subnet masks, consider the possibility of conflict between the ELAN and TLAN network interface IP addresses. Consult with the network administrator before making any changes to subnets.

When changing the Embedded LAN (ELAN) network interface IP address, this must be coordinated with the IP address on the Call Server (Active ELNK) network interface. Changes must also be coordinated with the following:

- Embedded LAN gateway, and other IP devices on the ELAN subnet
 - any other devices on the ELAN subnet and customer enterprise network subnet that need to communicate with IP Line
 - devices that are looking to receive SNMP traps
- e. **Voice LAN (TLAN) subnet mask:** Enter the Voice LAN subnet mask address in dotted decimal format. This is the subnet mask that is used, along with the TLAN network interface IP address, to identify the subnet to which the Voice Gateway Media Card belongs. Coordinate with the Voice LAN gateway (router). When changing the Voice LAN (TLAN) subnet mask, the change must be coordinated with a change to the subnet mask of the Voice LAN (TLAN) gateway (router) network interface.

4 Expand the **Cards** section and select the card to be changed.

5 Enter the **Card Properties** data for the Leader and Follower cards:

- a. **Role:** There must be at least one card in the node. This card is the Leader. Every IP Telephony node must have only one Leader. All other cards function as Followers. This field is read-only.
- b. **Embedded LAN (ELAN) IP address:** This is the ELAN network interface IP address for the card. Element Manager and the system use this address to communicate with the card.

If changing the Embedded LAN network interface IP address of the Leader card, Telnet to the card and use the **setLeader** command to make the same change (new Management IP address) in the NVRAM of the Leader card.

The Leader card must be reset to resume communication with the node.

Before resetting the Leader card, unplug all the other cards to prevent any other card from becoming the Master. When the Leader restarts, plug the cards back in. These other cards receive their new configuration from Leader 0.

- c. **Embedded LAN (ELAN) MAC address:** This is the motherboard Ethernet address from the [Table 62 "Voice Gateway Media Card installation summary sheet" \(page 223\)](#). All other IP address configuration depends on the accurate configuration of the

Management MAC address. The MAC address is located on the faceplate of the Voice Gateway Media Card and is labelled as MOTHERBOARD Ethernet address. The Management MAC address corresponds to the ELAN address.

- d. **Telephony LAN (TLAN) IP address:** This is the card Voice network interface IP address. This address is also known as the card TLAN network interface IP address. In an IP Telephony node, all cards must be assigned an IP address on the same TLAN subnet. The card Voice network interface IP address must be distinct from the node IP address.
- e. **Voice LAN (TLAN) gateway IP address:** This is the IP address of the router interface on the TLAN subnet. All cards in the IP Telephony node must be on the TLAN subnet; therefore, they all share the same Voice LAN /TLAN gateway IP address.

6 In the Element Manager navigator, click **System > Alarms > SNMP**.

- a. In the **Trap Source** section, enter the following applicable parameters:
 - Navigation Site Name
 - Navigation System Name
- b. In the **MIB-2 System Group Parameters** section, enter the following applicable parameters:
 - System Contact
 - System Location
 - System Name
- c. In the **Community** section, enter the following parameters for system management community strings for access to the Management Information Base (MIB) and trap generation, and administrator community strings for access to the MIB views:
 - System Management Read
 - System Management Write
 - Trap Community
 - Administrator Group

The SNMP community strings control access to the IP Telephony node. Element Manager uses the community strings to refresh the Voice Gateway Media Card status and to control the transmitting and retrieving of configuration data files for database synchronization.

- d. In the **Trap Destinations** section, enter the IP address of the trap destinations. SNMP traps are sent to the IP address entered. A maximum of eight IP addresses can be configured.
- e. Click **Save**.

The parameters are automatically synchronized with the Call Server, Signaling Server, Voice Gateway Media Cards, and Media Gateway Controller.

ATTENTION

You should perform an Equipment Data Dump (EDD) to save the configured information permanently.

After the parameters are synchronized, the associated host route entries are added to the routing table automatically. If a trap destination is removed, the corresponding routing table entry is removed as a result.

- 7 In the Element manager navigator, click **IP Network > Nodes: Servers, Media Cards**.
The **Node Configuration** window appears.
- 8 Click the **Edit** button for the node that is having the IP address changes.
The **Edit** window appears.
- 9 Enter the following **Embedded LAN (ELAN) configuration** settings:
 - a. **Call Server IP address:** This is the IP address of the Call Server on the ELAN subnet. Enter the Call Server ELAN network interface IP address (Active ELNK).

The Call Server ELAN network interface IP address must correspond to the Active ELNK IP address configured in LD 117. It must be on the same subnet as the ELAN IP address for the IP Line node.
 - b. **Survivable Media Gateway IP address:** This is the IP address of the Survivable Media Gateway on the ELAN subnet.

The Survivable Media Gateway IP address must correspond to the Active ELNK IP address. If configured, all Voice Gateway Media Cards in the same node should be in the same Survivable Cabinet.

The Survivable Media Gateway associated with the primary Signaling Server IP Telephony node is called the Alternate Call Server. It is usually located in the same equipment rack with the Call Server and Signaling Server. Therefore it is usually

connected to the same ELAN subnet as the Call Server and the primary Signaling Server IP Telephony node. The Alternate Call Server Media Gateway is equipped with sufficient trunk cards and Voice Gateway Media Cards, and centralized CallPilot. This provides a large degree of survivability in case of Call Server equipment failure for IP Phone users who normally register through the Signaling Server.

See *Communication Server 1000M and Meridian 1 Small System Installation and Commissioning (NN43011-310)*. See *Communication Server 1000M and Meridian 1 Large System Installation and Commissioning (NN43021-310)* for more information about survivability on the Meridian 1 and CS 1000M.

See *Communication Server 1000E Installation and Commissioning (NN43041-310)* for more information about survivability on the CS 1000E.

- c. **Signaling port:** The default value is 15000. The range is 1024 to 65535.
- d. **Broadcast port:** The default value is 15001. The range is 1024 to 65535.

10 Enter the following **Voice LAN (TLAN) configuration** settings:

- a. **Signaling port:** The default value is
The TLAN subnet signaling occurs on UDP ports 7300, 4100, 5100, and 5000.
- b. **Voice port:** Change the Voice port only as instructed by the IP network administrator to improve QoS for the IP Phones. This field displays the range for RTP packets sent to the IP Phones. For example, if RTP Header compression is used to reduce voice bandwidth on narrow band WAN links, then the TLAN voice port range must be set to 16 384 or higher.

The exact range is provided by the system administrator. In general, use the default of 5200. If, however, numerous IP Phones are working over low bandwidth WAN links using CISCO RTP header compression, then change the voice port to a number in the range of 16 384 to 32 767. Coordinate this value change with the system administrator.

The TLAN Voice port range is 1024 to 65535. The default Voice ports are 5200 to 5295. A check is performed to prevent the TLAN Voice and signaling UDP ports from having the same range.

11 If entries must be made to the card routing table, click the **Add** button to the right of **Routes**.

The Routes fields expand.

- 12 Enter the **IP address** and **Subnet mask** for any host that is not on the ELAN subnet but requires access to the Voice Gateway Media Card across the ELAN subnet.

A Telnet session for maintenance from a remote PC is an example of when this would be needed. The address of the remote PC would be added in the Route list.

The default route on the card causes packets for unknown subnets to be sent out the TLAN network interface. Packets from an external host arrive on the ELAN network interface. Responses are sent on the TLAN network interface. This process can cause one-way communication if the TLAN subnet is not routed to the ELAN subnet. It is necessary to add an entry in the Route list to correct the routing so that response packets are sent on the ELAN subnet. Each entry creates a route entry in the card route table that directs packets out the ELAN network interface. See [Figure 68 "Specifying additional ELAN routes"](#) (page 280).



CAUTION

Use caution when assigning card routing table entries. Do not include the IP address of an IP Phone. Otherwise, voice traffic to these IP Phones is incorrectly routed through the ELAN subnet and ELAN gateway. To avoid including the wrong IP address, Nortel recommends that Host IDs be defined for the card routing table entries.

To add additional routes, click the **Add** button again and enter the route information. Repeat this step for each route to be added.

- 13 Click **Save and Transfer** and then click **OK**.
- 14 In the **Node Configuration** window, click the **Transfer/Status** button associated with the node that had the IP address changes.

—End—

Restart a Voice Gateway Media Card

If the IP address of a single Voice Gateway Media Card has changed, it must be restarted in order for the changes to take effect.

ATTENTION

If IP addresses that affect the entire node are changed, all cards in the node must be restarted. See ["Restart all the Voice Gateway Media Cards"](#) (page 373).

Changes to the SNMP trap destination IP addresses take place immediately when the transfer occurs; restarting the cards is not required.

If the IP address of a Voice Gateway Media Card has changed, restart only that card.

Follow the steps in [Procedure 57 "Restarting a Voice Gateway Media Card at the CLI" \(page 372\)](#) to restart a specific card using the CLI. Alternatively, a Voice Gateway Media Card can be restarted from within Element Manager. Follow the steps in [Procedure 58 "Restarting a Voice Gateway Media Card in Element Manager" \(page 373\)](#) to restart the card using Element Manager.

Procedure 57

Restarting a Voice Gateway Media Card at the CLI

Step	Action

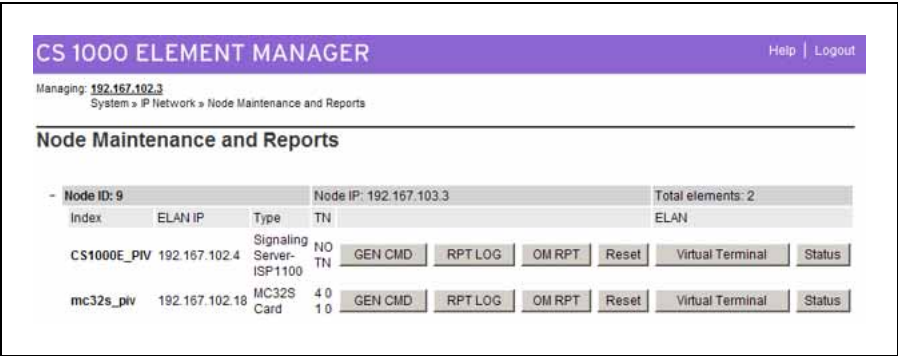
1	To prevent interruption to the speech path, log into LD 32.
2	Type the DISI command. This command disables the voice gateway channels when they become idle. DISI removes the call traffic but does not remove the IP Phones that are registered on that Voice Gateway Media Card. The Graceful TPS Disable command disiTPS removes the registered IP Phones.
3	Type disiTPS at the card IPL> or oam> prompt to disable the LTPS service on the Voice Gateway Media Card. This Graceful TPS Disable command prevents new IP Phones from registering on the card. All IP Phones registered on the card are redirected to another Voice Gateway Media Card when the IP Phone becomes idle. After the command is entered, an idle IP Phone should be updated with the Watchdog reset message. However, the LTPS sends a soft reset message to the IP Phone, redirecting it to the Connect Server. The disabled LTPS does not accept new registrations, so the IP Phones must register with another LTPS in the node. Eventually, as all of the LTPS IP Phones become idle, they are registered with other TPSs. The Voice Gateway Media Card can then be removed with no impact to any users.

—End—

Procedure 58
Restarting a Voice Gateway Media Card in Element Manager

Step	Action
1	In the Element Manager navigator, click IP Network > Maintenance and Reports . The Node Maintenance and Reports window appears.
2	Expand the node containing the Voice Gateway Media Card by clicking the plus sign (+) to the left of the Node ID.
3	Click the Reset button associated with the Voice Gateway Media Card. See Figure 92 "Reset button" (page 373).

Figure 92
Reset button



- 4 Click **OK** to confirm the Voice Gateway Media Card reset.

—End—

Restart all the Voice Gateway Media Cards

All the Voice Gateway Media Cards must be restarted if there has been a change to the following:

- node IP address
- subnet of either the TLAN or ELAN (by changing the subnet mask or the subnet fields of the IP address)

These changes affect the whole node. As a result, all the cards must be restarted.

If the Management (ELAN) network interface IP address of the Leader has changed, all the cards must be restarted. Even though this is a change to a single card, this change affects all cards, as this IP address is used to transmit properties to the node.

Follow the steps in [Procedure 59 "Changing the IP address of the Leader card" \(page 374\)](#) to restart all the Voice Gateway Media Cards.

Procedure 59

Changing the IP address of the Leader card

Step	Action
1	Telnet to the card.
2	Use the <code>setLeader</code> command to configure the new IP address. The Leader uses this new IP address when it reboots.
3	Reboot the Leader using the <code>cardReset</code> command. The Leader card reads the new IP address from NVRAM.
4	Restart all the other cards.
—End—	

Update other node properties

Some basic Voice Gateway Media Card configuration must be performed from the **IP Network >Nodes: Servers, Media Cards > Edit** window.

To update the node properties in the following sections:

- DSP Profile section – follow the steps in [Procedure 26 "Configuring DSP Profile data" \(page 270\)](#)
- QoS section – follow the steps in [Procedure 27 "Configuring QoS" \(page 274\)](#)

Telnet to a Voice Gateway Media Card using Virtual Terminal

To access the CLI on a Voice Gateway Media Card using Virtual Terminal from Element Manager, follow the steps in [Procedure 60 "Accessing a Voice Gateway Media Card using Telnet" \(page 375\)](#).

Procedure 60**Accessing a Voice Gateway Media Card using Telnet****Step Action**

- 1 In the Element Manager navigator, click **IP Network > Maintenance and Reports**.

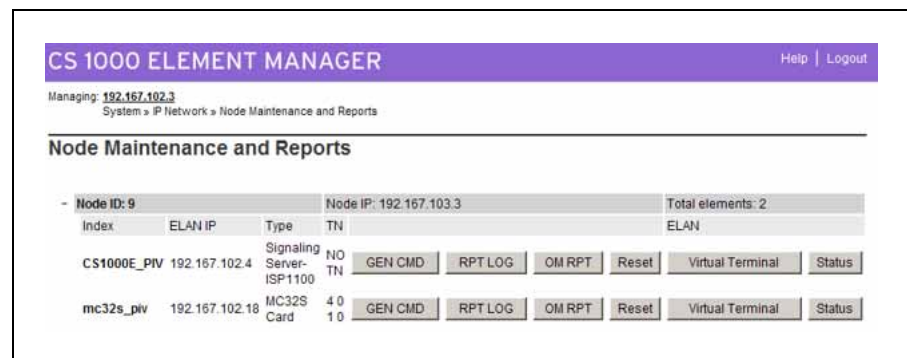
The **Node Maintenance and Reports** window appears.

- 2 Expand the node containing the Voice Gateway Media Card.

- 3 Click the **Virtual Terminal** button associated with the Voice Gateway Media Card.

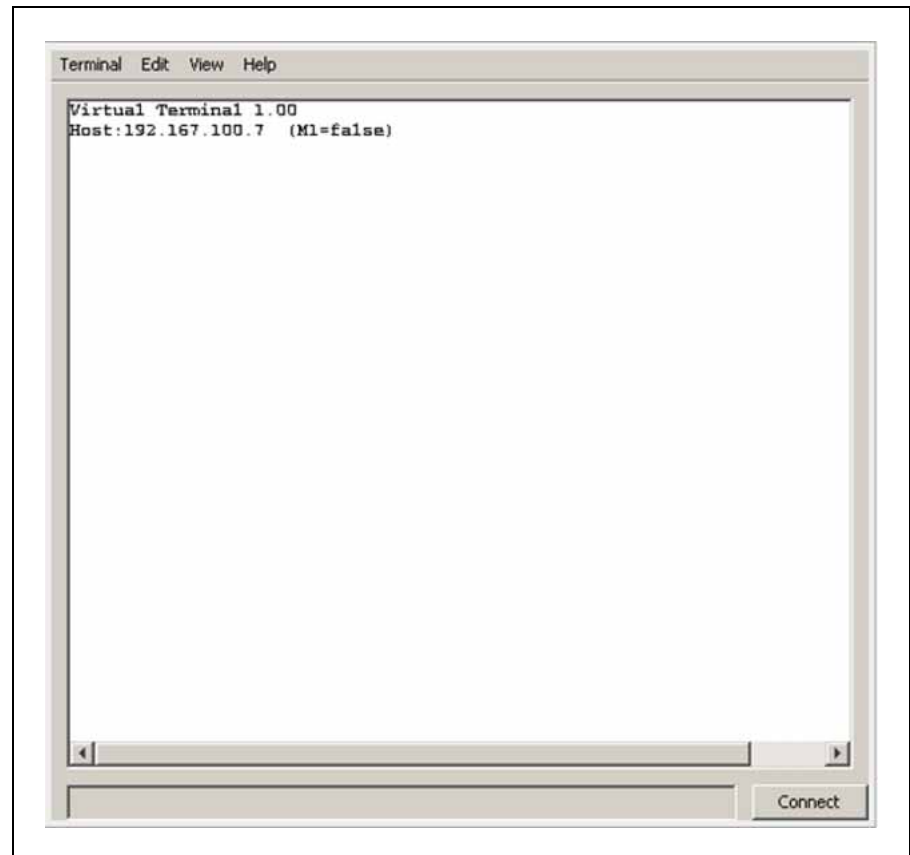
See [Figure 93 "Virtual Terminal" \(page 375\)](#).

Figure 93
Virtual Terminal



The **Virtual Terminal window** opens and automatically connects to the Voice Gateway Media Card by using the TLAN or ELAN network interface IP address. See [Figure 94 "Virtual Terminal window" \(page 376\)](#).

Figure 94
Virtual Terminal window



- 4 Enter a user name and password to access the IPL> or oam> CLI.
The IPL > or oam > prompt appears if the login is successful.
- 5 Type ? or Help (for the MC 32S card) at the prompt to display a list of available IPL > or oam> CLI commands.
See ["IP Line CLI commands" \(page 420\)](#) for a detailed list of commands.

—End—

Check the Voice Gateway Channels

To check the Voice Gateway Channels running on a Voice Gateway Media Card, follow the steps in [Procedure 61 "Checking the Voice Gateway Channels" \(page 377\)](#).

Procedure 61
Checking the Voice Gateway Channels

Step	Action
1	In the navigation tree, click IP Network > Maintenance and Reports . The Node Maintenance and Reports window appears.
2	Expand the node to show all its elements by clicking the plus sign (+) to the left of the Node ID.
3	Click the GEN CMD button associated with the Voice Gateway Media Card. The General Commands window appears.
4	From the Group drop-down list, select Vgw .
5	From the Command drop-down list, select vgwShowAll .
6	Click RUN . The output of the vgwShowAll command is displayed in the text area at the bottom of the window.
7	To view the VGW Channel configuration, from the Command drop-down list, select Print VGW Channels and click the RUN button.
—End—	

Setting the IP Phone Installer Password

Element Manager includes the CLI commands for setting the administrative and temporary IP Phone Installer Password. For detailed information about the IP Phone Installer Password, see the section "[IP Phone Installer Password](#)" (page 320).

To set the IP Phone Installer Password in Element Manager, follow the steps in [Procedure 62 "Setting the administrative and temporary IP Phone Installer Passwords"](#) (page 377).

Procedure 62
Setting the administrative and temporary IP Phone Installer Passwords

Step	Action
1	Click IP Network > Maintenance and Reports . The Node Maintenance and Reports window appears.

- 2 Expand the node to show all its elements.
- 3 Click the **GEN CMD** button associated with the Voice Gateway Media Card.
The **General Commands** windows opens.
- 4 From the **Group** drop-down list, select **NodePwd**.
- 5 From the **Command** drop-down list, select **nodePwdShow** and click the **RUN** button.

The output of the **nodePwdShow** command is displayed in the text area at the bottom of the window. If in the default state, the IP Phone Installer Password has never been set. The **nodePwdShow** output displays the following:

NodeID	PwdEna	Pwd	TmpPwd	Uses	Timeout
=====	=====	=====	=====	=====	=====
123	No			0	0d
0h 0m 0s					

where

NodeID – the IP Phone Installer Password configuration applies to all Voice Gateway Media Cards on the same TLAN subnet that belong to this Node ID.

PwdEna – by default the cards should be in disabled state (PwdEna=No). The PwdEna setting specifies the enabled (Yes) or disabled (No) state of the IP Phone Installer Password.

Pwd – this is the administrator IP Phone Installer Password. In the default state, the administrator password is null.

TmpPwd – this is the temporary IP Phone Installer Password. In the default state, the temporary password is null.

Uses – the Uses parameter applies to the temporary IP Phone Installer Password. In the default state, this setting is null. If the card is not in the default state, the Uses parameter is a numeric value from 0 – 1000. This number specifies the remaining number of uses for the temporary password. If zero is entered for the Uses parameter when setting the temporary password, the Time parameter is mandatory. When the Time parameter is in effect, the password expiration is based on time instead of the number of uses.

Timeout – the Timeout heading corresponds to the Timeout parameter of the temporary IP Phone Installer Password. In the default state the Timeout is null. If the card is not in the default state, this setting specifies the duration in hours in which the temporary password is valid. The range is 0 – 240 hours (which is a maximum of 10 days). The number specified under Timeout indicates the remaining time to expire of the temporary password.

The Timeout parameter is optional if the Uses parameter is non-zero. The Timeout parameter is mandatory if Uses is set to zero.

If both the Uses and Timeout parameters are entered, the password expires based on whichever happens first, that is, the number of Uses is reduced to zero or the Timeout has expired. If both the Uses and Timeout parameters are entered and are set to zero, it is the same as not setting the temporary password.

- 6 From the **Group** drop-down list, select **NodePwd**.
- 7 From the Command drop-down list, select **nodePwdSet** and click the **RUN** button.

The window refreshes and displays the blank **Node Password** field.

- 8 Enter the administrator IP Phone Installer Password in the **Node Password** field and click the **RUN** button.

This enables and configures the administrator password. The "password" parameter can be null, or 6 to 14 digits in length. The valid characters are 0 to 9, *, and #. This command can be entered at any time. The new password entered overwrites the previous password.

The text area returns the message *"Please run nodePwdShow to verify the result."*

- 9 From the Command drop-down list, select **nodePwdShow** and click **RUN**.

The text area data output is similar to the following:

NodeID	PwdEna	Pwd	TmpPwd	Uses	Timeout
=====	=====	=====	=====	=====	=====
123	Yes	1234567		0d 0h 0m 0s	



WARNING

If the **RUN** button in the Node Password field is clicked and no password is entered in the text box, then the password is enabled but is null. In the above output, the PwdEna field displays "Yes" and the Pwd field is blank.

- 10 To configure a temporary password, from the Command drop-down list, select **nodeTempPwdSet**.

The window refreshes and blank fields are displayed for the following: **Node Password**, **Uses**, and **Timeout**.

- 11 Enter the temporary Node Password, the number of uses, and the Timeout, and click **RUN**.

The text area returns the message *'Please run nodePwdShow to verify the result.'*

- 12** From the **Command** drop-down list, select **nodePwdShow** from the drop-down list box and click **RUN**.

The text area data output is similar to the following:

NodeID	PwdEna	Pwd	TmpPwd	Uses	Timeout
123	Yes	1234567	9876543	2	0d 0h 0m 0s

- 13** To clear the temporary IP Phone Installer password, select the **nodeTempPwdClear** command from the Command drop-down list and click **RUN**.

- 14** Confirm that the temporary password has been cleared.

From the **Command** drop-down list, select **nodePwdShow** and click **RUN**.

The text area data output is similar to the following:

NodeID	PwdEna	Pwd	TmpPwd	Uses	Timeout
123	Yes	1234567			0d 0h 0m 0s

—End—

IP Line administration using TM 3.1

Contents

This section contains the following topics:

- "Introduction" (page 381)
- "TM administration procedures" (page 381)
- "Back up and restore TM data" (page 395)
- "Add an IP Telephony node in TM by retrieving an existing node" (page 396)
- "IP Line CLI access using Telnet or local RS-232 maintenance port" (page 399)

Introduction

This chapter explains how to administer IP Line and the Voice Gateway Media Card on the systems using TM 3.1.

Telephony Manager (TM) provides a graphical user interface to the Voice Gateway Media Card. TM can be used to Telnet to the card, install and upgrade software, configure alarm event reporting, view and update card property and configuration data, add new cards to a node, schedule reports and other related tasks.



WARNING

The only support provided for nodes that reside on a CS 1000 system is the retrieval of OM reports. See [Procedure 63 "Scheduling Reports"](#) (page 383) through [Procedure 67 "Viewing IP Line info and error log"](#) (page 395).

TM administration procedures

This section describes the TM administration procedures using the TM 3.1 IP Line application. All references to TM in the following procedures assume the latest TM version.

Operational Measurement report scheduling and generation

Operational Measurement (OM) reports provide important statistical and traffic information and feedback to the system administrator to better engineer the system. The information stored in the OM file applies only to the calls routed over the IP network by way of IP Line. OM reports give a quantitative view of system performance, such as jitter.

TM is used to support Operational Measurements on the systems.

The OM reports are a collection of data from all the Voice Gateway Media Cards in the network. OM data is written to a file every hour. At midnight, the OM file is copied to a backup file, and the new day starts with a new file.

TM uses the following naming convention for the IP Line OM file names:

`ipline31_MM_YYYY_file1.csv`

The MM (month) portion of the file name is only one character for the months of January to September (1 to 9). The remaining three months appear as two-digit numbers (10, 11, and 12).

An example is **`ipline50_10_2002_file1.csv`**. This comma-delimited file opens in a program that interprets the .csv file, such as Microsoft Excel or any other comma-delimited file reader.

OM reports are generated on demand or on a preselected schedule. When a report is generated, the application retrieves the latest OM data from each Voice Gateway Media Card defined in TM.

Under certain conditions, the OM report is not available, as follows:

- the first hour after a Voice Gateway Media Card reboot
- the first hour after installing a new Voice Gateway Media Card

The following error messages are generated when requesting the OM report during the first hour:

- on TM: "fails to transfer the OM file"
- on the Voice Gateway Media Card console: "tfxl: Error File C:/OM/omreport.xxx not found"

Nortel recommends that report generation be scheduled once a day.

To schedule a generated OM Report, follow the steps in [Procedure 63 "Scheduling Reports" \(page 383\)](#).

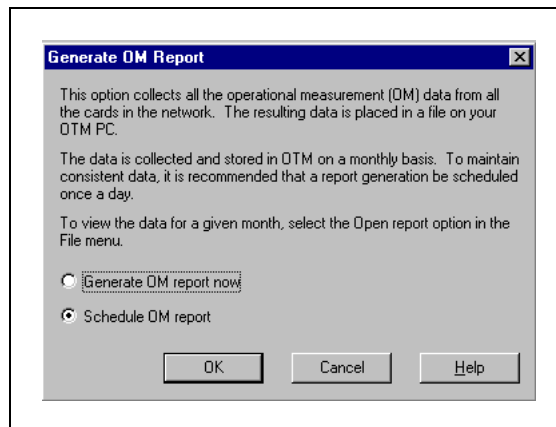
Procedure 63 Scheduling Reports

Step	Action

1	Select the node in the IP Telephony window. Click File > Report > Generate .

The **Generate OM Report** window appears. See [Figure 95 "Schedule an OM report" \(page 383\)](#).

Figure 95
Schedule an OM report



In the **Generate OM Report** window there are two choices, **Generate OM report now** and **Schedule OM report**.

2	Select the Schedule OM report radio button. Click OK .

The **Scheduling** window appears. See [Figure 96 "Scheduling an OM Report" \(page 384\)](#).

Figure 96
Scheduling an OM Report

- 3 Under **Job**, enter the **Name** and a **Description** for the scheduled OM Report.
- 4 Under **Run**, select the radio button that indicates the frequency of report generation.
- 5 Under **Start at**, enter the date and time of the start of the report period using the **Month**, **Day**, **Year**, **Hour**, and **Minute** list boxes and the **am** or **pm** radio buttons.
- 6 Under **Start at**, click the **Late execution** check box if the report is to run at a later time if the system is busy at the scheduled time.
- 7 Click **OK**.

—End—

The generated OM report includes information for all cards in all the nodes in the system. The report file accumulates data for the month. The data is stored in the generated file called `ipline_MM_YYYY_file#.csv`.

TM has a report feature called "Generate OM Report now". This feature enables an OM Report to be generated immediately.

**WARNING**

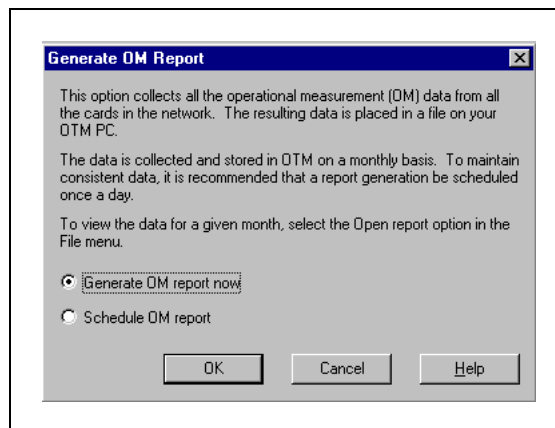
Running the "Generate OM Report now" feature while the Scheduled OM Reports feature is also running causes duplicate data to be displayed at the end of the OM Report. The data for the current day is appended to the end of the OM file by the "Generate OM Report Now" option.

Be careful to take into account any duplicate data when viewing system performance.

To generate an OM Report immediately, follow the steps in [Procedure 64 "Generating reports" \(page 385\)](#).

Procedure 64**Generating reports****Step Action**

- 1 In the **IP Telephony** window, click the node. Click **File > Report**.
The **Generate OM Report** window appears. See ["Generate OM Report – Generate OM report now" \(page 385\)](#).

Generate OM report now

- 2 Click **Generate OM report now** and then click **OK**.

TM creates and displays a report named **Operational Measurement Report**. This report is saved as a comma-delimited file (csv): `ipline31_MM_YYYY_file#.csv`. The default file that is generated opens in Microsoft Excel or any other application that can open.csv files.

—End—

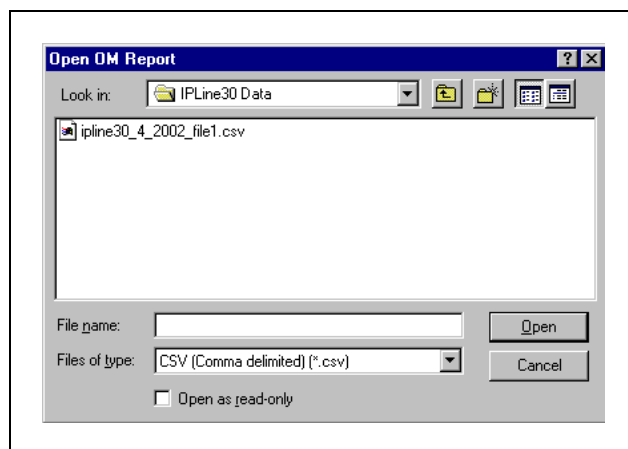
To open and view the OM Report file, follow the steps in [Procedure 65 "Opening an Operational Measurement \(OM\) report" \(page 386\)](#).

Procedure 65**Opening an Operational Measurement (OM) report****Step Action**

- 1 In the **IP Telephony** window, select the node in the top of the window.
- 2 Click **File > Report > Open**.

The **Open OM Report** window appears. See [Figure 97 "Open OM Report"](#) (page 386).

Figure 97
Open OM Report



- 3 Select a report file and click **Open**.

The file opens in a program that interprets.csv (comma-delimited) files such as Microsoft Excel. If Microsoft Excel is not installed on the PC, then TM notifies the user that the file is opened in Wordpad.

—End—

Operational Measurements (OM) information for a Voice Gateway Media Card in the node can be viewed using TM. This OM file is a view of the LTPS and Voice Gateway channel activity for each model of IP Phone on that card. (The TM OM Report Generation feature is an overview of all the cards in all sites and systems.)

The Voice Gateway Media Card OM file contains the following information for each model of IP Phone:

- the number of incoming and outgoing calls
- the number of call attempts
- the number of calls completed

- the total holding time for voice calls

To view a Voice Gateway Media Card OM file from TM, follow the steps in [Procedure 66 "Retrieving the current OM file from the Voice Gateway Media Card using TM"](#) (page 387).

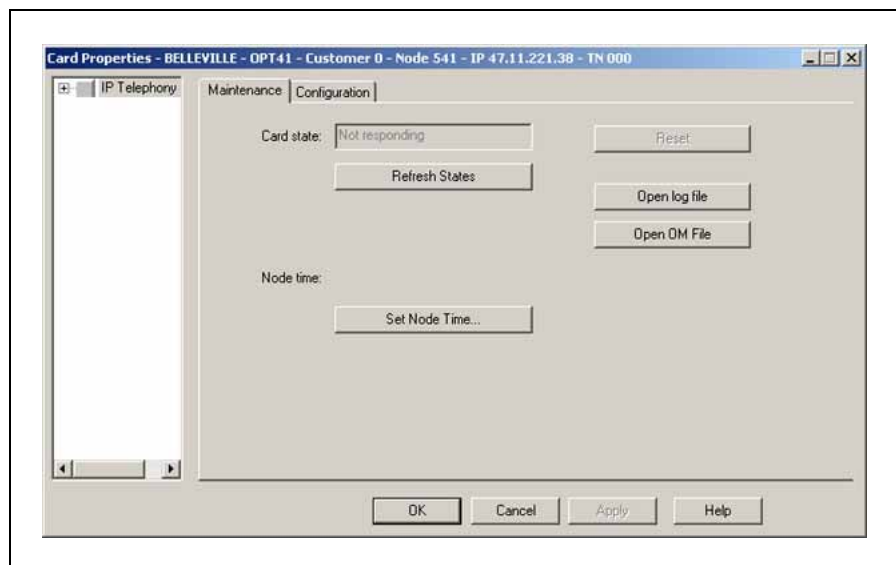
Procedure 66

Retrieving the current OM file from the Voice Gateway Media Card using TM

Step	Action
1	In the TM Navigator window, click the Services folder. Double-click the IP Telephony icon. The IP Telephony window appears.
2	Select the node in the upper portion of the window.
3	Select the Voice Gateway Media Card from the lower portion of the window.
4	Right-click the card and then select Properties from the pop-up menu. The Card Properties window appears to the Maintenance tab. See Figure 98 "Card Properties window Maintenance tab" (page 387).

Figure 98

Card Properties window Maintenance tab



5 Click the **Open OM File** button.

A file called **om.txt** opens in the WordPad application. The file contains collection period information for each hour of the day that the card was running, broken down for each model of IP Phone.

—End—

The file contains collection period information for each hour of the day that the card was running.

The collection periods start with the hour from midnight to 1:00 am. As each hour passes, TM adds another collection period to the OM file; therefore, there is a maximum of 24 collection periods each day.

Output

The OM report output tracks the statistics for each IP Phone type.

Data is first output for the IP Phones followed by the data for the gateway channels.

Output example

```
-> ommShow
collection_time : 11/7/2006 2:00
2004Reg_Att: 0
2004Reg_Fail: 0
2004Unreg_Att: 0
2004Aud_Setup: 0
2004Jitter_Avg: 0.0
2004Jitter_Max: 0
2004Latency_Avg: 0.0
2004Latency_Max: 0
2004Pkt_Lost: 0.00
2004Listen_RFactor: 0.0
2004Voice_Time: 0 mins 0 secs
2002Reg_Att: 0
2002Reg_Fail: 0
2002Unreg_Att: 0
2002Aud_Setup: 0
2002Jitter_Avg: 0.0
2002Jitter_Max: 0
2002Latency_Avg: 0.0
2002Latency_Max: 0
2002Pkt_Lost: 0.00
2002Listen_RFactor: 0.0
2002Voice_Time: 0 mins 0 secs
2001Reg_Att: 0
2001Reg_Fail: 0
2001Unreg_Att: 0
2001Aud_Setup: 0
2001Jitter_Avg: 0.0
2001Jitter_Max: 0
2001Latency_Avg: 0.0
```



```
2001Latency_Max: 0
2001Pkt_Lost: 0.00
2001Listen_RFactor: 0.0
2001Voice_Time: 0 mins 0 secs
1150Reg_Att: 0
1150Unreg_Att: 0
1150Aud_Setup: 0
1150Jitter_Avg: 0.0
1150Jitter_Max: 0
1150Latency_Avg: 0.0
1150Latency_Max: 0
1150Pkt_Lost: 0.00
1150Listen_RFactor: 0.0
1150Voice_Time: 0 mins 0 secs
1130Reg_Att: 0
1130Reg_Fail: 0
1130Unreg_Att: 0
1130Aud_Setup: 0
1130Jitter_Avg: 0.0
1130Jitter_Max: 0
1130Latency_Avg: 0.0
1130Latency_Max: 0
1130Pkt_Lost: 0.00
1130Listen_RFactor: 0.0
1130Voice_Time: 0 mins 0 secs
2004P2Reg_Att: 0
2004P2Reg_Fail: 0
2004P2Unreg_Att: 0
2004P2Aud_Setup: 0
2004P2Jitter_Avg: 0.0
2004P2Jitter_Max: 0
2004P2Latency_Avg: 0.0
2004P2Latency_Max: 0
2004P2Pkt_Lost: 0.00
2004P2Listen_RFactor: 0.0
2004P2Voice_Time: 0 mins 0 secs
2002P2Reg_Att: 0
2002P2Reg_Fail: 0
2002P2Unreg_Att: 0
2002P2Aud_Setup: 0
2002P2Jitter_Avg: 0.0
2002P2Jitter_Max: 0
2002P2Latency_Avg: 0.0
2002P2Latency_Max: 0
2002P2Pkt_Lost: 0.00
2002P2Listen_RFactor: 0.0
2002P2Voice_Time: 0 mins 0 secs
2033Reg_Att: 0
2033Reg_Fail: 0
2033Unreg_Att: 0
```

```
2033Aud_Setup: 0
2033Jitter_Avg: 0.0
2033Jitter_Max: 0
2033Latency_Avg: 0.0
2033Latency_Max: 0
2033Pkt_Lost: 0.00
2033Listen_RFactor: 0.0
2033Voice_Time: 0 mins 0 secs
2050Reg_Att: 0
2050Reg_Fail: 0
2050Unreg_Att: 0
2050Aud_Setup: 0
2050Jitter_Avg: 0.0
2050Jitter_Max: 0
2050Latency_Avg: 0.0
2050Latency_Max: 0
2050Pkt_Lost: 0.00
2050Voice_Time: 0 mins 0 secs
2210Reg_Att: 0
2210Reg_Fail: 0
2210Unreg_Att: 0
2210Aud_Setup: 0
2210Jitter_Avg: 0.0
2210Jitter_Max: 0
2210Latency_Avg: 0.0
2210Latency_Max: 0
2210Pkt_Lost: 0.00
2210Listen_RFactor: 0.0
2210Voice_Time: 0 mins 0 secs
1120Reg_Att: 0
1120Reg_Fail: 0
1120Unreg_Att: 0
1120Aud_Setup: 0
1120Jitter_Avg: 0.0
1120Jitter_Max: 0
1120Latency_Avg: 0.0
1120Latency_Max: 0
1120Pkt_Lost: 0.00
1120Listen_RFactor: 0.0
1120Voice_Time: 0 mins 0 secs
1110Reg_Att: 0
1110Reg_Fail: 0
1110Unreg_Att: 0
1110Aud_Setup: 0
1110Jitter_Avg: 0.0
1110Jitter_Max: 0
1110Latency_Avg: 0.0
1110Latency_Max: 0
1110Pkt_Lost: 0.00
1110Listen_RFactor: 0.0
```

```
1110Voice_Time: 0 mins 0 secs
2050MReg_Att: 0
2050MReg_Fail: 0
2050MUnreg_Att: 0
2050MAud_Setup: 0
2050MCJitter_Avg: 0.0
2050MCJitter_Max: 0
2050MCLatency_Avg: 0.0
2050MCLatency_Max: 0
2050MCPkt_Lost: 0.00
2050MCVoice_Time: 0 mins 0 secs
2211Reg_Att: 0
2211Reg_Fail: 0
2211Unreg_Att: 0
2211Aud_Setup: 0
2211Jitter_Avg: 0.0
2211Jitter_Max: 0
2211Latency_Avg: 0.0
2211Latency_Max: 0
2211Pkt_Lost: 0.00
2211Listen_RFactor: 0.0
2211Voice_Time: 0 mins 0 secs
1160Reg_Att: 0
1160Reg_Fail: 0
1160Unreg_Att: 0
1160Aud_Setup: 0
1160Jitter_Avg: 0.0
1160Jitter_Max: 0
1160Latency_Avg: 0.0
1160Latency_Max: 0
1160Pkt_Lost: 0.00
1160Listen_RFactor: 0.0
1160Voice_Time: 0 mins 0 secs
2212Reg_Att: 0
2212Reg_Fail: 0
2212Unreg_Att: 0
2212Aud_Setup: 0
2212Jitter_Avg: 0.0
2212Jitter_Max: 0
2212Latency_Avg: 0.0
2212Latency_Max: 0
2212Pkt_Lost: 0.00
2212Listen_RFactor: 0.0
2212Voice_Time: 0 mins 0 secs
2007Reg_Att: 0
2007Reg_Fail: 0
2007Unreg_Att: 0
2007Aud_Setup: 0
2007Jitter_Avg: 0.0
2007Jitter_Max: 0
```

```
2007Latency_Avg: 0.0
2007Latency_Max: 0
2007Pkt_Lost: 0.00
2007Listen_RFactor: 0.0
2007Voice_Time: 0 mins 0 secs
1140Reg_Att: 0
1140Reg_Fail: 0
1140Unreg_Att: 0
1140Aud_Setup: 0
1140Jitter_Avg: 0.0
1140Jitter_Max: 0
1140Latency_Avg: 0.0
1140Latency_Max: 0
1140Pkt_Lost: 0.00
1140Listen_RFactor: 0.0
1140Voice_Time: 0 mins 0 secs
1175Reg_Att: 0
1175Reg_Fail: 0
1175Unreg_Att: 0
1175Aud_Setup: 0
1175Jitter_Avg: 0.0
1175Jitter_Max: 0
1175Latency_Avg: 0.0
1175Latency_Max: 0
1175Pkt_Lost: 0.00
1175Listen_RFactor: 0.0
1175Voice_Time: 0 mins 0 secs
ChanAud_Setup: 0
ChanJitter_Avg: 0.0
ChanJitter_Max: 0
ChanPkt_Lost: 0.00
ChanVoice_Time: 0 mins 0 secs
H323VtrkInVoCallAttempt: 0
H323VtrkInVoCallComp: 0
H323VtrkOutVoCallAttempt: 0
H323VtrkOutVoCallComp: 0
H323VtrkTotalVoiceTime: 0 mins 0 secs
H323VtrkInFaxCallAttempt: 0
H323VtrkInFaxCallComp: 0
H323VtrkOutFaxCallAttempt: 0
H323VtrkOutFaxCallComp: 0
H323VtrkFallBack: 0
H323VtrkQoSFallBack: 0
H323VtrkATPMFallBack: 0
H323VtrkRelCompFallBack: 0
SIPVtrkInVoCallAttempt: 0
SIPVtrkInVoCallComp: 0
SIPVtrkOutVoCallAttempt: 0
SIPVtrkOutVoCallComp: 0
SIPVtrkTotalVoiceTime: 0 mins 0 secs
```

SIPVtrkInFaxCallAttempt: 0
SIPVtrkInFaxCallComp: 0
SIPVtrkOutFaxCallAttempt: 0
SIPVtrkOutFaxCallComp: 0
SIPVtrkFallBack: 0
SIPVtrkQoSFallBack: 0
SIPVtrkATPMFallBack: 0
SIPVtrkRelCompFallBack: 0
SIPVtrkTLSAuthenticationFailure: 0
SIPVtrkTLSIncomingAttempt: 0
SIPVtrkTLSIncomingComp: 0
SIPVtrkTLSIncomingFailure: 0
SIPVtrkTLSOutgoingAttempt: 0
SIPVtrkTLSOutgoingComp: 0
SIPVtrkTLSOutgoingFailure: 0
OutTotalH323OvlCallCount: 0
OutSuccessH323OvlCallCount: 0
OutOvl2EnblocCallCount: 0
InTotalH323OvlCallCount: 0
InSuccessH323OvlCallCount: 0
TotalARQGenerated: 0
TotalARJRcvd: 0
TotalACFRcvd: 0
H323NrsGatekeeperReq: 0
H323NrsGatekeeperConf: 0
H323NrsGatekeeperRej: 0
H323NrsRegistrationReq: 144
H323NrsRegistrationConf: 144
H323NrsRegistrationRej: 0
H323NrsUnregistrationReqRecd: 0
H323NrsUnregistrationConfSent: 0
H323NrsUnregistrationRejSent: 0
H323NrsAdmissionReq: 0
H323NrsAdmissionConf: 0
H323NrsAdmissionRej: 0
H323NrsLocationReqRecd: 0
H323NrsLocationConfSent: 0
H323NrsLocationRejSent: 0
H323NrsBandwidthReqRecd: 0
H323NrsBandwidthConfSent: 0
H323NrsBandwidthRejSent: 0
H323NrsDisengageReq: 0
H323NrsDisengageConf: 0
H323NrsDisengageRej: 0
SIPNrsRoutingAttempts: 0
SIPNrsRoutingSuccesses: 0
SIPNrsRoutingFailures: 0
SIPNrsRegistrationAttempts: 138
SIPNrsRegistrationSuccesses: 138
SIPNrsRegistrationFailures: 0

```
SIPCTITotalSoftClientlogonAttempts: 0
SIPCTITotalSoftClientlogonSuccesses: 0
SIPCTITotalAnswerCallRequests: 0
SIPCTITotalAnswerCallSuccesses: 0
SIPCTITotalClearConnectionRequests: 0
SIPCTITotalClearConnectionSuccesses: 0
SIPCTITotalConsultationCallRequests: 0
SIPCTITotalConsultationCallSuccesses: 0
SIPCTITotalDeflectCallRequests: 0
SIPCTITotalDeflectCallSuccesses: 0
SIPCTITotalHoldCallRequests: 0
SIPCTITotalHoldCallSuccesses: 0
SIPCTITotalMakeCallRequests: 0
SIPCTITotalMakeCallSuccesses: 0
SIPCTITotalRetrieveCallRequests: 0
SIPCTITotalRetrieveCallSuccesses: 0
SIPCTITotalSingleStepTransferRequests: 0
SIPCTITotalSingleStepTransferSuccesses: 0
SIPCTITotalTransferCallRequests: 0
SIPCTITotalTransferCallSuccesses: 0
SIPCTITotalMonitorStartRequests: 0
SIPCTITotalMonitorStartSuccesses: 0
SIPCTITotalMonitorStopRequests: 0
SIPCTITotalMonitorStopSuccesses: 0
SIPCTITotalConferenceCallRequests: 0
SIPCTITotalConferenceCallSuccesses: 0
SIPCTITotalSetForwardingRequests: 0
SIPCTITotalSetForwardingSuccesses: 0
SIPCTITotalGetForwardingRequests: 0
SIPCTITotalGetForwardingSuccesses: 0
SIPCTITotalSessionTerminated: 0
```

Each collection period provides the following information:

- The date and time for the collection period hour.
- LTPS information for IP Phones that are registered to the LTPS on the Voice Gateway Media Card during that hour. The LTPS information is prefixed by the model number (2001P2, 2002P1, 2002P2, 2004P1, 2004P2, 2050PC). During normal operation, the LTPS values for the Voice Gateway Media Card can be zeros as the IP Phones normally register to the LTPS on the Signaling Server.
- Voice Gateway channel information accumulated during the hour. The Voice Gateway data is prefixed by *Chan*.
- Notes indicating whether the machine has been rebooted during the hour.

The OM file relates to the omreport.xxx file on the Voice Gateway Media Card, where xxx indicates the numbers of days since December 31.

In general, no relationship exists between the IP Phones registered on a card and the Voice Gateway channels on the card (if two or more cards are used) in the node. If only one card is used (with multiple IP Phones), a partial correlation might exist between the IP Phones and the card information. However, even with only one card, there still is not a 100% correlation, as an IP Phone can still call another IP Phone without involving the Voice Gateway channels.

Viewing the IP Line log files

TM uses FTP to transfer the log file from the Voice Gateway Media Card to the PC. The file is opened in WordPad. The IP Line Error log file (syslog) displays error information, including error date/time, the originating module (IP Telephony node), and specific error data.

To view IP Line error conditions that are abnormal events, but not severe enough to raise an alarm, follow the steps in [Procedure 67 "Viewing IP Line info and error log" \(page 395\)](#).

Procedure 67

Viewing IP Line info and error log

Step	Action
1	In the TM Navigator window, click the Services folder.
2	Double-click the IP Telephony icon. The IP Telephony window appears.
3	Right-click the card and then select Properties from the pop-up menu. The Card Properties window appears on the Maintenance tab.
4	Click the Open log file button and review the file contents.
—End—	

Back up and restore TM data

The TM Backup Wizard is used to backup and restore any or all TM PC-based data, including IP Line TM data. All IP Line data is stored in an Access database file on the TM PC or Server. This file is backed up only when the "Full TM Backup" option is selected. This option backs up all TM data contained in the PC directory where TM is installed and can only be used to restore all data.

For more information about using the TM Backup Wizard, see *Telephony Manager 3.1 System Administration (NN43050-601)*.

Add an IP Telephony node in TM by retrieving an existing node

Use this optional procedure in the following cases:

- to add existing nodes to a particular TM PC to manage the IP Telephony network from a single point of view
- to restore the IP Telephony configuration database to an TM PC whose hard drive has crashed, as an alternative to restoring the TM IP Telephony nodes from the TM Disaster Recovery Backup

When the IP Telephony node is installed and configured manually, that node can then be added to another TM PC by retrieving the configuration data from the existing IP Telephony node.

Configure the site name, system name, and customer number in the TM Navigator before adding a new IP Telephony node. Only one IP Telephony node can be added in the TM IP Line application for each system customer.

If multiple TM PCs are used to manage the same IP Telephony network, care must be taken to synchronize the different copies of the IP Telephony database. The TM **Configuration > Synchronize > Retrieve** function can be used to synchronize the TM IP Telephony database with the database on the IP Telephony node.

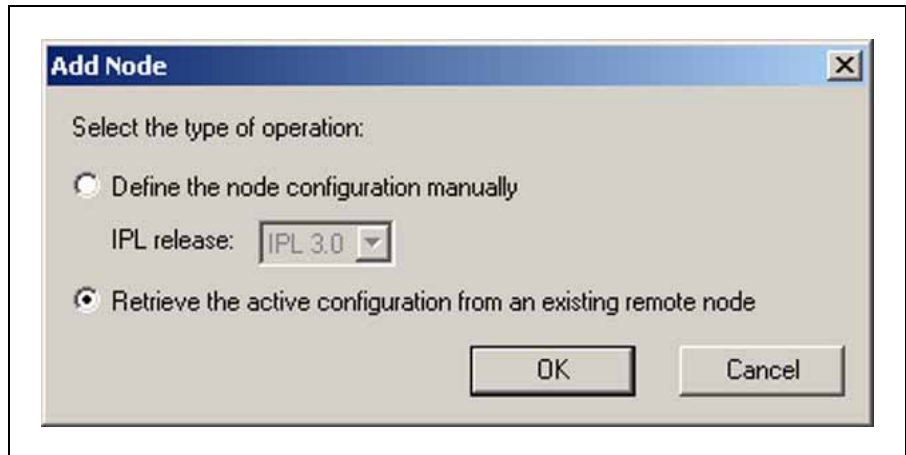
Follow the steps in [Procedure 68 "Adding a node by retrieving an existing node" \(page 396\)](#) to add an IP Telephony node by retrieving an existing node.

Procedure 68

Adding a node by retrieving an existing node

Step	Action
1	In the TM Navigator window, click the Services folder. Double-click the IP Telephony icon. The IP Telephony window appears.
2	Click Configuration > Node > Add . The Add Node dialog box opens. See Figure 99 "Add Node window Retrieve configuration from existing node" (page 397) .

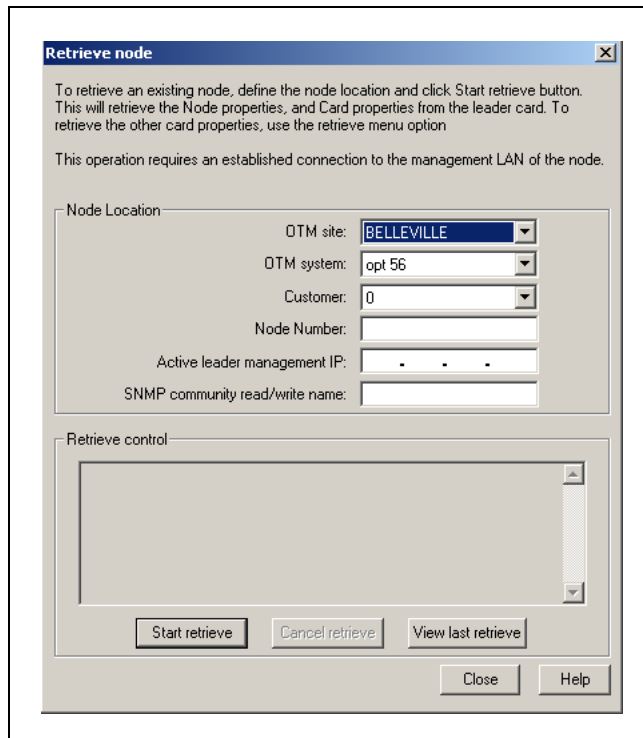
Figure 99
Add Node window Retrieve configuration from existing node



- 3 Click the **Retrieve the active configuration from an existing remote node** radio button, and then click **OK**.

The **Retrieve node** window appears. See [Figure 100 "Retrieve node"](#) (page 397).

Figure 100
Retrieve node



- 4 The TM site name, TM system name, and customer number must exist in the TM Navigator before a new IP Telephony node can be added.

Ensure the system type is defined correctly.

Under **Node Location** in the **Retrieve node** window:
 - a. **TM site:** Select the OM Site.
 - b. **TM system:** Select the system.
 - c. **Customer:** Select the Customer number.
 - d. **Node Number:** Ensure the node number is unique under the customer number. Also, ensure that all IP Telephony nodes connected to the same TLAN subnet have a unique node number regardless of the TM site and customer number.
 - e. **Active leader management (ELAN) IP:** Enter the active Leader management IP address field for the existing node.
 - f. **SNMP community read/write name:** Enter the SNMP read/write community string.

The SNMP read community string cannot be used.
- 5 Click **Start retrieve**.

The results of the retrieval are shown under **Retrieve control**. The node properties are retrieved from the active Leader. The card properties are retrieved from Leader 0.
- 6 Click **Close** when the download is complete.
- 7 In the **IP Telephony** window, select the newly added node in the top part of the window.
- 8 Refresh the card status (**View > Refresh**) and verify that the cards in the newly added node are responding.

A new node has been created by retrieving data from another node
- 9 Double-click on the new node in the **IP Telephony** window. The **Node Properties** window appears for the newly-added node.
- 10 Inspect each tab in the node properties and verify the data is correct and consistent with the node from which the data was retrieved.
- 11 Click the **Configuration** tab and ensure the Host names information, IP addresses, and TN are consistent.

—End—

IP Line CLI access using Telnet or local RS-232 maintenance port

There are two ways to access the Command Line Interface (CLI):

1. Use the NTAG81CA cable to connect the DIN8 pin connector on the faceplate, or the NTAG81BA cable to connect the DB9 I/O breakout cable to the COM port of a local PC. Use a null-modem adapter to connect a modem for remote dial-up access.
2. Telnet to the card from the TM **IP Telephony** window. This automatically Telnets to the IP address of the Management interface (ELAN) of the card. Alternatively, use the Telnet application on a PC and manually enter the Management (ELAN) IP address, Voice (TLAN) IP address, or the node IP address if trying to connect to the active Leader.



CAUTION

Do not connect two maintenance terminals to both the faceplate and I/O panel serial maintenance port connections at the same time.

Telnet to a Voice Gateway Media Card

To access the CLI on a Voice Gateway Media Card from the TM PC, follow the steps in [Procedure 69 "Accessing a Voice Gateway Media Card using Telnet" \(page 399\)](#).

Procedure 69

Accessing a Voice Gateway Media Card using Telnet

Step	Action
1	Click the Services folder. Double-click the IP Telephony icon. The IP Telephony window appears.
2	Right-click on the Voice Gateway Media Card to be accessed.
3	Select Telnet to ITG card from the popup menu. The TM PC opens a Telnet window and automatically connects to the Voice Gateway Media Card by using the Management (ELAN) IP address.
4	Enter a user name and password to access the IPL> or oam> CLI. The default user name and password is admin1 and 0000 . However, for security purposes, the user name and password should have been changed during installation. The IPL> or oam> prompt appears if the logon is successful.

- 5 Type ? or Help (MC 32S card) at the prompt to display a list of available IPL> and oam> CLI commands.

See "IP Line CLI commands" (page 420) for a detailed list of commands.

—End—

Voice Gateway Media Card maintenance

Contents

This section contains the following topics:

- "Introduction" (page 401)
- "Faceplate maintenance display codes" (page 401)
- "System error messages" (page 405)
- "IP Line and IP Phone maintenance and diagnostics" (page 410)
- "IP Line CLI commands" (page 420)
- "Lamp Audit and Keep Alive functions" (page 448)
- "Voice Gateway Media Card self-tests" (page 452)
- "Troubleshoot a software load failure" (page 452)
- "Troubleshoot an IP Phone installation" (page 455)
- "Maintenance telephone" (page 456)
- "Replace the Media Card's CompactFlash" (page 456)

Introduction

This chapter provides information about maintenance functions for the Voice Gateway Media Card.

Check the Nortel Web site for information about the latest software, firmware, and application releases.

Faceplate maintenance display codes

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

- [Table 82 "ITG-P 24-port line card faceplate maintenance display codes" \(page 402\)](#) lists the normal and fault display codes for the ITG-P 24-port line card.

- [Table 83 "Media Card faceplate maintenance display codes" \(page 403\)](#) list the normal and fault display codes for the Media Card 32-port line card.
- [Table 85 "Media Card 32 card diagnostic information" \(page 404\)](#) and [Table 86 "Messages displayed on the LED during Media Card 32S card normal operation" \(page 405\)](#) lists the messages on the faceplate for the Media Card 32S card.

During power-up, the card performs multiple self-tests, including an internal RAM test, ALU test, address mode test, boot ROM test, timer test, and 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 example, if the timer test fails on the ITG-P 24-port line card, F:05 is displayed.

If the other tests fail (up to and including the EEPROM test), a message is displayed for three seconds. If more than one test fails, the message displayed indicates the first failure. If verbose mode has been selected (by the test input pin on the backplane), the three-second failure message is not displayed.

If the maintenance display on the ITG-P 24-port line card shows a persistent T:20 indicating an IP Line software failure, and if this occurs after the card was reset during a loadware download procedure, call Nortel technical support for assistance in attempting to download new software onto the card.

Table 82
ITG-P 24-port line card faceplate maintenance display codes

Normal code	Fault code	Message
T:00	F:00	Initialization
T:01	F:01	Testing Internal RAM
T:02	F:02	Testing ALU
T:03	F:03	Testing address modes
T:04	F:04	Testing Boot ROM
T:05	F:05	Testing timers
T:06	F:06	Testing watchdog
T:07	F:07	Testing external RAM
T:08	F:08	Testing Host DPRAM
T:09	F:09	Testing DS30 DPRAM
T:10	F:10	Testing Security Device
T:11	F:11	Testing Flash memory
T:12	F:12	Programming PCI FPGA

Normal code	Fault code	Message
T:13	F:13	Programming DS30 FPGA
T:14	F:14	Programming CEMUX FPGA
T:15	F:15	Programming DSP FPGA
T:16	F:16	Testing CEMUX interface
T:17	F:17	Testing EEPROM
T:18	F:18	Booting processor, waiting for response with self-test information.
T:19	F:19	Waiting for application start-up messages from processor.
T:20		CardLAN enabled, transmitting BootP requests. If this display persists, then the ITG-P 24-port line card is running in BIOS ROM mode due to card software failure.

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

Table 83
Media Card 32-port card faceplate maintenance display codes

Normal code	Fault code	Message
T:00	F:00	Initialization
T:01	F:01	Testing Internal RAM
T:02	F:02	Testing ALU
T:03	F:03	Testing address modes
T:04	F:04	Testing watchdog
T:05	F:05	Testing 8051 coprocessor
T:06	F:06	Testing timers
T:07	F:07	Testing external RAM
T:08	F:08	Testing dongle
T:09	F:09	Programming timeswitch FPGA
T:10	F:10	Programming ISPD1 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

Normal code	Fault code	Message
T:14	F:14	Booting Host processor, waiting for response with selftest 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
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 84 "List of error codes for the Media Card" \(page 404\)](#) shows the list of error codes.

Table 84
List of error codes for the Media Card 32-port card

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

When the Media Card 32S card boots, diagnostic information, such as boot status, is displayed on the faceplate.

Table 85
Media Card 32 card diagnostic information

Message	Description
BOOT	Appears when the display becomes active.

POST	Power On Self Test (POST) Displays while the Media Card 32S card carries out hardware system tests during system power-up.
PASS	Displays when POST passes.
EXXX	Displays if a serious system error is detected. Error code where XXX is a numeric value.
LOAD	Displays when application software loads.

In normal operation, the messages appear in the following order:

- BOOT
- POST
- PASS
- LOAD

If there is a self-test error, an error code is displayed.

The faceplate displays Leader or Follower, and the number of registered IP Phones.

Table 86
Messages displayed on the LED during Media Card 32S card normal operation

Message	Description
Exxx	E indicates an error code when a serious system error is detected, and xxx is a numeric value.
Lxxx	L indicates the card is a Leader, and xxx is the number of registered IP Phones.
Fxxx	F indicates the card is a Follower, and xxx is the number of registered IP Phones.
Sxxx	S indicates a system link error code, and xxx is a numeric value.

System error messages

When an error or specific event occurs, SNMP agent on the Voice Gateway Media Card sends an alarm trap to TM or any SNMP manager that is configured in the SNMP Manager list in the ITG Card properties. System error message are also written to the error log file containing error messages.

View the error log in TM 3.1 IP Line by clicking the **Open Log File** button on the **Maintenance** tab of the **ITG Card Properties**. Alternatively, view the log file in any text browser after uploading it to an FTP host using the **LogFilePut** command.

ITG and ITS messages incorporate the severity category of the message in the first digit of the four digit number. Message numbers beginning with 0 do not follow this format.

- 1 = Critical
- 2 = Major
- 3 = Minor
- 4 = Warning
- 5 = Cleared (Info)
- 6 = Indeterminate (Info)

Error messages with a severity category of "Critical" are displayed on the Voice Gateway Media Card maintenance faceplate display in the form: "Gxxx" or "Sxxx", where xxx is the last three digits of the ITG or ITS message. The Signaling Server does not have a faceplate display. Alarms appear in the Signaling Serverreport log or by way of SNMP on an Alarm browser.

Table 87 "Critical ITG Error messages" (page 406) lists the critical ITG messages and Table 88 "Critical ITS Error messages" (page 409) lists the critical ITS messages.

All listed alarms can be sent by a Voice Gateway Media Card. Any alarm that can be sent by the Signaling Server has an "X" in the column labeled "Signaling Server."

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

Table 87
Critical ITG Error messages

Maintenance display	Corresponding critical error message	Signaling Server	Description
G000	ITG1000	X	Card (re)booted.
G001	ITG1001	X	Task spawn failure <name>.
G002	ITG1002	X	Memory allocation failure.
G003	ITG1003	X	File IO error <operation> <object> <errno> <errtext>.
G004	ITG1004	X	Network IO error <operation> <object> <errno> <errtext>.
G005	ITG1005	X	Message queue error <operation> <object> <errno> <errtext>.
G006	ITG1006	X	Unexpected state encountered <file> <line> <state>.

Maintenance display	Corresponding critical error message	Signaling Server	Description
G007	ITG1007	X	Unexpected message type <file> <line> <msg>.
G008	ITG1008	X	Null pointer encountered <file> <line> Name of pointer.
G009	ITG1009	X	Invalid block <file> <line> Type of block.
G010	ITG1010	X	Unable to locate data block <file> <line> Type of block.
G011	ITG1011	X	File transfer error: <operation> <file> <host>
G012	ITG1012	X	Module initialization failure: <moduleName>
G013	ITG1013		Ethernet receiver buffer unavailable, packet discarded.
G014	ITG1014	X	Ethernet carrier: <ifName> <state>
G015	ITG1015		Ethernet device failure: <ifName>
G017	ITG1017	X	Invalid or unknown SSD message: <ssdType> <TN> <msg>
G018	ITG1018		Invalid or unknown X12 SSD message <TN> <msg>
G019	ITG1019		DSP channel open failure <channel>.
G020	ITG1020	X	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		DSP failure <dsp> <errno> <errtext>
G025	ITG1025		DSP download: <dsp> <reason>
G026	ITG1026		DSP download retry succeeded <dsp>
G027	ITG1027		DSP memory test: <dsp> <reason>
G028	ITG1028	X	Voice packet loss: <channel> <%packetLoss> <direction> <dstAddr>

Maintenance display	Corresponding critical error message	Signaling Server	Description
G029	ITG1029		Error in DSP task <file> <line> <errno> <errtext>.
G030	ITG1030		Allocation failure in DSP memory pool.
G031	ITG1031	X	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: <call Server IP> <up/down>
G037	ITG1037		Wrong image downloaded. Binary was created for <cardType> card.
G038	ITG1038		IPL logon protection (logon available/locked)
G039	ITG1039		Bad DSP channel <channel id>
G040	ITG1040		Last reset reason for card: <reasonString> where the reason String can be: Reboot command issued (by software or through CLI); Watchdog Timer Expired; Manual reset; Internal XA problem; or Unknown
G041	ITG1041	X	perceivedSeverity = alarmSeverityWarning probableCause = alarmCauseRemoteTransmissionError TM displays the text "F/W file not received but IP Phones have registered. May have mixed F/W

Maintenance display	Corresponding critical error message	Signaling Server	Description
			versions across phones. When F/W file received, IP Phones will automatically be updated."
G042	ITG1042		perceivedSeverity = alarmSeverityWarning probableCause = alarmCauseOutOfMemory TM displays the text "Insufficient flash drive space to store F/W file."

Table 88
Critical ITS Error messages

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

Maintenance Display	Corresponding Critical Error Message	Signaling Server	Description
S012	ITS1012	X	User entered the wrong IP Phone Installer Password three times during Branch User Config. The IP Phone is locked out from doing any User Configuration for one hour. Action: Wait for the IP Phone to unlock in one hour, or use the IPL CLI command clearLockout to unlock the IP Phone.
S013	ITS1013	X	User entered the wrong Craftsperson Node Level TN Entry Password three times. The IP Phone is locked out. Action: To remove the lock, use LD 32 to disable, and then enable the IP Phone.

IP Line and IP Phone maintenance and diagnostics

LD 32

Table 89 "LD 32 Maintenance commands for the Voice Gateway Media Card" (page 411) summarizes the system maintenance commands available in LD 32.

The following ECNT commands are available in LD 117, as well as in LD 32:

- ECNT CARD
- ECNT NODE
- ECNT SS
- ECNT ZONE

As well, the following ECNT commands are available in LD 117:

- ECNT FW
- ECNT MODL
- ECNT PEC

For more information about the ECNT commands, see ["Counting IP Phones" \(page 160\)](#) and ["LD 117" \(page 414\)](#).

Table 89

LD 32 Maintenance commands for the Voice Gateway Media Card

Command	Description
DISC l s c	Disable the specified card, where: l = loop, s = shelf, c = card. Disable the Voice Gateway Media Card before transmitting card properties from the TM IP Line application. The card reset button is available only in the TM IP Line application when the card is disabled. When the Voice Gateway Media Card is disabled in LD 32, it does not disable the active Leader or backup Leader functions.
DISI l s c	Disable the specified card when idle, where: l = loop, s = shelf, c = card This temporarily prevents the IP Telephony node from seizing the port from incoming calls. Use the DISI command to disable the Voice Gateway Media Card instead of the DISC command. The disabled state of the Voice Gateway Media Card is indicated by the NPR0011 message.
DISU l s c u	Disable the specified unit, where: l = loop, s = shelf, c = card, u = unit

Command	Description
ECNT CARD L S C <customer>	Counts and prints the number of IP Phones registered for the specified card. - If the <customer> parameter is specified, the count is specific to that customer. A card must be specified to enter a customer; otherwise, the count is across all customers. - If no parameters are entered, the count is printed for all zones. A partial TN can be entered for the card (L or L S) which then prints the count per that parameter. A customer cannot be specified in this case. Example: <pre>ECNT CARD 81 << Card 81 >> Number of Registered Ethersets: 5 Number of Unregistered Ethersets: 27</pre>
ECNT ZONE zoneNum <customer>	Counts and prints the number of IP Phones registered for the specified zone. - If <customer> parameter is specified, the count is specific to that customer. A zone must be specified to enter a customer; otherwise, the count is across all customers. - If no parameters are entered, the count is printed for all zones. - If an IP Phone is logged in to Virtual Office and the parameter entered for Current Zone (CUR_ZONE) is different from the parameter entered for Configured Zone (CFG_ZONE), registered and unregistered Ethersets are counted for both zones. Example: <pre>ECNT ZONE 0 0 << Zone 0 Customer 0 >> Number of Registered Ethersets: 4 Number of Unregistered Ethersets: 17</pre>

Command	Description
ECNT NODE nodeNum	Counts and prints the number of IP Phones registered for the specified node. If the nodeNum parameter is not entered, the count is printed for all nodes. Example: ECNT NODE 8765 << Zone 8765 >> Number of Registered Ethersets: 3
ECNT SS <hostName>	Counts and prints the number of IP Phones registered for the specified Signaling Server. If hostName parameter is not entered, the count is printed for all Signaling Servers. Example: ECNT SS << Signaling Server: BVWAlphaFox IP 10.10.10.242>> Number of Register Ethersets: 1000 If the hostName variable contains an underscore (_), then an NPR001 error message is returned, as an underscore is considered to be an invalid character.
ENLC l s c	Enable the specified card, where: l = loop, s = shelf, c = card
ENLU l s c u	Enable the specified unit, where: l = loop, s = shelf, c = card, u = unit
IDC l s c	Print the Card ID information for the specified card, where: l = loop, s = shelf, c = card This command displays the PEC (Product Engineering Code) and serial number for the card. The IP Line PEC is NTZC80AA.
STAT l s c	Print the CS 1000 software status of the specified card, where: l = loop, s = shelf, c = card
STAT l s c u	Print the CS 1000 software status of the specified unit, where: l = loop, s = shelf, c = card, u = unit

LD 117

Table 90 "LD 117 Count registered IP Phones" (page 414) summarizes the system maintenance commands available in LD 117.

The following ECNT commands are also maintained in LD 32:

- ECNT CARD <Loop> <Shelf> <Card> <CustomerNumber>
- ECNT NODE <NodeNumber>
- ECNT SS <HostName>
- ECNT ZONE <ZoneNumber> <CustomerNumber>

For more information about the ECNT commands, see "Counting IP Phones" (page 160).

Table 90
LD 117 Count registered IP Phones

Command	Description
ECNT CARD L S C <customer>	Counts and prints the number of IP Phones registered for the specified card. • If the <customer> parameter is specified, the count is specific to that customer. A card must be specified to enter a customer; otherwise, the count is across all customers. • If no parameters are entered, the count is printed for all zones. A partial TN can be entered for the card (L or L S) which then prints the count per that parameter. A customer cannot be specified in this case. Example: <pre>ECNT CARD 81 << Card 81 >> Number of Registered Ethersets: 5 Number of Unregistered Ethersets: 27</pre>

Command	Description
ECNT ZONE zoneNum <customer>	Counts and prints the number of IP Phones registered for the specified zone. - If <customer> parameter is specified, the count is specific to that customer. A zone must be specified to enter a customer; otherwise, the count is across all customers. - If no parameters are entered, the count is printed for all zones. Example: ECNT ZONE 0 0 << Zone 0 Customer 0 >> Number of Registered Ethersets: 4 Number of Unregistered Ethersets: 17
ECNT NODE nodeNum	Counts and prints the number of IP Phones registered for the specified node. If the nodeNum parameter is not entered, the count is printed for all nodes. Example: ECNT NODE 8765 << Zone 8765 >> Number of Registered Ethersets: 3
ECNT SS <hostName>	Counts and prints the number of IP Phones registered for the specified Signaling Server. If hostName parameter is not entered, the count is printed for all Signaling Servers. Example: ECNT SS << Signaling Server: BVWAlphaFox IP 10.10.10.242>> Number of Register Ethersets: 1000 If the hostName variable contains an underscore (_), then an NPR001 error message is returned, as an underscore is considered to be an invalid character.

Command	Description
ECNT FW <XX> <A> <BB> <FF>	Prints the number of IP Phones with specified firmware ID and running specified firmware version. <XX> – firmware ID <A> – major version designator <BB> – minor version designator <FF> – filter to apply on firmware version; can be one of the following: = – equal to ~ – not equal to < – less than > – greater than Only the XX parameter is mandatory. ECNT FW <XX> <A> <BB> defaults to ECNT FW <XX> <A> <BB> = ECNT FW <XX> <A> counts all registered IP Phones with firmware ID equal to <XX> and major version designator equal to <A>. ECNT FW <XX> counts all registered IP Phones with firmware ID equal to <XX>. ECNT FW is equivalent to ECNT FW ALL; that is, the list containing firmware IDs and the quantity of IP Phones with this firmware ID is printed.

Command	Description
ECNT MODL <MMM>	Prints the number of IP Phones of specified model. <MMM> – specifies model name. If this parameter is omitted, then a list of the model names and associated mnemonics is printed.
ECNT PEC <PEC>	Prints the number of IP Phones with specified PEC, where: <PEC> – Product Engineering Code ECNT PEC is equivalent to ECNT PEC ALL; that is, the list containing the PECs and the quantity of IP Phones with this PEC is printed.

TNs

For Nortel IP Phones, there are two kinds of TNs to consider:

- physical TN – represents a physical unit of the Voice Gateway Media Card
- virtual TN – configured on a virtual superloop and represents an IP Phone

Physical TNs

Physical TNs, that are seen as trunk units, are managed using existing LD 32 commands.

Virtual TNs

Because virtual TNs are configured on a virtual superloop, virtual TN maintenance has no meaning; that is, what is already provided by the CS 1000 for phantom loops.

In LD 32, any command affecting a phantom loop leads to an NTP665 message because the loop does not physically exist. LD 32 supports STAT, DISU, ENLU, and IDU commands on an IP Phone Virtual TN. All other commands generate the NPR047 message.

Maintenance commands for the IP Phone

Table 91 "LD 32 maintenance commands for IP Phones" (page 418) contains the maintenance commands in LD 32 for the IP Phone. For more information about commands, see *Software Input Output Reference—Maintenance* (NN43001-711).

Table 91
LD 32 maintenance commands for IP Phones

Command	Description
STAT l s c u	Display the IP Phone state. UNEQ, IDLE, BUSY, and DSBL have the usual meaning. IDLE and DSBL state are precise by the following information: • UNREGISTERED identifies an IP Phone that is configured in the system but has not yet registered. • REGISTERED identifies an IP Phone that has registered.
DISU l s c u	Change the IP Phone state to DSBL. UNREGISTERED/REGISTERED state is not modified.
ENLU l s c u	Change the IP Phone state to IDLE. UNREGISTERED/REGISTERED state is not modified.
IDU l s c u	Displays selected IP Phone information. Displays the TN number, MAC address, device code, NT code, color code, release code, software code, serial number, IP Phone IP address, and LTPS IP address.
STAT VTRK <cust#> <route#> <start_mb#> <number of members>	Displays the status of the virtual trunks for a customer route starting from a specified starting member for the number of members specified.

IDU command

Because the system 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.

An example of the output format of the IDU command in LD 32 is shown in [Figure 101 "IDU command output" \(page 419\)](#).

Figure 101
IDU command output

```

>LD 32
.idu 61 0
I2004 TN: 061 0 00 00 V
TN ID CODE: i2004

ISET MAC ADR: 00:60:38:76:C7:9D
ISET IP ADR: 30.1.1.10:5200
LTPS IP ADR: 47.11.216.49

MANUFACTURER CODE: [NAME]
MODEL:
NT CODE: NT2K00GI
COLOR CODE: 66
RLS CODE: 0
SER NUM: 76C79D
FW/SW VERSION: 0602B59

.idu 61 1
I2004 TN: 061 0 00 01 V
TN ID CODE: i2004

ISET MAC ADR: 00:60:38:76:38:E0
ISET IP ADR: 30.1.1.100:1250 (192.168.1.13)
LTPS IP ADR: 47.11.216.50

MANUFACTURER CODE: [NAME]
MODEL:
NT CODE: NT2K00GI
COLOR CODE: 66
RLS CODE:
SER NUM: 7638E0
FW/SW VERSION: 0602B59

```

Any information about attached IP Phone KEMs, or the Expansion Module for IP Phone 1100 Series is also displayed.

In the example in [Figure 101 "IDU command output" \(page 419\)](#), the first IP Phone is not behind a NAT device; the second IP Phone is behind a NAT device. The ISET IP ADR field displays the IP Phone signaling IP address as seen by the LTPS. If the IP Phone is behind a NAT device, the ISET IP ADR field displays the public address (the address seen by the LTPS) followed by the private IP address (the address configured at the IP Phone) in parenthesis.

This format applies only for IP Phone Virtual TNs.

If the IP Phone is not registered with the Call Server, an NPR0048 message is generated. If the IP Phone is registered but idle, the system prints the IP Phone IP address and Voice Gateway Media Card IP address and generates an NPR0053 message. As well, if the IP Phone is registered, but the Call Server is not responding, an NPR0503 message is generated.

IP Line CLI commands

IP Line CLI commands are designed to supplement Overlay commands and to introduce features specific to the ITG-P 24-port card, Media Cards, and Signaling Server platform.

All the CLI commands are supported on the ITG-P 24-port card and Media Cards. The CLI commands are also available on the Signaling Server if an "X" is shown in the Signaling Server column of the table. For more information about commands, see *Software Input Output Reference—Maintenance (NN43001-711)*.

The IP Line CLI commands are accessed by connecting a TTY to the MAINT port on the Voice Gateway Media Card faceplate. Alternatively, use Telnet to access the CLI. These IP Line CLI commands are entered at the **IPL>** prompt or **oam>** prompt. Instructions for connecting to the maintenance port of the Signaling Server are described in *Communication Server 1000M and Meridian 1 Small System Installation and Commissioning (NN43011-310)*.

The commands are grouped into the following categories:

- [Table 92 "General purpose commands" \(page 421\)](#)
- [Table 93 "File Transfer commands" \(page 424\)](#)
- ["IP configuration commands" \(page 428\)](#)
- [Table 95 "Reset commands" \(page 429\)](#)
- [Table 96 "DSP commands" \(page 429\)](#)
- [Table 97 "Upgrade commands" \(page 430\)](#)
- [Table 98 "IPL> shell command" \(page 430\)](#)
- [Table 99 "IP Phone Installer Password commands" \(page 431\)](#)
- [Table 100 "Voice Gateway commands" \(page 433\)](#)
- [Table 101 "Data Path Capture Tool commands" \(page 434\)](#)
- [Table 102 "Translation IP/DN commands" \(page 435\)](#)
- [Table 103 "Graceful Disable commands" \(page 439\)](#)
- [Table 104 "IP Phone Loss Plan commands" \(page 440\)](#)
- [Table 105 "Patch commands" \(page 442\)](#)
- [Table 106 "General trace tool commands" \(page 445\)](#)

- Table 107 "Protocol trace tool CLI commands for the NCS" (page 447)
- Table 108 "Maintenance audit commands" (page 451)

General purpose commands

Table 92 "General purpose commands" (page 421) lists the general purpose IPL> and oam> commands.

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

Table 92
General purpose commands

Command	Description	Signaling Server
i	Displays the current task list. This command does not appear on the MC 32S card.	X
itgHelp Help	Displays the complete command list. ? also shows the command list. Help displays the complete command list for the MC 32S card.	
logout	Exits the IPL> Command Line Interface.	
routeAdd	Adds a route to the network routing table.	X
routeShow	Displays the current host and network routing tables.	X
logPrintOff rptPrintOff	Turns off logging in the TTY session currently logged in. rptPrintOff is for the MC 32S card.	
logPrintOn rptPrintOn	Turns on logging in the TTY session currently logged in. rptPrintOn is for the MC 32S card.	
chkdsk	chkdsk "/C:" Checks the internal file system for errors. chkdsk "/C:", 1 Repairs the file system errors and saves the damaged cluster in files. chkdsk "/C:", 2 Repairs file system errors and returns damaged clusters to the free pool.	X

Command	Description	Signaling Server
	This command does not appear on the MC 32S card.	
<code>ping "host", "numpackets"</code>	Sends an ICMP ECHO_REQUEST packet to a network host. The host matching the destination address in the packets responds to the request. If a response is not returned, the sender times out. This command is useful to determine if other hosts or Voice Gateway Media Cards are communicating with the sender card. The "numpackets" parameter specifies how many packets to send. If it is not included, ping runs until it is stopped by Ctrl-C (also exits the IPL> CLI). Example: IPL> ping "47.82.33.123", 10	X
<code>electShow</code>	Displays a list of cards in the node and information about each card. This includes showing all registered followers to a leader. The output has two sections: • cards currently registered • cards that are in the BOOTP.TAB configuration but not yet registered. This command does not appear on the MC 32S card.	X
<code>itgCardShow</code>	Displays Voice Gateway Media Card information.	X
<code>itgMemShow</code>	Displays memory usage.	X
<code>ifShow</code>	Displays detailed IP address information, including MAC addresses.	X
<code>IPInfoShow</code>	Displays IP address information.	X
<code>serialNumShow</code>	Displays card serial number. This command displays the same Voice Gateway Media Card serial number that is displayed in the LD 32 IDC command.	
<code>firmwareVersionShow</code>	Displays firmware version number.	X

Command	Description	Signaling Server
numChannelsShow	Displays number of available channels.	
swVersionShow	Displays software version.	X
logFileOn	Turns on error logging to the syslog file. This command does not appear on the MC 32S card.	
logFileOff	Turns off error logging to the syslog file. This command does not appear on the MC 32S card.	
logShow	Displays information about the current logging configuration. Indicates whether logging is on or off.	
logConsoleOn	Turns on error logging to the console.	
logConsoleOff	Turns off error logging to the console.	
isetShow	Displays general information for all registered IP Phones. For example, the command displays the IP address of the IP Phone, the VTN that the IP Phone is associated with, indicates the type of IP Phone such as IP Phone 2001, IP Phone 2002, and IP Phone 2004, or IP Softphone 2050, IP Phone 1110, IP Audio Conference Phone 2033, IP Phone 2007, IP Phone 1120E, IP Phone 1140E, IP Phone 1150E and provides the type of registration and the new registration status.	X
isetShowByTN	Displays general information about all registered IP Phones, sorted by TN.	X
isetShowByIP	Displays general information about all registered IP Phones, sorted by IP address.	X
pbxLinkShow	Displays information about the link to the CPU, including the configuration and link status.	X
itgAlarmTest	Generates ITGxxxx test alarms. This command does not appear on the MC 32S card.	X
itsAlarmTest	Generates ITSxxxx test alarms.	
itgPLThreshold	Sets the IP Phone and gateway alarm packet loss threshold (units 0.1%). An alarm is generated when the threshold is reached.	
elmShow	Displays a list of supported languages.	X
itgChanStateShow	Displays the state for channels; for example, if they are idle or busy.	

File transfer commands

Table 93 "File Transfer commands" (page 424) lists the file transfer commands.

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

Table 93
File Transfer commands

Command	Description	Signaling Server
swDownload "hostname", "username", "password", "directory path", "file name"	Loads a new version of software from the FTP host to the Voice Gateway Media Card. Updates the software on the Voice Gateway Media Card with the binary file received from an FTP server corresponding to the <i>hostname</i> IP address. The Voice Gateway Media Card FTP client performs a Get which downloads the file to the flash bank. A checksum is calculated to verify correct delivery. After the new software version is successfully downloaded, the Voice Gateway Media Card must be rebooted with <code>cardReset</code> to run the new software. <i>Hostname</i> refers to the either IP address of the FTP host, or the Voice Gateway Media Card itself or another Voice Gateway Media Card when a PC Card in the /A: drive of the Voice Gateway Media Card contains the software binary file. Example: <pre>IPL> swDownload "47.82.32.346", "anonymous", "guest", "/software", "VxWorks.mms"</pre>	

Command	Description	Signaling Server
configFileGet "hostname", "username", "password", "directory path", "file name"	Sends an updated CONFIG.INI file from TM to the Voice Gateway Media Card. Updates the CONFIG.INI file on the Voice Gateway Media Card with the CONFIG.INI file on the specified host, account, and path. The configFileGet task on the ITG host initiates an FTP session with the given parameters and downloads the file to flash file system. The CONFIG.INI file also contains the NRS IP address, gateway password, and gateway DN-port mapping table. Example: IPL> configFileGet "ngals042", "anonymous", "guest", "/configDir", "config.ini"	X
bootPFileGet "hostname", "username", "password", "directory path", "file name"	Updates the BOOTPtab file on the Voice Gateway Media Card with the BOOTPtab file on the specified host, account and path. The bootpFileGet task on the ITG host initiates an FTP session with the given parameters and downloads the file to flash file system. Example: IPL> bootPFileGet "ngals042", "anonymous", "guest", "/bootpDir", "bootptab"	X
hostFileGet "hostname", "username", "password", "directory path", "file name", "ITGfile name", listener	Transfers any file from an FTP Server to the Voice Gateway Media Card. This command gets any file from the host and does a Get using FTP to the Voice Gateway Media Card. ITGfile name is the full path AND file name of where the file is to be placed. The listener parameter indicates which module to inform of the successful file transfer. It can be set to -1 to be disabled. Example: IPL> hostFileGet "ngals042", "anonymous", "guest", "/hostfileDir", "hostFile.txt",	X

Command	Description	Signaling Server
	"/C:ITGFILRDIR/ITGFILE.TXT", -1	
currOMFilePut "hostname", "username", "password", "directory path", "file name"	Sends the current Operational Measurements (OM) file to the specified host. The OMFilePut task on the ITG host initiates an FTP session with the given parameters and downloads the Voice Gateway Media Card Operational Measurements file to the specified location on the host. Example: IPL> currOMFilePut "ngals042", "anonymous", "guest", "/currDir", "omFile"	X
prevOMFilePut "hostname", "username", "password", "directory path", "file name"	Sends the previous Operational Measurements (OM) file to the specified host. The OMFilePut task on the ITG host initiates an FTP session with the given parameters and downloads the Voice Gateway Media Card Operational Measurements file to the specified location on the host. Example: IPL> prevOMFilePut "ngals042", "anonymous", "guest", "/prevDir", "omFile"	X
LogFilePut "hostname", "username", "password", "directory path", "file name"	Sends the syslog file from the Voice Gateway Media Card to TM. The LogFilePut task on the ITG host initiates an FTP session with the given parameters and downloads the Voice Gateway Media Card log file to the specified location on the host. Example: IPL> LogFilePut "ngals042", "anonymous", "guest", "/currDir", "logFile" This command does not appear on the MC 32S card.	

Command	Description	Signaling Server
bootPFilePut "hostname", "username", "password", "directory path", "file name"	Sends the BOOTPtab file from the Voice Gateway Media Card to TM. Example: IPL> bootPFilePut "ngals042", "anonymous", "guest", "/bootpDir", "bootpFile"	X
hostFilePut "hostname", "username", "password", "directory path", "file name", ITGfile name	Transfers any file from the Voice Gateway Media Card to an FTP Server. Example: IPL> hostFilePut "ngals042", "anonymous", "guest", "/hostDir", "hostFile", "/C:/CONFIG/CONFIG1.INI"	X
omFilePut "hostname", "username", "password", "directory path", "file name", ITGfile name	Sends the current Operational Measurements (OM) file to the specified host. Example: IPL> omFilePut "ngals042", "anonymous", "guest", "/hostDir", "omFile"	X
firmwareFileGet "hostname" "username" "password" "directory path" "file name"	Initiates a firmware download from a specified FTP server. After the download is completed, the downloaded file is checked for Enhanced Header (or proper naming). If the file is considered a valid F/W file, the UMS database is updated accordingly. Example: pdt> firmwareFileGet "192.168.0.1","admin1","0000","/u/fw","0604D45.BIN"	X
firmwareFilePut "hostname", "username", "password", "directory path", "file name",	Downloads F/W file to the specified FTP server. It is added for consistency with existing firmwareFilePutI2004 and firmwareFilePutI2002. Example: pdt> firmwareFilePut "192.168.0.1","admin1","0000","/u/fw","0604D45.BIN"	X

Configuration commands

Table 94 "Configuration commands" (page 428) lists the IP configuration IPL> and oam> commands.

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

Table 94
Configuration commands

Command	Description	Signaling Server
NVRIPSet	Configures the IP address in NVRAM.	
NVRGWSet	Configures the default gateway address in NVRAM.	
NVRSMSet	Configures the subnet mask in NVRAM.	
NVRIPShow	Prints the values of the IP parameters that reside in NVRAM.	
NVRClear	Clear IP parameters in NVRAM.	
nvrAmLeaderSet	Configures the Leader bit in NVRAM.	
nvrAmLeaderClr	Clears the Leader bit in NVRAM, but does not erase the IP parameters in NVRAM.	
setLeader	Configures a Leader card, including the IP address, gateway, subnet mask, boot method to static, and Leader bit in NVRAM. This one command does all the necessary actions to make a Leader.	
clearLeader	Clears the Leader information in NVRAM, sets the boot method to use BOOTP, and removes the old configuration files. This command makes a Leader card into a Follower card.	
tLanDuplexSet	Configures the TLAN Ethernet duplex mode. This command does not appear on the MC 32S card.	
tLanSpeedSet	Configures the TLAN Ethernet speed. This command does not appear on the MC 32S card.	

Reset commands

Table 95 "Reset commands" (page 429) lists the Reset IPL> and oam> commands. For more information about reset commands, see *Software Input Output Reference—Maintenance (NN43001-711)*.

Table 95
Reset commands

Command	Description	Signaling Server
<code>cardReset</code>	Resets a Voice Gateway Media Card. This command performs a warm reboot of the Voice Gateway Media Card. The card must be in the OOS state to use this command.	
<code>isetReset "tn"</code>	Where <i>tn</i> is l s c u	X
<code>isetResetAll</code>	Resets all registered IP Phones.	X
<code>resetOM</code>	Resets the operational measurement file timer. This command resets all operational measurement parameters collected since last log dump.	X
<code>lastResetReason</code>	Displays the reason for the last card reset. This command does not appear on the MC 32S card.	

DSP commands

Table 96 "DSP commands" (page 429) lists the DSP IPL> and oam> commands applicable to the Voice Gateway Media Card. For more information about DSP commands, see *Software Input Output Reference—Maintenance (NN43001-711)*.

Table 96
DSP commands

Command	Description	Signaling Server
<code>DSPReset</code>	Resets the specified DSP.	
<code>DSPNumShow</code>	Displays the number of DSPs on the Voice Gateway Media Card.	
<code>DSPChanStateShow</code>	Lists the state of all the channels on the DSPs.	
<code>DSPHwCheck</code>	Performs a basic DSP hardware diagnostic check.	
<code>DSPLoopTest</code>	Performs a DSP loopback test for all currently inactive channels or given channels.	

IP Phone firmware upgrade commands

Table 97 "Upgrade commands" (page 430) lists the upgrade IPL> and oam> commands. For more information about IP Phone firmware upgrade commands, see *Software Input Output Reference—Maintenance (NN43001-711)*.

Table 97
Upgrade commands

Command	Description	Signaling Server
<code>umsPolicyShow</code>	Displays the current upgrade policy. This command does not appear on the MC 32S card.	X
<code>umsUpgradeAll</code>	Upgrades all registered IP Phones according to policy and firmware file. This command does not appear on the MC 32S card.	X
<code>umsUpgradeTimerShow</code>	Shows the upgrade schedule. This command does not appear on the MC 32S card.	X
<code>umsUpgradeTimerCancel</code>	Cancels the scheduled upgrade. This command does not appear on the MC 32S card.	X
<code>firmwareFileGet</code>	Uploads new firmware to the Signaling Server	X
<code>firmwareFilePut</code>	Downloads F/W file to the specified FTP server.	X
<code>uftpTurboMode</code>	Used in conjunction with RST FW and RST Zone commands to initiate and obtain the status of the firmware downloads Maintenance Mode.	X
<code>uftpTurboModeShow</code>		X
<code>uftpTurboModeTimeoutSet</code>		X

IPL shell commands

Table 98 "IPL> shell command" (page 430) lists the command to change the IPL> shell password.

Table 98
IPL shell command

IPL> command	Description	Signaling Server
<code>shellPasswordSet</code>	Changes the current user name and password of the IPL> CLI shell.	

IPL> command	Description	Signaling Server
	This command does not appear on the MC 32S card.	

IP Phone Installer Password commands

Table 99 "IP Phone Installer Password commands" (page 431) lists the IP Phone Installer Password commands.

For more information about IP Phone installer password commands, see *Software Input Output Reference—Maintenance (NN43001-711)*.

Table 99
IP Phone Installer Password commands

Command	Description	Signaling Server
nodePwdSet "password"	Sets and enables the administrative IP Phone Installer (node) Password. This is also known as the node level IP Phone Installer Password. If a null password (0 characters in length) is configured, all IP Phones that attempt to register after this command has been issued display a prompt for node password before the TN can be modified. The "password" parameter must be null or 6 to 14 digits in length; The valid characters are 0 to 9, *, and #. The null password causes the Node ID and Password screen on the IP Phone to be skipped during restart. This command can be entered at any time; the new password entered overwrites the prior password.	X
nodePwdShow	Displays the settings of the IP Phone Installer Password. The command displays the current password, the state of password entry (enable/disable), the temporary password, and the number of uses and time to expiry.	X
nodePwdEnable	Enables the administrative IP Phone Installer Password setting. After this command is entered, all IP Phones registering display the password screen.	X

Command	Description	Signaling Server
nodePwdDisable	Disables both the administrative and the temporary IP Phone Installer Password settings. After this command is entered, all IP Phones display the original Node ID and TN screen during registration.	X
nodeTempPwdSet "tempPwd", uses, <time>	Configures the temporary IP Phone Installer Password. This password is disabled by default. The password must be a string 6 to 14 digits in length. A null password cannot be entered. The valid tempPwd characters are 0 to 9, *, and #. The uses parameter is a numeric value from 0 to 1000. This parameter specifies the number of uses for which the temporary password is valid. The range for the time parameter is 0 to 240 hours, which is a maximum of 10 days. The time parameter specifies the duration in hours that the password is valid. • If the uses parameter is set to zero, the time parameter is mandatory. As a result, the password only expires based on time. • If the uses parameter is non-zero, the time parameter is optional. • If both the uses and time parameters are entered, the password expires on whichever comes first, that is, uses is reduced to zero or the time has expired. • If both uses and time are entered and both are set to zero, it is the same as not setting the temporary password at all. This command can be entered at any time and the new parameters overwrite the existing temporary password parameters.	X
nodeTempPwdClear	Deletes the temporary IP Phone Installer Password. It also reset the uses and time parameters to zero.	X

Voice Gateway commands

Table 100 "Voice Gateway commands" (page 433) lists the Voice Gateway commands used on the Voice Gateway Media Card.

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

Table 100
Voice Gateway commands

Command	Description	Signaling Server
vgwPLLog	Toggles gateway packet loss logging on and off. This command does not appear on the MC 32S card.	
vgwShow	Displays information about the active (non-idle and equipped) gateway channels. Entering this command with the IP address of an IP Phone at the Command Line Interface of any node Voice Gateway Media Card displays the identification of the card that has a gateway channel in use by the IP Phone. This information is useful when there is a need to identify from which card to collect gateway statistics (for example, packet loss).	
vgwShowALL	Displays information about all gateway channels.	

vgwShow

The **vgwShow** command can be issued with no parameters or with the IP address of an IP Phone using one of the Voice Channels.

vgwShow "x.x.x.x"

where

"x.x.x.x" is the IP address of one of the IP Phones.

The IP address "x.x.x.x" is the PUBLIC IP address of the IP Phone. If there are multiple IP Phones using the same public IP address, the output is similar to the example shown in [Figure 102 "vgwShow command sample output"](#) (page 433).

Figure 102
vgwShow command sample output

```

IPL> vgwShow "47.11.217.102
Found on Card TN 009-G0 , ELAN IP 47.11.217.21, TLAN IP 47.11.216.185, number of matches 2
Chan ChanState EspMode Codec Tn Reg AirTime rxTsap txTsap
-----
0 Busy Voice 6.711-20 0x0804 yes 55 47.11.216.185:5200 47.11.217.102:10008

```

The number of IP Phones that use that public IP address is printed (**2** in this example), but only one of the IP Phones is displayed. To see the other IP Phone, determine the Public IP address and Public Media Port using the command `isetNATShow`. Then enter `vgwShow` using the Public IP address and Public Media Port. An example of the output is shown in [Figure 103 "vgwShow sample with Public information"](#) (page 434).

Figure 103
vgwShow sample with Public information

```
IPL> vgwShow "47.11.217.102",10104
value = 0 = 0x0
IPL>
Found on Card TN      009-00      , ELAN IP 47.11.217.21, TLAN IP 47.11.216.185, number of matches 1
Chan ChanState DspMode Codec      Tn      Reg AirTime      rxTsap      txTsap
-----
2 Busy      Voice      G.711-20 0x0806 yes      856      47.11.216.185:5204 47.11.217.102:10104
```

Data Path Capture Tool commands

[Table 101 "Data Path Capture Tool commands"](#) (page 434) lists the commands used with the Data Path Capture Tool.

For more information about Data Path Capture Tool commands, see *Software Input Output Reference—Maintenance (NN43001-711)*.

Table 101
Data Path Capture Tool commands

IPL> command	Description	Signaling Server
<code>captureStart</code>	Begins the capture operation. When the command is entered, data for the gateway channel <tcid> (0 to 23 for ITG-P 24-port card and 0 to 31 for Media Cards) begins to be captured to the circular queue. This command does not appear on the MC 32S card.	
<code>captureStop</code>	Stops the audio data capture. This command does not appear on the MC 32S card.	
<code>captureSaveLocal</code>	Dumps the contents of the circular queue to the specified file on the memory PC Card inserted in the /A: drive on the Voice Gateway Media Card faceplate. This command does not appear on the MC 32S card.	

IPL> command	Description	Signaling Server
captureSaveRemote	FTP's the contents of the circular queue to the specified file on the remote server. This command does not appear on the MC 32S card.	
captureFree	Frees the capture queue. This command does not appear on the MC 32S card.	

Translation IP/DN commands

Table 102 "Translation IP/DN commands" (page 435) lists the LD 117 commands to translate an IP Phone DN to its IP address and its IP address to its DN.

For more information about Translation IP/DN commands, see *Software Input Output Reference—Maintenance (NN43001-711)*.

Table 102
Translation IP/DN commands

LD 117 command	Description	Signaling Server
PRT DNIP <DN> [<CustomerNo>]	Prints a list of IP addresses for every IP Phone registered with the specified DN. This command does not appear on the MC 32S card.	
PRT IPDN <IPAddress>	Prints a list of DNs configured for the specified IP addresses. This command does not appear on the MC 32S card.	

Search criteria

If a customer number is entered, only that customer is searched for the designated DN. If no customer number is entered, the database for all customers on the system is searched.

The **PRT DNIP** command accepts a partially defined DN; that is, a DN entered with only partial leading digits. For example, entering a DN of 34 with no customer number results in output for any DN in the system starting with 34.

PRT DNIP output

The PRT DNIP command generally produces the following output:

- an initial line displaying the DN and customer number. If there is output for multiple customers, this line is repeated before each customer output.
- information for each occurrence of the DN on any IP Phone for that customer.
 - TN
 - set type
 - key number of DN appearance and type of DN
 - current IP address of the IP Phone
 - configured zone for the IP Phone
 - state of the IP Phone registration

If the IP Phone is behind a NAT device, the public IP address is displayed, with the private IP address underneath in parenthesis.

PRT IPDN

The PRT IPDN command produces the following output:

- an initial line displaying the IP address for the search
- a second line displaying the customer number, TN, set type, zone and registration status of the IP Phone using the specified IP address
- information for all DNs configured on that IP Phone
 - key number of DN appearance and type of DN
 - DN
 - configured CPDN for the DN

If the IP Phone is behind a NAT device, the public IP address is displayed, followed by the private IP address in parenthesis.

An example of the output is shown in ["LD 117 PRT IPDN and PRT DNIP output" \(page 437\)](#).

LD 117 PRT IPDN and PRT DNIP output

```

Example:
>ld 117
=> prt dnip 2214

CUST 00 DN 2214
TN      Type      Key      Signaling IP Address  Media IP Address  CfgZone  CurZone  Status
-----
061-14      1140      00 SCR  10.10.1.197:5000      10.10.1.197:5200      00002    00002    REG

=> prt ipdn 10.10.1.197

Signaling IP 10.10.1.197:5000
Media IP 10.10.1.197:5200
CUST 00 TN 061-14 TYPE 1140 CFG_ZONE 00002 CUR_ZONE 00002 REG
Key      DN      CPND Name
-----
00 SCR   2214

```

Partial IP addresses

Partial IP addresses can be entered. Partial IP addresses can be entered with only the leading digits of the IP address (for example, 142.10), or as the IP address with zeroes at the end (for example, 142.10.0.0).

The following examples for "PRT IPDN <IP_ADDR>" shows a partial IP address of 47.0.0. The zeroes in the <IP_ADDR> are handled as if they are trimmed off. This means that the output of **PRT IPDN 47** is the same as that of **PRT IPDN 47.0.0**.

A sample of IP Phones has been configured in the following manner:

IP Address	TN	DN
47.11.216.138	063-20	4120
47.11.216.140	061-02	4002
47.11.215.39	061-00	4000
47.11.215.38	063-00	4100
47.11.215.41	063-01	4101

Example 1

To print the information about the IP Phones whose IP address starts with 47.11.215, enter the following:

```
=> prt ipdn 47.11.215
```

The following output is printed:

```

IP 47.11.215.38
CUST 01 TN 063-00 TYPE 2004P2 ZONE 001 REG
Key      DN      CPND Name
-----
00 SCR   4100      2004P2_Cust_1 VLN63_00
IP 47.11.215.39
CUST 00 TN 061-00 TYPE 2004P2 ZONE 000 REG
Key      DN      CPND Name

```

```
-----  
00 SCR 4000 2004P2_Cust_0 VLN61_00  
IP 47.11.215.41  
CUST 01 TN 063-01 TYPE 2001P2 ZONE 001 REG  
Key DN CPND Name  
-----  
00 SCR 4101 2001P2_Cust_1 VLN63_01
```

Example 2

Alternatively, to print the information about the IP Phones whose IP address starts with 47.11.215, enter the following:

=> prt ipdn 47.11.215.0

The following output is printed:

```
IP 47.11.215.38  
CUST 01 TN 063-00 TYPE 2004P2 ZONE 001 REG  
Key DN CPND Name  
-----  
00 SCR 4100 2004P2_Cust_1 VLN63_00  
IP 47.11.215.39  
CUST 00 TN 061-00 TYPE 2004P2 ZONE 000 REG  
Key DN CPND Name  
-----  
00 SCR 4000 2004P2_Cust_0 VLN61_00  
IP 47.11.215.41  
CUST 01 TN 063-01 TYPE 2001P2 ZONE 001 REG  
Key DN CPND Name  
-----  
00 SCR 4101 2001P2_Cust_1 VLN63_01
```

Example 3

To print the information about the IP Phones whose IP address starts with 47.11.216, enter the following:

=> prt ipdn 47.11.216

The following output is printed:

```
IP 47.11.216.138  
CUST 01 TN 063-20 TYPE 2002P2 ZONE 001 REG  
Key DN CPND Name  
-----  
00 SCR 4120 2002P2_Cust_1 VLN63_20  
IP 47.11.216.140  
CUST 00 TN 061-02 TYPE 2002P2 ZONE 000 REG  
Key DN CPND Name  
-----  
00 SCR 4002 2002P2_Cust_0 VLN61_02
```

Example 4

Alternatively, to print the information about the IP Phones whose IP address starts with 47.11.216, enter the following:

```
=> prt ipdn 47.11.216.0
```

The following output is printed:

```
IP 47.11.216.138
CUST 01 TN 063-20 TYPE 2002P2 ZONE 001 REG
Key   DN      CPND Name
-----
00 SCR  4120    2002P2_Cust_1 VLN63_20
IP 47.11.216.140
CUST 00 TN 061-02 TYPE 2002P2 ZONE 000 REG
Key   DN      CPND Name
-----
00 SCR  4002    2002P2_Cust_0 VLN61_02
```

Graceful TPS commands

[Table 103 "Graceful Disable commands" \(page 439\)](#) lists the commands used to gracefully disable the LTPS and Voice Gateway services and the commands to enable these services after they have been disabled.

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

Table 103
Graceful Disable commands

IPL> command	Description	Signaling Server
disServices	Causes the Voice Gateway Media Card or Signaling Server to gracefully switch the registered resources to the other Voice Gateway Media Cards or Signaling Servers located in the same node. This command does not interrupt established calls.	X
disiAll	Gracefully disables both the LTPS and voice gateway service on the Voice Gateway Media Card. Gracefully disables the LTPS on the Signaling Server.	X

IPL> command	Description	Signaling Server
disiTPS	Gracefully disables the LTPS service on the Voice Gateway Media Card. Prevents new IP Phones registering on the card, and all registered IP Phones are redirected to another card when idle.	X
disiVGW	Gracefully disables voice gateway service.	
enaAll	Enables both the LTPS and voice gateway service on the Voice Gateway Media Card. Enables the LTPS on the Signaling Server.	X
enlServices	Enables all the Voice Gateway Media Cards or Signaling Servers to accept registrations of resources.	X
enaTPS	Enables the LTPS service.	X
enaVGW	Enables the voice gateway service.	
forcedisServices	Forces all registered resources on the Voice Gateway Media Card or Signaling Server to re-register with the other Voice Gateway Media Cards or Signaling Servers in the node. This command will interrupt established calls.	X
loadBalance	Causes the Voice Gateway Media Card or Signaling Server to attempt to balance the registration load between this card/server and the rest of the node components.	X

IP Phone Loss Plan (UK) commands

These commands set and adjust the gains for the UK (or other places where loss plan adjustment of IP Phones is needed).

For more information about the UK Loss Plan, see ["United Kingdom" \(page 282\)](#).

For more information about IP Phone Loss Plan (UK) commands, see *Software Input Output Reference—Maintenance (NN43001-711)*.

Table 104
IP Phone Loss Plan commands

IPL> command	Description	Signaling Server
UKLossPlanSet	Increases the Tx level of the IP Phone to match the requirement for the UK.	X

IPL> command	Description	Signaling Server
UKLossPlanClr	Removes the loss plan adjustment and returns the IP Phone to the default loss plan levels.	X
lossPlanPrt	Prints the current IP Phone loss plan settings.	X
lossPlanSet <transducer> <rlrOffset> <slrOffset>	Allows a variable offset from the default loss plan to be entered for the specified transducer (handset, handsfree, or headset). The rlrOffset adjusts the level heard at the IP Phone. The slrOffset adjusts the level transmitted from the IP Phone. Positive numbers reduce the level (add loss). Negative numbers increase the level (add gain).	X
lossPlanClr	Removes the loss plan adjustment and returns the IP Phone to the default loss plan levels.	X

Nortel recommends that the loss plan commands be entered on the node Leader card while it is the node master. This process ensures that the data is correctly propagated to all cards in the node. When installing a new Leader card in a node with modified levels, always enter the loss plan command on the Leader card CLI, even if the command was previously entered on another card CLI.

When a node has a modified loss plan (that is, the command **ULKLossPlanSet** or **lossPlanSet** has been used), a new card that is added to the node is updated with the modified loss plan 30 seconds after the card has booted. Prior to the modified loss plan being received by the new card, calls made by IP Phones registered to that new card have the default loss plan levels.



CAUTION

Care must be taken when altering the IP Phone loss plan. Increasing the gain increases the possibility of echo and other audio problems. Only adjust the levels when instructed by this document or by Nortel support staff.

Patch and Patching Tool commands

A patch is a piece of code that is inserted or patched into an executable program. The Patching Tool enables loadware on the Voice Gateway Media Cards to be patched or fixed without having to upgrade the card loadware and without service interruption. All patch commands on the Voice Gateway Media Cards and Signaling Server are accessible at the PDT prompt level. These commands are summarized in [Table 105 "Patch commands" \(page 442\)](#).

The parameter string supplied to the command must be enclosed with double quotes. For example, the syntax for the **pload** command is

```
pload "patch1.p"
```

These commands are used to manage patches on the Voice Gateway Media Card. Patches must be downloaded from a workstation to the Voice Gateway Media Card using a modem, an FTP session, or Element Manager. Patch files are stored in Flash memory and are loaded into DRAM memory. After a patch is in DRAM memory it can be activated, deactivated, and its status can be monitored.

Perform the following tasks before loading a patch:

- Verify that the patch matches the platform CPU type.
- Verify the loadware version on the card.
- Block the installation if there is a mismatch.

The installation of a patch is blocked if either the CPU type or the loadware version of the card is different than the patch. If the installation is blocked, the reason for blocking the install is printed at the CLI. The CPU type and loadware version are also verified during a power-up or reboot cycle. This prevents active patches from being reinstalled if the loadware version of the card is changed. Patching commands listed in [Table 105 "Patch commands" \(page 442\)](#) apply to the Signaling Server and Voice Gateway Media Cards.

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

Table 105
Patch commands

Command	Description
pload	Loads a patch file from the file system in Flash memory into DRAM memory. The loaded patch is inactive until it is put into service using the pins command. When a patch is successfully loaded, the pload command returns a patch handle number. The patch handle number is used as input to other patch commands (pins, poos, pout, and plis). Syntax: <pre>pload "[patch-file name]"</pre> where [patch-file name] is the file name or path of the patch file. If a file name alone is provided, the patch must be in the /C:/u/patch directory; otherwise, the full or relative path must be provided.

Command	Description
	If the pload command is issued without a parameter, enter the patch file name and other information when prompted.
pins	Puts a patch that has been loaded into memory (using the pload command) into service. This command activates a patch. If issued successfully, the pins command indicates that global procedures, functions, or areas of memory are affected by the patch. When prompted, choose to proceed or not to proceed. Syntax: pins "[handle]" where [handle] is the number returned by the pload command If the pins command is issued without a parameter, enter a handle when prompted.
poos	Deactivates a patch (takes it out-of-service) by restoring the patched procedure to its original state. Syntax: poos "[handle]" If the poos command is issued without a parameter, enter a handle when prompted.
pout	Removes a patch from DRAM memory. The patch must be taken out-of-service (using the poos command) before it can be removed from the system. Syntax: pout "[handle]" If the pout command is issued without a parameter, enter a handle when prompted.

Command	Description
pstat	Gives summary status information for one or all loaded patches. For each patch, the following information is displayed: patch handle, file name, reference number, whether the patch is in-service or out-of-service, the reason why the patch is out-of-service (if applicable), and whether the patch is marked for retention or not. Patch retention means that if a reset occurs, then the patch is automatically reloaded into memory and its state (active or inactive) is restored to what it was prior to the system going down. Syntax: pstat "[handle]" If the handle is provided, only the information for the specified patch is displayed. If the pstat is issued without a parameter, information for all the patches is displayed.
plis	Gives detailed patch status information for a loaded patch. Syntax: plis "[handle]" If the plis command is issued without a parameter, information about all loaded patches is printed.
pnew	Creates memory patches for the Voice Gateway Media Card. • The release of the patch is assumed to be the same as that of the current load. • The address to be patched is checked to ensure that it is in range. • For each address that is changed, the "old" contents are assumed to be the current contents of that memory address. • If a path is not provided for the new path file name then it is assumed that the patch is in the /C:/u/patch directory. After a memory patch is created using the pnew command, it can be loaded and activated like any other patch. Syntax: pnew

Command	Description
	The <code>pnew</code> command has no parameter.

Patch Directories

There are two patch directories on a Voice Gateway Media Card:

1. **/C:/u/patch**

This is the default directory for patch files. Patch files should be copied to this directory.

2. **/C:/u/patch/reten**

Use this directory to store patch retention control files. Do not use this directory to store patches and do not remove files from this directory.

Patch Synchronization Across a Node

Element Manager provides a mechanism for downloading and putting patches in service across a node.

Patch synchronization across a node cannot be carried out from the IPL> prompt.

General trace tool commands

ATTENTION

A warm boot of the system causes all tracing to cease. Traces must be reentered after the system has restarted.

Table 106 "General trace tool commands" (page 445) lists the general trace tool commands applicable to the Voice Gateway Media Cards. They are issued from the LTPS prompt of the Voice Gateway Media Cards.

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

Table 106
General trace tool commands

CLI Command	Description	Signaling Server
<code>traceShow</code>	Displays the names of active traces in the system.	X
<code>traceAllOff</code>	Causes all traces that use the monitorLib server to stop their output. This is a temporary disabling function.	X

CLI Command	Description	Signaling Server
<code>tracePrintOff</code>	Blocks all logging of information received by the monitorLib service to the TTY output. This does not include traces directed through the monitorLib service to the RPT.LOG or SYSLOG.n services.	X
<code>traceFileOff</code>	Causes the monitorLib server to stop logging to the log files any and all trace information received by the service. The log files include syslog.n for the Voice Gateway Media Card and rpt.log for the Signaling Server.	X
<code>traceAllOn</code>	Clears the blocking of all trace information imposed on the monitorLib service by the traceAllOff command, the tracePrintOff command, and the traceFileOff command. By default, all tracing is on.	X
<code>tracePrintOn</code>	Clears only the TTY output blocking that was imposed by the traceAllOff and tracePrintOff commands.	X
<code>traceFileOn</code>	Clears only the blocking of logging to files that was imposed by the traceAllOff and traceFileOff commands.	X

If no directory path is supplied with the file name specified, then the file is written to the C:/U/trace directory on the Voice Gateway Media Cards and to the /u/trace directory on the Signaling Server.

If no file name is given, then no trace file is generated and output is directed to the TTY. If the file name does not meet the DOS 8.3 restriction, then the file name is rejected and no file is generated. If the file is deleted, cannot be found, or has a write error, then the output is directed to the TTY.

If the output for the trace cannot be determined, then the output is directed to the TTY.

Protocol trace tool commands for the Network Connection Service

ATTENTION

A warm boot of the system causes all tracing to cease. Traces must be reentered after the system has restarted.

Table 107 "Protocol trace tool CLI commands for the NCS" (page 447) includes the protocol trace tool commands for the Network Connection Service (NCS) applicable to the Voice Gateway Media Cards. They are issued from the OAM shell.

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

Table 107
Protocol trace tool CLI commands for the NCS

CLI Command	Description	Signaling Server
tpsARTrace IP <IP Address> ID <user ID> ALL	Allows tracing of the tpsAR protocol, which is used to determine where an IP Phone should register. Where: - IP Address - a string containing the IP Phone IP address - user UID - the ID of the IP Phone to be traced (the DN used to log in) or the H323_Alias of where the IP Phone is trying to register - ALL - all IP Phones are to be monitored	X
tpsARTraceOff IP <IP Address> ID <user ID> ALL	Removes the specified endpoint from the list of endpoints to be traced.	X
tpsAROutput <Output_Destination> <"File Pathname">	Sets the output for all tpsAR protocol traces. Where: Output_Destination specifies where all the trace messages for the tpsARTraceSet are to be directed. If the command is run from the Voice Gateway Media Card or the vxshell prompt: The values are: 1 = TTY	X

CLI Command	Description	Signaling Server
	2 = RPTLOG 3 = File 4 =TTY + File If the command is run from the OAM prompt or PDT prompt on the Signaling Server: The values are the actual word, not a number: TTY RPTLOG FILE TTY+FILE "File Pathname" is a string encapsulated in quotes. It specifies the file to output to if option 3 or 4 was selected.	
tpsARTraceSettings	Displays the trace tool settings, which endpoints are being traced, and where the trace output is being directed.	X
tpsARTraceHelp	Displays a list of all CLIs used for tracing tpsAR protocol messages, including usage and parameters.	X

Lamp Audit and Keep Alive functions

The Lamp Audit function provides a continuous source of heartbeat messages to ensure the IP Phone is powered and the IP connection is alive. Because there is a reliable UDP connection from the core through to the IP Phones, any failure of the IP Phone, the Voice Gateway Media Card, or the IP connection is detected.

Network Signaling Diagnostics

Network Signaling Diagnostics can be run as part of the midnight routines defined in LD 30. For more information, see *Software Input Output Reference—Maintenance (NN43001-711)*.

IP Phone Keep Alive

When the Voice Gateway Media Card detects that the IP Phone has been disconnected, the Voice Gateway Media Card logs the event and sends an UNREGISTER message to the system for that IP Phone.

Card or ELAN subnet failure

When the Call Server detects a loss of connection with the Voice Gateway Media Card, the Call Server logs a message and unregisters all the IP Phones and gateway channels associated with that Voice Gateway Media Card.

Maintenance audit

A background audit watches for tasks that go into a suspended state. Under normal operation, a task should not go into a suspended state. However, if it occurs, the card processing is affected.

If the audit task finds a suspended task, it performs the following actions:

- outputs a stack and register dump to the debug port
- outputs a file on the /C: drive
- resets the card

This function provides an automatic way to return the card to service and provides critical debug information. The information is output to the EXCPLOG.n files (where n is a number from 0-3) that are located in the /C:/LOG directory. The new information is placed in these files where it cannot be overwritten by the usual information output to the SYSLOG file when the card reboots.

The `auditRebootSet` command disables the card reboot if any task is found in a suspended state.

The maintenance audit enhancement differentiates between tasks that are critical and noncritical.

- A critical task is any task that the IP Line application needs to function. When a critical task is not functioning properly, it causes noticeable degradation in the IP Line application.
- A noncritical task is any other task that does not cause noticeable degradation to the IP Line application.

If a critical task is found suspended, the stack and register information is dumped and the card is then reset. If a task on the critical task list disappears, it is treated as a suspended task. Therefore, a missing critical task triggers a reboot and a missing noncritical task does not trigger a reboot.

If a noncritical task is found suspended, the information is dumped but the card is not reset. The card is reset when the Voice Gateway Media Card clock reaches 2:00 a.m. (default reset time). The reset time is configured from the CLI. This eliminates card resets that impact service for noncritical tasks by delaying them to a non-service impacting time.

Additional CLI commands have been added enabling any task to be marked as critical or noncritical, regardless of its default designation. This could be used, for example, to mark a "misbehaving" task as noncritical to avoid a card reset. This would enable the problem to be debugged.

The maintenance audit is available only for the IP Line application running on the ITG-P 24-port and Media Card line cards. It is not available on the Signaling Server as it does not have the exception handler, stack dump, and syslog file functions of the other cards.

Critical task list

All application tasks default to the critical task list. These applications include: TPS, VTM, SET, VTILIB, UMS, UMC, RDP, VGW, RTP, RTCP, ELC, baseMMintTask, and A07.

The following VxWorks system tasks are also on the critical task list: tShell, tNetTask, tExcTask, and tTelnetd.

All other tasks are on the noncritical task list. The monitor task is called tMonTask.

Any data entered at the CLI that deviates the operation from the default is saved in the /C:/CONFIG/AUDIT.INI text file. The contents of the file are loaded as the application boots up and provides the required non-volatile storage for entered settings. It is applicable only to the card on which it resides. It can be manually copied from one card to all other cards in the node if desired.

History file

A history file is created when the card starts. The text file is called audit.his and it is stored in the /C:/LOG directory. This file contains a list of the problems found and the actions taken by the maintenance audit. The audit.his file has a fixed size of 4096 bytes.

The most recent records in the file overwrite the oldest records with newer events appear at the beginning of the file. A record in the file is a one-line string with maximum size of 256 characters.

The format for the records in the history file is:

```
index : (timeString) TMxx taskName: DescriptionString
```

where:

- index – monotonically increasing record count; wraps after 9999 events
- (timeString) – the time the event was detected
- TMxx – record type: 0-reboot, 1-Suspend, and 2-TaskDisappear
- taskName – the name of problematic task

- DescriptionString – a description of the action taken

An example of the output follows.

```
IPL> auditHistoryShow
0001 : (APR 25 12:26:25) TM01 tCSV:Suspend
0002 : (APR 25 12:26:50) TM01 tSET:Suspend
0003 : (APR 25 12:26:50) TM00 tExcTask:Reboot
0004 : (APR 25 12:35:55) TM02 tELC:Disappear
0005 : (APR 25 12:35:55) TM00 tELC:Reboot
0006 : (APR 25 12:48:27) TM01 tUMC:Suspend
0007 : (APR 25 12:48:27) TM00 tExcTask:Reboot
0008 : (APR 25 13:15:56) TM01 tUMC:Suspend
0009 : (APR 25 13:15:56) TM00 tExcTask:Reboot
0010 : (APR 25 13:29:35) TM01 tLogTask:Suspend
0011 : (APR 25 13:45:35) TM01 tLogTask:Suspend
```

Maintenance audit CLI commands

There are five CLI commands that support the maintenance audit function as outlined in [Table 108 "Maintenance audit commands" \(page 451\)](#). These commands do not appear on the MC 32S card.

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

Table 108
Maintenance audit commands

Command	Description
auditShow	Displays the following information: • whether a card reboot is enabled • the time a card reboot will occur if a noncritical task is found suspended • a list of all tasks being monitored and their designation (critical or noncritical) Example: <pre>IPL> auditShow Reboot when detect a suspended task --- Disabled Critical Task: tTPS tVTM tSET tVTI tUMS tUMC tRDP tPBX tVGW tRTP tRTCP tELC</pre>

Command	Description
	baseMMintTask tA07 tShell tNetTask tExcTask tTelnetd noncritical Task: tTest
auditHistoryShow	Displays the recent history of the audit task activity in the audit.his file.
auditRebootSet 0/1	Globally disables the card reboot from this audit task. By default, this is set to 1. If it is set to 0, no card reboot occurs when a suspended task is found for critical or noncritical tasks. The debug information is dumped; however, recovery requires a manual reset of the card.
auditRebootTimeSet "timeString"	Sets the reset time for noncritical tasks to the value defined by the timeString parameter. The timeString is formatted as HH:MM and is in 24-hour clock format. By default, the time is set to 02:00 (2 AM).
auditTaskSet tTaskName, 0/1	Forces a task to be considered critical or noncritical. This command overrides the audit default setting for the task. The tTaskName parameter specifies the task (the VxWorks taskname), as displayed by the "i" command. The value of 0 marks the task as noncritical, the value of 1 marks it as critical.

Voice Gateway Media Card self-tests

During power-up, the Voice Gateway Media Card performs diagnostic tests to ensure correct operation. The faceplate RS-232 port on the Voice Gateway Media Card can be used to monitor the progress of these tests. When the processor responds correctly, the controller switches its serial port to provide Card LAN communication and connects the processor with the external RS-232 port.

Troubleshoot a software load failure

Symptoms

TM cannot establish connection with the Voice Gateway Media Card. The faceplate LCD display reads "BIOS."

Problem

The Voice Gateway Media Card has booted the BIOS load.

Diagnosis

In the event of a failure to load and run the IP Line software, the Voice Gateway Media Card defaults to the BIOS load. This load consists of a prompt that enables commands to reload the IP Line loadware and reboot.

There are three known reasons for the failure to load the IP Line software:

- Not enough memory due to a faulty or missing SIMM.
- Corruption of the IP Line loadware image in flash memory.
- The escape sequence to boot from the BIOS has been inadvertently sent down the serial line due to noise.

To determine the cause of the IP Line load failure, reboot and monitor the booting sequence through the serial port. Capture the booting sequence to aid in communication with technical support personnel.

Examples of booting sequences**Case 1**

The following excerpt from the booting sequence indicates the amount of memory onboard.

```
Memory Configuration
Onboard:  4MB
SIMM: 16MB
Total:  20MB
```

In the absence or failure of the SIMM, the total memory is 4MB; that is not enough memory to support the IP Line application.

Case 2

The following excerpt from the booting sequence indicates the Voice Gateway Media Card locating and loading the IP Line loadware from flash memory:

```
Cookie array value:  0x111111100
Checksum Validation at Bank Address:  0xF9800000 Checksum in
ROM = 35582602
Length of bank = 0004FEF8
Calculated Checksum = 35582602
Checksum array value:  0x111111100
Loading code from address:  F9800010
Verifying ROM to RAM copy...
ROM to RAM copy completed OK
Jumping to VxWorks at 0x00E00000
EIP = 0x00E0011E
Jumping to romStart at 0x00E00300
```

In the event of a software load failure, the boot sequence indicates that the BIOS is being loaded:

```
Cookie array value: 0x11111111
Booting from BIOS ROM
```

Case 3

The boot sequence indicates that the "xxx" sequence has been entered and the BIOS is being loaded.

Solutions

Case 1

If a SIMM is missing, install a 16MB SIMM into the SIMM slot which is underneath the daughterboard. If the SIMM is present, check that the SIMM is properly seated. Otherwise, the SIMM is faulty and needs replacement.

Case 2

Reattempt a software download from the FTP Server. Use the following commands:

```
upgradeErase
upgrade "hostname","hostAccount","hostPassword",
      "hostDirectoryPath","hostSWfile name"
```

After the software loads to flash, reboot the card:

```
sysReboot
```

If the failure to load the IP Line software into RAM persists, then the flash device is faulty. Replace the Voice Gateway Media Card.

Case 3

The escape sequence "xxx" is rarely transmitted. Reboot the card.

Warm reboot of the Voice Gateway Media Card

The `cardReset` IP Line CLI command performs a warm reboot of an out-of-service Voice Gateway Media Card:

Test the Voice Gateway Media Card DSPs

At the IPL> CLI, the following two tests can be performed on the Voice Gateway Media Card DSPs:

- To run a self-test on the DSP daughterboard: `DSPselfTest`

ATTENTION

If the DSP self-test fails, the Voice Gateway 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)

ATTENTION

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

Work with alarm and log files

Alarm and log file output is turned on using the IPL> CLI. The following commands can be performed at the IPL> prompt:

- To turn on or turn off the error log file, type: **logFileOn** or **logFileOff**.
- To display the modes of all log files and alarms, type: **logFileShow**.

Troubleshoot an IP Phone installation

If an IP Phone cannot be installed because the prompt for the node ID or TN does not display, follow the steps in [Procedure 70 "Troubleshooting an IP Phone installation" \(page 455\)](#).

Procedure 70

Troubleshooting an IP Phone installation

Step	Action
1	Log into one Signaling Server or Voice Gateway Media Card in the node.
2	Type the nodePwdShow command at the IPL> or oam prompt.
3	If the administrative password is enabled (PwdEna=Yes) and there is a null (zero-length) password (the Pwd field is blank), then the IP Phone cannot be installed on that Voice Gateway Media Card.
	<pre> Node1 PwdEn Pwd TmpPw Uses Timeout D a ===== d ===== ===== == 0d 0h 0m 0s = == == 123 Yes </pre>
4	Use the nodePwdSet "password" command to set the administrative password and to enable IP Phones to be installed. Ensure the "password" parameter is included.

—End—

Maintenance telephone

An IP Phone functions as a maintenance telephone when the CLS is defined as MTA (Maintenance Telephone Allowed) in the Multiline Telephone Administration program (LD 11). A maintenance telephone enables commands to be sent to the system; however, only a subset of the commands that can be entered from a system terminal can be used. To access the system using the maintenance telephone, a Special Service Prefix (SPRE) code (defined in the Customer Data Block) is entered and 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##).

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

The above maintenance overlay operations are supported on IP Phones except for the Tone and Digit Switch (TDS) commands of LD 34 and TONE command of LD 46.

Replace the Media Card CompactFlash

The Media Card must have the CompactFlash card installed in order to be used as a Voice Gateway Media Card. If the CompactFlash card is removed from the Media Card, another CompactFlash card must be installed before using the Media Card.

If it is necessary to remove the CompactFlash card, follow the steps in [Procedure 71 "Removing the CompactFlash" \(page 456\)](#). To reinstall a CompactFlash card, see [Procedure 13 "Installing the CompactFlash card on the Media Card" \(page 231\)](#).

Procedure 71

Removing the CompactFlash

Step	Action
1	Lift the metal clip that holds the CompactFlash card in the socket on the Voice Gateway Media Card.
2	Slide the card out of the socket and carefully remove the CompactFlash card.
3	Return the CompactFlash card to an antistatic package.

—End—

Voice Gateway Media Card maintenance using Element Manager

Contents

This section contains the following topics:

- ["Introduction" \(page 457\)](#)
- ["Replace a Voice Gateway Media Card" \(page 457\)](#)
- ["Add another Voice Gateway Media Card" \(page 463\)](#)
- ["Access CLI commands from Element Manager" \(page 465\)](#)
- ["Access the IPL CLI from Element Manager" \(page 476\)](#)

Introduction

This chapter provides information about the maintenance functions for the Voice Gateway Media Card performed in Element Manager.

Replace a Voice Gateway Media Card

Replace the Voice Gateway Media Card when the card is removed or when the following conditions occur:

- The Voice Gateway Media Card displays a code of the form F:xx on the faceplate LED following a reboot. This code indicates an unrecoverable hardware failure. The card cannot register with the system. The exception is the F:10 code, which indicates that the Security Device is missing from the card.
- The Management (ELAN) network interface or the Voice (TLAN) network interface on the Voice Gateway Media Card has failed. This is indicated by failing to show a link pulse on the voice IP interface status LED or on the switch. It can also be indicated if the maintenance port continuously prints "InIsa0 Carrier Failure" messages after determining that the hub or switch port and ELAN cable are good.
- A voice channel on the Voice Gateway 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.

Note that there are separate procedures for replacing a Voice Gateway Media Card, depending on the role it is to play. Be aware of the role the card will perform and choose the correct procedure. To replace a Follower card, see ["Replace a Follower Voice Gateway Media Card" \(page 458\)](#). To replace a Leader card, see ["Replace a Leader Voice Gateway Media Card" \(page 460\)](#).

Replace a Follower Voice Gateway Media Card

To replace a Follower Voice Gateway Media Card, follow the steps in [Procedure 72 "Replacing a Follower Voice Gateway Media Card" \(page 458\)](#).

Procedure 72

Replacing a Follower Voice Gateway Media Card

Step	Action
1	Locate the faulty card by the TN, MAC address, and IP address.
2	Disable the faulty Voice Gateway Media Card in LD 32 with the <code>DISI</code> command. The system outputs "NPR0011" when the card has been completely disabled by the DISI command.
3	Use the <code>disiTPS</code> command at the IPL> CLI to disable the LTPS on the faulty Voice Gateway Media Card. This forces all IP Phones registered on this card to re-register. If there are sufficient resources, this can take up to several minutes. If there are not sufficient resources, IP Phones can remain unregistered indefinitely.
4	Use the <code>isetShow</code> command to monitor the status of the card and the re-registration of the IP Phones. The Voice Gateway Media Card is completely disabled when there are no IP Phones registered on the card.
5	Remove the faulty Voice Gateway Media Card from the system.
6	Install the replacement Voice Gateway Media Card into the card slot in the system. To do this: - Pull the top and bottom locking devices away from the card faceplate. - Insert the Voice Gateway Media Card into the card guides and gently push the card until it makes contact with the backplane connector. Hook the locking devices.

When cards are installed, the red LED on the faceplate remains lit until the card is configured and enabled in the software, at which point it turns off. If the LED does not follow the pattern described or operates in any other manner (such as continually flashing or remaining weakly lit), replace the card.

Observe the faceplate maintenance display to see start-up self-test results and status messages. A display of the type F:xx indicates a failure. See [Table 82 "ITG-P 24-port line card faceplate maintenance display codes" \(page 402\)](#) for a listing of the ITG-P 24-port line card display codes and to [Table 83 "Media Card faceplate maintenance display codes" \(page 403\)](#) for a list of the Media Card display codes.

- 7 In the Element Manager navigator, click **IP Network > Nodes: Servers, Media Cards** .
The **Node Configuration** window appears.
- 8 Click the **Edit** button associated with the node containing the card to be replaced. The **Edit** window appears.
- 9 Expand the **Cards** section by clicking the plus sign (+) to the left of **Cards**.
- 10 Select the desired Voice Gateway Media Card from the list of cards in the node.
- 11 Change the **Embedded LAN (ELAN) MAC address** field to the MAC address of the replacement Voice Gateway Media Card.
The MAC address is the Ethernet address labeled on the faceplate of the replacement Voice Gateway Media Card.
ELAN: xx:xx:xx:xx:xx:xx
TLAN: xx:xx:xx:xx:xx:xx
- 12 Click **Save and Transfer**.
The **Node Configuration** window appears.
- 13 Click the **Transfer/Status** button associated with the node containing the Voice Gateway Media Card.
- 14 After the transfer is complete, restart the new card.
Restarting the card causes the follower card to obtain its BOOTP parameters from the Leader, and also establishes ELAN and TLAN subnet connectivity.
- 15 Follow the steps in [Procedure 35 "Configuring the Follower cards" \(page 292\)](#) to load the CONFIG.INI file onto the card.

- 16 Follow the steps in [Procedure 40 "Upgrading the card loadware" \(page 299\)](#) to download the latest software to the Voice Gateway Media Card.
- 17 Follow the steps in [Procedure 41 "Rebooting the Voice Gateway Media Card" \(page 300\)](#) to reboot the card and run the new software.
- 18 Follow the steps in [Procedure 43 "Upgrading the IP Phone firmware" \(page 302\)](#) to update the card firmware.

—End—

Replace a Leader Voice Gateway Media Card

To replace a Leader Voice Gateway Media Card, follow the steps in [Procedure 73 "Replacing a Leader Voice Gateway Media Card" \(page 460\)](#).

Procedure 73

Replacing a Leader Voice Gateway Media Card

Step	Action
1	Locate the faulty card by the TN, MAC address, and IP address.
2	Disable the faulty Voice Gateway Media Card in LD 32 with the DISI command. The system outputs "NPR0011" when the card has been completely disabled by the DISI command.
3	Use the <code>disiTPS</code> command at the IPL> CLI to disable the LTPS on the faulty Voice Gateway Media Card. This forces all IP Phones registered on this card to re-register. If there are sufficient resources, this can take up to several minutes. If there are not sufficient resources, IP Phones can remain unregistered indefinitely.
4	Use the <code>isetShow</code> command to monitor the status of the card and the re-registration of the IP Phones. The Voice Gateway Media Card is completely disabled when no IP Phones are registered on the card.
5	Remove the faulty Voice Gateway Media Card from the system.
6	Install the replacement Voice Gateway Media Card into the card slot in the system. To do this: a. Pull the top and bottom locking devices away from the card faceplate.

- b. Insert the Voice Gateway Media Card into the card guides and gently push the card until it makes contact with the backplane connector. Hook the locking devices.

When cards are installed, the red LED on the faceplate remains lit until the card is configured and enabled in the software, at which point it turns off. If the LED does not follow the pattern described or operates in any other manner (such as continually flashing or remaining weakly lit), replace the card.

Observe the faceplate maintenance display to see start-up self-test results and status messages. A display of the type F:xx indicates a failure. See [Table 82 "ITG-P 24-port line card faceplate maintenance display codes" \(page 402\)](#) for a listing of the ITG-P 24-port line card display codes and to [Table 83 "Media Card faceplate maintenance display codes" \(page 403\)](#) for a listing of the Media Card display codes.

- 7 Go to the VxWorks shell. Configure the Voice Gateway Media Card as a Leader using the ELAN network interface IP address and subnet mask.
- 8 Restart the card.
The card obtains the ELAN network interface IP address and subnet mask.
- 9 In the Element Manager navigator, click **IP Network > Nodes: Servers, Media Cards**.
The **Node Configuration** window appears.
- 10 Click the **Edit** button associated with the node containing the card to be replaced.
The **Edit** window appears.
- 11 Expand the **Cards** section by clicking the plus sign (+) to the left of **Cards**.
- 12 Select the Voice Gateway Media Card from the list of cards in the node.
- 13 Change the **Embedded LAN (ELAN) MAC address** field to the MAC address of the replacement Voice Gateway Media Card. The MAC address is the Ethernet address labeled on the faceplate of the replacement Voice Gateway Media Card.
ELAN: xx:xx:xx:xx:xx:xx
TLAN: xx:xx:xx:xx:xx:xx

- 14 Follow the steps in [Procedure 40 "Upgrading the card loadware" \(page 299\)](#) to download the latest software to the Voice Gateway Media Card.
- 15 Follow the steps in [Procedure 41 "Rebooting the Voice Gateway Media Card" \(page 300\)](#) to reboot the card and run the new software.
- 16 Follow the steps in [Procedure 43 "Upgrading the IP Phone firmware" \(page 302\)](#) to update the card firmware.

—End—

Verify Voice Gateway Media Card loadware and firmware

The following steps are required to verify and upgrade the card loadware and IP Phone firmware:

Step	Action
1	Check the version of the loadware currently installed on the Voice Gateway Media Card. See "Determine Voice Gateway Media Card software version" (page 294) .
2	Check the version of the firmware that is currently running on the Voice Gateway Media Card. See Procedure 36 "Determining the IP Phone firmware version" (page 295) .
3	Obtain the latest files from the Signaling Server installation CD. See "Download files from Nortel web site" (page 509) .
4	Upload the loadware and firmware files using the File Upload system utility in Element Manager. See Procedure 39 "Uploading loadware and firmware files" (page 298) .
5	Upgrade the Voice Gateway Media Card software. See Procedure 40 "Upgrading the card loadware" (page 299) .
6	Restart the Voice Gateway Media Card. See Procedure 41 "Rebooting the Voice Gateway Media Card" (page 300) .
7	Upgrade and distribute the firmware to the IP Phones on the Voice Gateway Media Card. See Procedure 43 "Upgrading the IP Phone firmware" (page 302) .

—End—

ATTENTION

Use the loadware supplied on the Signaling Server installation CD only.

Add another Voice Gateway Media Card

Follow the steps in [Procedure 74 "Add another Voice Gateway Media Card to the system" \(page 463\)](#) to add another Voice Gateway Media Card to the system.

Procedure 74

Add another Voice Gateway Media Card to the system

Step	Action
1	Install and cable the Voice Gateway Media Card, as described in "Install the hardware components" (page 226) .
2	Go to the VxWorks shell. Configure the Voice Gateway Media Card as a Follower using the ELAN network interface IP address and subnet mask. Restart the card. The card obtains the ELAN network interface IP address and subnet mask.
3	In the Element Manager navigator, click IP Network > Nodes: Servers, Media Cards . The Node Configuration window appears.
4	Click the Edit button associated with the node containing the card to be replaced. The Edit window appears.
5	Expand the Cards section by clicking the plus sign (+) to the left of Cards .
6	Click Cards and then click the Add button. The fields to be configured for the new card are displayed.
7	Enter the Card Properties data. Role: The role is assigned based on the information that Element Manager reads from the card configuration. This is a read-only field. Embedded LAN (ELAN) IP address: This is the ELAN network interface IP address for the card. Element Manager and the system use this address to communicate with the card.

- c. **Embedded LAN (ELAN) MAC address:** The MAC address is the Motherboard Ethernet address labeled on the faceplate of the Voice Gateway Media Card.
 - d. **Telephony LAN (TLAN) IP address:** This is the TLAN network interface IP address for the card.
 - e. **Voice LAN (TLAN) gateway IP address:** This is the IP address of the router interface on the TLAN subnet.
 - f. **Hostname:** This is the Host name.
 - g. **Card TN:** Enter the card slot number between 1 – 50.
 - h. **Card processor type:** Choose either Pentium or Media Card. Select Pentium if using the ITG-P 24-port line card (dual-slot card). Select Media Card if using the Media Card 32-port MC 32S card (single-slot card).
 - i. **Telephony LAN (TLAN) DSP IP address:**
 - i. **H323 ID:** The H323 ID within IP Line is for the Virtual Office/ Media Gateway 1000B feature. Keep the H323 ID the same for all the elements within one node.
 - j. **Enable LTPS:** Select the check box.
 - k. **Primary Call Server IP address** Enter the IP address of the primary Call Server.
 - l. **Alternate Call Server1 IP address** Enter the IP address for the Alternate Call Server, if one is configured.
 - m. **Alternate Call Server2 IP address** Enter the IP address for the Alternate Call Server, if one is configured.
- 8 Click **Save and Transfer**.
- The **Node Configuration** window appears.
- 9 Click the **Transfer/Status** button associated with the node containing the Voice Gateway Media Card.
- 10 After the transfer is complete, restart the new card.
- Restarting the card causes the follower card to obtain its BOOTP parameters from the Leader, and also establishes ELAN and TLAN subnet connectivity.
- 11 Follow the steps in [Procedure 35 "Configuring the Follower cards" \(page 292\)](#) to load the CONFIG.INI file onto the card.
- 12 Follow the steps in [Procedure 40 "Upgrading the card loadware" \(page 299\)](#) to download the latest software to the Voice Gateway Media Card.

- 13 Follow the steps in [Procedure 41 "Rebooting the Voice Gateway Media Card" \(page 300\)](#) to reboot the card and run the new software.
- 14 Follow the steps in [Procedure 43 "Upgrading the IP Phone firmware" \(page 302\)](#) to update the card firmware.

—End—

Access CLI commands from Element Manager

Table 109 "Informational CLI commands by group for Voice Gateway Media Card" (page 465) lists the informational CLI commands (by group) available from Element Manager for the Voice Gateway Media Cards.

Table 109
Informational CLI commands by group for Voice Gateway Media Card

Group	Command
Dsp	dspSWVersion Show dSPNumShow
Election	electShow
Iset	isetShow isetNATShow isetLocShow isetLocNeedUpdateShow isetFWShow isetFWGet
Mam	disServices enlServices forcedisServices IPinfoShow itgCardShow servicesStatusShow
NodePwd	nodePwdDisable nodePwdEnable nodePwdShow nodeTempPwdClear nodePwdSet nodeTempPwdSet
pbxLink	pbxLinkShow
QoS	isetInfoShow RTPStatShow rping rTraceRoute

Group	Command
System	ifShow routeShow rudpShow
Tps	disTPS enlTPS forcedisTPS loadBalance echoServerShow
Ums	umsPolicyshow
Vgw	vgwShowAll Print VGW Channels
Misc	cardRoleShow ipstatShow
Media Gateway Controller	swVersionShow macShow mgcInfoShow memShow dsikShow
Media Card 32S card	mc32sSetup dspchatstateshow dsphwcheck dsplooptest dspnumshow ommshow pcmcapturestart pcmcapturestop vgwcardshow macshow mgcinfoshow mc32scliupgrade diskformat ethportmirror ethportautoneg rmonstatshow resetpwd diskshow

Table 110 "Informational CLI commands by group for Signaling Server" (page 467) lists the informational CLI commands (by group) available from Element Manager for the for the Signaling Server.

Table 110
Informational CLI commands by group for Signaling Server

Group	Command
Election	electShow
Iset	isetShow isetNATShow isetFWShow isetFWGet
Mam	disServices enlServices forcedisServices IPinfoShow itgCardShow servicesStatusShow
NodePwd	nodePwdDisable nodePwdEnable nodePwdShow nodeTempPwdClear nodePwdSet nodeTempPwdSet
pbxLink	pbxLinkShow
QoS	isetInfoShow RTPStatShow rping rTraceRoute
Sip	SIPGwShow SIPGwShowch SIPGwShownum
System	ifShow routeShow rudpShow
Tps	distPS enlTPS forcedistPS loadBalance echoServerShow
Uftp	uftpTurboMode uftpTurboModeShow uftpTurboModeTimeoutSet uftpAutoUpgradeTimeoutSet
Ums	umsPolicyshow

Group	Command
Vtrk	vtrkShow disVTRK enlVTRK forcedisVTRK
Misc	cardRoleShow DCHstatus help ipstatShow

See "IP Line CLI commands" (page 420) for descriptions of these commands.

To access these commands in Element Manager, follow the steps in Procedure 75 "Accessing the CLI commands from Element Manager" (page 468).

Procedure 75

Accessing the CLI commands from Element Manager

Step	Action

1	In the Element Manager navigator, click IP Network > Maintenance and Reports .

The **Node Maintenance and Reports** window appears.

2	Expand the node containing the Voice Gateway Media Card by clicking the plus sign (+) to the left of the Node ID.

3	Click the GEN CMD button associated with the Voice Gateway Media Card.

The **General Commands** window appears.

The line shown on the top of the General Commands window, under **General Commands**, displays the IP address of the element and what the selected element is, as follows:

- ITG Pentium – ITG-P 24-port card
- Media Card 32-port card
- SS – Signaling Server
- Media Card 32S

4	Select the CLI command group from the Group drop-down list box, select the CLI command from the Command drop-down list, and click RUN .

The output of the command is displayed in the text area at the bottom of the General Commands window.

—End—

Sample Output of Element Manager CLI commands

cardRoleShow

Card Role = Follower

dspSWVersionShow

DSP software version R8.01

DSPNumShow

Number of DSPs = 8

electShow

The following is an example of the output on a Signaling Server:

```
oam> electShow
Node ID      : 541
Node Master  : No
Up Time     : 10 days, 3 hours, 5 mins, 30 secs
TN          : 10 00
Host Type    : SMC
TLAN IP Addr : 47.11.151.148
ELAN IP Addr : 47.11.221.48
Election Duration : 15
Wait for Result time : 35
Master Broadcast period : 30
===== master tps =====
Host Type  TN          TLAN IP Addr
ISP 1100  00 00      47.11.151.144
Next timeout : 30 sec
AutoAnnounce : 1
Timer duration : 60 (Next timeout in 7 sec)
===== all tps =====
Num TN      Host Type  ELAN MAC      TLAN
IP Addr    ELAN IP Addr  Up Time    NumOfSets
TimeOut
001 10 00    SMC        00:60:38:bd:d1:01
47.11.151.148 47.11.221.48  010 03:05:30 0
0
002 00 00    ISP 1100   00:02:b3:c5:51:2c
47.11.151.144 47.11.221.38  010 05:24:41 0
-73
===== All cards in node configuration are registered =====
```

+master tps

```
PlatForm  TN      TLAN
ISP 1100  0000   47.104.39.245
Next timeout = 71 sec
```

```
AutoAnnounce: 1
Timer duration : 60 (Next timeout in 25 sec)
```

all tps

Num	Platform	TN	TLAN	ELAN	TimeOut
0	ITG SA	080c	47.104.39.243	47.104.39.115	0
1	ISP 1100	0000	47.104.39.246	47.104.39.118	0
2	ISP 1100	0000	47.104.39.245	47.104.39.117	0
3	ITG SA	0c04	47.104.39.244	47.104.39.116	1

i

NAME	ENTRY	TID	PRI	STATUS	PC	SP	ERRNO	DELAY
tExcTask	_excTask	339a824	0	PEND	2aca80	339a758	3006b	0
tShell	_shell	2e31e30	1	PEND	231e08	2e316d4	0	0
...	...	...	...	...	...	...	...	...
tSET	19be9c	2b6263c	200	PEND	256d84	2b62518	320001	0
tSyslogd	10a58	3aff168	255	READY	22f6d0	3afeac4	0	0

ifShow

```
ixpMac (unit number 1):
Flags: (0x8863) UP BROADCAST MULTICAST ARP RUNNING
Type: ETHERNET_CSMACD
Internet address: 47.104.39.115
Broadcast address: 47.104.39.127
Netmask 0xffff0000 Subnetmask 0xfffffff80
Ethernet address is 00:60:38:bd:bb:cd
Metric is 0
Maximum Transfer Unit size is 1500
298604 packets received; 23909 packets sent
278631 multicast packets received
4608 multicast packets sent
0 input errors; 0 output errors
0 collisions; 0 dropped
lo (unit number 0):
Flags: (0x8069) UP LOOPBACK MULTICAST ARP RUNNING
Type: SOFTWARE_LOOPBACK
Internet address: 127.0.0.1
Netmask 0xffff0000 Subnetmask 0xffff00000
Metric is 0
Maximum Transfer Unit size is 32768
4 packets received; 4 packets sent
0 multicast packets received
0 multicast packets sent
0 input errors; 0 output errors
0 collisions; 0 dropped
ixpMac (unit number 0):
Flags: (0x8863) UP BROADCAST MULTICAST ARP RUNNING
Type: ETHERNET_CSMACD
Internet address: 47.104.39.243
Broadcast address: 47.104.39.255
```

```

Netmask 0xff000000 Subnetmask 0xfffff80
Ethernet address is 00:60:38:bd:bb:cc
Metric is 0
Maximum Transfer Unit size is 1500
88686 packets received; 15027 packets sent
78030 multicast packets received
5044 multicast packets sent
0 input errors; 0 output errors
0 collisions; 0 dropped

```

IPInfoShow

```

Maintenance Interface = ixpMac1
Maintenance IP address = 47.104.39.115
Maintenance subnet mask = 255.255.255.128
Voice Interface = ixpMac0
Voice IP address = 47.104.39.243
Voice subnet mask = 255.255.255.128

```

ROUTE NET TABLE

destination	gateway	flags	Refcnt	Use	Interface
0.0.0.0	47.104.39.129	3	0	675	ixpMac0
47.104.39.0	47.104.39.115	101	0	0	ixpMac1
47.104.39.128	47.104.39.243	101	0	0	ixpMac0

ROUTE HOST TABLE

destination	gateway	flags	Refcnt	Use	Interface
127.0.0.1	127.0.0.1	5	0	0	lo0

ipstatShow

```

total 128099
badsum 0
tooshort 0
toosmall 0
badhlen 0
badlen 0
infragments 0
fragdropped 0
fragtimeout 0
forward 0
cantforward 486
redirectsent 0
unknownprotocol 0

```

```

nobuffers 0
reassembled 0
outfragments 0
noroute 0

```

isetShow

Set Information						
IP Address	NAT	Model Name	Type	RegType	State	Up
192.168.253.25		IP Phone 2001 Phase 2	i2001	Regular	online	1
192.168.253.23		IP Phone 2001 Phase 2	i2001	Regular	online	1
192.168.253.26		IP Phone 2002 Phase 2	i2002 Ph2	Regular	online	1
192.168.253.13		IP Phone 2004 Phase 0/1	i2004	Regular	online	1
192.168.253.14		IP Phone 2004 Phase 0/1	i2004	Regular	online	1
Total sets = 5						

itgCardShow

```

Index      : 2
Type       : EXUT
Role       : Follower
Node       : 541
Leader IP  : 47.11.151.145
Card IP    : 47.11.151.148
Card TN    : Slot 10
Card State : ENBL
Uptime     : 10 days, 3 hours, 11 mins, 24
secs (875484 secs)
Codecs     : G711Ulaw(default), G711Alaw, G711CC, T38FAX
ELAN (ixpMac1) stat: 10 Mb/s, Half duplex (Carrier OK)
TLAN (ixpMac0) stat: 100 Mb/s, Full duplex (Carrier OK)

```

nodePasswordDisable

Please run nodePwdShow to verify the result.

Run nodePwdShow and get the following results:

NodeID	PwdEna	Pwd	TmpPwd	Use	TimeOut
=====	=====	===	=====	s	=====
		=		===	
				=	
444	No			0	0d 0h 0m 0s

nodePasswordEnable

Please run nodePwdShow to verify the result.

Run nodePwdShow and get the following results:

NodeID =====	PwdEna =====	Pwd ===	TmpPwd =====	Use s	TimeOut =====
		=		==	
				=	
444	No			0	0d 0h 0m 0s

nodePasswordShow

NodeID =====	PwdEna =====	Pwd ===	TmpPwd =====	Use s	TimeOut =====
		=		==	
				=	
444	No			0	0d 0h 0m 0s

nodeTempPwdClear

Please run nodePwdShow to verify the result.

Run nodePwdShow and get the following results:

NodeID =====	PwdEna =====	Pwd ===	TmpPwd =====	Use s	TimeOut =====
		=		==	
				=	
444	No			0	0d 0h 0m 0s

pbxLinkShow

```
Active CS type = CS 1K
Active CS S/W Release = 201R
Supported Features: GetCSVsn TCP ShiftKey I2050
I2002 CorpDir UserKeyLabel VirtualOffice UseCSPwd
CS Main: ip = 47.104.39.112, ConnectID = 0x2bbfb4c,
BroadcastID = 0x2bc059c, Link is up
CS Signaling Port = 15000
CS Broadcast Port = 15001
Broadcast PortID = 0x2bc06fc
RUDP portID = 0x2bc0684
Tcp Link state = up
Tcp Signaling Port: 15000
Tcp socket fd:      30
Tcp msgs sent:      77
Tcp msgs recd:      47
```

routeShow**ROUTE NET TABLE**

destination	gateway	flags	Refcn t	Use	Interface
0.0.0.0	47.104.39.129	3	0	675	ixpMac0
47.104.39.0	47.104.39.115	101	0	0	ixpMac1
47.104.39.128	47.104.39.243	101	0	0	ixpMac0

ROUTE HOST TABLE

destination	gateway	flags	Refcnt	Use	Interface
127.0.0.1	127.0.0.1	5	0	0	lo0

rudpdShow

RUDP Port Summary

Port ID	Src IP	Src Port
+-----+		
0x02bcb904	0.0.0.0	15001
0x02bcb878	47.11.221.48	15000
0x02b4b748	47.11.151.148	7300
0x0231d808	47.11.151.148	5100

RUDP Connection Summary

Src IP	Src Port	Connect ID	Dst IP	Dst Port	Status	Msg rcv	Msg sent	Retries
0.0.0.0	15001	0x02bcb77c	47.11.221.41	15000	DUDP	1	0	0
47.11.221.48	15000	0x02bcad18	47.11.221.41	15000	Established	2	44305	3075

umsPolicyShow

Total firmware = 2

FirmWare	Term Type	Policy Name	Server	File Name	Limit	When	Upgrade	Protocol	Retry
0602B38	2004P2	DEFAULT_2004P2	47.104.39.243	/ums/i2004.fw	10	ALWAYS	ANY	TFTP	-1
0603B38	2002P2	DEFAULT_2002P2	47.104.39.245	/ums/i2002.fw	10	ALWAYS	ANY	TFTP	-1

vgwShowAll

VGW Service is: Enabled

Chan n	Chan State	Dsp Mode	Cod ec	Tn	Reg	Air Tim e	rxTsap	txTsap
0	Idle	Closed	n/a	0x080c	yes	0	0.0.0.0:0000	0.0.0.0:0000
1	Idle	Closed	n/a	0x080d	yes	0	0.0.0.0:0000	0.0.0.0:0000
2	Idle	Closed	n/a	0x080e	yes	0	0.0.0.0:0000	0.0.0.0:0000
3	Idle	Closed	n/a	0x080f	yes	0	0.0.0.0:0000	0.0.0.0:0000
4	Idle	Closed	n/a	0x084c	yes	0	0.0.0.0:0000	0.0.0.0:0000
5	Idle	Closed	n/a	0x084d	yes	0	0.0.0.0:0000	0.0.0.0:0000
6	Idle	Closed	n/a	0x084e	yes	0	0.0.0.0:0000	0.0.0.0:0000
7	Idle	Closed	n/a	0x084f	yes	0	0.0.0.0:0000	0.0.0.0:0000
8	Idle	Closed	n/a	0x088c	yes	0	0.0.0.0:0000	0.0.0.0:0000
9	Idle	Closed	n/a	0x088d	yes	0	0.0.0.0:0000	0.0.0.0:0000
10	Idle	Closed	n/a	0x088e	yes	0	0.0.0.0:0000	0.0.0.0:0000
11	Idle	Closed	n/a	0x088f	yes	0	0.0.0.0:0000	0.0.0.0:0000
12	Idle	Closed	n/a	0x08cc	yes	0	0.0.0.0:0000	0.0.0.0:0000
13	Idle	Closed	n/a	0x08cd	yes	0	0.0.0.0:0000	0.0.0.0:0000
14	Idle	Closed	n/a	0x08ce	yes	0	0.0.0.0:0000	0.0.0.0:0000
15	Idle	Closed	n/a	0x08cf	yes	0	0.0.0.0:0000	0.0.0.0:0000
16	Idle	Closed	n/a	0x090c	yes	0	0.0.0.0:0000	0.0.0.0:0000
17	Idle	Closed	n/a	0x090d	yes	0	0.0.0.0:0000	0.0.0.0:0000
18	Idle	Closed	n/a	0x090e	yes	0	0.0.0.0:0000	0.0.0.0:0000
19	Idle	Closed	n/a	0x090f	yes	0	0.0.0.0:0000	0.0.0.0:0000
20	Idle	Closed	n/a	0x094c	yes	0	0.0.0.0:0000	0.0.0.0:0000
21	Idle	Closed	n/a	0x094d	yes	0	0.0.0.0:0000	0.0.0.0:0000
22	Idle	Closed	n/a	0x094e	yes	0	0.0.0.0:0000	0.0.0.0:0000
23	Idle	Closed	n/a	0x094f	yes	0	0.0.0.0:0000	0.0.0.0:0000
24	Idle	Closed	n/a	0x098c	yes	0	0.0.0.0:0000	0.0.0.0:0000
25	Idle	Closed	n/a	0x098d	yes	0	0.0.0.0:0000	0.0.0.0:0000
26	Idle	Closed	n/a	0x098e	yes	0	0.0.0.0:0000	0.0.0.0:0000
27	Idle	Closed	n/a	0x098f	yes	0	0.0.0.0:0000	0.0.0.0:0000
28	Idle	Closed	n/a	0x09cc	yes	0	0.0.0.0:0000	0.0.0.0:0000
29	Idle	Closed	n/a	0x09cd	yes	0	0.0.0.0:0000	0.0.0.0:0000

Chan	Chan	Dsp	Cod	Tn	Reg	Air	rxTsap	txTsap
n	State	Mode	ec			Tim		
						e		
30	Idle	Closed	n/a	0x09ce	yes	0	0.0.0.0:0000	0.0.0.0:0000
31	Idle	Closed	n/a	0x09cf	yes	0	0.0.0.0:0000	0.0.0.0:0000

Access the CLI from Element Manager

To access the CLI with Element Manager, follow the steps in [Procedure 69 "Accessing a Voice Gateway Media Card using Telnet"](#) (page 399).

Convert IP Trunk Cards to Voice Gateway Media Cards

Contents

This section contains the following topics:

- ["Introduction" \(page 477\)](#)
- ["Before you begin" \(page 478\)](#)
- ["Convert the IP Trunk cards" \(page 478\)](#)
- ["Add the converted cards to an IP Telephony node" \(page 479\)](#)

Introduction

Media Card 32-port trunk card and ITG-P 24-port trunk cards that are no longer being used as Trunk cards can be converted to Voice Gateway Media Cards running the IP Line application.

Recommendation

Nortel recommends using the TM 3.1 ITG ISDN trunk service (used to manage the trunk node) to download the IP Line application loadware to the existing trunk cards.

Post-conversion

After the trunk cards have been converted to run the IP Line application, perform the following actions:

- manually add the converted Voice Gateway Media Cards to an IP Telephony node
- configure the corresponding Voice Gateway TNs on the Call Server

To perform these actions using Element Manager, see ["Add a Voice Gateway Media Card to the node" \(page 357\)](#).

ITG Trunk 2.x nodes that contain Media Cards must be upgraded to IP Trunk 3.0x and rebooted. This is necessary to enable TM 3.1 to transmit the IP Line application to the trunk cards that are to be converted.

Before you begin

Before beginning the conversion procedure, ensure that all IP Trunk 3.0x cards have received their IP address configuration data from the Active Leader (Leader 0 or Leader 1) and are functioning in the role of Active Leader, Backup Leader, or Follower.

Convert the IP Trunk cards

Follow the steps in [Procedure 76 "Converting IP Trunk card to Voice Gateway Media Cards" \(page 478\)](#) to convert the IP Trunk cards to Voice Gateway Media Cards.

Procedure 76

Converting IP Trunk card to Voice Gateway Media Cards

Step	Action
1	Obtain the CS 1000 Release 5.0 IP Line software (IPL500xx.p2 and IPL500xx.sa). Place the Signaling Server Installation CD in the drive of the TM Server, or use FTP to obtain the IP Line software from the Signaling Server.
2	Use the TM 3.1 ITG ISDN Trunk service to select the node, or to select all cards in the node of the same host type (Media Card or ITG-P).
3	Right-click and select Configuration > Synchronize > Transmit . Click the appropriate radio buttons for selected node or selected cards, and for the card software.
4	Click Browse and locate the IP Line loadware file for the appropriate card type (Media Card or ITG-P).
5	Click Open > Start Transmit . Monitor the progress in the Transmit Control window to ensure that the IP Line loadware is transmitted successfully to all selected cards.
6	At the Call Server CLI, use the LD 32 DISI command to disable each IP Trunk card that is being converted.
7	In the TM 3.1 ITG ISDN Trunk service, double-click on each disabled card that is being converted. Click the Reset button for each card.
8	Verify the firmware version of each Media Card and ITG-P 24-port card. In TM 3.1 ITG ISDN Trunk service, Telnet to each card and log into the IPL> shell. Check the firmware version by entering the following: IPL>firmwareVersionShow

- 9 If part of the IP trunk node is being retained, then the IP Trunk cards that are being converted must be deleted from the existing IP Trunk node in TM. The IP Trunk node properties must be transmitted from TM to the Leader of the IP Trunk node.

If none of the IP Trunk node is being retained, delete the node in TM 3.1.

—End—

Add the converted cards to an IP Telephony node

Before adding the converted cards to an IP Telephony node, ensure the following:

- the Signaling Server is functioning properly
- the ELAN and TLAN network interfaces are properly configured
- the Signaling Server is configured as the Leader in the node
- the Call Server software is upgraded to CS 1000 Release 5.0 software
- all unused IP Trunk TNs have been removed from the Call Server database
- all IP Trunk cards have been converted to Voice Gateway Media Cards (upgraded to the IP Line application)
- a PC is connected to the LAN

Choose one of the following methods:

1. ["Manually add converted Voice Gateway Media Cards to the existing IP Telephony node" \(page 479\).](#)
2. ["Import all converted Voice Gateway Media Cards into a new IP Telephony node" \(page 482\).](#) Use this method if the entire IP Trunk node has been converted and the converted Voice Gateway Media Cards do not have to be added to a larger existing node.

Manually add converted Voice Gateway Media Cards to the existing IP Telephony node

Follow the steps in [Procedure 77 "Adding the converted Voice Gateway Media Cards into an existing IP Telephony node" \(page 480\)](#) to add the converted Voice Gateway Media Cards to an existing IP Telephony node using Element Manager.

Procedure 77**Adding the converted Voice Gateway Media Cards into an existing IP Telephony node**

Step	Action
1	Log in to Element Manager from the Web browser by entering the IP address of the Signaling Server.
2	Enter the User ID and password (usually the same as the Call Server User ID and password).
3	In the Element Manager navigator, click IP Network > Nodes: Servers, Media Cards . The Node Configuration window appears.
4	Click the Edit button of the node to which the converted cards are added as Followers. The Edit window appears.
5	In the Edit window, click the Add button in the Cards field. The card properties fields are displayed.
6	Enter the data for the following fields: • Management LAN (ELAN) IP address • Management LAN (ELAN) MAC address • Voice Lan (TLAN) IP address • Voice Lan (TLAN) gateway IP address • Hostname • Card TN • Select the card processor type (ITG-P or Media Card) • H323 ID • Select the Enable set TPS checkbox • System name • System location • System contact

The following is an example of the card properties data:

Table 111
Example of card properties data

ELAN IP address	47.11.215.115
ELAN MAC address	00:60:38:bd:fe:80
TLAN IP address	47.11.215.234
TLAN gateway IP address	47.11.215.1
Hostname	
Card TN	9
Card Processor Type	Media Card
H.323 ID	
Enable set TPS	check mark
System name	MGC1
System location	BWM system 1
System contact	John Smith

- 7 Repeat the previous step for each card that is to be added to the node.
- 8 When the card property data has been entered for all the cards, click the **Save and Transfer** button.

This action saves the configuration changes to the Call Server and transfers the changes to the Signaling Servers and Voice Gateway Media Cards in the node. The BOOTP and CONFIG.INI files are saved on the Call Server and transferred to the Signaling Server Leader. The BOOTP table is updated so that the converted cards can receive their IP address configuration.

The Transfer Progress window appears.

It might be necessary to press the Reset button on the faceplate of the converted cards to trigger a new BOOTP request. Do not continue with this procedure until all converted cards have received their IP addresses.

- 9 Click the **Transfer to Failed Elements** button to transfer the bootp.tab and CONFIG.INI files to the converted cards.
- 10 Configure the new Voice Gateway TNs on the Call Server using one of the following methods:
 - a. Use LD 14 from the Call Server CLI to configure the new Voice Gateway TNs.

or

- b. In the Element Manager navigator, click **IP Network > Nodes: Servers, Media Cards**.

The **Node Configuration** window appears.

1. Expand the desired node by clicking the plus sign (+) to the left of the Node ID.
2. Click **VGW CHANNELS** next to the appropriate Voice Gateway Media Card.

The VGW Channels window appears.

3. Click **Add**.

if an Alert Box appears, log into the CLI of the Call Server. Use LD 22 to determine if Package 167 is enabled or restricted by entering 167 as a response to the TYPE prompt.

If Package 167 is restricted, obtain a new keycode to enable GPRI Package 167.

In LD 73, enter DDB at the TYPE prompt and press <CR> through the overlay, accepting all the defaults.

—End—

Import all converted Voice Gateway Media Cards into a new IP Telephony node

Follow the steps in [Procedure 78 "Importing all converted Voice Gateway Media Cards into a new IP Telephony node" \(page 482\)](#) to import all newly-converted Voice Gateway Media Cards into a new IP Telephony node using Element Manager.

Procedure 78

Importing all converted Voice Gateway Media Cards into a new IP Telephony node

Step	Action
1	Log into Element Manager from the Web browser by entering the IP address of the Signaling Server.
2	Enter the User ID and password (usually the same as the Call Server User ID and password).
3	When logged into Element Manager, click IP Network > Nodes: Servers, Media Cards .

The **Node Configuration** window appears.

- 4 Click the **Import Node Files** button.

The **Import Node Files** window appears.

- 5 In the box, enter the Leader Management Lan (ELAN) IP address of the former Leader 0 of the IP Trunk node that has been converted. Click **Import**.

The following text is displayed.

The BOOTP.1 and CONFIG1.INI files were retrieved from
Voice Gateway Media Card x.x.x.x.

- 6 As the BOOTP.1 file does not have a node ID, enter the node ID for this node.

If a Signaling Server has already been installed, the Signaling Server is the leader for this node. If IP Phones have been configured to point to the Signaling Server node ID, use the node ID of that Signaling Server to create this node. Add the Signaling Server to this node in Step 8.

- 7 Enter the node ID.

- 8 Click **Continue**.

When the new node has been created with the imported data, the following warning is displayed.

Warning: Call Server address in CONFIG.INI is o.o.o.o.
Please edit the node and update it.
BOOTP.TAB AND CONFIG.INI files for node yyy were
retrieved from Voice Gateway Media Card x.x.x.x. and
stored on Call Server z.z.z.z. The new node will
appear
on the Node Summary page (Configuration > IP
Telephony).

- 9 In the **Node Configuration** window, click the **Edit** button for the new node.

The **Edit** window appears.

- 10 Expand the LAN section by clicking the plus sign (+) to the left.

- 11 On the **Edit** page, in the **Management LAN (ELAN) configuration** section, enter the correct IP address of the Call Server:

- 12 Add the Signaling Server (if it exists and is not already part of a larger IP Telephony node).

Click **Add** next to the **Signaling Server** section.

- 13** Add any additional Voice Gateway Media Cards.

Click **Add** next to the **Cards** section.

- 14** After all required fields for the card properties have been entered, click **Submit and Transfer**.

This action saves the configuration changes to the Call Server and transfers the changes to the Signaling Servers and Voice Gateway Media Cards in the node.

The **Transfer Progress** window is displayed.

The BOOTP.1 and CONFIG.INI file are saved on the Call Server and transferred to the Signaling Server Leader. The BOOTP table is updated so that the converted cards can receive their IP addresses.

It might be necessary to press the Reset button on the faceplate of the converted cards to trigger a new BOOTP request. Do not continue with this procedure until all converted cards have received their IP addresses.

- 15** Configure the new Voice Gateway TNs on the Call Server using one of the following methods:

- a. Use LD 14 from the Call Server CLI to configure the new Voice Gateway TNs.

or

- b. In the Element Manager navigator, click **IP Network > Nodes: Servers, Media Cards**.

The **Node Configuration** window appears.

1. Expand the node by clicking the plus sign (+) to the left of the Node ID.
2. Click the appropriate Voice Gateway Media Card.
3. Click **VGW CHANNELS** next to the appropriate Voice Gateway Media Card.

The **VGW Channels** window appears.

4. If an Alert Box appears, log into the CLI of the Call Server. In LD 22, enter 167 as a response to the TYPE prompt to determine if Package 167 is enabled or restricted.

If it is restricted, obtain a new keycode to enable GPRI Package 167.

In LD 73, enter DDB at the TYPE prompt.:

Press <CR> through the overlay, accepting all the defaults.

- 16** If no Signaling Server is added to the imported node, Telnet to the former IP Trunk Leader 0 card and use the `clearLeader` command to remove the Leader Flag from Leader 0.

—End—

Appendix A

NAT router requirements for NAT Traversal feature

Contents

This section contains the following topics:

- ["Description" \(page 487\)](#)
- ["Requirements" \(page 488\)](#)
- ["Natcheck output" \(page 490\)](#)

Description

This appendix describes the requirements of a Network Address Translation (NAT) router to enable it to support the NAT Traversal feature.

For a NAT device to work correctly between an IP Phone and the CS 1000 system, the following requirements must be met:

1. A cone NAT must be used.
2. The Private-to-Public mapping should have a long time-out configured.
3. If multiple IP Phones are supported behind the same NAT router, hairpinning must be supported.
4. The Private-to-Public mapping created by a NAT router must be kept alive by packets in only one direction (standard in most NAT routers).
5. The IP Phone must be running the correct minimum firmware version (not a NAT device requirement, but still important).

Most of the issues encountered can be confirmed using either an IP Phone behind the NAT device or a PC running the third-party tool "natcheck".

ATTENTION

Nortel is not affiliated in any manner with the natcheck tool, and therefore is not liable or responsible for any problems that may be encountered with this tool.

The natcheck tool can be downloaded at no cost from the Internet at: <http://midcom-p2p.sourceforge.net/>. The natcheck tool runs in Windows on a PC connected to the internet through a NAT router.

Requirements

Cone NAT

The NAT Traversal feature cannot work unless the NAT device has a cone NAT implemented.

Confirm using natcheck

Run the natcheck program. Look for the following message:

```
UDP consistent translation:  YES (GOOD for peer-to-peer)
```

If YES is displayed, then the NAT router uses a cone NAT.

Confirm using IP Phone

The NAT router uses a cone NAT if no error message is displayed when the IP Phone registers to the system. The NAT device does not use a cone NAT if the IP Phone behind it displays the following error message:

```
NAT Error!  ITG3053
Please try upgrading firmware on the NAT device or
replacing it with a different NAT device that has a cone NAT
implemented.
```

Time-out configuration

Confirm using natcheck

Time-out configuration cannot be performed using natcheck.

Confirm using IP Phone

If the IP Phone connection times out and the IP Phone reboots, use LD 117 to lower the NAT Keep Alive Timer value on the Call Server. The reboots could indicate that the NAT device address/port mapping is being cleared because there is no message traffic from the IP Phone. By lowering the NAT Keep Alive Timer value in the Call Server, keep-alive messages are sent more frequently to keep the mapping "alive".

```
>ld 117
->chg nkt 20
```

If lowering the NAT Keep Alive Timer value to the minimum value of 20 seconds does not stop the time-outs, try replacing the NAT device.

Hairpinning

Hairpinning occurs when an IP Phone behind a NAT router can send packets to the Public IP address and Port of another IP Phone connected to the same NAT router. Determine if hairpinning is supported on the NAT router.

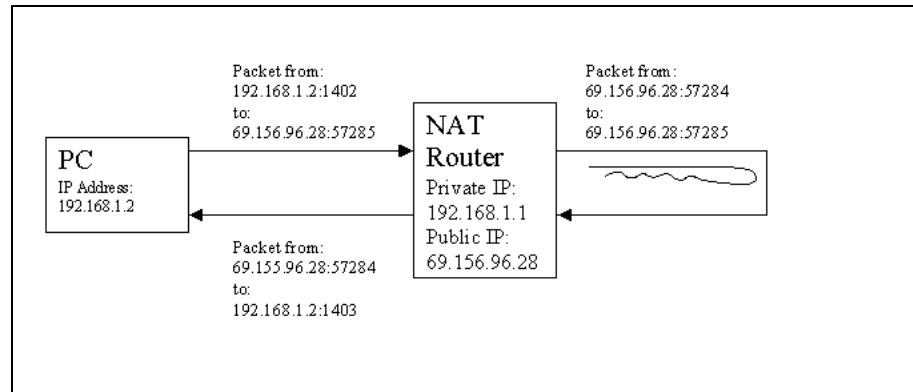
Confirm using natcheck

Run the natcheck program. Look for the message:

UDP loopback translation: YES (GOOD for peer-to-peer)

If this messages prints, then a two-way speech path should be available between two IP Phones behind the NAT device. See [Figure 104 "Speech path"](#) (page 489).

Figure 104
Speech path



Confirm using IP Phone

Connect two IP Phones to the same NAT device and call from one phone to the other. Confirm that a two-way speech path is achieved during the call.

Unidirectional packet flow

Confirm using natcheck

The natcheck tool cannot be used to determine if the private-to-public mapping created by the NAT device is being kept alive by a unidirectional packet flow.

Confirm using IP Phone

If an IP Phone behind a NAT device has a two-way speech path immediately after being registered, and continues to have a two-way speech path 2 to 30 minutes later, then the NAT device address/port mapping is being kept alive by the packets. If a one-way speech path occurs after this time period, ensure that the IP Phone has the latest firmware version. If the IP Phone has the latest firmware, then the problem lies with the NAT device. Try replacing the NAT device with a different model.

If the one-way speech path problem is fixed after rebooting the IP Phone, it is likely that the NAT device does not meet the requirement of unidirectional packet flow. As well, ensure that the firmware on the IP Phone has the latest firmware version (older firmware versions can be a possible source of the one-way speech path problem).

Firmware versions

The IP Phone must have the correct minimum firmware version loaded.

Confirm using natcheck

The natcheck tool cannot be used to determine the IP Phone firmware version.

Confirm using IP Phone

On the IP Phone, go to the **Services > Telephone Options > Set Info** menu and scroll down to the **FW Version** menu item. The minimum firmware versions (based on the vintage of the IP Phone) that support the NAT Traversal feature are:

- IP Phone 2002 and IP Phone 2004: xxxxB64
- Phase II IP Phone 2002 and IP Phone 2004: xxxxD41
- IP Softphone 2050: xxxx375

Earlier firmware versions do not correctly support the NAT Traversal feature.

Natcheck output

A NAT router using CONE NAT will have output similar to the following.

```
D:\natcheck>natcheck -v
server 1: pdos.lcs.mit.edu at 18.26.4.9:9856
server 2: tears.lcs.mit.edu at 18.26.4.77:9856
server 3: sure.lcs.mit.edu at 18.26.4.29:9856
Local TCP port: 1400
Local UDP port: 1401
Request 1 of 20...
Connection to server 2 complete
Server 1 reports my UDP address as 69.156.96.28:57283
Server 2 reports my UDP address as 69.156.96.28:57283
Server 3 reports my UDP address as 69.156.96.28:57283
Connection to server 1 complete
Server 1 reports my TCP address as 69.156.96.28:57281
Connection from 18.26.4.29:9856
Server 3 reports my TCP address as 69.156.96.28:57281
Request 2 of 20...
Loopback packet from 69.156.96.28 port 57285
Request 3 of 20...
Loopback packet from 69.156.96.28 port 57285
Request 4 of 20...
Loopback packet from 69.156.96.28 port 57285
Request 5 of 20...
Loopback packet from 69.156.96.28 port 57285
Server 2 reports my TCP address as 69.156.96.28:57281
Initiated TCP server 3 connection
Initiated TCP loopback connection
Connection from 69.156.96.28:57289
```

```
Loopback received
Request 6 of 20...
Loopback packet from 69.156.96.28 port 57285
Request 7 of 20...
Loopback packet from 69.156.96.28 port 57285
Request 8 of 20...
Loopback packet from 69.156.96.28 port 57285
Request 9 of 20...
Loopback packet from 69.156.96.28 port 57285
Request 10 of 20...
Loopback packet from 69.156.96.28 port 57285
Request 11 of 20...
Loopback packet from 69.156.96.28 port 57285
Request 12 of 20...
Loopback packet from 69.156.96.28 port 57285
Request 13 of 20...
Loopback packet from 69.156.96.28 port 57285
Request 14 of 20...
Loopback packet from 69.156.96.28 port 57285
Request 15 of 20...
Loopback packet from 69.156.96.28 port 57285
Request 16 of 20...
Loopback packet from 69.156.96.28 port 57285
Request 17 of 20...
Loopback packet from 69.156.96.28 port 57285
Request 18 of 20...
Loopback packet from 69.156.96.28 port 57285
Request 19 of 20...
Loopback packet from 69.156.96.28 port 57285
Request 20 of 20...
Loopback packet from 69.156.96.28 port 57285
TCP RESULTS:
  TCP consistent translation:      YES (GOOD for peer-to-peer)
  TCP simultaneous open:          YES (GOOD for peer-to-peer)
  TCP loopback translation:       YES (GOOD for peer-to-peer)
  TCP unsolicited connections filtered: NO (BAD for security)

UDP RESULTS:
  UDP consistent translation:      YES (GOOD for peer-to-peer)
  UDP loopback translation:       YES (GOOD for peer-to-peer)
  UDP unsolicited messages filtered: NO (BAD for security)
```

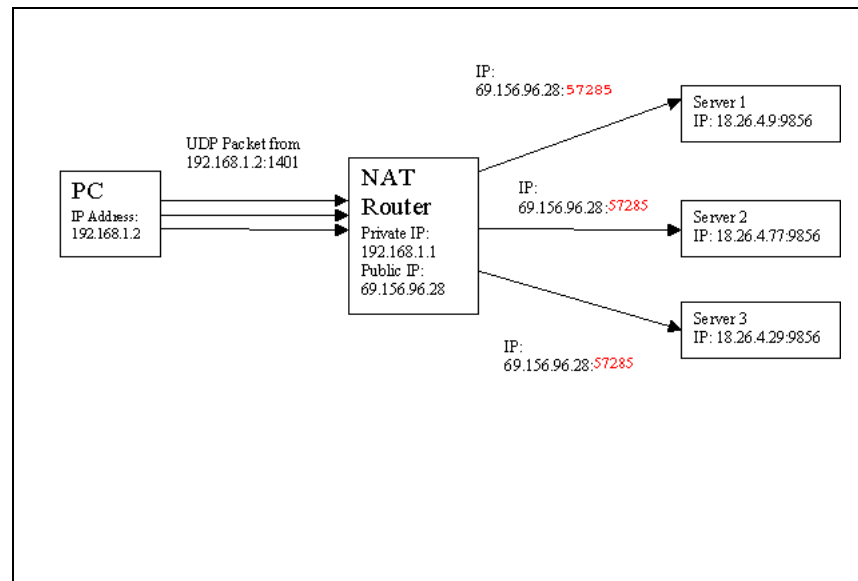
In order for the NAT router to support the NAT Traversal feature, natcheck must print the following to the screen:

```
UDP consistent translation:      YES (GOOD for peer-to-peer)
```

YES indicates that Cone NAT is being used. NO indicates that Symmetric NAT is present. Symmetric NAT is not supported.

Near the beginning of the printout, the PUBLIC port seen by various servers is printed out. In this case, all three servers receive the packets from the same PUBLIC port of 57283. This Private-to-Public port mapping is seen in Figure 105 "Private-to-Public port mapping" (page 492).

Figure 105
Private-to-Public port mapping



Because all three servers see the same PUBLIC port, the NAT router is using Cone NAT.

Appendix B

I/O, maintenance, and extender cable description

Contents

This section contains the following topics:

- ["Introduction" \(page 493\)](#)
- ["NTMF94EA I/O cable" \(page 493\)](#)
- ["Connector pin assignments" \(page 494\)](#)
- ["NTAG81CA maintenance cable description" \(page 497\)](#)
- ["NTAG81BA maintenance extender cable" \(page 498\)](#)
- ["Replace the NT8D81BA cable with the NT8D1AA cable and install the NTCW84JW special IPE filter" \(page 499\)](#)

Introduction

This appendix describes the NTMF94EA, NTAG81CA, and NTAG81BA cables and explains how to replace the NT8D81BA backplane ribbon cable and install the NTCW84JA filter, if required.

NTMF94EA I/O cable

The NTMF94EA cable provides the ELAN and TLAN network interfaces from the Voice Gateway Media Card to the customer network equipment. This cable also has one DB9 serial port that provides serial connection between the card and the customer PC or TTY. See [Figure 106 "NTMF94EA ELAN, TLAN and RS-232 serial maintenance I/O cable" \(page 494\)](#).

It is important to use the mounting screw provided to secure the top of the NTMF94EA cable 25-pair Amphenol connector to the system. The screw ties the LAN cable shield to the CS 1000 frame ground for EMC compliance.

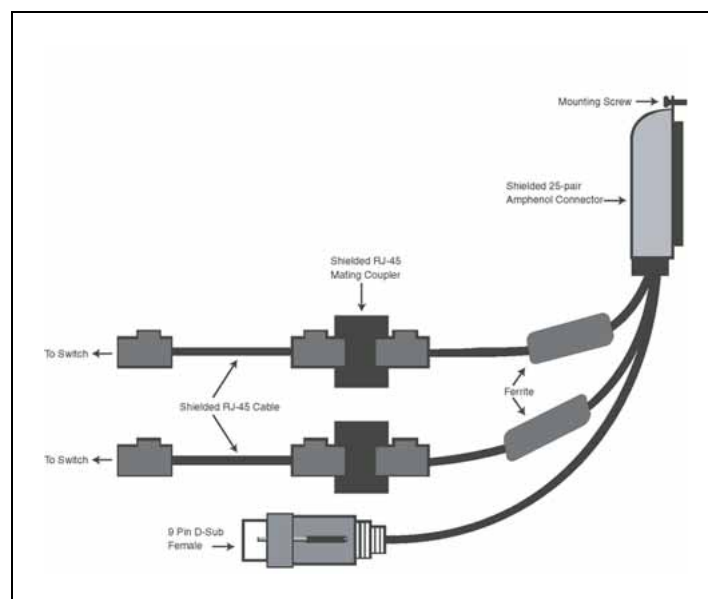
The NTMF94EA cable provides a factory-installed, shielded, RJ-45-to-RJ-45 coupler at the end of both the ELAN and the TLAN network interfaces. An unshielded coupler is provided to prevent ground loops (if required). See ["Prevent ground loops on connection to external customer LAN equipment" \(page 496\)](#), to determine if the unshielded coupler should be used. Both ends of the RJ-45 ports of the cables are labeled to distinguish the TLAN network interface and the ELAN network interface. The ports provide the connection point to the customer ELAN and TLAN equipment. Use shielded CAT5 cable to connect to the customer equipment.

To improve EMC performance, use standard cable ties to bundle all LAN cables as they route out of the system.

ATTENTION

To avoid damage to CAT5 cable, do not overtighten cable ties.

Figure 106
NTMF94EA ELAN, TLAN and RS-232 serial maintenance I/O cable



Connector pin assignments

[Table 112 "Voice Gateway Media Card I/O Panel Pinout" \(page 494\)](#) shows the I/O connector pin designations for the Voice Gateway Media Card.

Table 112
Voice Gateway Media Card I/O Panel Pinout

Pin	Normal Assignment	ITG Assignment	Pin	Normal Assignment	ITG Assignment
2	R1	Not Used	26	T0	Not Used

Pin	Normal Assignment	ITG Assignment	Pin	Normal Assignment	ITG Assignment
3	R2	Not Used	27	T1	Not Used
4	R3	Not Used	28	T2	Not Used
5	R4	Not Used	29	T3	Not Used
6	R5	AGND	30	T4	AGND
7	R6	Not Used	31	T5	Not Used
8	R7	Not Used	32	T6	Not Used
9	R8	Not Used	33	T7	Not Used
10	R9	AGND	34	T8	AGND
11	R10	PGT0	35	T9	PGT1
12	R11	PGT2	36	T10	PGT3
13	R12	PGT4	37	T11	PGT5
14	R13	PGT6	38	T12	PGT7
15	R14	PGT8	39	T13	PGT9
16	R15	PGT10	40	T14	PGT11
17	R16	SGNDA	41	T15	BDCDA-
18	R17	BSINA-	42	T16	BSOUTA-
19	R18	BDTRA-	43	T17	SGND
20	R19	BDSRA-	44	T18	BRTSA-
21	R20	BCTSA-	45	T19	BSINB-
22	R21	BSOUTB-	46	T20	BDCDB-
23	R22	BDTRB-	47	T21	BDSRB-
24	R23	DI+	48	T22	DI-
25	no connect	DO+	49	T23	DO-
2	R1	no connect	50	no connect	no connect

Table 113
NTMF94EA cable pin description

I/O Panel: P1	Signal Name	P2, P3,P4	Color
P1-21	BSOUTB-	P2-2	RED
P1-22	BDTRB-	P2-4	GREEN
	SGRND	P2-5	BROWN
P1-45	BSINB-	P2-3	BLUE
P1-46	BDCDB-	P2-1	ORANGE
P1-47	BDSRB-	P2-6	YELLOW

I/O Panel: P1	Signal Name	P2, P3,P4	Color
P1-25	SHLD GRND		
P1-50	SHLD GRND		
P1-18	RXDB+	P4-3	GREEN/WHITE
P1-19	TXDB+	P4-1	ORANGE/WHITE
P1-43	RXDB-	P4-6	WHITE/GREEN
P1-44	TXDB-	P4-2	WHITE/ORANGE
P1-23	RX+	P3-3	GREEN/WHITE
P1-24	TX+	P3-1	ORANGE/WHITE
P1-48	RX-	P3-6	WHITE/GREEN
P1-49	TX-	P3-2	WHITE/ORANGE
P1-25	SHLD GRND		BARE
P1-50	SHLD GRND		BARE

Prevent ground loops on connection to external customer LAN equipment

The shielded RJ-45 coupler is the connection point for the customer shielded CAT5 LAN cable to the hub, switch, or router supporting the TLAN and ELAN subnets. Use shielded CAT5 RJ-45 cable to connect to the customer TLAN/ELAN equipment. Follow the steps in [Procedure 79 "Preventing ground loops" \(page 496\)](#) to prevent ground loops when connecting to external customer LAN equipment.

Follow the steps in [Procedure 79 "Preventing ground loops" \(page 496\)](#) to prevent ground loops.

Procedure 79

Preventing ground loops

Step	Action
1	Connect the customer-provided shielded CAT5 LAN cable to the external LAN equipment. Ensure that the external LAN equipment is powered-up.
2	Use an ohmmeter to measure resistance to ground between the free end of the shielded RJ-45 cable and the building ground. The ohmmeter must measure Open to ground before plugging it into the shielded RJ-45 coupler on the end of the NTMF94EA.

If the ohmmeter does not measure Open, install the unshielded RJ-45 coupler (provided) on the end of the NTMF94EA to prevent ground loops to external LAN equipment.



WARNING

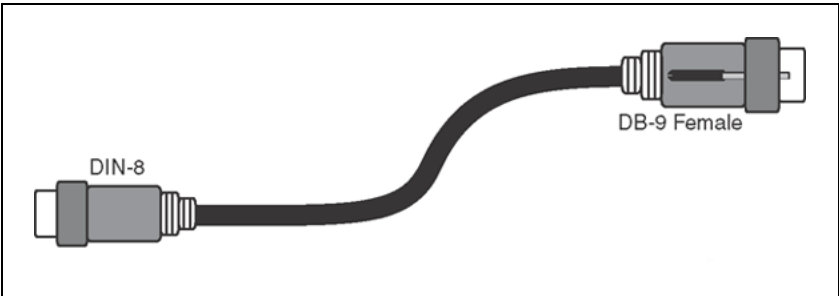
The serial maintenance ports on the faceplate connector and the DB-9 female connector of the NTMF9DA cable assembly are identical. Do not connect a serial device to both access points simultaneously. This results in incorrect and unpredictable operation of the Voice Gateway Media Card.

—End—

NTAG81CA maintenance cable description

The NTAG81CA maintenance cable is connected between the nine-pin D-type RS-232 input on a standard PC and the MAINT connector on the NT8R17AB faceplate or through the I/O cable serial port. See [Figure 107 "NTAG81CA Maintenance cable" \(page 497\)](#).

Figure 107
NTAG81CA Maintenance cable



The NTAG91CA maintenance cable pin description is outlined in [Table 114 "NTAG81CA maintenance cable pin description" \(page 497\)](#).

Table 114
NTAG81CA maintenance cable pin description

Signals (MIX Side)	eight-pin Mini-DIN (MIX Side)	nine-pin D-Sub (PC Side)	Signals (PC Side)

	Male	Female	
DTRB-	1	6	DSR-
SOUTB-	2	2	SIN-
SINB-	3	3	SOUT-
GND	4	5	GND
SINA-	5	nc	nc
CTSA-	6	nc	nc
SOUTA-	7	nc	nc
DTRA-	8	nc	nc

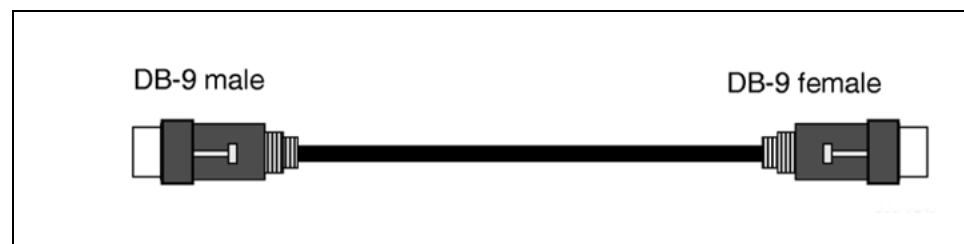
NTAG81BA maintenance extender cable

The NTAG81BA maintenance extender (3 m) cable connects the NTAG81CA cable to a PC or terminal. It has a nine-pin D-type connector at both ends; one male and one female. See [Table 115 "NTAG81BA Maintenance cable pin description" \(page 498\)](#). The cable can also be used to extend the serial port presented by the NTMF94EA I/O panel cable. The extender cable is shown in [Figure 108 "NTAG81BA Maintenance Extender cable" \(page 498\)](#).

Table 115
NTAG81BA Maintenance cable pin description

nine-pin D-Sub (Male)	nine-pin D-Sub (Female)
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9

Figure 108
NTAG81BA Maintenance Extender cable



Replace the NT8D81BA cable with the NT8D1AA cable and install the NTCW84JW special IPE filter

This procedure explains how to replace the NT8D81BA cable with the NT8D81AA cable and how to install the NTCW84JA special IPE filter in the IPE module.

Cables are designated by the letter of the I/O panel cutout, such as A, B, and C, where the 50-pin cable connector is attached. Each cable has three 20-pin connectors (16 positions are used), designated 1, 2, and 3, that attach to the backplane. Using the designations described, the backplane ends of the first cable are referred to as A-1, A-2, and A-3. The locations of the cable connectors on the backplane are designated by the slot number (L0 through L9 for NT8D11, L0 through L15 for NT8D37) and the shroud row (1, 2, and 3). Using these designations, the slot positions in the first slot are referred to as L0-1, L0-2, and L0-3.

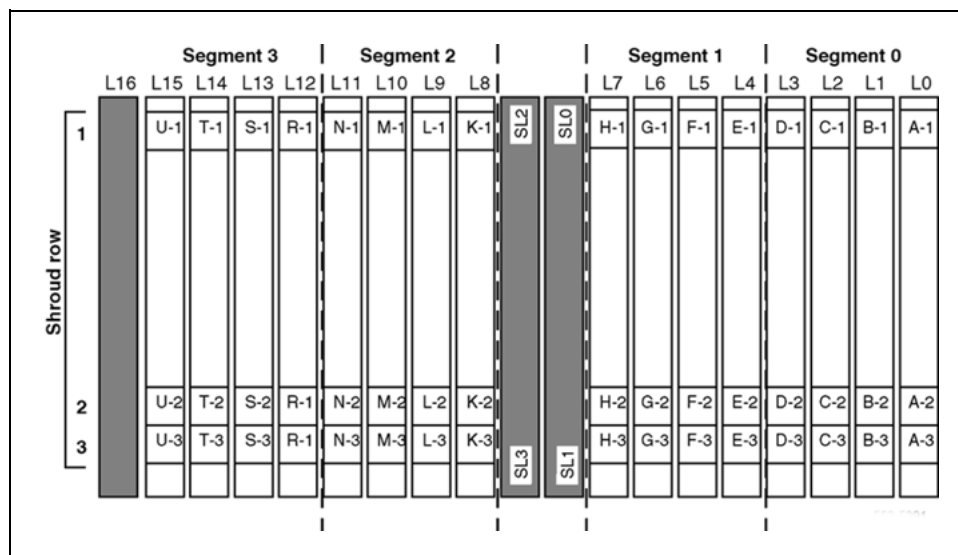
In NT8D37BA and NT8D37EC (and later vintage) IPE Modules, all 16 IPE card slots support 24-pair cable connections. [Table 116 "NT8D37 cable connections" \(page 499\)](#) shows the cable connections from the backplane to the inside of the I/O panel.

Table 116
NT8D37 cable connections

Backplane slots – shroud rows	I/O panel/cable designation
L0–1, 2, 3	A
L1–1, 2, 3	B
L2–1, 2, 3	C
L3–1, 2, 3	D
L4–1, 2, 3	E
L5–1, 2, 3	F
L6–1, 2, 3	G
L7–1, 2, 3	H
L8–1, 2, 3	K
L9–1, 2, 3	L
L10–1, 2, 3	M
L11–1, 2, 3	N
L12–1, 2, 3	R
L13–1, 2, 3	S
L14–1, 2, 3	T
L15–1, 2, 3	U

[Figure 109 "Backplane slot designations" \(page 500\)](#) shows the designations for the backplane end of the cables, the backplane slot designations for the cable connections, and the associated network segments for the backplane slots.

Figure 109
Backplane slot designations



Tools list

The following tools are required to perform this procedure.

- Ty-wrap cutter
- Ty-wraps
- Needle nose pliers
- Slotted screwdriver

Remove the NT8D81BA cable

Follow the steps in [Procedure 80 "Removing an NT8D81BA cable"](#) (page 500) to remove the NT8D81BA cable.

Procedure 80

Removing an NT8D81BA cable

Step	Action
1	Identify the I/O panel and backplane designation that corresponds to the LEFT slot of the pair of card slots, viewed from the front, in which the ITG ISL Trunk card is installed.
2	Disconnect the filter from the I/O panel using a screwdriver and needle nose pliers. Retain the fasteners.
3	Power down the IPE shelf.
4	Remove the IPE module I/O safety panel.

- 5 To remove the ribbon cables from the IPE backplane, apply gentle pressure on the tab on the right side of the shroud while pulling on the connector until it pulls free from the shroud.
- 6 Remove connector 1 first, then remove connectors 2 and 3.
- 7 Discard the NT8D81BA cable.

—End—

Install the NTCW84JA filter and NT8D81AA cable

Follow the steps in [Procedure 81 "Installing an NTCW84JA filter and NT8D81AA cable"](#) (page 501) to install the NTCW84JA filter and NT8D81AA cable.

Procedure 81

Installing an NTCW84JA filter and NT8D81AA cable

Step	Action
1	Install the NTCW84JA special IPE filter connector in the vacant I/O panel slot using retained hardware.
2	Install the NT8D81AA ribbon cable connectors in the IPE module backplane shroud. Be sure to install the connector so the label is facing right with the arrow pointing up and the connector is fully engaged into the shroud: a. Install connector 1, (labeled UP1^) into backplane shroud 1. b. Install connector 2, (labeled UP2^) into backplane shroud 2. c. Install connector 3, (labeled UP3^) into backplane shroud 3.
3	Dress the ribbon cables back individually inside the rear of IPE module and restore the original arrangement. Start with the cables that are going to be underneath.
4	Attach the NTCW84JA special IPE filter to the NT8D81AA 50-pin connector using bail clips.
5	Restore power to the IPE module.
6	Replace the I/O safety panel.

—End—

Appendix C

Product integrity

Contents

This section contains the following topics:

- ["Introduction" \(page 503\)](#)
- ["Reliability" \(page 503\)](#)
- ["Environmental specifications" \(page 504\)](#)

Introduction

This chapter presents information about the Voice Gateway Media Card reliability, environmental specifications, and electrical regulatory standards.

Reliability

Reliability is measured by the Mean Time Between Failures (MTBF).

Mean Time Between Failures (MTBF)

The Mean Time Between Failure (MTBF) is 46 years for Voice Gateway Media Cards. Failures per 106 hours of operation are 2.483, based on 40 degrees C (140 degrees F).

Voice Gateway Media Card power consumption

The worst case current drawn by the Voice Gateway Media Cards from each Backplane voltage supply is provided in [Table 117 "Voice Gateway Media Card power consumption" \(page 503\)](#):

Table 117

Voice Gateway Media Card power consumption

Card Type	Power Consumption
ITG-Pentium 24-port card	± 15 volt = 19.3 watts => 0.640 amps

Card Type	Power Consumption
	+5 volt = 10.5 watts => 2.1 amps
Media Card	+ 15 volt = 6 watts => 0.2 amps
	+5 volt = 7.25 watts => 1.45amps

Environmental specifications

Table 118 "Environmental specifications (maximum)" (page 504) shows the environmental specifications of the Voice Gateway Media Card. The Voice Gateway Media Card provides external interface protection to –52 V DC, but does not provide lightning or hazardous voltage protection.

Table 118
Environmental specifications (maximum)

Parameter	Specifications
Operating temperature	0° to +45° C (+32 to +113° F), ambient
Operating humidity	5 to 95% RH (non-condensing)
Storage temperature	–20° to +60° C (–4° to +140° F)

Measurements of performance in regards to temperature and shock were made under test conditions. Table 119 "Environmental specifications (recommended)" (page 504) shows recommended temperature and humidity ranges for the Voice Gateway Media Card based on results from this test.

Table 119
Environmental specifications (recommended)

Specification	Minimum	Maximum
Normal Operation		
Recommended	15° C	30° C
Relative humidity	20%	55% (non-condensing)
Absolute	10° C	45° C
Relative humidity	20%	80% (non-condensing)
Short Term (less than 72 hr)	−40° C	70° C
Rate of change	Less than 1° C for every 3 minutes	
Storage		
Recommended	−20° C	60° C

Specification	Minimum	Maximum
Relative humidity	5%	95% (non-condensing)
	−40° C to 70° C, non-condensing	
Temperature Shock		
In 3 minutes	−40° C	25° C
In 3 minutes	70° C	25° C
	−40° to 70° C, non-condensing	

Appendix D

Subnet Mask Conversion from CIDR to Dotted Decimal Format

Introduction

Subnet masks are expressed in Classless InterDomain Routing (CIDR) format, appended to the IP address, such as 10.1.1.1/20. The subnet mask must be converted from CIDR format to dotted decimal format in order to configure IP addresses.

The CIDR format expresses the subnet mask as the number of bits counting from the most significant bit of the first IP address field. A complete IP address consists of 32 bits. Therefore, a typical CIDR format subnet mask is in the range from /9 to /30. Each decimal number field in the dotted decimal format has a value from 0 to 255, where decimal 255 represents binary 1111 1111.

Follow the steps in [Procedure 82 "Converting a subnet mask from CIDR format to dotted decimal format" \(page 507\)](#) to convert a subnet mask from CIDR format to dotted decimal format.

Procedure 82

Converting a subnet mask from CIDR format to dotted decimal format

Step	Action
1	Divide the CIDR format value by 8. The quotient (the number of times that eight divides into the CIDR format value) equals the number of dotted decimal fields containing 255. In the example above, the subnet mask is expressed as /20. Twenty divided by eight equals a quotient of two, with a remainder of four. Therefore, the first two fields of the subnet mask in dotted decimal format are 255.255.
2	If there is a remainder, see Table 120 "CIDR format remainders" (page 508) to obtain the dotted decimal value for the field following the last field containing "255". In the example of /20 above, the remainder is four. In Table 120 "CIDR format remainders" (page

508), a remainder of four equals a binary value of 1111 0000 and the dotted decimal value of the next and last field is 240. Therefore the first three fields of the subnet mask are 255.255.240.

- 3 If there are any remaining fields in the dotted decimal format, they have a value of 0. Therefore, the complete subnet mask in dotted decimal format is 255.255.240.0.

—End—

Table 120
CIDR format remainders

Remainder of CIDR format value divided by eight	Binary value	Dotted decimal value
1	1000 0000	128
2	1100 0000	192
3	1110 0000	224
4	1111 0000	240
5	1111 1000	248
6	1111 1100	252
7	1111 1110	254

Appendix E

Download IP Line files from Nortel Web site

Contents

This section contains the following topics:

- "Introduction" (page 509)
- "Download files from Nortel web site" (page 509)

Introduction

This appendix provides instruction for downloading files from the Nortel Web site.

Download files from Nortel Web site

Follow the steps in [Procedure 83 "Downloading files from the Nortel web site" \(page 509\)](#) to download IP Line-related software and firmware files from the Nortel Web site.

Procedure 83

Downloading files from the Nortel Web site

Step	Action
1	Connect to www.nortel.com using any PC with Internet access.
2	Click Software Downloads under Support & Training . The Software Downloads window appears and displays the list Product Family .
3	Select CS 1000 . If Meridian was selected, click IP Line and Internet Telephony Gateway (ITG) Line product, and select Software.

This product list includes the following:

- IP Line for Media Cards (this *.zip file contains the IP Line loadware for the Media Cards, the IP Phone firmware, and a readme.txt file)
- IP Line for ITG-P cards (this *.zip file contains the IP Line loadware for the ITG-P cards, the IP Phone firmware, and a readme.txt file)
- Media Card firmware
- ITG-P 24-port line card firmware
- IP Line Readmefirst document

- b. If **CS 1000** was selected, click **CS 1000E** or **CS 1000M**, and select **Software**.

This product list includes the following:

- Signaling Server SSE-5.00.xx CD-ROM Image (this image contains the IP Line loadware for the Media Cards and the ITG-P 24-port card, the IP Phone firmware, and other key components)
- Media Cards firmware
- ITG-P 24-port line card firmware

- 4 Click the file to be downloaded.
- 5 If not already logged into the My Nortel account, enter the User ID and Password on the **Sign In** window and then click **Sign In**.
- 6 If not registered to access this Web site, see the CS 1000 product bulletin for directions on how to register.
- 7 After you are logged on, ignore the security alert.
- 8 The **Software Downloads: Software Details Information** window appears. Click the link next to **File Download**.
- 9 In the **Save As** window, choose the desired path to save the file to local disk on the PC and click **Save**.

—End—

Appendix F

Moving Voice Gateway Media Cards between systems

Contents

This section contains the following topics:

- ["Introduction" \(page 511\)](#)
- ["Reconfiguring the Voice Gateway Media Card" \(page 511\)](#)

Introduction

You can move a Voice Gateway Media Card to a different system, but you may have to restore the default values of the logon account before the card functions properly. When the card is reconfigured, security information, accounts, and passwords are synchronized with the new Call Server.

Always attempt to install and upgrade the Voice Gateway Media Card using Element Manager first. Use the standard installation and upgrade procedures in Element Manager to configure the Voice Gateway Media Card ELAN MAC address, IP address settings, IP Telephony service settings, and Call Server Voice Gateway TNs. When the information is added, ensure the addition of the new card successfully transferred to the Leader, which is the current node master and BootP Server.

For information about installing and upgrading Voice Gateway Media Cards using Element Manager, see ["Configuration of IP Telephony nodes using Element Manager" \(page 259\)](#). Verify that the ELAN MAC address of the Voice Gateway Media Card is removed through Element Manager from the IP Telephony nodes of any other systems in which the Voice Gateway Media Card was previously installed and operational.

Reconfiguring the Voice Gateway Media Card

This section explains how to reconfigure the Voice Gateway Media Card in the following situations:

- The node already has the Leader configured.

A Leader is already configured in the destination node.

- The node has no Leader configured.

A Leader is not configured in the destination node.

Node has Leader configured

After you install the Voice Gateway Media Card, you should encounter one of the three scenarios described in this section. Reconfigure the card by following the directions for the applicable scenario.

If you encounter a scenario other than the three described in this section, contact your Nortel representative.

Scenario 1

This scenario applies if the Voice Gateway Media Card:

- came from a system running CS 1000 Release 4.5 or later
- was a Follower in that system
- is moving to a CS 1000 Release 4.5 system or later

If the startup message that appears is similar to that shown in [Figure 110 "Message output for the Voice Gateway Media Card when the BootP response is received and accounts are synchronized \(Follower\)"](#) (page 513), use [Procedure 84 "Reconfiguring a Voice Gateway Media Card running CS 1000 Release 4.5 or later \(Follower on original system\)"](#) (page 514) to reconfigure the Voice Gateway Media Card.

If you see a startup message different than what is shown in [Figure 110 "Message output for the Voice Gateway Media Card when the BootP response is received and accounts are synchronized \(Follower\)"](#) (page 513) check your network connections, and make sure the configurations for the ELAN MAC address are entered correctly in Element Manager. Then use [Procedure 85 "Reconfiguring a Voice Gateway Media Card running CS 1000 Release 4.5 or later \(Leader in original system\)"](#) (page 515) to reconfigure the Voice Gateway Media Card.

ATTENTION

If the BootP Server IP address is not the BootP Server IP address of the new system, the response may be from the original BootP Server. Review the message to make sure the IP address from which the card received the BootP response is the Leader, or the current node master and BootP Server of the new system. Verify the MAC address, and network connectivity.

Figure 110

Message output for the Voice Gateway Media Card when the BootP response is received and accounts are synchronized (Follower)

```
...Getting IP over BootP via network interface ixpMac1
Enter +++ to escape to Shell for manual configuration

      ixpMac0 IP:          192.168.29.135
      ifAuxSubnetMask:     0xffffffff00
      Secondary Gateway:   192.168.29.1
      Bootp Server:       192.168.25.142
      Default Gateway:    192.168.25.1
      ixpMac1 IP:         192.168.25.135
      Subnet mask:        255.255.255.0

netmask = 0xffffffff00
...
OCT 12 09:46:16 SYS: Info Got bootp response from 192.168.25.142
...
OCT 12 09:46:18 SYS: Info pbxLibInit
OCT 12 09:46:18 SYS: Info pbxLinkStart
...
OCT 12 09:46:21 MAM: Info Account updated.
OCT 12 09:46:21 MAM: Info Account updated.
```

Scenario 2

This scenario applies if the Voice Gateway Media Card:

- came from a system running CS 1000 Release 4.5 or later
- was a Leader in the original system, and is therefore getting its IP configuration from its local NVRAM
- is moving to a CS 1000 Release 4.5 system or later

You see a startup message similar to that shown in [Figure 111 "Message output for the Voice Gateway Media Card \(Leader\)"](#) (page 513). Use [Procedure 85 "Reconfiguring a Voice Gateway Media Card running CS 1000 Release 4.5 or later \(Leader in original system\)"](#) (page 515) to reconfigure the Voice Gateway Media Card.

Figure 111

Message output for the Voice Gateway Media Card (Leader)

```
ipMethodInit, gIPMethod = 2
IP Data in NVRAM is Valid, Boot Line updated
      IP Address:192.168.25.135
      Gateway Address:192.168.25.1
      Subnet Mask::ffffff00

...
OCT 12 09:46:18 SYS: Info pbxLibInit
OCT 12 09:46:18 SYS: Info pbxLinkStart
...
OCT 12 09:46:21 MAM: Info Account updated.
OCT 12 09:46:21 MAM: Info Account updated.
```

Scenario 3

This scenario applies if the Voice Gateway Media Card:

- came from a system running CS 1000 Release 4.0 or earlier
- was a Leader or a Follower in the original system
- is moving to a CS 1000 Release 4.5 system or later

Use [Procedure 86 "Reconfiguring a Voice Gateway Media Card running CS 1000 Release 4.0 or earlier \(Leader or Follower\)" \(page 516\)](#) to reconfigure a Voice Gateway Media Card running CS 1000 Release 4.5 or later, where the card was configured as a Follower on the original system.

Procedure 84

Reconfiguring a Voice Gateway Media Card running CS 1000 Release 4.5 or later (Follower on original system)

Step	Action
1	Enter the user name and password that was synchronized from the Call Server.
2	Access the card by the EIA232 Maintenance port.
3	Upgrade the Voice Gateway Media Card 8051XA Controller firmware, if necessary.
4	Upgrade the Voice Gateway Media Card software, if necessary. To upgrade the Voice Gateway Media Card software using Element Manager, see "Upgrade the Voice Gateway Media Card software and IP Phone firmware" (page 293) .
5	Use Element Manager to select this Voice Gateway Media Card.
6	Click Transfer to Selected Elements to transfer config.ini and bootp.tab files to the card. See "Transmit node properties" (page 290) .

—End—

Use [Procedure 85 "Reconfiguring a Voice Gateway Media Card running CS 1000 Release 4.5 or later \(Leader in original system\)" \(page 515\)](#) to reconfigure a Voice Gateway Media Card running CS 1000 Release 4.5 on a system running CS 1000 Release 4.5 or later, where the card was configured as Leader in the original system.

Procedure 85**Reconfiguring a Voice Gateway Media Card running CS 1000 Release 4.5 or later (Leader in original system)**

Step	Action
1	Press the reset button on the Voice Gateway Media Card faceplate.
2	Access the card by the EIA232 Maintenance port.
3	At the prompt, to escape to BIOS VxWorks shell, enter <code>jk1</code>
4	At the prompt, enter <code>nvrnCleaR</code> The <code>nvrnCleaR</code> command clears the Leader flag and allows a BootP request to be sent.
5	Enter <code>sysReboot</code> After this command executes, the card has the correct IP and accounts information synchronized with the node. Try to access the IPL>CLI using the user name and password from your Call Server.
6	Upgrade the Voice Gateway Media Card 8051XA Controller firmware, if necessary.
7	Upgrade the Voice Gateway Media Card software, if necessary. To upgrade the Voice Gateway Media Card software using Element Manager, see Procedure 40 "Upgrading the card loadware" (page 299) .
8	In Element Manager, select this Voice Gateway Media Card.
9	Click Transfer to Selected Elements to transfer config.ini and bootp.tab files to the card. See "Transmit node properties" (page 290) .

—End—

Use [Procedure 86 "Reconfiguring a Voice Gateway Media Card running CS 1000 Release 4.0 or earlier \(Leader or Follower\)" \(page 516\)](#) to reconfigure a Voice Gateway Media Card running CS 1000 Release 4.0 or earlier on a system running CS 1000 Release 4.5 or later, where the card was configured as a Leader or a Follower in the original system.

Procedure 86**Reconfiguring a Voice Gateway Media Card running CS 1000 Release 4.0 or earlier (Leader or Follower)**

Step Action

- 1 Press the reset button on the Voice Gateway Media Card faceplate.
- 2 Access the card by the EIA232 Maintenance port.
- 3 At the prompt, to escape to BIOS VxWorks shell, enter
`jk1`
- 4 At the prompt, enter
`nvrnClea`
After this command executes, the card becomes a Follower; the Leader flag is cleared, and the IP parameters are reset to the default values of the logon account.
- 5 Reboot the card to trigger a new BootP request. At the prompt, enter
`sysReboot`
After this command executes, the card has the correct IP and accounts information synchronized with the default card. The following user name and password is available for CS 1000 Release 4.0 and earlier: **itgadmin, itgadmin**
- 6 Upgrade the Voice Gateway Media Card 8051XA Controller firmware, if necessary.
- 7 Upgrade the Voice Gateway Media Card software, if necessary.
To upgrade the Voice Gateway Media Card software, see "[Upgrading the software](#)" (page 523).

—End—

Node has no Leader configured

In this section, the Voice Gateway Media Card is configured as the Leader, because it is the first element added to this new node. Neither a Signaling Server nor a Voice Gateway Media Card is present on the node.

After you install the Voice Gateway Media Card, you should encounter one of the four scenarios described in this section. Reconfigure the card by following the directions for the applicable scenario.

Scenario 1

This scenario applies if the ITG-P 24-port card:

- came from a system running CS 1000 Release 4.5 or later
- was a Leader or a Follower in that system
- is moving to a system running CS 1000 Release 4.5 or later

Use [Procedure 87 "Reconfiguring the ITG-P 24-port card running CS 1000 Release 4.5 or later \(Leader or Follower\)" \(page 518\)](#) to reconfigure the ITG-P 24-port card.

Scenario 2

This scenario applies if the ITG-P 24-port card:

- came from a system running CS 1000 Release 4.0 or earlier
- was a Leader or a Follower in that system
- is moving to a system running CS 1000 Release 4.5 or later

Use [Procedure 88 "Reconfiguring an ITG-P 24-port card running CS 1000 Release 4.0 \(Leader or Follower\)" \(page 519\)](#) to reconfigure the ITG-P 24-port card.

Scenario 3

This scenario applies if the Media Card 32-port card:

- came from a system running CS 1000 Release 4.5 or later
- was a Leader or a Follower in that system
- is moving to a system running CS 1000 Release 4.5 or later

Use [Procedure 89 "Reconfiguring the Media Cards running CS 1000 Release 4.5 or later \(Leader or Follower\)" \(page 521\)](#) to reconfigure the Media Card 32-port card.

Scenario 4

This scenario applies if the Media Card 32-port card:

- came from a system running CS 1000 Release 4.0 or earlier
- was a Leader or a Follower in that system
- is moving to a system running CS 1000 Release 4.5 or later

Use [Procedure 90 "Reconfiguring the Media Cards running CS 1000 Release 4.0 or earlier \(Leader or Follower\)" \(page 522\)](#) to reconfigure the Media Card 32-port card.

Use [Procedure 87 "Reconfiguring the ITG-P 24-port card running CS 1000 Release 4.5 or later \(Leader or Follower\)" \(page 518\)](#) to reconfigure the ITG-P 24-port card running CS 1000 Release 4.5 or later on a system running CS 1000 Release 4.5 or later, where the card was a Leader or a Follower in the original system.

Procedure 87

Reconfiguring the ITG-P 24-port card running CS 1000 Release 4.5 or later (Leader or Follower)

Step	Action
1	Press the reset button on the ITG-P 24-port card faceplate.
2	Access the card by the RS-232 Maintenance port.
3	At the prompt, to escape to BIOS VxWorks, enter <code>jkl</code>
4	To change the ELAN IP address configuration, the IP Telephony application Leader flag, and the IPL> prompt logon parameters in NVRAM, enter <code>BIOS>nvrnClea</code> The card becomes a Follower; the Leader flag is cleared and the IP telephony parameters are reset to the default values.
5	To set the flag so the ELAN IP address configuration data is read from the NVRAM instead of a BootP query, enter <code>BIOS>lnIsaIPMethodSet 2</code>
6	At the prompt, enter

Command	Description
<code>BIOS>lnIsa_progIP</code>	ELAN IP Address
<code>BIOS>lnIsa_progSubnetMask</code>	ELAN subnet mask
<code>BIOS>lnIsa_ProgGW</code>	ELAN Gateway IP address

7	Every node must have a Leader. To set the Leader flag for the ITG-P 24 port card, enter <code>BIOS>nvrnLeaderSet</code>
8	At the prompt, enter <code>sysReboot</code>
9	Use Element Manager to select this Voice Gateway Media Card.

- 10 Click **Transfer to Selected Elements** to transfer the config.ini and bootp.tab files to the card.
See
The account information is synchronized with the Call Server.
- 11 Logon to the card using the current username and password.
- 12 At IPL> prompt, enter
`cardReset`
- 13 Use standard procedures to upgrade the Voice Gateway Media Card 8051XA Controller firmware and the software, if necessary.

—End—

Use [Procedure 88 "Reconfiguring an ITG-P 24-port card running CS 1000 Release 4.0 \(Leader or Follower\)" \(page 519\)](#) to reconfigure the ITG-P 24-port card running CS 1000 Release 4.0, or earlier on system running CS 1000 Release 4.5 or later, where the card was a Leader or a Follower in the original system.

Procedure 88

Reconfiguring an ITG-P 24-port card running CS 1000 Release 4.0 (Leader or Follower)

Step	Action
1	Press the reset button on the ITG-P 24-port card faceplate.
2	Access the card by the EIA232 Maintenance port.
3	At the prompt, to escape to BIOS VxWorks, enter <code>jkl</code>
4	To change the ELAN IP address configuration, the IP Telephony application Leader flag, and the IPL> logon parameters in NVRAM, enter <code>BIOS>nvrnClea</code> The card becomes a Follower; the Leader flag is cleared, and the IP telephony parameters are reset to the default values of the logon account.
5	To set the flag so the ELAN IP address configuration data is read from the NVRAM instead of a BootP query, enter <code>BIOS>lnIsaIPMethodSet 2</code>

6 At the prompt, enter

Command	Description
BIOS>lnIsa_progIP	ELAN IP Address
BIOS>lnIsa_progSubnetMask	ELAN subnet mask
BIOS>lnIsa_ProgGW	ELAN Gateway IP address

7 Every node must have a Leader. To set the Leader flag for the ITG-P 24 port card, enter

```
BIOS>nvrAmLeaderSet
```

You reformat the C drive. The C drive is formatted the next time the ITG-P 24-port card restarts (after the **sysReboot** command). Reformatting the C drive deletes all existing configuration files, syslog files, and OM report logs on the ITG-P 24 port card.

8 To reformat the C drive and to remove the configuraton files the next time the card restarts, enter

```
BIOS>reformatCdrive
```

```
BIOS>sysReboot
```

After the sysReboot command is executed, the Voice Gateway Media Card restarts and the following default user name and password is available for CS 1000 Release 4.0 and lower: **itgadmin, itgadmin**
itgadmin, itgadmin

9 Use standard procedures to upgrade Voice Gateway Media Card 8051XA Controller firmware and the software, if necessary.

To upgrade the software for the ITG-P 24-port card, see ["Upgrading the software" \(page 523\)](#).

10 Use Element Manager to select this Voice Gateway Media Card.

11 Click **Transfer to Selected Elements** to transfer the config.ini and bootp.tab files to the card.12 See ["Transmit node properties" \(page 290\)](#).

—End—

Use [Procedure 89 "Reconfiguring the Media Cards running CS 1000 Release 4.5 or later \(Leader or Follower\)" \(page 521\)](#) to reconfigure the Media Card 32-port card running CS 1000 Release 4.5 or later on a system running CS 1000 Release 4.5 or later, where the card was a Leader or a Follower in the original system.

Procedure 89**Reconfiguring the Media Cards running CS 1000 Release 4.5 or later (Leader or Follower)**

Step	Action
1	Press the reset button on the Media Card 32-port card faceplate.
2	Access the card by the EIA232 Maintenance port.
3	At the prompt, to escape to BIOS VxWorks, enter <code>jk1</code>
4	To change the ELAN IP address configuration, the IP Telephony application Leader flag, and the IPL> logon parameters in NVRAM, enter <code>->nvrAmClear</code> The card becomes a Follower; the Leader flag is cleared, and the IP telephony parameters are reset to the default values of the log in account.
5	To set the flag so the ELAN IP address configuration data is read from the NVRAM instead of a BootP query, enter <code>->lnIsaIPMethodSet 2</code>
6	At the prompt, enter

Command	Description
<code>->lnIsa_writeIP</code>	ELAN IP Address
<code>->lnIsa_writeSubnetMask</code>	ELAN subnet mask
<code>->lnIsa_writeGW</code>	ELAN Gateway IP address

- 7 Every node must have a Leader. To set the Leader flag for the Media Card, enter

`BIOS>nvrAmLeaderSet`
- 8 To reboot the Media Card, enter

`->sysReboot`
- 9 Use Element Manager to select this Voice Gateway Media Card.

For more information about adding Voice Gateway Media Cards using Element Manager, see ["Configuration of IP Telephony nodes using Element Manager" \(page 259\)](#).
- 10 Click **Transfer to Selected Elements** to transfer the config.ini and bootp.tab files to the card.

See ["Transmit node properties" \(page 290\)](#).

The account information is synchronized with the Call Server.

- 11 Logon to the card using the current user name and password.
- 12 At IPL> prompt, enter
`cardReset`
- 13 Use standard procedures to upgrade Voice Gateway Media Card 8051XA Controller firmware and the software, if necessary.

—End—

Use [Procedure 90 "Reconfiguring the Media Cards running CS 1000 Release 4.0 or earlier \(Leader or Follower\)" \(page 522\)](#) to reconfigure the Media Card 32-port card running CS 1000 Release 4.0 or earlier on a system running CS 1000 Release 4.5 or later, where the card was a Leader or a Follower in the original system.

Procedure 90

Reconfiguring the Media Cards running CS 1000 Release 4.0 or earlier (Leader or Follower)

Step	Action

1	Press the reset button on the Media Card 32-port card faceplate.
2	Access the card by the EIA232 Maintenance port.
3	At the prompt, to escape to BIOS VxWorks, enter <code>jk1</code>
4	To change the ELAN IP address configuration, the IP Telephony application Leader flag, and the IPL> logon parameters in NVRAM, enter <code>->nvrnClea</code> The card becomes a Follower; the Leader flag is cleared and the IP telephony parameters are reset to the default values of the logon account.
5	To set the flag so ELAN IP address configuration data is read from the NVRAM instead of a BootP query, enter <code>->lnIsaIPMethodSet 2</code>

6 At the prompt, enter

Command	Description
->lnIsa_writeIP	ELAN IP Address
->lnIsa_writeSubnetMask	ELAN subnet mask
->lnIsa_writeGW	ELAN Gateway IP address

7 Every node must have a Leader. To set the Leader flag for the Media Card 32-port card, enter

```
->nvrAmLeaderSet
```

8 At the prompt, to remove the configuration files and backups, enter

```
->cd C:/:/config
```

```
->rm config.ini
```

```
->rm config.bak
```

```
->rm bootp.tab
```

```
->rm bootp.bak
```

9 To restart the Media Card, enter

```
-> sysReboot
```

After the sysReboot command is executed, the Media Card restarts and the following default user name and password is available for CS 1000 Release 4.0 and lower: **itgadmin, itgadmin**

10 Use Element Manager to select this Voice Gateway Media Card.

For more information about adding Voice Gateway Media Cards using Element Manager, see ["Configuration of IP Telephony nodes using Element Manager" \(page 259\)](#).

11 Click **Transfer to Selected Elements** to transfer the config.ini and bootp.tab files to the card.

See ["Transmit node properties" \(page 290\)](#).

—End—

Upgrading the software

Use [Procedure 91 "Upgrading the software for the ITG-P 24-port card or the Media Card running CS 1000 Release 4.0 or earlier" \(page 524\)](#) to upgrade the software on the ITG-P 24-port card or the Media Card running Succession Release 3.0, or CS 1000 Release 4.0.

Procedure 91

Upgrading the software for the ITG-P 24-port card or the Media Card running CS 1000 Release 4.0 or earlier

Step	Action
1	Access the IPL> prompt using the following default user name and password for CS 1000 Release 4.0 and lower: itgadmin, itgadmin
2	If you have an ITG-P 24-port card, enter <pre>IPL>upgradeErase</pre> This command erases the application binaries from the ITG-P 24-port card Flash memory.
3	To initiate software download, enter <pre>IPL>swDownload</pre> where <pre>svrIP</pre> FTP server IP address <pre>uid, passwd</pre> used to log on to the server <pre>path, fname</pre> path and name of the file on the server to retrieve The swDownload command downloads the IPL application binary from the specified FTP server. The command is only applicable to Voice Gateway Media Cards. The command is executed from the IPL VXWorks, and BIOS CLIs. If the loadware resides locally on the card (for example, on a flash card in /A: drive), use the swCopy command instead. The syntax is : swCopy "/path/and/name/of/loadware/file"

ATTENTION

Drive letters must be uppercase and file names must be lowercase. All files must follow the 8.3 format.

ATTENTION

The uid and passwd fields are both default.

File is on the Voice Gateway Media Card /A: drive (previously transferred there by FTP):

```
IPL>swDownload
```

```
"127.0.0.1", "<uid>", "<passwd>", "</A:/path>",
"<fname>"
```

File is on the ITG-P card /C: drive (previously copied there or transferred there by FTP):

```
PL>swDownload
```

```
"127.0.0.1", "<uid>", "<passwd>", "</C:/path>",
"<fname>"
```


File is on the Signaling Server (loaded during install/upgrade):**IPL>swDownload**

```
"<SS ELAN IPaddr>", "<uid>", "<passwd>", "</u/fw>",
"<fname>"
```

File is on another Voice Gateway Media Card /C: drive (previously transferred there by FTP):**IPL>swDownload**

```
"<VGMC ELAN IPaddr>", "<uid>", "<passwd>",
"</C:/path>", "<fname>"
```

File is on the MAT/TM PC:**IPL > swDownload**

```
"<PC's IP addr>", "itguser", "itguser", ",",
"<fname>"
```

File is on a network FTP server:**IPL>swDownload**

```
"<server's IP addr>", "<uid>", "<passwd>", "<path>",
"<fname>"
```

File is on the Call Server CPU drive:**IPL > swDownload**

```
"<Call Server IPaddr>", "<dummyuid>", "<pdtpswd>",
"<path>", "<fname>"
```

- 4 At the IPL> prompt, enter

cardReset

The **cardReset** command resets a Voice Gateway Media Card. This command restarts the Voice Gateway Media Card. This process takes about 4 minutes to complete. The LEDs on the faceplate indicate when the card completes the start up process.

- 5 Use Element Manager to select this Voice Gateway Media Card.
- 6 Click **Transfer to Selected Elements** to transfer config.ini and bootp.tab files to the card.
- 7 See ["Transmit node properties" \(page 290\)](#).

—End—

Index

Symbols/Numerics

802.1Q Support 179
911 315

A

Active Leader 478
add additional cards to the node 285
alarm files 455
Alternate Call Server 369
Automatic IP Phone TN conversion 54

B

backplanes
 connectors 499
 I/O panel connections
backup 352, 395
bandwidth used 160
Basic IP User License 42
blocked calls 160
BOOTP parameters 459, 464
Branch Office 178

C

caching 261
call attempts and completions 160
Call Processor Pentium Mobile 23
Call Statistics 160
Card processor type 284
Card TN 284
CHG ES1 121
CHG ES2 121
CHG NKT 121
CLI commands, informational 465, 467

Codec 185
community string 268
CompactFlash 230
CONFIG.INI 160
CONFIG.INI file 459, 464
Configuring a virtual Superloop in Element Manager 250
connector pin assignments
 NT8D02 Digital Line Card 494
connectors 499
convert IP Trunk cards 478
Corporate Directory 131, 312
CP PM 23
CRPA/CRPD 312

D

Data Path Capture tool 182
define the physical TNs 246
Digital Signaling Processor (DSP) 78
Digital Signaling Processor
 daughterboards 20
DISI 478
DSP daughterboard self-test 454
DSP daughterboards 20

E

e911 315
echo cancellation 38
Echo Server 120
echoServerShow 127
echoServerShow 99 127
EDD 320
electShow 422
Element Manager 22, 159

Emergency Services Access 315
 Emulation Mode 54
 Enable set TPS 285
 environmental specs 504
 existing Voice Gateway Media Card
 properties 285

F

F
 10 code 457
 xx 457, 459, 461
 faceplate
 LED 29, 29
 fallback configuration data 159, 160
 FIBN 248
 FIBN, Package 365 248
 Firmware
 IP Phone 182
 Follower 159
 Follower Voice Gateway Media Card 458
 forgotten user ID and password 288

G

GEN CMD button 468
 Graceful Disable 183
 Group maximums 248

H

H323 ID 284
 hardware 226
 Hardware Watchdog Timer 184
 hex codes
 faceplate display 30
 Hold 118
 Hostname 284
 HP-DL320-GA 23

I

I/O panels
 backplane connections
 IBM-X360m 23
 informational CLI commands available from
 Element Manager 465, 467
 Install the replacement Voice Gateway
 Media Card 458, 460

Internet Explorer 226, 259, 261
 Internet Telephone Firmware 182
 IP client cookies 52
 IP Phone configuration data summary
 sheet 223
 IP Trunk 3.0 477
 IP Trunk cards 477
 IP User License 42
 IPE modules
 cable connections 499
 isetGet 124
 isetNATShow 125, 125
 isetReset 124, 124
 isetScpwModify 124
 isetScpwQuery 124
 isetScpwVerify 124
 isetShow 123, 458, 460
 ISP 1100 23
 ITG ISDN trunk service 477, 477
 ITG ISDN Trunk service 478
 ITG Trunk 2.x 477
 ITG-P 24-port card 30
 ITG-P 24-port line card 25, 25
 ITG-P 24-port line card display codes 459
 ITG-P Line Card 228
 itgadmin 288

K

Keep Alive Time-out setting 121

L

Language synchronization 52
 LD 97 249
 Leader 160
 LED on faceplate 29
 License 43
 Live Dialpad 50
 InIsa0 Carrier Failure 457
 log files 455
 loopback test 454

M

maintenance
 hex display 30
 Maintenance Audit 449

Manual IP Phone TN conversion 55
Mapping 115
mean time between failures 503
Media Card 27
Media Card 32S card 25
Mute 117
MVC 2050 38, 49, 50, 50, 146, 175, 256,
272, 314

N

NAT 115, 116
NAT Keep Alive timeout setting 120
NAT Mapping Keep Alive 117
NAT Mapping Keep Alive Time-out
setting 121
Network Address Translation 114
New IP Phone Types 53
nodePwdShow 327
NPR0011 460
NT8D02 Digital Line Card
connector pin assignments 494
NT8D37 IPE Modules
cable connections
NT8D37BA IPE Modules 499
NT8D37EC IPE Modules 499
NT8D81BA cable 499
NTCW84JW special IPE filter 499

O

Operational Measurement report scheduling
and generation 382
operational parameters 340
operational report 342, 382
overrides 327

P

Package 365 248
password 288
Patching 441
phantom superloops 249
physical TNs 246
Pop-up and USB keyboard support for
Unicode 51
port 5200 116
primary Signaling Server BOOTP 159

Private Zone 170
Proactive Voice Quality Management 125
PRT DNIP 435
PRT ES1 121
PRT ES2 121
PRT ESS 121
PRT IPDN 435
PRT ZONE 244
PRT ZONE ALL 244
PRT ZONE xxx 244
PUBLIC RTCP port number 119
PVQM 125
PWD1 288, 320

Q

QoS 160
Quality of Service 160

R

reboot 454
red LED on Voice Gateway Media Card 459
reliability 503
replace a Follower Voice Gateway Media
Card 458
replace a Leader Voice Gateway Media
Card 460
restart a specific card using the CLI. 372
restart the card using Element Manager 372
RS-232

maintenance port 30
RTCP 125
Run-time configuration 173, 173

S

schedule a generated OM Report 382
Security Device is missing 457
SNMP IP addresses 372
standalone IP Telephony node 160
status of password 327
superloop 42
survivability 369
Survivable Media Gateway 369
Survivable Succession Media Gateway IP
address 369

T

Telephony Manager 3.1 22
temperature specifications 504
temporary IP Phone Installer Password 327
Temporary IP User License 42
TM 22
Traffic printouts 160
Type II socket, dual type 29

U

Unicode support 51
unrecoverable hardware failure 457
user ID 288

V

Virtual Office 174
virtual superloop 42, 248, 249, 249
virtual Superloop in Element Manager 250
Virtual Superloops 249
virtual superloops for IP Phones 248
VLAN ID 118

VLANs 118
Voice Gateway Media Card 25
Voice Gateway Media Card installation
summary sheet 222
Voice LAN (TLAN) gateway IP address 284
VTNs 42
VxWorks shell 461, 463

W

warm reboot 454
WLAN Handset 2210 43, 48
WLAN Handset 2210/2211/2212 175
WLAN Handset 2211 43, 48
WLAN Handset 2212 43, 48
WLAN Handset 6120 43, 48
WLAN Handset 6140 43, 48
WLAN Handsets 2210 2211/2212 153
WLAN Handsets 2210/2211/2212. 153

Z

Zones 44

Nortel Communication Server 1000

IP Line Fundamentals

Copyright © 2003–2007, Nortel Networks
All Rights Reserved.

Publication: NN43100-500
Document status: Standard
Document version: 01.01
Document date: 30 May 2007

To provide feedback or to report a problem with this document, go to www.nortel.com/documentfeedback.

Sourced in Canada.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

Nortel, the Nortel logo and the Globemark are trademarks of Nortel Networks.

All other trademarks are the property of their respective owners.

