

Nortel Communication Server 1000

Signaling Server IP Line Applications Fundamentals

Release: 6.0
Document Revision: 01.04

www.nortel.com

NN43001-125

Nortel Communication Server 1000
Release: 6.0
Publication: NN43001-125
Document release date: 19 February 2010

Copyright © 2010 Nortel Networks. All Rights Reserved.

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

Nortel, Nortel Networks, the Nortel logo, and the Globemark are trademarks of Nortel Networks.

All other trademarks are the property of their respective owners.

Contents

New in this release 9
Revision history 9
Structure 9
Legacy products and releases 9
Related information 9

How to get help 11
Getting help from the Nortel Web site 11
Getting help over the telephone from a Nortel Solutions Center 11
Getting help from a specialist by using an Express Routing Code 12
Getting help through a Nortel distributor or reseller 12

Overview 13
Hardware platforms 13
Software installation 14
Software delivery 14
Software applications description 14
Line Terminal Proxy Server 15
SIP and H.323 signaling gateway (Virtual Trunk) 15
Application Server for the Personal Directory, Callers List, and Redial List feature 16
UCM - Common Services 16
System configurations 17

Description 19
Contents 19
Introduction 19
Digital Signaling Processor daughterboards 19
Interworking 21
Required packages 21
Fax/Modem pass-through 22
Modem traffic 24
Voice Gateway Media Cards 26
Media Card 32S 27
Reliable User Datagram Protocol 29

Copyright © 2010 Nortel Networks. All Rights Reserved.

Virtual superloops, Virtual TNs, and physical TNs 30
Licenses 31
Scalability 32
Redundancy 32
Administration 33

Features **35**
Contents 35
Introduction 36
Live Dialpad 38
Diagnostics 39
Unicode 39
Language synchronization 40
Unicode Name Directory 40
Virtual Office interaction 44
IP Client cookies 44
e2dsetShow () 45
IP Phone Types 45
Unique TN Types for existing IP Phone models 46
Automatic IP Phone TN conversion (Flexible Registration) 47
Manual IP Phone TN conversion 48
Active Call Failover for IP Phones 48
DSP peg counter for CS 1000E systems 70
Enhanced UNIStim Firmware Download for IP Phones 70
Firmware download using UNIStim FTP 98
NAT Traversal feature 105
Corporate Directory 119
Personal Directory, Callers List, and Redial List 120
IP Call Recording 120
pbxLink connection failure detection 129
Display pbxLink information using LD 117 STAT SERV 130
IP Phone support 134
Element Manager support 134
Call Statistics collection 135
Programmable line/DN feature keys (self-labeled) 141
Zones 142
Network wide Virtual Office 144
Bandwidth Management for Network wide Virtual Office 147
Branch Office and Media Gateway 1000B 147
802.1Q support 148
Data Path Capture tool 149
IP Phone firmware 149
Hardware watchdog timer 149
Codecs 150

Copyright © 2010 Nortel Networks. All Rights Reserved.

IP Phone type checking and blocking 150
Enhanced Redundancy for IP Line nodes 152
Patch Management 154
Migration from Solid database to MySQL 154

Personal Directory application 157
Contents 157
Introduction 157
Personal Directory 159
Callers List 160
Redial List 162
IP Phone Application Server configuration and administration 163
IP Phone Application Server database maintenance 168
Call Server configuration 172
Password administration 172
Unicode Name Directory 174
Unicode Name Directory feature restrictions and limitations 175
IP Phones configuration 176

Codecs 177
Contents 177
Introduction 177
Codec configuration 179
Codec registration 180
Codec negotiation 184
Codec selection 186
H.323 Master/Slave algorithm 187
SIP Offer/Answer model 187

Installation task flow 189
Contents 189
Introduction 189
Before you begin 189
Installation summary 189

Signaling Server software installation using Deployment Manager 193
Contents 193
Introduction 193
Installation Task Flow 193
Software Deployment Packages 194
Pre-installation checklist 195
Nortel Linux Base installation 195
Signaling Server application installation 195
Access UCM 197
Element Manager configuration 198

Copyright © 2010 Nortel Networks. All Rights Reserved.

Configuring the Internet Explorer browser 198

Signaling Server Software upgrade 203
Contents 203
Introduction 203
Overview 204
Signaling Server software upgrade task flow 204
Upgrade paths 205
Upgrade from Succession 1000 Release 3.0 205
Upgrade from CS 1000 Release 4.0 205
Upgrade from Communication Server 1000 Release 4.5 207
Upgrade from Communication Server 1000 Release 5.0 207
Upgrade from Communication Server 1000 Release 5.5 207
Upgrade procedures 207

Installation and initial configuration of an IP Telephony node 215
Contents 215
Introduction 215
Equipment considerations 216
Install the hardware components 217
Initial configuration of MC 32S card 225
Initial configuration of IP Line data 226
Configure the Expansion Module for IP Phone 1100 Series 236
Configure the IP Phone 1200 Series Key Expansion Module 238
Node election rules 243

Configuration of IP Telephony nodes using Element Manager 245
Contents 245
Introduction 245
Configure IP Line data using Element Manager 246
Transfer node configuration from Element Manager to the Voice Gateway Media Cards 263
Upgrade the Voice Gateway Media Card and IP Phone firmware 264
Download the current loadware and IP Phone firmware 266
Assemble and install an IP Phone 275
Change the default IPL CLI Shell password 275
Configure the IP Phone Installer Passwords 275
Import node configuration from an existing node 276

IP Line administration 279
Contents 279
Introduction 279
IP Line feature administration 280
Password security 285
IP configuration commands 298

Copyright © 2010 Nortel Networks. All Rights Reserved.

TLAN network interface configuration commands 298
Display the number of DSPs 299
Display IP Telephony node properties 299
Packet loss monitor 302
Transfer files using the CLI 303
Reset the Operational Measurements file 304

IP Line administration using Element Manager 305
Contents 305
Introduction 305
Element Manager administration procedures 305
View Traffic reports 316
Backup and restore data 338
Update IP Telephony node properties 341
Update other node properties 348
Import or Export an IP Node Configuration File 348
Telnet to a Voice Gateway Media Card using Virtual Terminal 350
Check the Voice Gateway Channels 351
Setting the IP Phone Installer Password 352

Maintenance 357
Contents 357
Introduction 357
IP Line and IP Phone maintenance and diagnostics 357
IP Line CLI commands 366
Lamp Audit function 368
Troubleshoot an IP Phone installation 368
Maintenance telephone 368
Faceplate maintenance display codes 369
System error messages 371
Voice Gateway Media Card self-tests 376
Replace the Media Card CompactFlash 376

Voice Gateway Media Card maintenance using Element Manager 379
Contents 379
Introduction 379
Replace a Voice Gateway Media Card 379
Add another Voice Gateway Media Card 380
Access CLI commands from Element Manager 381

NAT router requirements for NAT Traversal feature 383
Contents 383
Description 383
Requirements 384
Natcheck output 386

Copyright © 2010 Nortel Networks. All Rights Reserved.

I/O, maintenance, and extender cable description **389**
Contents 389
Introduction 389
NTMF94EA I/O cable 389
Connector pin assignments 390
NTAG81CA maintenance cable description 393
NTAG81BA maintenance extender cable 394
Replace the NT8D81BA cable 395

Product integrity **399**
Contents 399
Introduction 399
Reliability 399
Environmental specifications 400

Subnet Mask Conversion from CIDR to Dotted Decimal Format **403**
Introduction 403

Copyright © 2010 Nortel Networks. All Rights Reserved.

New in this release

Revision history

February 2010
Standard 01.04. This document is issued to support Communication Server 1000 Release 6.0.

June 2009
Standard 01.03. This document is issued to support Communication Server 1000 Release 6.0.

May 2009
Standard 01.02. This document is issued to support Communication Server 1000 Release 6.0.

Structure

Legacy products and releases

This document contains information about systems, components, and features that are compatible with Nortel Communication Server 1000 Release 6.0 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)
- *Branch Office Installation and Commissioning* (NN43001-314)
- *Telephony Manager 4.0 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)
- *Unified Communication Management Fundamentals* (NN43001-116)

Copyright © 2010 Nortel Networks. All Rights Reserved.

- *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)
- *IP Phone 1210 User Guide* (NN43140-101)
- *IP Phone 1220 User Guide* (NN43141-101)
- *IP Phone 1230 User Guide* (NN43142-101)
- *IP Phone 1200 Series Key Expansion Module User Guide*

Copyright © 2010 Nortel Networks. All Rights Reserved.

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

Copyright © 2010 Nortel Networks. All Rights Reserved.

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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Overview

This document describes the functional and operational characteristics of IP Line applications, and associated features, in Nortel Communication Server (CS) 1000 Release 6.0. It also describes how to install, configure, administer and maintain an IP Telephony node.

The IP Line applications manage IP Phone signaling, Session Initiation Protocol (SIP) gateway signaling, H.323 gateway signaling, Personal Directory, and IP Peer Networking, in CS 1000E and CS 1000M systems.

Hardware platforms

The following supported platforms can host the IP Line applications in a CS 1000 Release 6.0 system:

- Nortel CP PM (Call Processor Pentium Mobile)

  The CP PM card can host a Co-resident Call Server and Signaling Server configuration in CS 1000 Rel. 6.0. For more information, see *CP PM Co-resident Call Server and Signaling Server Fundamentals* (NN43001-509).

- IBM x306m
- IBM x3350
- HP DL320-G4
- DELL R300

The Nortel CP PM platform is a circuit card and is hosted in slots of Media Gateways in CS 1000E systems, or in slots of Universal Equipment Modules (UEM) in CS 1000M SG and CS 1000M MG systems. The other platforms are commercial off-the-shelf (COTS) servers. For more information about the platforms, and instructions to install, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

All hardware platforms have an ELAN and a TLAN network interface. The IP Line applications communicate with the system Call Processor through the system ELAN subnet.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Software installation

IP Line applications are deployed to a Linux-based Signaling Server (hardware platform) from the Primary Security Server in the CS 1000 system by using the Deployment Manager tool in the Unified Communications Management (UCM) application. This is known as Central Deployment.

You can also deploy IP Line applications to a Linux-based Signaling Server by using the Deployment Manager tool on the local Signaling Server. This is known as Local Deployment. Local Deployment allows a hardware platform to be initialized prior to joining the primary security domain.

Local Deployment and Central Deployment require that all IP Line application software be copied to the Signaling Server prior to the software deployment. In effect, the Signaling Server acts as the Primary Security Server and deploys IP Line applications software to itself.

ATTENTION
Nortel recommends that you deploy IP Line applications from the Primary Security Server (Central Deployment) to ensure application consistency on all hardware platforms targeted to host IP Line applications in your CS 1000 system.

You can install IP Line applications on more than one Signaling Server in CS 1000E and CS 1000M systems to provide a load-sharing, redundant configuration for high scalability and enhanced reliability. See “Redundancy” (page 32).

Software delivery

IP Line software is deployed using Deployment Manager. For more information, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

Software applications description

A Signaling Server provides a signaling interface to the IP network using the following software applications:

- Line Terminal Proxy Server
- SIP signaling gateway
- H.323 signaling gateway
- Application Server for the Personal Directory (Unicode Directory), Callers List, and Redial List features
- UCM - common services

Copyright © 2010 Nortel Networks. All Rights Reserved.

Line Terminal Proxy Server

The Line Terminal Proxy Server (LTPS) application is the signaling interface for IP Phones. The LTPS application runs on the primary Signaling Server and the Signaling Servers added to the network for load balancing and redundancy. Each instance of the LTPS application supports a maximum of 5 000 IP Phones.

With the Call Server, the LTPS delivers a full suite of telephone features. If the Signaling Server is co-resident with the Call Server, the maximum number of IP Phones is 1 000. For more information, see *CP PM Co-resident Call Server and Signaling Server Fundamentals* (NN43001-509).

The Unified Network IP Stimulus protocol (UNIStim) is the stimulus-based protocol used for communication between IP Phones and the LTPS. The LTPS also manages the firmware for all connected IP Phones.

For a list of all support Nortel IP Phones, see *IP Phones Fundamentals* (NN43001-368).

Phase 2 IP Phones support all CS 1000 Release 6.0 features. Phase 1 IP Phones do not.

You can configure each IP Phone through the Dynamic Host Configuration Protocol (DHCP) to register with a Call Server for feature control. For more information, see “DHCP server” (page 20).

SIP and H.323 signaling gateway (Virtual Trunk)

The Virtual Trunk application manages the SIP and H.323 signaling gateways on the system.

Session Initiation Protocol trunking

Session Initiation Protocol (SIP) is a signaling protocol for creating, modifying, and terminating sessions with one or more participants. These sessions can include IP Phone calls, multimedia distribution, and multimedia conferences. Basic SIP connectivity, referred to as SIP trunking, provides a direct media path between users in a network.

The SIP trunking software functions as

- SIP User Agent
- signaling gateway for all SIP Phones

For more information about SIP trunking, see *IP Peer Networking Installation and Commissioning* (NN43001-313) and *Network Routing Service Fundamentals* (NN43001-130).

Copyright © 2010 Nortel Networks. All Rights Reserved.

H.323 trunking

H.323 is a standard that specifies the components, protocols, and procedures that provide multimedia communication services over packet networks.

The H.323 signaling software (Virtual Trunk) provides the industry-standard H.323 signaling interface to H.323 gateways. It supports both en bloc and overlap signaling. This software uses an H.323 Gatekeeper to resolve addressing for systems at various sites.

> ***Note:*** For overlap signaling to provide the maximum benefit, Nortel highly recommends that all Signaling Servers in the network be overlap-enabled. Failure to do so results in call-completion delays caused by converting between overlap and en bloc.

The H.323 gateway supports direct, end-to-end voice paths using Virtual Trunks with the following benefits:

- elimination of multiple IP Telephony to circuit-switched conversions
- improved voice quality
- simplified troubleshooting
- interoperability

For more information about H.323 signaling, see *IP Peer Networking Installation and Commissioning* (NN43001-313) and *Network Routing Service Fundamentals* (NN43001-130).

Application Server for the Personal Directory, Callers List, and Redial List feature

The Application Server for the Personal Directory, Callers List, and Redial List features (IP Phones Application Server) runs on the Signaling Server. Only one database can exist in the network; redundancy is not supported. The IP Phones Application Server database can coexist with the other software applications on a Signaling Server. However, if you have more than 1 000 users, Nortel recommends that you store the database on a dedicated Signaling Server (preferably a Follower). The IP Phones Application Server cannot be run on a Signaling Server at a branch office.

You can configure a standalone PD server. You can create a node for the PD where LTPS and VTRK applications are disabled.

UCM - Common Services

The following UCM common services are supported in CS 1000 Release 6.0:

- Security server: Security Services enables element and service management applications to access a common application security

Copyright © 2010 Nortel Networks. All Rights Reserved.

infrastructure. The framework manages secure access to Web applications and provides security for Web interfaces and Web utilities.

- Element Manager: Element Manager is a Web interface that provides an alternative to the traditional CLI and overlays.
- Deployment Manager: Linux platform uses Centralized Deployment Manager (CDM) to remotely deploy application software from the primary security server to other Linux servers located in the same security domain.
- Subscriber Manager: Subscriber Manager is deployed as a plug-in application above the UCM framework. Subscriber Manager provides a centralized location for the management of subscriber information for enterprise services. With Subscriber Manager, users can easily manage subscribers and subscriber accounts (phone services) within a network.

System configurations

Although you can use IP Line applications in various system configurations and the use can vary in those configurations, support is available for two basic system configurations in CS 1000 Release 6.0. See Table 1 "Possible system configurations" (page 17).

CS 1000 systems have a Signaling Server in the 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.

The LTPS runs on the Signaling Server. Nortel IP phones or redirect supported IP phones list register with the Signaling Server.

Table 1
Possible system configurations

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

Copyright © 2010 Nortel Networks. All Rights Reserved.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Description

Contents

This chapter contains the following topics:

- "Introduction" (page 19)
- "Interworking" (page 21)
- "Required packages" (page 21)
- "Voice Gateway Media Cards" (page 26)
- "Virtual superloops, Virtual TNs, and physical TNs" (page 30)
- "Licenses" (page 31)
- "Administration" (page 33)

Introduction

The IP Line application provides an interface that connects IP Phones to a CS 1000 Call Server. CS 1000 Release 6.0 requires a Signaling Server. This chapter provides a description of the IP Line application.

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

Voice Gateway Media Cards cannot run IP Line application software.

Digital Signaling Processor daughterboards

Digital Signaling Processor (DSP) daughterboards on the Media Gateway Controller (MGC) provide DSP resources to connect IP and Time Divisional Multiplexing (TDM) devices in a CS 1000E Media Gateway (MG 1000E). The following DSP daughterboards are available:

- 32 port daughterboard
- 96 port daughterboard

Copyright © 2010 Nortel Networks. All Rights Reserved.

A daughterboard provides an optional solution to installing the Voice Gateway Media Cards within the CS 1000E Media Gateway (MG 1000E). However, support for Voice Gateway Media Cards remains available within an MG 1000E with a Media Gateway Controller (MGC) and DSP daughterboards. The MGC is used only in a Media Gateway chassis, cabinet, or in an MG 1010.

However speech path delay can occur when DSP resources are involved in call scenarios with modified speech path. This affects IP-TDM calls combined with features such as

- Conferencing
- ACD Observe
- Call monitoring
- OVR - Override
- BKIN - Break-In
- QPR - QSIG Path Replacement
- TRO - Trunk Route Optimization
- ROP - Route Optimization
- EES - End to End Signaling

The delay sums up from a time required to close used channel, to fill in ARP header for new channel and a time required to bring the DSP in working mode on a micro-engine level. The delay depends on the Media Card type and on the number of DSP resources that are taken in any given call scenario. The more DSP resources involved the more open/close pairs need to be processed, increasing the delay. The longest possible delay is up to 3 seconds for MC/ITG cards, up to 1 second for MGC/MS32S cards.

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

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 Line Terminal Proxy Server (LTPS).

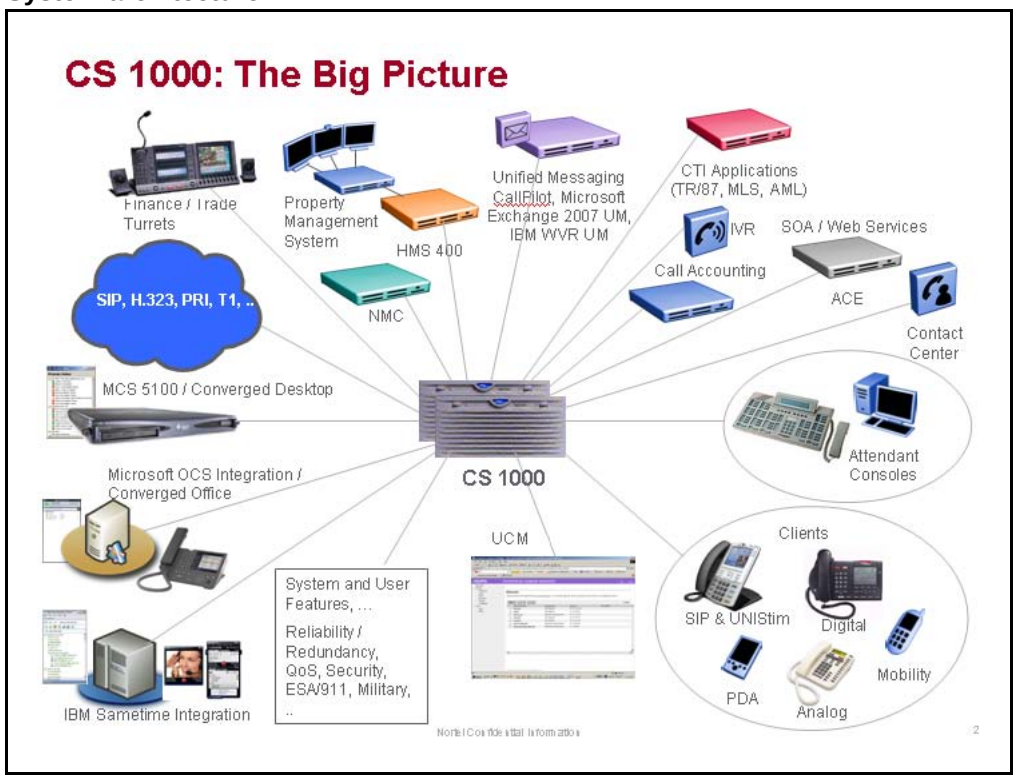
For more information about DHCP, see *Converging the Data Network with VoIP Fundamentals* (NN43001-260) and *IP Phones Fundamentals* (NN43001-368).

Copyright © 2010 Nortel Networks. All Rights Reserved.

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



Required packages

IP Phones require the software packages listed in Table 2 "Required packages" (page 21).

Table 2
Required packages

Package mnemonic	Package number	Package description	Package type (new, existing, or dependency)	Applicable Market
DSET	88	M2000 Digital Sets	Existing	All
ARIE	170	Aries Digital Sets	Existing	All

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

Copyright © 2010 Nortel Networks. All Rights Reserved.

Fax/Modem pass-through

The Fax/Modem pass-through feature provides a modem pass through allowed (MPTA) class of service (CoS) for an analog phone TN. MPTA CoS dedicates an analog phone TN to a modem or a fax machine terminal. A connection that initiates from the dedicated TN or calls that terminate at the dedicated TN through a Digital Signal Processor (DSP), use a G.711 NO VAD codec on the Call Server.

Modem pass-through is a specific configuration of a G.711 VoIP channel that improves modem performance compared to standard VoIP configuration. Automatic switching to Voice Band Data (VBD) is a feature of the DSP; the DSP monitors the data stream to distinguish between voice and data calls. The DSP reconfigures to modem pass through mode when it determines the call is a modem call.

The DSP mode on the Mindspeed DSP (MC32S/DB96/DB32) for MPTA to MPTA fax or modem calls displays ModemPT in the dspMode field of the vgwShow command. The Telogy DSP (ITGSA) displays PassThrough.

For modem calls between CS 1000 systems connected by analog and digital trunks, you must configure MPTA CoS on the Call Server of each CS 1000 system for analog units connected to modems. MPTA CoS configuration is necessary because the call setup negotiation does not occur end to end as it is for virtual trunks. If the analog unit on one Call Server uses MPTA CoS and the analog unit on the other Call Server uses modem pass through denied (MPTD) CoS, the modem call fails.

When you configure MPTA CoS on a TN, support is no longer available for the T.38 protocol for that particular TN. Any call setup with an analog phone TN that has MPTA configured must use G.711 codec exclusively, as this is the only codec available for making calls using this TN. G.711 codec exists by default in the DSP configuration.

To ensure the MPTA CoS works correctly, you must select the Enable Modem/Fax pass-through mode check box in the Gateways section of Element Manager. This check box is selected by default in Element Manager. To enable SG3 fax calls over Telogy DSP, you must select the Enable V.21 FAX tone detection check box in Element Manager must. For SMC and MC32S cards, this setting is available in the codec profile section on the Nodes summary page. In the modem pass-through mode of operation, the DSP state appears as MPT on the MGC and MC32S cards and as PassThru on SMC cards.

Telephony Manager (TM) and Basic Client Configuration (BCC) do not support MPTA CoS. BCM 50 supports only modem pass-through over G.711 in Release M50R3.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Only the G.711 codec supports MPT CoS. MPT CoS includes no other codecs. The packet interval for G.711 codec is assigned a value of 20 milliseconds (ms) in MPT.

The maximum speed supported for modem and fax is 33.6 Kbps. This limit is imposed by the analog line card.

MPT allows CS 1000 to support the following:

- modem pass through
- Super G3 (SG3) fax at V.34 (33.6 Kbps)
- V.34 rate (33.6 Kbps) modems
- Fax machines that support V.17, V.27, V.29, and V.34

Note: IP trunks do not support MPT CoS.

When the TN on the CS 1000 is configured with MPTA CoS, it supports V.17, V27 and V29 Fax calls. However, the DSP mode is “FaxBegin,” not “ModemPT”. The MPTA CoS forces calls originated or terminated on the TN to use the G.711 NO VAD Codec. This codec selection supersedes the existing bandwidth management strategy on the CS 1000.

When a CS 1000E connects with a system from another vendor, the modem pass-through feature works if the third-party system supports the modem pass-through mode of operation.

The Voice Gateway application displays different auto-switch states (ModemPT, Passthru) in the dspMode field of the vgwShow command, based on tones detected by the DSP. These tones are generated by modem and fax machines connected in the TDM domain. The Voice Gateway application does not control auto-switch states during fax and modem calls, and the dspMode reports tone indications from DSP. The Mindspeed DSP sends tone-detection events to the host processor and changes to Modem Passthrough and Pass-through auto-switch states (with or without Redundancy), based on the tones detected, as it is configured in Auto-switch mode.

For interface commands, responses, and definitions for MPT, see Table 3 "Interface commands and responses" (page 23).

Table 3
Interface commands and responses

Command prompt	User response	Description
CLS	MPTA	Turn on the MPT feature.
CLS	MPTD	Turn off the MPT feature.

Copyright © 2010 Nortel Networks. All Rights Reserved.

ATTENTION
CLS MPTA and CLS MPTD are included in LD 10 for analog line card units.

MPTA-to-MPTA and MPTA-to-MPTD fax or modem calls succeed over the G.711 codec in ModemPT DSP mode. However; MPTD-to-MPTD modem calls fail.

MPTD-to-MPTD fax calls succeed (best effort) over G.711 if the Enable Modem/Fax pass through mode and Enable V.21 FAX tone detection options are configured to On in the gateway. If the Enable Modem/Fax pass through mode is cleared, the fax call goes over the T.38 codec. Nortel recommends the T.38 fax codec for fax calls over SIP and H.323 trunks. To select the T.38 fax codec, the analog line units at both originating and terminating systems must be set to MPTD CoS.

For information about feature packaging requirements, see Table 4 "Feature packaging requirements" (page 24).

Table 4
Feature packaging requirements

Package mnemonic	Package number	Package description	Package type (new, existing, or dependency)	Applicable market
Softswitch	402	Identifies a softswitch system	Existing	All
IPMG	403	Identifies a system that is equipped with IPMGs	Existing	All

Modem traffic

CS 1000E supports modem traffic in a campus-distributed network with the following characteristics:

- Media card configuration:
  - G.711 codec
  - 20 ms packet size
- one-way delay less than 5 ms
- low packet loss
- V.34 rate (33.6 Kbps)

Performance degrades significantly with packet loss (must be less than 0.5 percent) and when the delay (round trip) is greater than 50 ms and mean jitter is greater than 5 ms.

Copyright © 2010 Nortel Networks. All Rights Reserved.

ATTENTION
Nortel conducted extensive but not exhaustive tests of modem-to-modem calls, data transfers, and file transfers between a CS 1000E and a MG 1000E, using Virtual Trunks and PRI tandem trunks. While all tests succeeded, Nortel cannot guarantee that all modem brands can operate properly over all G.711 Voice over IP (VoIP) networks. Before you deploy modems, test the modem brand within the network to verify reliable operation. Contact your system supplier or your Nortel representative for more information.

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.

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

For more information about Signaling Server load-balancing and redundancy, see *Communication Server 1000M and Meridian 1 Small System Planning and Engineering* (NN43011-220).

IP Phone registration

Table 5 "Registration process" (page 25) describes the registration process.

Table 5
Registration process

Step	Description
1	The IP Phone receives the IP address of the Connect Server (co-located 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 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 Leader.
5	The IP Phone contacts the Node Leader. The Node Leader 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

IP Phone unregistration

Table 6 "Unregistration process" (page 26) describes the unregistration process.

Table 6
Unregistration process

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

Voice Gateway Media Cards

In this document, Media Card 32-port card and Media Card 32S card are referred to as Voice Gateway Media Card, unless explicitly stated. The media cards plug into shelf slots in Intelligent Peripheral Equipment (IPE) units in CS 1000M systems and into slots on Media Gateway 1000E units and Media Gateway 1000E Expander units in CS 1000E systems. The MC32-port and Media Card 32S cards occupy one slot.

The Media Card 32-port card provides a channel density of 32 ports.

The Media Card 32S card provides the following features:

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

ITG-P media cards are not supported in CS 1000 Release 6.0.

IP Line applications are not supported on the Voice Gateway Media Cards in CS 1000 Release 6.0.

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 Telephony LAN (TLAN) 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 Media Card faceplates.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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

For more information about the card faceplates and components, see *Circuit Card Reference* (NN43001-311).

Media Card 32S

The Media Card 32S provides a security layer to secure IP media paths between cards.

Secure Real-time Transport Protocol

The MC32S media card uses Secure Real-time Transport Protocol (SRTP) to secure the IP media path between the card and another MC32S media card or associated DSP daughterboards. When Media Security is configured to On, the Call Server sends a message to the Voice Gateway software on the MC32S card to activate SRTP for the media connection established for that call.

The system administrator configures Media Security.

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

There are two processors on the MC 32S card:

- Control and Signaling Processor (CSP) which runs application and signaling code
- Media Stream Processor (MSP) which processes the media streams.

Table 7 "Files downloaded to the MC 32S card" (page 27)lists the file names and paths for files that are downloaded from the Signaling Server to the MC 32S card.

Table 7
Files downloaded to the MC 32S card

File name	Path on Signaling Server	Path on MC 32S card	Description
IPL6.00XX.mc32s	/var/opt/nortel/tps/fw/	/p	Software binaries
bootp.tab	/etc/opt/nortel/sigServerShare/config/	/u	bootp parameter file
config.ini	/etc/opt/nortel/sigServerShare/config/	/u	config file

Copyright © 2010 Nortel Networks. All Rights Reserved.

The software for the MC 32S consists of five files, which are located in the IPL6.00XX.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 8
Files within the zipped file

File name	Description
bootrom.bin	MC 32S boot code image
mainos.sys	VxWorks 6.0 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

Unsupported products

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

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

Signaling and messaging

The LTPS sends Scan and Signaling Distribution (SSD) messages to the Call Processor 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 (UNIStim). The Reliable User Datagram Protocol (RUDP) is the transport protocol.

Copyright © 2010 Nortel Networks. All Rights Reserved.

UNIStim

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

UNIStim is the stimulus-based protocol used for communication between an IP Phone and an LTPS on the Signaling Server.

Reliable User Datagram Protocol

Reliable User Datagram Protocol (RUDP) is used for the following purposes:

- 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 30).

Description

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

The features of RUDP are as follows:

- 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 the order in the sequence.

- If the packet is successfully transmitted to B, B returns an ACK to A, acknowledging that the packet was received.
- If A receives no message within a configured time, it retransmits the packet.
- If B receives a packet without first receiving the 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

ELAN TCP transport

Although TCP is the signaling protocol between the Call Processor and the Signaling Server, RUDP remains for the keepalive mechanism for the link. This means that RUDP messages are exchanged to maintain the link status between the Call Server and the Signaling Server.

The TCP protocol enables bundled messages. 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.

The Call Server and LTPS software use handshaking to automatically enable TCP. The LTPS application checks the software version each time it attempts to establish a TCP link with the CS 1000 CPU. TCP transports messages, whereas RUDP establishes and maintains the link.

The LTPS software version must match the Call Processor software version; otherwise, the LTPS terminates the link and logs an error message.

Virtual superloops, Virtual TNs, and physical TNs

Virtual TNs (VTN) enable configuration of service data for an IP Phone, such as key layout and CoS, without requiring the IP Phone to be dedicated (hard-wired) to a TN.

The concentration of IP Phones is made possible by dynamically allocating a port (also referred to as a physical TN) for a circuit-switched-to-IP Phone call. All system speech path management occurs with a physical TN instead of a virtual TN. Calls occur 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 to perform the encoding or decoding required to connect the IP Phone to the circuit-switched network.

The IP Phones (virtual TN) are defined on virtual superloops. To create an IP Phone using VTNs, create a virtual superloop in LD 97 or in Element Manager. See “Configure virtual superloops for IP Phones” (page 230).

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 TN)-to-IP Phone calls.

Each Media Card 32-port card provides 32 physical TNs. The physical TNs are the gateway channels (DSP ports). The channels (ports) on the Voice Gateway Media Cards are pooled resources.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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

Licenses

Three types of licenses exist:

- 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, IP Phone 1110, and IP Phone 1210
- IP User License for the IP Phone 2002, IP Phone 2004, IP Phone 2007, IP Phone 1120E, IP Phone 1140E, IP Phone 1150E, IP Phone 1220, IP Phone 1230, 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, you can use Basic IP User License and IP User License.

If insufficient Basic IP User Licenses are available for the IP Phone 2001, IP Audio Conference Phone 2033, IP Phone 1110, and IP Phone 1210 then you can also use the IP User License.

If no Basic IP User Licenses are available for the IP Phone 2001, IP Audio Conference Phone 2033, IP Phone 1110, and IP Phone 1210 and IP User Licenses are used, an error message appears:

> **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 you configure an IP Phone, the system TN ISM counter decrements.

Customers must purchase one license for each IP Phone installed on a 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).

Copyright © 2010 Nortel Networks. All Rights Reserved.

ATTENTION
Functional Pricing does not support individual licenses. 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 TN configured with Basic IP User Licenses must not exceed 32 767. The total number of TN 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.

Scalability

The following table summarizes the operational limits of a single Signaling Server. Use the values in the table as a quick overview for planning. For detailed calculations, see *Communication Server 1000E Planning and Engineering* (NN43041-220) or *Communication Server 1000M and Meridian 1 Large System Planning and Engineering* (NN43021-220) as appropriate for your CS 1000 system.

Note: You must consider real-time capacity for a specific application, which can constrain an application in reaching resource limits.

Signaling Server application	Limit
Terminal Proxy Server (TPS)	up to 5 000 IP Phones on non Co-Res systems and up to 1 000 IP Phones on Co-Res SS-CS systems.
Virtual Trunk	***Note:*** This limit depends on the split between SIP and incoming and outgoing H.323 calls. For more information see the Planning and Engineering documentation appropriate for your system.
PD	Up to 22 500 IP Phones for each PD server. Up to 2000 IP Phones on Co-Res SS only systems. Up to 1 000 IP Phones on Co-Res SS-CS systems.

Redundancy

Redundancy provides load-sharing for the Terminal Proxy Server (TPS) and an alternative route for the SIP and H.323 Gateway software. Signaling Server redundancy ensures that telephony services can withstand single hardware and network failures.

When you plan survivability strategies for the Signaling Server, include a second Signaling Server in the plan to load share. One Signaling Server is a Leader Signaling Server that is the primary TPS. The other Signaling Server is a Follower Signaling Server that is a secondary, redundant TPS.

Copyright © 2010 Nortel Networks. All Rights Reserved.

If the Leader Signaling Server fails, an election process occurs and the Follower Signaling Server becomes the primary TPS. The IP Phones reregister to the Follower Signaling Server, and system operation resumes. If the Follower fails, the IP Phones registered to the Follower reregister to the Leader Signaling Server.

The following scenario explains how redundancy works:

- The IP Phones are distributed between the two Signaling Servers (load-sharing). The SIP and H.323 Gateways run on the Leader Signaling Server.
- The Leader Signaling Server fails.
- The Follower Signaling Server takes on the role of the Leader Signaling Server and acquires the IP address of the Leader Signaling Server if necessary.
- The Time-to-Live (TTL) of IP Phones registered with the failed Signaling Server expires, which causes those IP Phones to reset and register with the new Leader Signaling Server.

  Note: Only IP Phones registered with the failed Signaling Server are reset.

- The new Leader Signaling Server assumes responsibility for the SIP and H.323 Gateways.
- Normal operation resumes.

Administration

The following administration interfaces are available to manage IP Line applications:

- Element Manager: Element Manager is used to administer IP Line application software.
- Command Line Interface (CLI): The CLI prompts depends on the type of Voice Gateway Media Card in the system. IPL> prompt appears for the Media Card 32-port. oam> or PDT> prompt appears for the Media Card 32S card.
- CLI on the Signaling Server: Access the CLI through the Linux shell. The commands that you can access will depend on the security role that you use to log on. Use a space between Linux CLI parameters
- Administration and maintenance overlays of Call Servers.
- Telephony Manager 4.0. TM is used to obtain OM reports only.

Copyright © 2010 Nortel Networks. All Rights Reserved.

TM 4.0

IP Line uses TM 4.0 to obtain OM reports only.

Element Manager

Element Manager is a Web-based user interface used to configure and maintain CS 1000 components. Use the Element Manager to configure and manage IP Line from a Web browser.

The Element Manager Web server resides on the Signaling Server within Unified Communications Manager (UCM) framework. For more information about Element Manager residing on a Signaling Server, see *Element Manager System Reference—Administration* (NN43001-632).

Command Line Interface

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

Access

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

For more information about the CLI commands, see "IP Line CLI commands" (page 366).

Overlays

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

Copyright © 2010 Nortel Networks. All Rights Reserved.

Features

Contents

This section contains the following topics:

- “Introduction” (page 19)
- “Active Call Failover for IP Phones” (page 48)
- “DSP peg counter for CS 1000E systems” (page 70)
- “Enhanced UNIStim Firmware Download for IP Phones” (page 70)
- “Firmware download using UNIStim FTP” (page 98)
- “NAT Traversal feature” (page 105)
- “Personal Directory, Callers List, and Redial List” (page 120)
- “IP Call Recording” (page 120)
- “pbxLink connection failure detection” (page 129)
- “Display pbxLink information using LD 117 STAT SERV” (page 130)
- “IP Phone support” (page 134)
- “Corporate Directory” (page 119)
- “Element Manager support” (page 134)
- “Call Statistics collection” (page 135)
- “Programmable line/DN feature keys (self-labeled)” (page 141)
- “Zones” (page 142)
- “Network wide Virtual Office” (page 144)
- “Branch Office and Media Gateway 1000B” (page 147)
- “802.1Q support” (page 148)
- “Data Path Capture tool” (page 149)
- “IP Phone firmware” (page 149)
- “Hardware watchdog timer” (page 149)
- “Codecs” (page 150)

Copyright © 2010 Nortel Networks. All Rights Reserved.

- “IP Phone type checking and blocking” (page 150)
- “Enhanced Redundancy for IP Line nodes” (page 152)

Introduction

Table 9 "IP Line feature support" (page 36) outlines the IP Line features available for CS 1000 systems with CS 1000 Release 6.0 software.

Table 9
IP Line feature support

Feature	CS 1000M	CS 1000E
Support for Element Manager	Yes	Yes
Support for Signaling Server	Yes	Yes
Support for the following IP Phones: • 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 Phone 1210, IP Phone 1220, IP Phone 1230 • WLAN Handset 2210, 2211, 2212 • WLAN Handset 6120, 6140	Yes	Yes
Support for the following software clients: • IP Softphone 2050 • Mobile Voice Client (MVC) 2050	Yes	Yes
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
IP Phone 1200 Series Key Expansion Module (KEM)	Yes	Yes
Live Dialpad	Yes	Yes
Unicode support	Yes	Yes
Node level patching is not provided by TM 4.0. You can use the patching CLI command of the Media Card 32-port card and MC 32S card.		

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 9
IP Line feature support (cont'd.)

Feature	CS 1000M	CS 1000E
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
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	No	No
Node level patching is not provided by TM 4.0. You can use the patching CLI command of the Media Card 32-port card and MC 32S card.		

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 9
IP Line feature support (cont'd.)

Feature	CS 1000M	CS 1000E
Maintenance Audit enhancement	Yes	Yes
Multilanguage 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 4.0. You can use the patching CLI command of the Media Card 32-port card and MC 32S card.		

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, by 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
- IP Phone 1210
- IP Phone 1220
- IP Phone 1230

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

Copyright © 2010 Nortel Networks. All Rights Reserved.

Diagnostics

Output of the vxShell command `e2dsetShow()` contains a state of the Live Dialpad feature.

Unicode

IP Phones use the Unicode feature to work in languages other than English. Using the Unicode feature, the Call Processor can display multilingual text on the following types of IP Phones:

- IP Phone 2007
- IP Phone 1120E
- IP Phone 1140E
- IP Phone 1150E
- IP Phone 2050V3
- IP Phone 1110
- IP Phone 1210

The Call Processor can display text in the following languages on the specified types of IP Phones:

- Japanese – Kanji
- Japanese – Katakana
- Chinese – Traditional
- Chinese – Simplified
- Arabic
- Korean
- Hebrew
- Greek

The languages listed are not available on IP Phones that do not have Unicode support. If an IP Phone without Unicode support registers to a TN with a Unicode-only language configured, the IP Phone defaults to English.

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

Japanese – Katakana and Japanese – Kanji cannot be supported simultaneously.

Copyright © 2010 Nortel Networks. All Rights Reserved.

You can enter only a limited subset of Unicode characters locally using an IP Phone dialpad. The Special Characters Input Screen includes the character set used by the currently configured language. For languages with large amounts of characters (for example, Traditional Chinese, Japanese, and Korean), support is not available for localized dialpad input. The Pop-up and USB keyboard add-ons support English input only.

On IP Phones that support Unicode, you use the desired language command in the Telephone Options, Language menu option when configuring the IP Phone. All IP Phones that support Unicode need a special font file to support Asian languages. This font file must be loaded to the IP Phones during configuration using TFTP.

Language synchronization

Language synchronization occurs strictly through UNIStim messaging. If the IP Phone receives an Assign IT Language from the Call Processor, the IP Phone changes the local prompts to match the specified language.

If a user configures the IP Phone language using the Telephone Options menu, the IP Phone sends a UNIStim Assign NI Language message to the Call Processor. The Call Processor then synchronizes the language with the IP Phone. The Call Processor 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 Processor, then the IP Phone uses the same language that is previously used.

The Call Processor determines the languages for which the IP Phone has fonts and font mappings. The Call Processor retrieves a list of language codes using the Display Manager Query Supported IT Languages.

Unicode Name Directory

The Unicode Name Directory supports the display of called or caller party name (CPND) in multiple languages on IP Phones that support Unicode. The Unicode Name Directory (UND) is integrated with the Personal Directory (PD), and is part of the PD installation.

You use Unicode Name Directory to:

- display localized names in UTF-8 Unicode character encoding for incoming and outgoing calls
- store up to seven localized names in the database for a subscriber
- support traditional and simplified Chinese, Korean, Japanese and other Unicode languages for called or caller party name display

Copyright © 2010 Nortel Networks. All Rights Reserved.

The content of UND is managed through Unicode Name Directory functionality in the Subscriber Manager (SM) application. This functionality provides the ability to provision localized names for each subscriber account. It also generates calling line IDs/URLs (CLID/URL) for each subscriber telephony account. All of this information is stored in Subscriber Manager for ease of access by all system elements. UND synchronizes with Subscriber Manager to obtain data. For more information about provisioning localized subscriber telephony accounts using Unicode Name Directory functionality in Subscriber Manager, see *Subscriber Manager Fundamentals* (NN43001-120).

Unicode Name Directory configuration

You can configure the Unicode Name Directory (UND) application using Element Manager (EM) on the member server where the UND application is installed, or from the CLI of the Call Processor. You can configure the UND only if the Personal Directory (PD) application is configured.

Configuration of the UND application consists of two steps:

- Enable the UND application.
- Schedule automatic synchronization of the Unicode Name Directory (UND) with the Subscriber Manager.

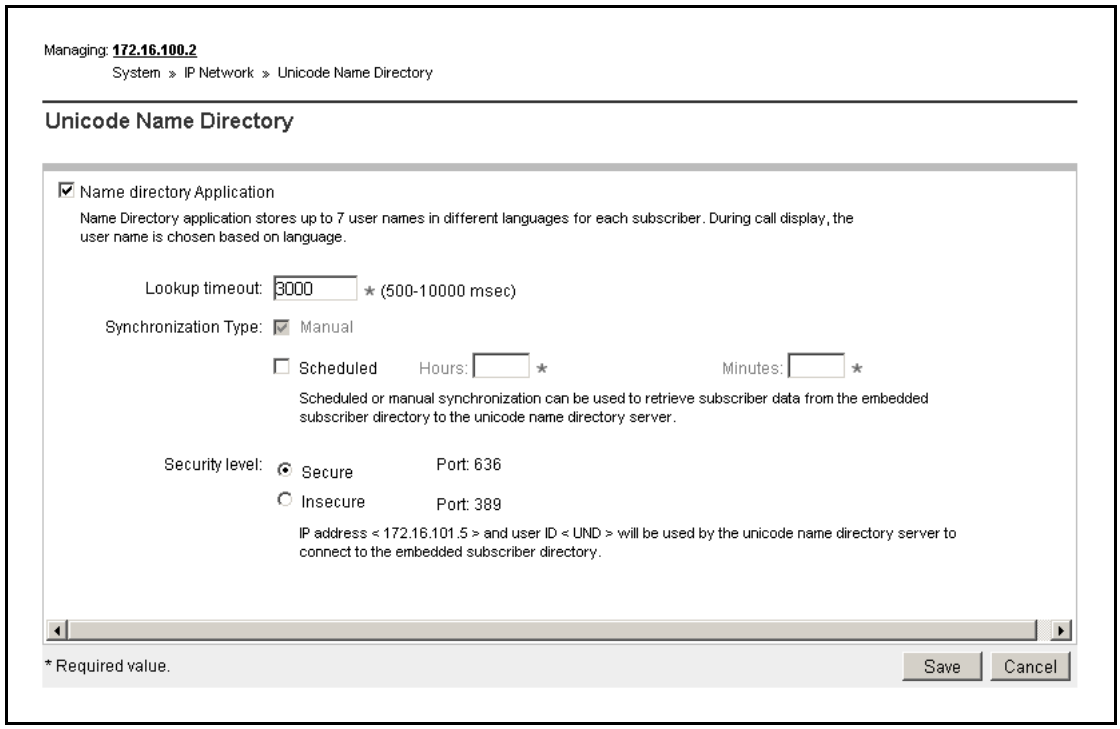
When you configure the UND application using EM, the scheduling parameters for the automatic synchronization of the UND data with the Subscriber Manager are retrieved from the UCM primary security server and used to populate the Unicode Name Directory web page.

For instructions to configure the UND using EM, see “Configuring the Unicode Name Directory using EM” (page 41) .

Procedure 1
Configuring the Unicode Name Directory using EM

Step	Action
1	Log on to Element Manager on the member server where the UND application is installed.
2	Choose **System, IP Network, Unicode Name Directory**. The Unicode Name Directory window appears.

Copyright © 2010 Nortel Networks. All Rights Reserved.



3 Select the **Name directory Application** check box to enable the PD/UND.

> ***Note:*** If the Personal Directory application is not configured, you are redirected to the **Server Configuration** option in the Personal Directory section of Element Manager. For information about the Personal Directory application and configuration, see "Personal Directory application" (page 157).

4 Enter a value in the **Lookup timeout** field.

This value is a time in milliseconds.

Allowed values are 500 to 10 000. The default value is 3 000.

5 Select a **Synchronization type**.

The **Manual** check box is always selected and cannot be cleared.

Select the **Scheduled** check box to schedule synchronizations of the UND data with the Subscriber Manager data.

6 Enter a value in the **Hours** field.

Valid values are 1 to 24.

7 Enter a value in the **Minutes** field.

Valid values are 0 to 59.

8 Select a **Security level** for the synchronization.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Enables or disables a secure SSL connection for the UND <-> Subscriber Manager synchronization.

Note: Insecure synchronization will not work when the UCM firewall rules prevent insecure connection.

9 Click **Save** .

10 The content of UND is managed through Unicode Name Directory functionality in the Subscriber Manager (SM) application. For detailed information about management, data migration, and configuration of numbering groups, refer to *Subscriber Manager Fundamentals* (NN43001-120).

--End--

Note: To synchronize the UND with the Subscriber Manager data, use the Linux shell command (**`nd ldapSync`**) on the member server to start a manual synchronization. Otherwise, the data will be synchronized at the scheduled time.

Unicode Name Directory synchronization

The PD/UND server retrieves user names and phone numbers from Subscriber Manager using the secure LDAP protocol. Entries in the PD/UND database that are associated with subscribers are updated for each subscriber. If the LDAP connection is lost during the synchronization, only those subscribers processed prior to the failure are updated (synchronized). The remaining entries are not updated. Start UND <-> Subscriber Manager synchronization by running the **`SYNC SYS`** command in LD 117.

PD/UND synchronization is initiated in one of three ways:

- Scheduled synchronization

  Synchronization is initiated automatically once a day at the specified time to retrieve data from Subscriber Manager.

  Note: Nortel recommends that you schedule synchronization for various PD/UND servers at different times to facilitate load balancing.

- Manual synchronization

  Synchronization can start manually from a Virtual Terminal (VT). VT starts from the Links, Virtual Terminal or System, IP Network, Maintenance and Reports section of EM, on the member server where the PD/UND application is configured.

  You can also use the Unicode Name Directory shell on the member server to start a manual synchronization using the following command:

Copyright © 2010 Nortel Networks. All Rights Reserved.

```
[nortel@und-pd ~]$ nd ldapSync
```

- UND application startup

Unicode Name Directory requirements for IP Phones

The Unicode Name Directory application requires that you configure a Calling or Called Party Name Display (CPND) block on the Call Processor for each customer in the CS 1000 system, to correctly display the calling or called party names on customer IP Phones. In addition, you must configure the CNDA and DNDA CoS on each IP Phone to properly display the calling or called party names.

Language selection on an IP Phone occurs through the Telephone Options, Language command, during initial configuration of the IP Phone, or as required.

Virtual Office interaction

Virtual Office logon can occur from an IP Phone that does not support Unicode, to an IP Phone with Unicode entries in the Personal Directory (PD) or the Unicode Name Directory (UND). <Unicode name> appears instead of the entry name.

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 that 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

Copyright © 2010 Nortel Networks. All Rights Reserved.

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	UFT-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, the IP Phone need not support Unicode.	

Output from the **`e2dsetShow()`** command shows the contents of all display lines, soft keys, feature keys (including feature keys on KEM and Expansion Module) and programmable line/DN keys associated with the IP Phone. This command is available only from the VxShell.

e2dsetShow ()

The **`e2dsetShow ()`** command expects a pointer to a DSET emulator, which you can obtain by running the **`dsetShow ()`** command.

Figure 2
dsetShow

```
TN   IP Address  Private IP Addr Hardware ID        Model Name     ItType   KEM    Emulator
---- ----------- ------------    -----------       -------------  ------   ---    --------
6144 192.168.29.8                180019e1e7016e662a IP Phone 1220   1220     0     0x09e581c8

value = 0x0 (0)
vxshell> tps e2dsetShow 0x09e581c8
 === SBI Data ===
isSBIset           0

Для отображения куков используется: cookieShowByTN

=== TPS ===

cookieShowByTN TN

Print the cookie list for a set specified by TN

e.g. cookieShowByTN "96 0 1 20"

=== TPS ===

Set cookies
-----------
Name                 Value
-------------------- --------------------
RingerVolume         1
CallerIDDisplay      0
ElapsedSecond        55
ElapsedMinute        58
ElapsedHour          0
ElapsedDay           18
ElapsedMonth         11
ElapsedYear          8
HandsfreeRxVolume    3
HandsetRxVolume      16
HomeVPNI             0
HomeZone             0
TN                   0x6144
CallState            IDLE
CustNo               0
VPNI                 0
Zone                 0
PrimeDN              86120

Total: 18 items
```

IP Phone Types

IP Phones Types provide the following functionality:

- unique TN types for existing IP Phone models
- special emulation mode for IP Phones that are not known to the TPS

Copyright © 2010 Nortel Networks. All Rights Reserved.

- automatic and manual IP Phone TN type conversion
- enhanced Model Names support is accessed from LD 20 and TM 4.0

Unique TN Types for existing IP Phone models

TN Types match the brand name of the IP Phone model. The following table identifies the TN_TYPE for each IP Phone model.

Table 11
TN Type naming convention

IP Phone model name	TN_TYPE
IP Phone 2001	2001P2
IP Phone 2002 Phase I	2002P1
IP Phone 2002 Phase II	2002P2
IP Phone 2004 Phase 0/I	2004P1
IP Phone 2004 Phase II	2004P2
IP Audio Conference Phone 2033	2033
IP Softphone 2050	2050PC
Mobile Voice Client 2050	2050MC
WLAN Handset 2210	2210
WLAN Handset 2211	2211
WLAN Handset 2212	2212
WLAN Handset 6120	6120
WLAN Handset 6140	6140
IP Phone 2007	2007
IP Phone 1110	1110
IP Phone 1120E	1120
IP Phone 1140E	1140
IP Phone 1150E	1150
IP Phone 1210	1210
IP Phone 1220	1220
IP Phone 1230	1230

Emulation Mode

During IP Phone registration, the LTPS determines the IP Phone TN Type (TN_TYPE) by looking up the User Interface capabilities (UI_TYPE) and Firmware ID (FW_ID) in a mapping table. The mapping table maps the

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 (CoS) for all IP Phones is configured in LD 11. Flexible Registration CoS can be 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 that have Flexible Registration Allowed (FRA), Flexible Registration on Upgrade (FRU), and Flexible Registration Denied (FRD) classes of service.

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

- If the TN has FRD CoS, the Call Server checks the IP Phone type against the TN type. Registration is rejected if the types do not match. The Call Server checks the Emulation Flag and blocks registration in the Emulation Mode.
- If the TN has FRA CoS, 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 FRU CoS, 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 CoS value becomes FRD. The Call Server checks the Emulation Flag and blocks registration in the Emulation Mode.

The <insert table link> lists groups of IP Phone types that can be converted or interchanged without losing configuration.

Table 12
IP Phone TN_TYPE groups

2004P1, 2004P2, 2210, 2211, 2212, 2007, 1140, 2050PC, 2050MC, 6140
2002P1, 2002P2, 1120, 1220, 6120
2001P2, 2033, 1110, 1210

Copyright © 2010 Nortel Networks. All Rights Reserved.

1230
1150

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 13
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, 1140,1150,1210, 1220,1230	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, 1140,1150,1210, 1220,1230	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.

- IP and IP/TDM calls survive LTPS ELAN subnet failures.

Copyright © 2010 Nortel Networks. All Rights Reserved.

- 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.

- For Call Server call processor types 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 run CS 1000 Release 4.5 or later.
- 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

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 resumes. If the user presses a key during the failover, the display clears and a localized "Server Unreachable" message appears.

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

You can have one LTPS supporting the ACF feature and one 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 remain 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 configured if

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

ACF scenarios

Table 14 "ACF behaviors" (page 50) describes ACF behavior in different scenarios.

Table 14
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 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

Copyright © 2010 Nortel Networks. All Rights Reserved.

Scenario	Result
• The IP Phones detect the lost connection and periodically try to re-register. • The TLAN subnet is up in 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.	following transitions: UNREGISTERED ->HALF-REGISTERED -> NO ACF
Signaling Server 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 lost connection and periodically try to re-register. • The LTPS node is up in 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.
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 cold 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Scenario	Result
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.
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 re-register with the secondary site. IP Phone A re-registers first.	The call is not lost. IP Phones can be configured in two 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

Copyright © 2010 Nortel Networks. All Rights Reserved.

Scenario	Result
	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 register 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 restarts. 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
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 restarts. 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 on to home TN before IP Phones A and B go offline.	IP Phone C cannot log on to the home TN if another active IP Phone is logged on to its TN. IP Phone C can log on to its home TN only when the call register is released or becomes PARTIAL REBUILT. See "Virtual Office login failure (scenario 1)" (page 53) and "Virtual Office login failure (scenario 2)" (page 53) .
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 restarts.	The call is not lost. The scenario is the same as if the far end were a local IP Phone.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Scenario	Result
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 restarts.	The call is not lost. The scenario is the same as if the far end were a local IP Phone.
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 restarts.	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 the branches in local mode.	The call is not lost. 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 restarts.	The call is not lost. The scenario is the same as "Network TLAN subnet failure" (page 53) . The call has the following transitions: NO ACF -> HALF REGISTERED -> UNREGISTERED.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Scenario	Result
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 restarts.	The call is not lost. The scenario is same as if the far end were a local IP Phone.
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 server as the TLAN subnet restarts.	The call is lost as the Call Server restarts.

After some failover scenarios (PARTIAL REBUILT calls), call modifications (for example, hold, conf, transfer) are not allowed. In this case localized string "Postfailure Limited Mode" appears when the user initiates call modification.

Firmware downloads

If the IP Phone has an active media stream, the LTPS does not request the firmware download to avoid resetting the IP Phone and losing the call. Therefore, a system can have IP Phones with a mixture of firmware versions registered. 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 the firmware supports UNIStim 2.9.

Operating parameters

IP Peer calls

IP Peer calls survive the following failure types:

- TLAN subnet failures.
- Signaling Server platform failures or restarts. When the Signaling Server restarts 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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

The zone bandwidth usage in the zone table remains zero for all IP Peer calls on this side; zone bandwidth usage is cleared for all calls as the Call Server restarts after the warm start. In this case, Network Bandwidth Management information is lost and the Call Server cannot restore the correct zone bandwidth usage for IP Peer calls.

IP/TDM calls

IP/TDM calls do not survive a Call Server cold start; all DSP channels are closed as the Call Server restarts 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.

Ringing calls 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 changed but no datadump occurred, the changes are lost if the Call Server fails.

SIP telephones

SIP telephones appear as IP Peer endpoints to the system. See “IP Peer calls” (page 55).

Copyright © 2010 Nortel Networks. All Rights Reserved.

NAT devices

The ACF feature cannot handle a NAT device changing the media path mapping between the IP Phone private address and public address during the failover period. No method exist 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 changes 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, then the held calls cannot be retrieved until after the firmware download finishes.

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

Copyright © 2010 Nortel Networks. All Rights Reserved.

Handsfree

In this scenario, IP Phone A has handsfree denied and IP Phone B has handsfree allowed. IP Phone A logs 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 the home TN (with handsfree disabled), handsfree 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 fails.

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 at 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 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 locally handles the Release, Onhook, and Mute events from IP Phone A in the Logged Out state.

Survivable Remote Gateway

The Survivable Remote Gateway (SRG) 1.0 and SRG 50 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 who uses 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. 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 did not fail or is not on the Signaling Server that restarts 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 restarts, the Converged Desktop call is affected.

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

The following are example scenarios.

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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 on 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 restarts before the IP Phone changes the call state (that is, releases the call), then the multimedia session is not affected.

If the IP Phone releases the call when the ELAN subnet is still down, the PCC status is updated 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 restarts and the Converged Desktop AML ELAN subnet link is enabled (the CSA104 message is output on the Call Server).

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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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, the following can occur:

- 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 off.

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

TPS failures do not affect general ACD functionality because the Call Server uses the ACD feature.

CS 1000 base features

No feature works when the active IP Phone disconnects and tries to re-register with the Call Server. All the features are available 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 if the Call Server fails.

The feature context is not lost on the Call Server if the TLAN/ELAN subnet fails. 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 if the Call Server fails (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 to dial 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 restarts 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 failure occurs and the active IP Phone has some features activated, the feature context and data is not lost on the Call Server. The user can use the feature after the IP Phone re-registers. Only the LTPS display is lost when the IP Phone re-registers.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Example: IP Phone A is in a call; the user presses the Transfer key and starts to dial 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 restarts 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.

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

If the LTPS or network fails, CDR continues. The CDR stops 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 if the Call Server fails and over-charged if the LTPS or network fails.

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 56) and Table 14 "ACF behaviors" (page 50).

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. You can restart the session by, for example, cold start, warm start, or ungraceful switchover.

During any failure, user input does not pass to CallPilot. The user must resume entering responses after the IP Phone re-registers.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 ACF 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 61).
  - — 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

MCS 5100

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

Installation and configuration

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

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

Configurable RUDP Time-out and Retries Count

When a network failure occurs and the IP Phone connection is lost, the IP Phone does not instantly start the failover. The IP Phone waits for a period of time for a reply from the server (the length of time is the value of RUDP timeout in milliseconds). 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 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.

You can configure the time-out and number of retries in the Linux shell of the Signaling Server. See Table 15 "RUDP Timeout and Retries Count commands" (page 64).

Table 15
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, you can increase the values to prevent the IP Phones from being reset due to significant network delay.	

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 15
RUDP Timeout and Retries Count commands (cont'd.)

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, you can increase the values to prevent the IP Phones from being reset due to significant network delay.	

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. When a supported IP Phone registers with the Signaling Server, the IP Phone downloads the new values.

You must configure these values on every Signaling Server 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 telephone 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 occurs 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

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 occurs 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. 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 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 passes to the far-end telephone involved in the HREG, HREB, and PREB calls. This means that any features that involve both parties do not work with such calls.

REB
The ACF call is REBUILT (REB). 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>
```

<status> is

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

<timer> is

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

Copyright © 2010 Nortel Networks. All Rights Reserved.

See Figure 3 "LD 32 STAT output with ACF example" (page 67).

Figure 3
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>
```

<status> is

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

<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 4 "LD 80 TRAC with ACF example" (page 68) is a sample output for IP Phones involved in UNREGISTERED and PARTIAL-REBUILT calls.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 4
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_PM  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_PM  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 subcommand **ACF** is added to the existing LD 117 STIP command.

Table 16
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

Copyright © 2010 Nortel Networks. All Rights Reserved.

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

Output

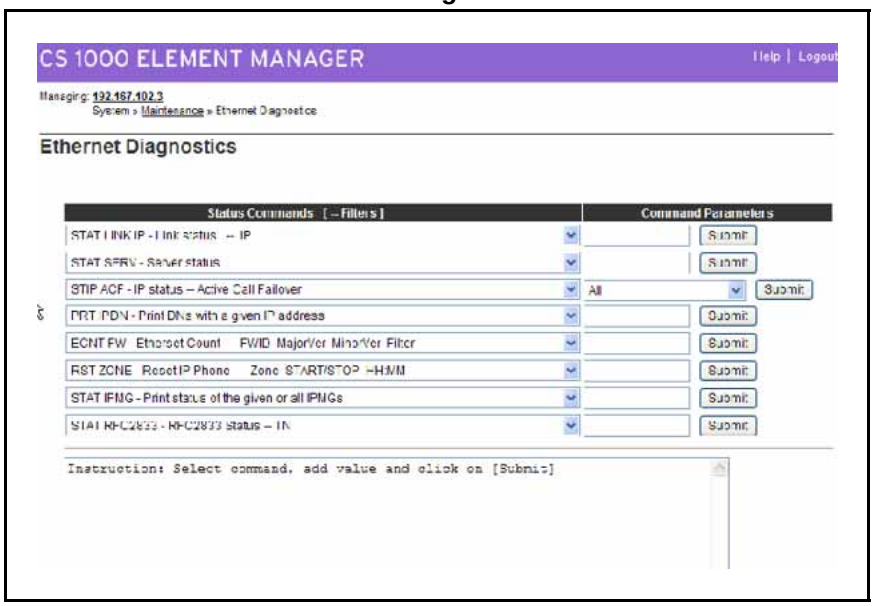
The output is similar to the existing LD 117 STIP output, with the addition of a column titled ACF STATUS. If the call is in an inactive state, the value of the Call Server ACF timer follows that status, separated by a colon (:).

LD 117 STIP ACF in Element Manager

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

Figure 5 "LD 117 STIP ACF in Element Manager" (page 69) illustrates the placement of the **STIP ACF** command with the other STIP commands.

Figure 5
LD 117 STIP ACF in Element Manager



A list of command parameters are available after you select the STIP ACF command. The ALL command parameter is the default.

Click the Submit button after you select an available parameters to run the command. The output appears in the box in the lower portion of the Web page.

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

Copyright © 2010 Nortel Networks. All Rights Reserved.

DSP peg counter for CS 1000E systems

Digital Signaling Processor (DSP) resources residing on a Voice Gateway Media Card in the IP Media Gateway (IPMG) of a CS 1000E system convert TDM voice to IP packets. The Voice Gateway Media Cards have a limited number of DSP resources that perform the conversion. When all DSP resources are busy, IP-to-TDM calls and TDM-to-TDM calls between 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

Firmware files are stored on and are downloaded from the Signaling Server.

The Enhanced UNIStim Firmware Download for IP Phones provides a method of delivering new firmware for Nortel IP Phones.

Specifically, this feature provides 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.
- Maintenance Mode for the Signaling Server that allows simultaneous firmware downloads from the UFTP server. The administrator manually initiates Maintenance Mode (Turbo Mode) in which premarked node Signaling Servers use all possible resources for processing firmware upgrade jobs.

Copyright © 2010 Nortel Networks. All Rights Reserved.

- Identification of the registered IP Phones using string names and providing detailed identification of IP Phones that register in Emulation Mode.
- UNIStim IP Phones can register with a previous version of firmware if the UFTP servers are busy, and then periodically offer 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, models, and firmware.

Operating parameters

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

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

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

- Supports only firmware downloads performed by the UFTP server to the UNIStim IP Phones that support the UFTP download protocol.
- Enhanced functionality is provided only if the recommended commands are used. For example, using the shell **`cp`** 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 most recent firmware, or perform any automatic comparisons and update operations. The Branch Office LTPS receives firmware files only 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

The Active Call Failover scenario is the same as the postponed firmware upgrade scenario described in Table 21 "IP Phone registration and download scenarios" (page 75). 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 48).

System view

IP Phone firmware upgrades

Each IP Phone that registers with the LTPS is queried for the firmware ID and IT_TYPE. The system response depends on the results of the query. See Table 17 "System response" (page 72).

Table 17
System response

Query result	Response
LTPS software supports the reported IT_TYPE (see Table 18 "Supported IT_TYPES" (page 73)) and the Upgrade Manager has firmware for the firmware ID.	Registration of the IP Phone continues. The IP Phone firmware upgrade occurs if possible.
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.	Registration of the IP Phone continues with no firmware download.

Firmware file management

To manage available firmware, the following information is collected about each firmware file on the Signaling Server:

- firmware ID
- firmware version
- applicable IT_TYPE (see Table 18 "Supported IT_TYPES" (page 73))
- applicable model names

IT_TYPEs

Table 18 "Supported IT_TYPES" (page 73) lists the IT_TYPES supported by the Upgrade Manager for CS 1000 Release 5.5

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 18
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
0x08	IP Phone 1210
0x09	IP Phone 1220
0x0B	IP Phone 1230

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

1. LTPS restart
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 the 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 the firmware can be downloaded.

Firmware file names

Firmware file names are originally in the format SSFFYxx.bin. See Table 19 "Original firmware file name format" (page 73).

Table 19
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, IP Phone 2002, IP Phone 2004

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 19
Original firmware file name format (cont'd.)

Designator	Definition	Values
Y	Alphabetic character	A – 0 B – 1 C – 2 D – 3 (and so on)
XX	Release number	Two-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 xFF.fw:
  - **x** emphasizes that FF is a hexadecimal number
  - **FF** is the firmware ID for the file

Table 20
Firmware file naming conventions

x00.fw	IP Phone 2004 Phase 0/1
x00.fw	IP Phone 2002 Phase 1
x02.fw	IP Phone 2004 Phase 2
x02.fw	IP Phone 2002 Phase 2
x02.fw	IP Phone 2001 Phase 2
x10.fw	IP Phone 2033 (Conference Phone)
x21.fw	IP Phone 2007 Phase 2
x23.fw	IP Phone 1110
x24.fw	IP Phone 1120E
x25.fw	IP Phone 1140E
x27.fw	IP Phone 1150E
x2A.fw	IP Phone 1200

The xFF.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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Download maximums

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

- The default number of allowed simultaneous downloads is 50.
- Maintenance Mode (Turbo Mode) that the administrator manually initiates is available in which premarked node Signaling Servers use all possible resources to process firmware upgrades. The following commands are used to manage the Maintenance Mode:

  — uftpTurboMode

  — uftpTurboModeTimeoutSet

  — uftpTurboModeShow

  The uftpTurboMode command is used 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 22 "Maintenance Mode commands" (page 78).

  For more information about Maintenance Mode, see “Maintenance Mode” (page 77).

Immediate and delayed firmware downloads

The IP Phones display various messages to indicate the status of IP Phone registration and firmware downloads. Table 21 "IP Phone registration and download scenarios" (page 75) lists some scenario examples with the resulting IP Phone information.

Table 21
IP Phone registration and download scenarios

Scenario	Result
Normal firmware download for known IP Phone type	The IP Phone is connecting to the LTPS. The firmware download starts. If download is successful, IP Phone continues with normal registration.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 21
IP Phone registration and download scenarios (cont'd.)

Scenario	Result
Postponed firmware upgrade	The IP Phone is connecting to the LTPS. IP Phone cannot download firmware. It can proceed with registration using old firmware. At the completion of call (if download resources are available), IP Phone displays "Upgrade F/W now?" IP Phone displays Yes and No soft keys to use to select choice. If you select **Yes** , the firmware download begins. If you choose nothing, the IP Phone downloads the firmware after the timer expires. If you select No, the 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	The IP Phone is connecting to the LTPS. No firmware upgrade occurs, but the IP Phone can register.
Unknown IT_TYPE	IP Phone has no display. The IP Phone resets continuously. IP Phone registration is not allowed. Log message is sent to LTPS administrator.
Branch Office LTPS determines IP Phone requires firmware upgrade	The firmware download is initiated. The IP Phone is placed into local mode. The message appears until firmware is downloaded. The IP Phone upgrade starts.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 21
IP Phone registration and download scenarios (cont'd.)

Scenario	Result
	If firmware download is unsuccessful after 10 retries, the IP Phone remains in local mode.

Note: When you issue the umsUpgradeAll command on TPS all IP phones (with "old" Firmware) are restarted and try to upgrade to the new firmware. However, if TPS is not in maintenance mode and doesn't have enough resources to start a firmware upgrade then some IP Phones might be registered with "old" firmware. Please refer to "Postponed firmware upgrade" section in the table "IP Phone registration and download scenarios". If TPS is in maintenance mode, umsUpgradeAll upgrades all IP phones. If there are not enough resources for upgrade, then IP Phone will be put in pending queue and upgraded as soon as TPS has CPU resources to proceed.

Maintenance Mode

Maintenance Mode enables the UFTP server to use most of the processing resources to handle the downloads.

The actual number of simultaneous downloads is determined by measuring the CPU idle time, so each new firmware download session starts if there are less than 50 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 percent
- Signaling Server is in Maintenance Mode and its CPU usage is less than 100 percent

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

ATTENTION
When Maintenance Mode is enabled, UFTP download process can affect call processing signaling.

Maintenance Mode 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 starts
  This prevents a time-out while the system is configured and the downloads start. After a download starts, if MM minutes pass

Copyright © 2010 Nortel Networks. All Rights Reserved.

with no new firmware upgrade jobs starting, the normal mode of operation resumes. Configure the idle timeout timer 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 is available only on the Signaling Server. Maintenance Mode affects only Signaling Servers designated for Maintenance Mode. Some Signaling Servers in the node can 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 restarted. Firmware downloads do not affect Call processing for Signaling Servers operating in normal mode.

  Firmware upgrades are postponed when at least one Signaling Server is in Maintenance Mode.

Table 22 "Maintenance Mode commands" (page 78) lists the commands used for Maintenance Mode.

Table 22
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

Copyright © 2010 Nortel Networks. All Rights Reserved.

Command	Description
	If you enter no parameter, Upgrade Manager uses 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 starts before returning the Signaling Server to normal mode If this parameter is 0 (zero), the Upgrade Manager never exits Maintenance Mode unless the **umsUpgradeModeSet** command is issued with the "stop" parameter. If you enter no parameter, then the current timeout setting appears.
uftpTurboModeShow	Displays current status of Maintenance Mode.

The following is an example of output when Maintenance Mode is to start at 11:00 p.m.

```
uftpTurboMode "23:00"
```

The log file /var/log/nortel/ss_common.log will contain the following record:

```
Mar 31 02:53:12 si-linux tps:  (INFO) tUMS: F/W download Turbo
Mode is scheduled for 23:00.  Will run after 408 seconds
```

Call Server commands

LD 20

A response ISET is introduced to the LD 20 TYPE prompt. When you enter ISET, the prompt MODEL_NAME appears. The MODEL_NAME prompt allows you to specify the Short Model Name mnemonic to filter TN block output. If you use only the ISET response, printed TN blocks contain the long IP Phone Model Name.

Table 23
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	ISET	Enable filtering by IP Phone model name.
...	...	
MODEL_NAME	xxxxxx	IP Phone model (for example, 2004P2).
...	...	

Copyright © 2010 Nortel Networks. All Rights Reserved.

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
```


Copyright © 2010 Nortel Networks. All Rights Reserved.

```
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 RCBD
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 CCBD RTDD RBDD RBHD PGND FLXD FTTC DNDY DNO3 MCBN
FDSD NOVD 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
```


Copyright © 2010 Nortel Networks. All Rights Reserved.

```
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 24 "LD 117 commands" (page 83).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 24
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>.
STIP MODL <MMMM>	Displays information from the RLM for all IP Phones of the specified model, where: MMMM = IP Phone model If you omit the <MMMM> parameter, a table of existing model names and associated mnemonics appears.
RST ZONE <ZoneNumber>	Immediately hard-resets all IP Phones, where: ZoneNumber = zone number

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 24
LD 117 commands (cont'd.)

Command	Description
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 you omit the last parameter, then IP Phones 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 resets prints.
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 you select START and you omit the last parameter, then IP Phones reset immediately. <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 prints.

LTPS CLI commands

LTPS CLI commands are as follows:

- firmwareFileGet
- uftpAutoUpgradeTimeoutSet
- isetFWShow

See Table 25 "LTPS CLI commands" (page 85).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 25
LTPS CLI commands

Command	Description
firmwareFileGet "ServerIP", "UserID", "Password", "/path/to/file", "file name" ProtocolID	Uploads 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 a valid firmware file, the UMS database is updated accordingly. ServerIP: FTP server IP address to download the firmware from 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) file name: name of the firmware file on the FTP server Use the firmwareFileGet command instead of firmwareFileGetI2004, firmwareFileGetI2002, and firmwareFileGetIPP2. ProtocolID: 0 - FTP protocol; 1 - SFTP protocol. ProtocolID is optional. SFTP is used by default.
uftpAutoUpgradeTimeoutSet <MM>	Configures the length of time the IP Phone waits for a user response after "Upgrade F/W now?" appears 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 prints.
isetFWShow	Displays the status of IP Phones firmware.

firmwareFileGet example

```
firmwareFileGet "192.168.0.1","admin1","0000
"/var/opt/nortel/tps/fw"
```

firmwareFilePut example

```
firmwareFilePut "192.168.0.1","admin1","0000
"/var/opt/nortel/tps/fw"
```


Copyright © 2010 Nortel Networks. All Rights Reserved.

uftpAutoUpgradeTimeoutSet output example

```
uftpAutoUpgradeTimeoutSet 4
Log file /var/log/nortel/ss_common.log will contain the
following line:  Mar 31 02:53:12 si-linux tps:  (INFO) tUMS: New
value of auto F/W upgrade timeout is 240 seconds.
uftpAutoUpgradeTimeoutSet
Log file /var/log/nortel/ss_common.log will contain the
following line:  Mar 31 02:53:12 si-linux tps:  (INFO) tUMS:
Current value of auto F/W upgrade timeout is 240 seconds.
```

isetFWShow output example

```
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
```

LTPS CLI commands

The output for the following commands prints IP Phone model name (long or short), firmware ID, firmware version:

- uftpShow
- umsPolicyShow
- isetGet

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

uftpShow output example

The output displays the IP Phone Model Name, firmware ID, and firmware version in ABB format.

Copyright © 2010 Nortel Networks. All Rights Reserved.

```
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 displays the IP Phone Model Name, firmware ID, and firmware version in ABB format.

```
[nortel@si-linux ~]$ umsPolicyShow
 === TPS ===

Total policies = 1

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

Available firmware:

FW ID  FWVsn  Model                          Policy Name   File name
-----  -----  -----------------------------  ------------  --------------------------------

0x00   B76    IP Phone 2004 Phase 0/1         DEFAULT       /var/opt/nortel/tps/fw/x00.fw
0x00   B76    IP Phone 2002 Phase 1           DEFAULT       /var/opt/nortel/tps/fw/x01.fw
0x02   DCG    IP Phone 2004 Phase 2           DEFAULT       /var/opt/nortel/tps/fw/x02.fw
0x02   DCG    IP Phone 2002 Phase 2           DEFAULT       /var/opt/nortel/tps/fw/x02.fw
0x02   DCG    IP Phone 2001 Phase 2           DEFAULT       /var/opt/nortel/tps/fw/x02.fw
0x10   S74    IP Audio Conference Phone 2033  DEFAULT       /var/opt/nortel/tps/fw/x10.fw
0x21   C6H    IP Phone 2007 Phase 2           DEFAULT       /var/opt/nortel/tps/fw/x21.fw
0x23   C6J    IP Phone 1110                   DEFAULT       /var/opt/nortel/tps/fw/x23.fw
0x24   C6J    IP Phone 1120E                  DEFAULT       /var/opt/nortel/tps/fw/x24.fw
0x25   C6J    IP Phone 1140E                  DEFAULT       /var/opt/nortel/tps/fw/x25.fw
0x27   C6J    IP Phone 1150E                  DEFAULT       /var/opt/nortel/tps/fw/x27.fw
0x2a   C6J    IP Phone 1210                   DEFAULT       /var/opt/nortel/tps/fw/x2A.fw
0x2a   C6J    IP Phone 1220                   DEFAULT       /var/opt/nortel/tps/fw/x2A.fw
0x2a   C6J    IP Phone 1230                   DEFAULT       /var/opt/nortel/tps/fw/x2A.fw

Total firmware = 10
```

isetGet output

The output displays the IP Phone Model Name and firmware version in ABB format.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Element Manager

To support the Enhanced UNIStim Firmware Download for IP Phones feature, Element Manager provides the following functions:

- 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.
- An interface to initiate or obtain the status for the firmware download Maintenance Mode using the CLI commands **`uftpTurboMode`**, **`uftpTurboModeShow`**, and **`uftpTurboModeTimeoutSet`**.

  The uftpTurboMode CLI commands are used with the RST FW and RST ZONE commands.
- An interface to reset IP Phones by firmware ID and zone using the LD 117 commands **`RST FW`** and **`RST ZONE`**.

  See Table 22 "Maintenance Mode commands" (page 78) for a description of LD 117 commands.
- Output of either ECNT MODL is parsed to obtain the list of available IP Phone models. Use this output to allow a user to transparently specify the model name; that is, Element Manager replaces the actual model name with associated mnemonic.
- An interface to display the output of the LD 117 commands ECNT MODEL, ECNT FW, ECNT PEC, STIP MODL, and STIP FW.
- Management of the compatibility matrix of various 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 and IP Phone firmware” (page 264).

Ethernet Diagnostics in Element Manager

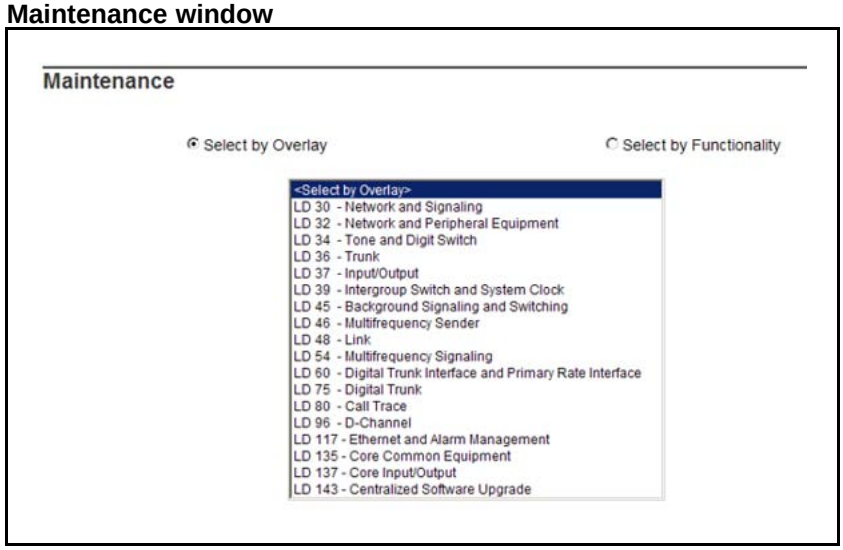
To access Ethernet Diagnostics in Element Manager, perform the steps in Procedure 2 “Accessing Ethernet Diagnostics in Element Manager” (page 89).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Procedure 2
Accessing Ethernet Diagnostics in Element Manager

Step	Action
1	In the Element Manager navigator, select **System, Maintenance**. The Maintenance window appears. See Figure 6 "Maintenance window" (page 89).

Figure 6
Maintenance window



By default, **Select by Overlay** 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 7 "Ethernet Diagnostics window" (page 90). Alternatively, select **Select by Functionality**. Select **Ethernet Diagnostics** from the **<Select by Functionality>** list. See Figure 8 "Select by Functionality list" (page 90). The Ethernet Diagnostics window appears.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 7
Ethernet Diagnostics window

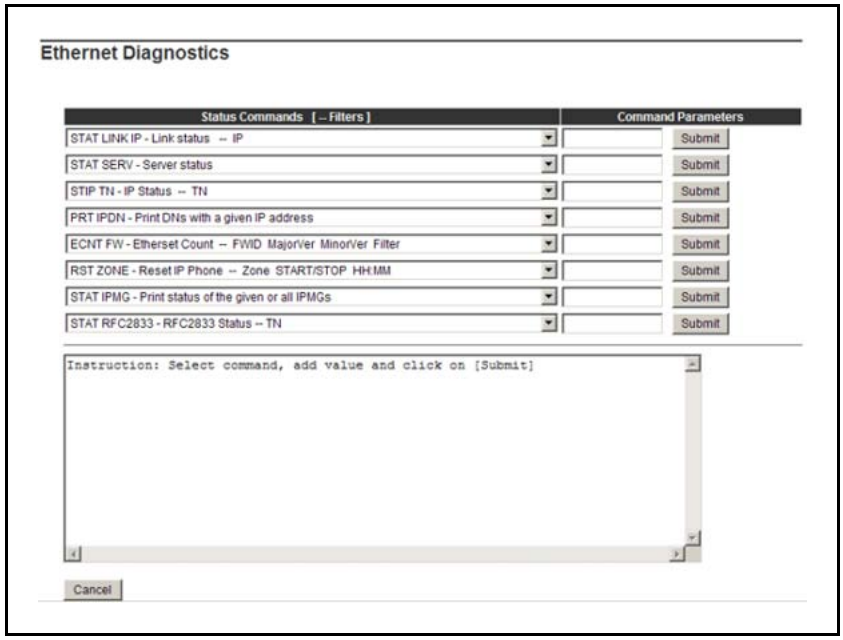
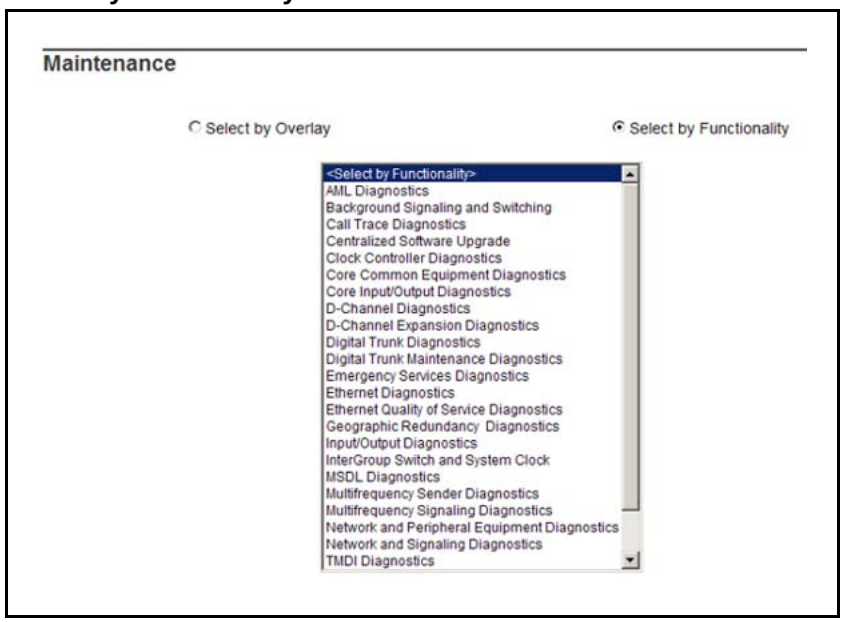


Figure 8
Select by Functionality list



--End--

For more information about the LD 117 commands, see “LD 117” (page 82).

Copyright © 2010 Nortel Networks. All Rights Reserved.

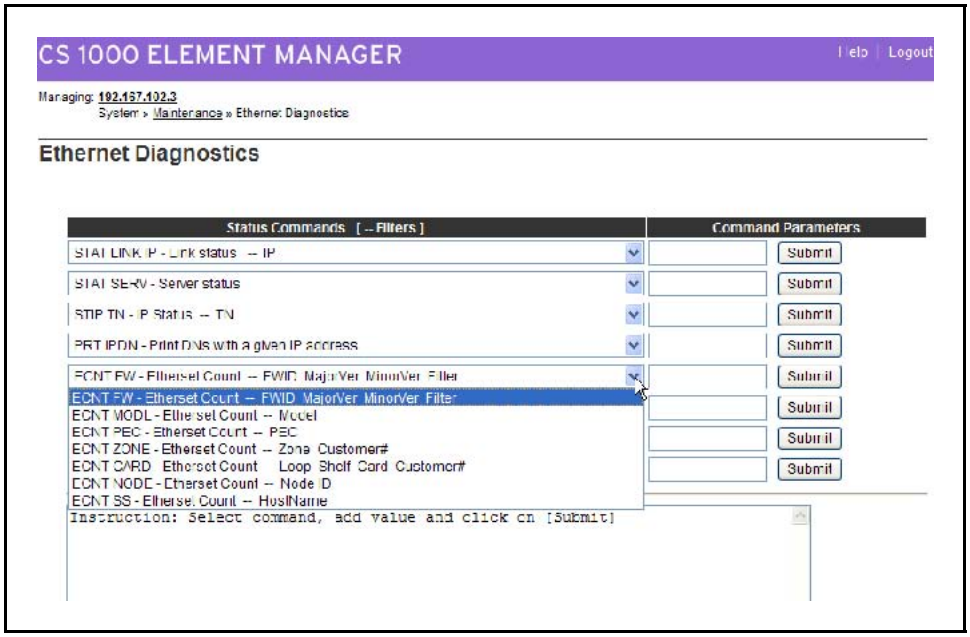
ECNT commands

The following commands are available in LD 117 under ECNT in the Status Command list. See Figure 9 "ECNT commands" (page 91).

- 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 9
ECNT commands

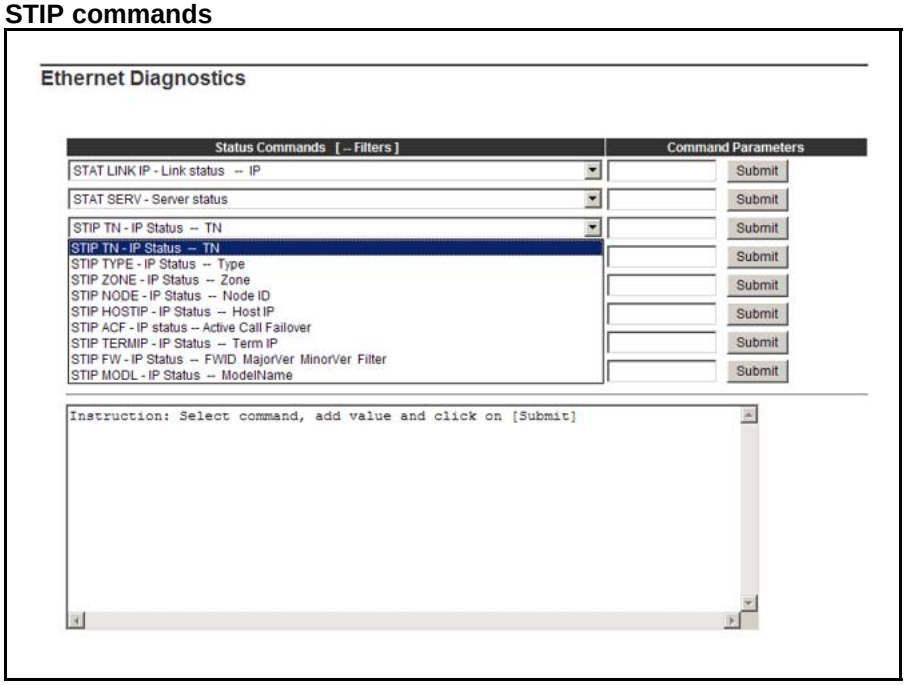


STIP commands

STIP MODL and STIP FW are listed in the STIP commands in the Status Command list. See Figure 10 "STIP commands" (page 92).

Copyright © 2010 Nortel Networks. All Rights Reserved.

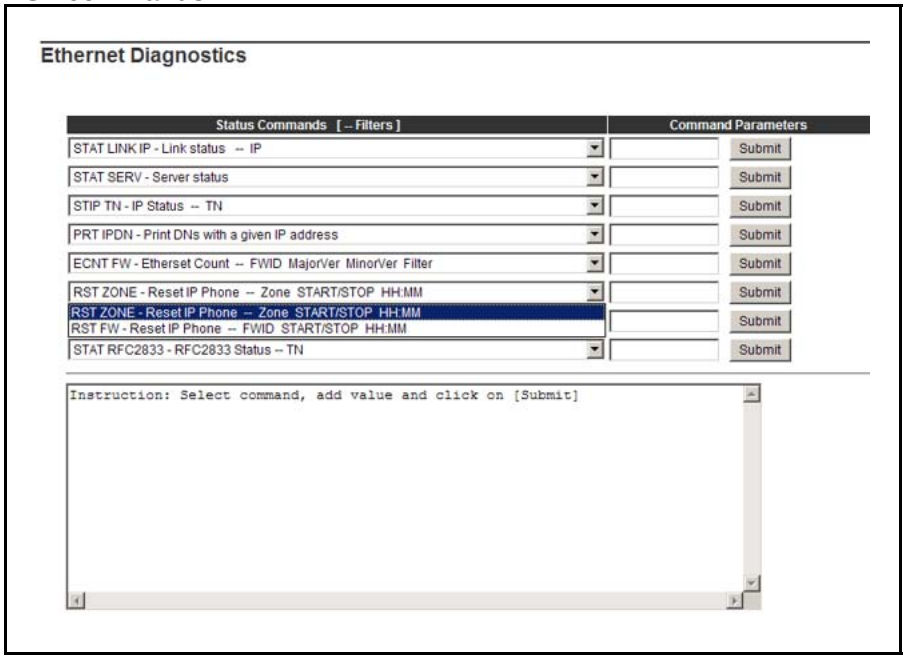
Figure 10
STIP commands



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 11 "RST commands" (page 92).

Figure 11
RST commands



Copyright © 2010 Nortel Networks. All Rights Reserved.

Maintenance Mode commands in Element Manager

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

- uftpTurboMode
- uftpTurboModeShow
- uftpTurboModeTimeoutSet
- uftpAutoUpgradeTimeoutSet

uftpTurboMode

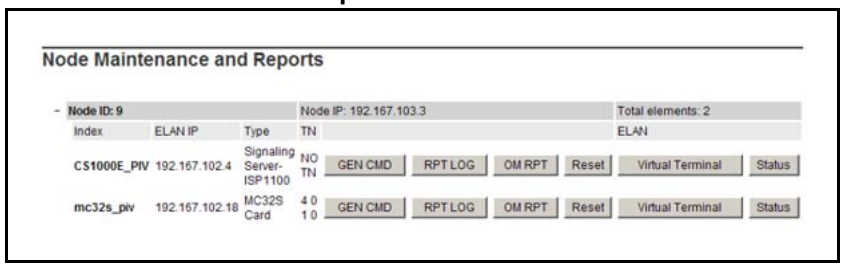
Use the uftpTurboMode command to designate one or more Signaling Servers for firmware upgrade Maintenance Mode, or to schedule Maintenance Mode on the designated Signaling Server to either start immediately or at a specific time. See Figure 14 "uftpTurboMode window in Element Manager" (page 94).

To access the uftpTurboMode command, perfrom the steps in Procedure 3 “Accessing the uftpTurboMode command” (page 93).

Procedure 3
Accessing the uftpTurboMode command

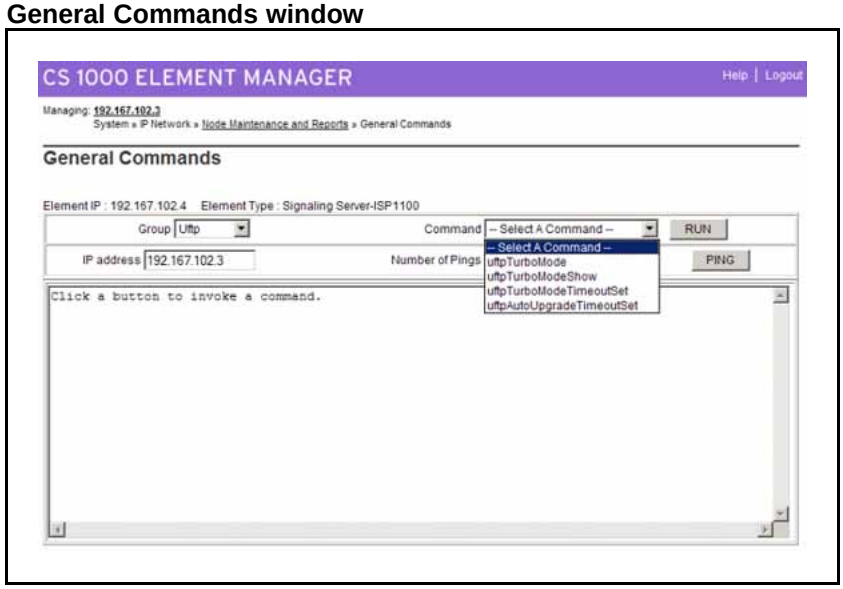
Step	Action
1	In the navigator, select **IP Network, Maintenance and Reports**. The Node Maintenance and Reports window appears. See Figure 12 "Node Maintenance and Reports window" (page 93).
2	Click the plus sign (+) to the left of the Node ID of the desired node to view the node elements.
3	Click **GEN CMD** for a Signaling Server. The General Commands window appears. See Figure 13 "General Commands window" (page 94).

Figure 12
Node Maintenance and Reports window



Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 13
General Commands window

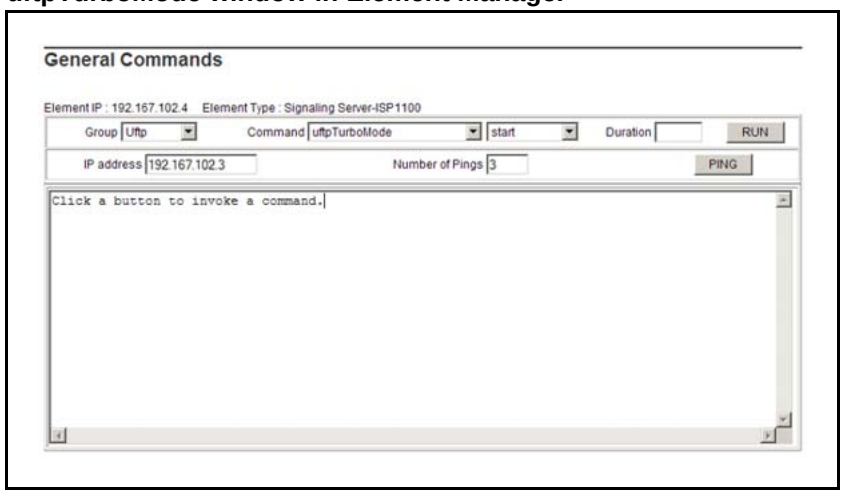


4 From the **Group** list, select **uftp**.

5 From the **Command** list, **uftpTurboMode**.

6 If you select **HH:MM** , enter the time in the Hours and Minutes boxes. No other option requires parameters.

Figure 14
uftpTurboMode window in Element Manager



7 Click **Run**.

The command output appears in the pane below the command.

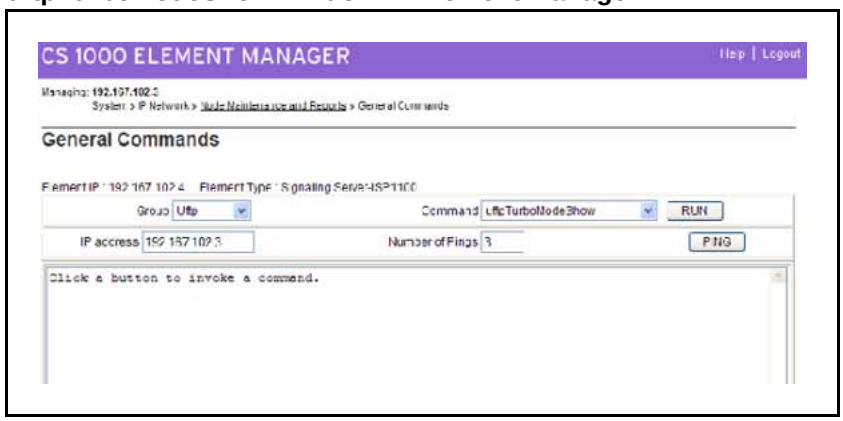
--End--

uftpTurboModeShow

Copyright © 2010 Nortel Networks. All Rights Reserved.

The uftpTurboModeShow command displays the current status of Maintenance Mode (None, Active, or Scheduled). To access the uftpTurboModeShow command using Element Manager, perform the steps in Procedure 4 “Accessing the uftpTurboModeShow command” (page 95).

Procedure 4
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 12 "Node Maintenance and Reports window" (page 93).
2	Click the plus sign (+) to the left of the Node ID of the desired node to view the node elements.
3	Click **GEN CMD** for the desired Signaling Server. The General Commands window appears. See Figure 13 "General Commands window" (page 94).
4	From the **Group** list, select **uftp**.
5	From the **Command** list, select **uftpTurboModeShow**. See Figure 15 "uftpTurboModeShow window in Element Manager" (page 95). **Figure 15** **uftpTurboModeShow window in Element Manager**  The command output appears in the pane below the command.
6	Click **Run**.

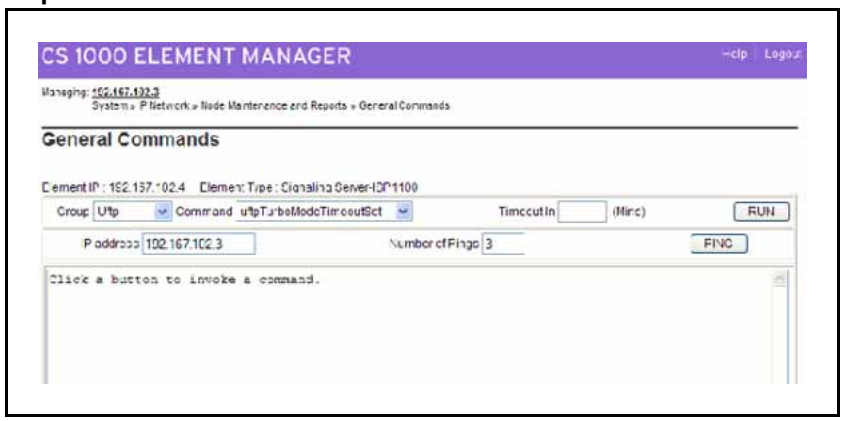
--End--

uftpTurboModeTimeoutSet

Copyright © 2010 Nortel Networks. All Rights Reserved.

The uftpTurboModeTimeoutSet command configures the idle timer for Maintenance Mode. To access the uftpTurboModeTimeoutSet command using Element Manager, follow Procedure 5 “Accessing uftpTurboModeTimeoutSet command ” (page 96).

Procedure 5
Accessing uftpTurboModeTimeoutSet command

Step	Action
1	In the navigator, select **IP Network, Maintenance and Reports**. The Node Maintenance and Reports window appears.
2	Click the plus sign (+) to the left of the Node ID of the desired node to view the node elements.
3	Click **GEN CMD** for a Signaling Server. The General Commands window appears. See Figure 13 "General Commands window" (page 94).
4	From the **Group** list, select **uftp**.
5	From the **Command** list, select **uftpTurboModeTimeoutSet**. See Figure 16 "uftpTurboModeTimeoutSet window" (page 96). This command accepts the MM parameter. **Figure 16** **uftpTurboModeTimeoutSet window** 
6	Enter the time in minutes in the **Timeout In** box.
7	Click **Run**. The command output appears in the pane below the command.

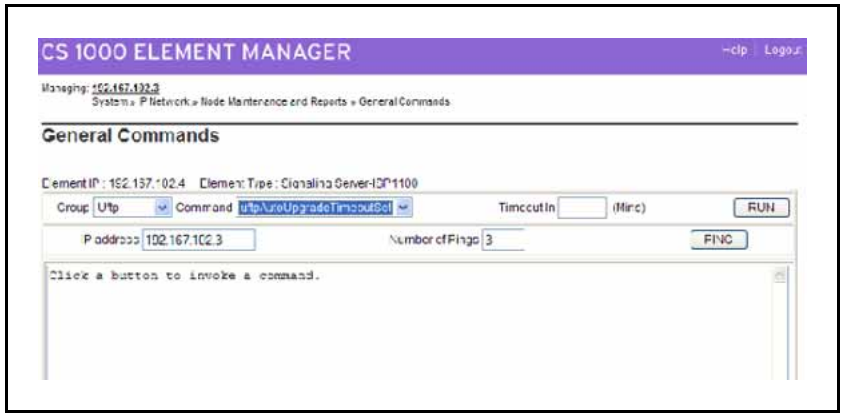
--End--

uftpAutoUpgradeTimeoutSet

Copyright © 2010 Nortel Networks. All Rights Reserved.

The uftpAutoUpgradeTimeoutSet command configures the idle timer for starting the firmware download. To access the uftpAutoUpgradeTimeoutSet command using Element Manager, follow Procedure 6 “Accessing uftpAutoUpgradeTimeoutSet command” (page 97).

Procedure 6
Accessing uftpAutoUpgradeTimeoutSet command

Step	Action
1	In the navigator, select **IP Network, Maintenance and Reports**. The Node Maintenance and Reports window appears.
2	Click the plus sign (+) to the left of the Node ID of the desired node to view the node elements.
3	Click **GEN CMD** for a Signaling Server. The General Commands window appears. See Figure 13 "General Commands window" (page 94).
4	From the **Group** list, select **uftp**.
5	From the **Command** list, select **uftpAutoUpgradeTimeoutSet**. See Figure 17 "uftpAutoUpgradeTimeoutSet window in Element Manager" (page 97). This command accepts the MM parameter. **Figure 17** **uftpAutoUpgradeTimeoutSet window in Element Manager** 
6	Enter the time in minutes in the **Timeout In** box.
7	Click **Run**. The command output appears in the pane below the command.

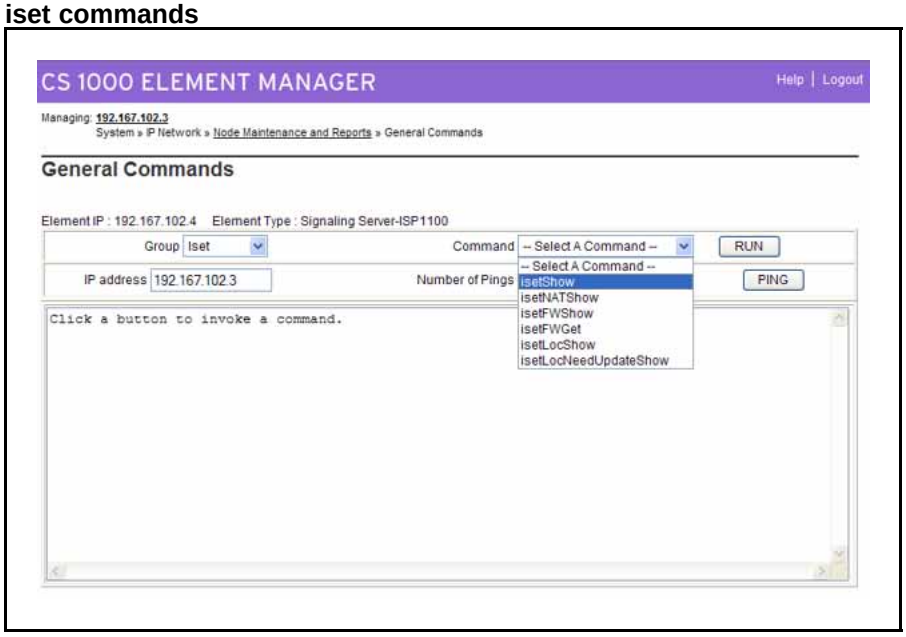
--End--

Copyright © 2010 Nortel Networks. All Rights Reserved.

iset commands in Element Manager

Access **isetFWShow** in the General Commands window from the iset group in the **Group** list. See Figure 18 "iset commands" (page 98).

Figure 18
iset commands



Firmware download using UNIStim FTP

Previously, IP Phones on CS 1000 systems downloaded firmware using Trivial File Transfer Protocol (TFTP). Firewalls often have the 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.

To eliminate the file transfer problem with the firewalls and TFTP, a UNIStim 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 the firewall security by closing port 69 to block TFTP in the firewall and policy-based switches and routers.

ATTENTION
For the UFTP IP Phone firmware download to work, you must explicitly open port 5100 (UNIStim signaling) and port 5105 (UFTP signaling).

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

Copyright © 2010 Nortel Networks. All Rights Reserved.

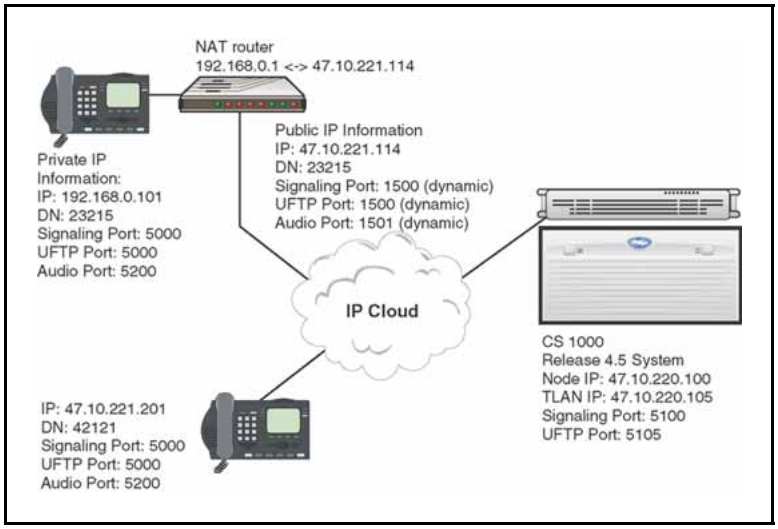
download messages to travel through the firewall. Firewalls can safely enable both ports. See Table 26 "Source and destination port usage on either side of the connection" (page 99).

Table 26
Source and 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 19 "Using NAT with UFTP" (page 99).

Figure 19
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 the Signaling Server, the log files are in the /var/log/nortel/ folder. The Download log files are limited to 400 K each, for a total of 800 K. Approximately 5 000 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 startup of the UFTP Server task, new Download log files are created.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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:

- Firmware download date
- Firmware download start time
- Firmware download status (specifies if the download succeeded or failed)
- IP Address of the IP Phone
- IP Phone type
- Firmware download error code. If the Firmware 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 corrupt
  - 03 = RUDP connection down
  - 04 = Response time out
  - 05 = Reason: Unknown

The format of the download log message is as follows:

<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

Copyright © 2010 Nortel Networks. All Rights Reserved.

uftpNodeShow

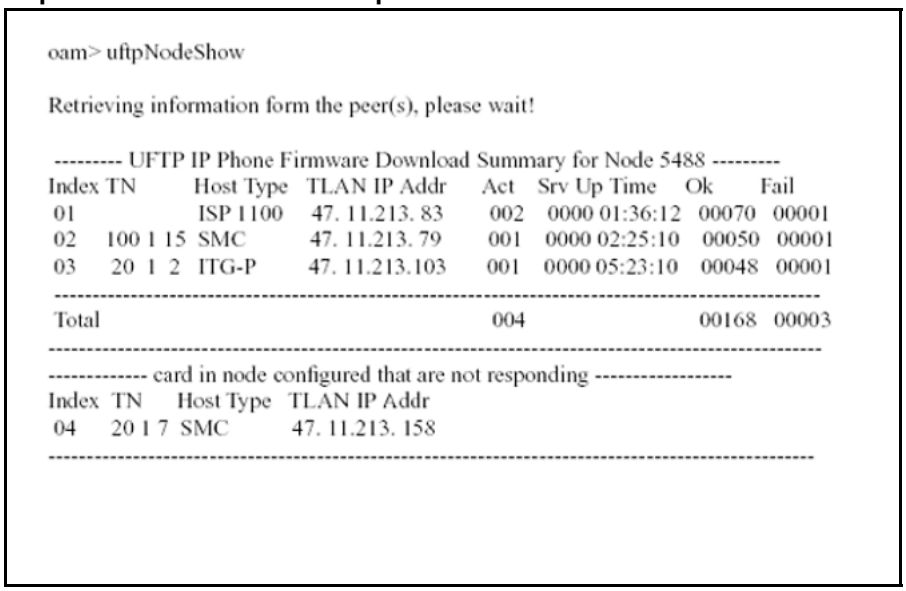
The **uftpNodeShow** command provides a complete UFTP IP Phone firmware download summary of each node. This includes the configured cards in the node that are not responding.

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 20 "uftpNodeShow command output" (page 101) is an example of output from the **uftpNodeShow** command.

Figure 20
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
-------------------------------------------------------------------------------------
```


Copyright © 2010 Nortel Networks. All Rights Reserved.

uftpShow

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

- configuration information about UFTP
- count of successful downloads because the Signaling Server restarted
- count of downloads that failed or prematurely ended because the Signaling Server restarted
- number of active downloads, and a list of each, including the following information:
  - type of IP Phone
  - IP addresses of the IP Phones that downloaded firmware
  - number of bytes downloaded

Figure 21 "uftpShow command output" (page 102) is an example of output from the **uftpShow** command.

Figure 21
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]
---------- ----------------- ------------------
```


Copyright © 2010 Nortel Networks. All Rights Reserved.

uftpRunTimeDataReset

The **uftpRunTimeDataReset** command resets the run-time data field in the UFTP data block.

Figure 22 "uftpRunTimeDataReset command output" (page 103) is an example of output from the **uftpRunTimeDataReset** command.

Figure 22
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 you enter no parameter, the output displays the contents of the entire active log file. When you enter a line number, **activeDlogShow[numOfLine]**, the output displays the active log file by the number of lines.

Figure 23 "activeDlogShow command output" (page 103) is an example of output from the **activeDlogShow** command.

Figure 23
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
```


Copyright © 2010 Nortel Networks. All Rights Reserved.

inactiveDlogShow

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

Figure 24 "inactiveDlogShow command output" (page 104) is an example of output from the **inactiveDlogShow** command.

Figure 24
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
```

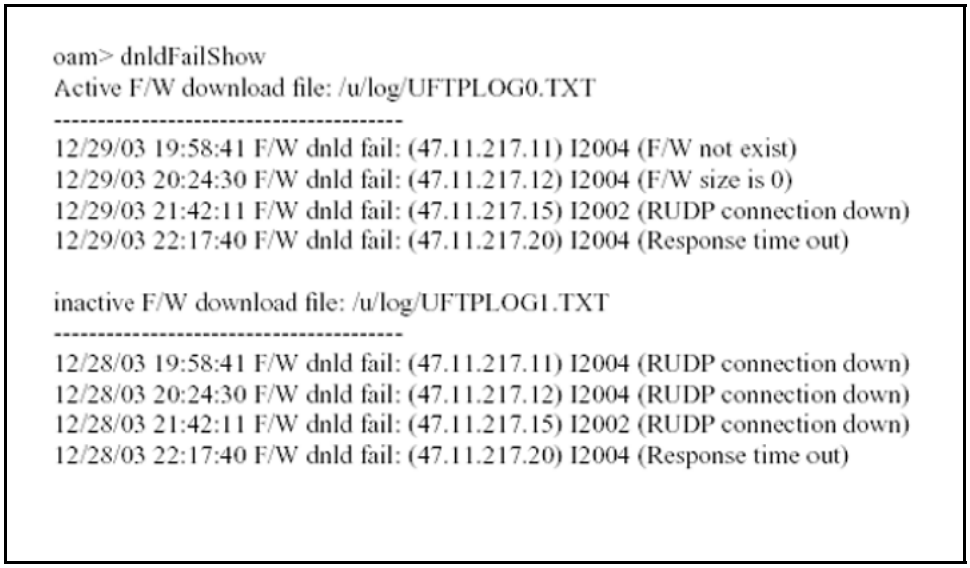
dnldFailShow

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

Figure 25 "dnldFailShow command output" (page 105) is an example of output from the **dnldFailShow** command.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 25
dnldFailShow command output



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.

The following Cone NAT routers are supported:

- Full Cone
- Restricted Cone
- Port Restricted Cone

Copyright © 2010 Nortel Networks. All Rights Reserved.

ATTENTION
A Cone NAT router with more than one connected IP Phone 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
Support is not available for Symmetric NAT routers. 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 CS 1000 Release 4.5 or later, and not a function of the NAT router. NAT Traversal uses two Echo Servers that reside 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 appears on the IP Phone display and the IP Phone cannot 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 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. A mapping exists for both a signaling port and a media (voice) port.

Placing an IP Phone behind Multiple NAT devices is an unsupported configuration. If you need 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.

Use the NAT device to implement and configure mapping. The IP Line application implements no mappings.

NAT and signaling

NAT hides the true identity of the IP Phone from the LTPS. The LTPS is aware of an IP Phone based only on the public IP address and port of the signaling messages. A signaling message originates from the IP Phone on

Copyright © 2010 Nortel Networks. All Rights Reserved.

the private side from port 5000. That signaling message then maps from the private side to a public IP and port; that is, the IP address detected by the LTPS.

Signaling messages between the Voice Gateway Media Card and IP Phones are carried by RUDP. Each RUDP connection is distinguished by the 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 27 "Signaling UDP Ports" (page 107) lists the UDP port number used.

Table 27
Signaling UDP Ports

UDP Port	Device	Use
5 000	IP Phone	Incoming signaling messages to the IP Phones, including UFTP messaging
5 100	LTPS	Incoming call processing messages to the LTPS
5 105	UFTP	Incoming UFTP packets to the UFTP server
4 100	LTPS	Incoming registration message to Connect Server
7 300	LTPS	Iincoming 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 remainder 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 28
IP Line UDP Ports

UDP Port	Device	Use
5 200–5 262	Media Card	RTP packets (configurable starting port number – IP Phoneport matches it)
5 201–5 263	Media Card	RTCP packets into Media Card (port number is RTP port number + 1)

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 28
IP Line UDP Ports (cont'd.)

UDP Port	Device	Use
5 200	IP Phone	RTP packets into IP Phone (port matches first RTP port of the Voice Gateway Media Card)
5 201	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. Nortel recommends using the default values. However, if you must increase the frequency of the Reset Watchdog message, increase the NAT Mapping Keep Alive timer value.

You can configure NAT Traversal to provision the length of time the audio and signaling port mapping is refreshed. You can configure NAT Traversal 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. You can decrease the value to 20 seconds or increase it to 600 seconds.

Mute and Hold considerations

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

Mute

Table 29 "Mute process" (page 108) describes the Mute process.

Table 29
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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 29
Mute process (cont'd.)

	Description
2	If the IP Phone uses 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 frames until Mute is cancelled.
3	Data sent from the IP Phone stops.
4	The NAT device determines 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 time out 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.
9	Data sent to the far end device arrives but the data returning 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 30 "Hold process" (page 109) describes the Hold process.

Table 30
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 sends periodic non-RTP packets to keep the NAT translation alive. Therefore, when a call is placed 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

NAT and VLAN

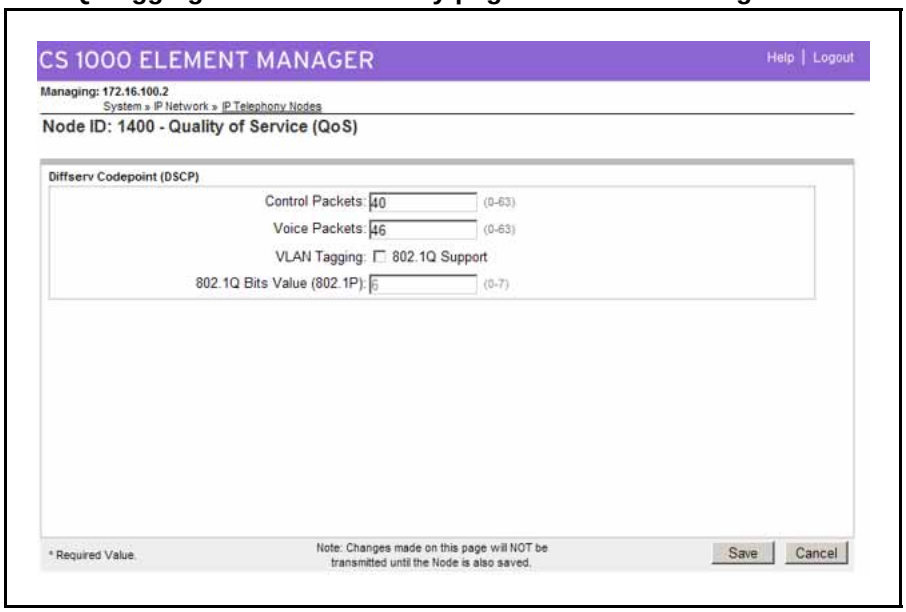
Support of Virtual LAN (VLAN) depends entirely on the Layer 2 switch to which the IP Phone is immediately connected. Users behind a NAT router may find that the configuration of a VLAN ID is unsupported by the NAT router. See the documentation of the NAT router to determine if VLAN ID support is available.

Users who attempt to use an IP Phone with VLAN enabled on a NAT router that does not support VLAN cannot connect to the CS 1000 system. If DHCP is used, the IP Phone cannot 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 802.1Q support in Element Manager under the QoS section must remain unchecked. See Figure 26 "802.1Q Tagging on Node Summary page in Element Manager" (page 110). 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 26
802.1Q Tagging on Node Summary page in Element Manager



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 plus 1. For example, if the PUBLIC RTP port is 12 000, then the PUBLIC RTCP port must be 12 001.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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

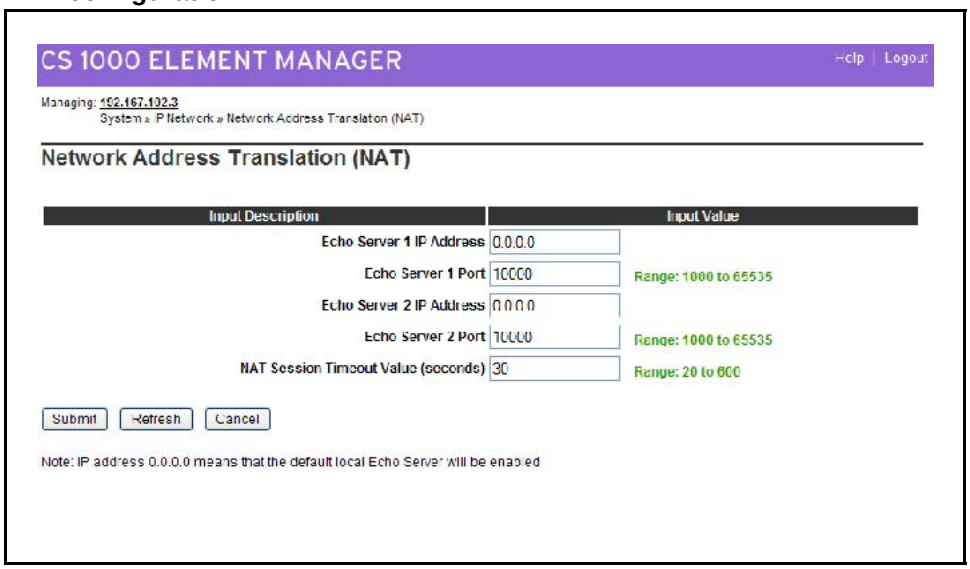
The NAT Traversal feature attempts a best effort approach to initiate the NAT router to properly assign the RTPC port number. The best effort approach depends on the NAT router implementation, can vary from NAT router to NAT router, and cannot be guaranteed by the NAT Traversal feature.

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 27 "NAT configuration" (page 111).

Figure 27
NAT configuration



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.

Echo Servers require no configuration 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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

ATTENTION
The NAT Traversal feature is essentially automatic. Change the IP addresses or ports only in exceptional cases when you use an Echo Server external to the CS 1000 system.

If IP addresses are specified, they must be for servers external to the system. The IP addresses cannot be the same. You can use duplicate IP addresses only 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 31
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: • 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 leader 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 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. You can enter any value from 1 000 to 60 000

Copyright © 2010 Nortel Networks. All Rights Reserved.

for the port. If the port value is outside of that range, an error message is generated. You can configure only the port (and not the IP addresses) 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 you configure an IP address, you must configure the port. If you configure no port or IP address, then an error message appears.

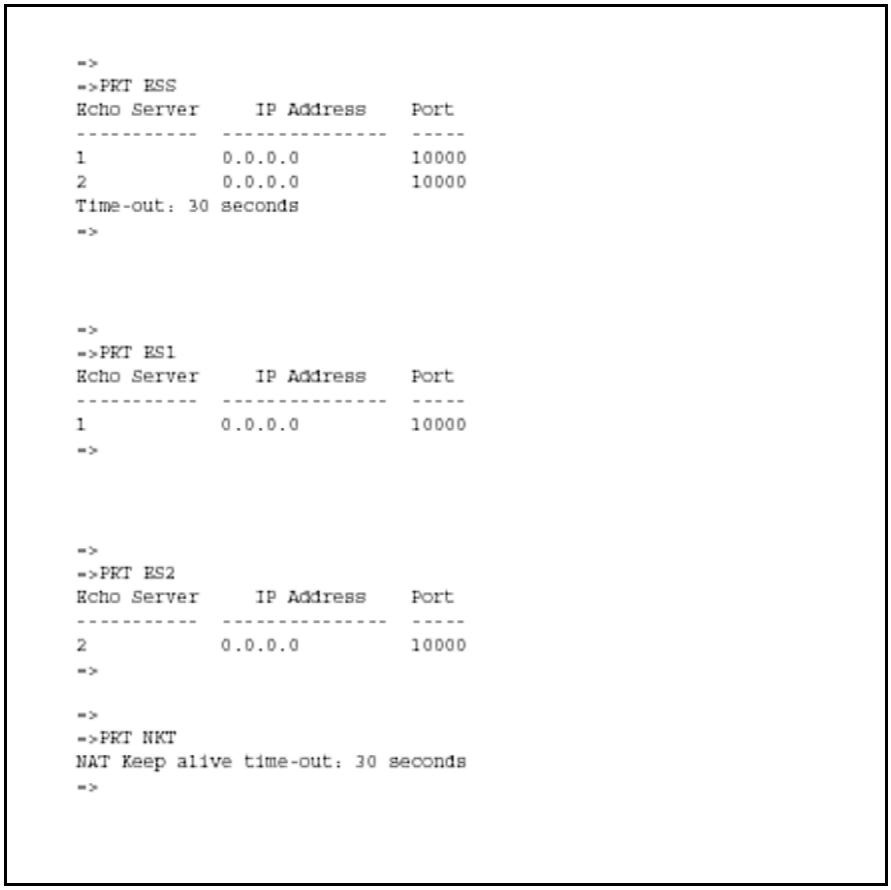
If you configure neither Echo Server, then the LTPS on the Signaling Server uses two local instances of the Echo Server. If you configure both Echo Servers, then the LTPS uses the external Echo Servers. If an external Echo Server fails, that functionality is lost unless the external Echo Server implements a transparent redundancy scheme. The external Echo Server handles its own redundancy and reliability.

PRT commands

Figure 28 "PRT commands output" (page 114) is an example of the output of the PRT commands when the default values s are used. If other IP addresses or port numbers are configured, then these appear in place of the 0.0.0.0 or 10 000 in the examples in Figure 28 "PRT commands output" (page 114).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 28
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.

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 shares 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, as shown in the following example, indicates there is more than one IP Phone using the IP address, lists the IP Phones and the TNs, and recommends that you use the **`isetReset`** TN command.

Copyright © 2010 Nortel Networks. All Rights Reserved.

```
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 you enter an IP address that multiple IP Phones use, an error message prints, as shown in the following 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

The following example shows:

```
isetGet "NAT == Y"
```

displays 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
```

echoServerShow

The **echoServerShow** command provides configuration information about the Echo Servers and information about interactions with the Echo Servers for the IP Phones on an LTPS. Use this command on an LTPS card to

Copyright © 2010 Nortel Networks. All Rights Reserved.

investigate a problem with an IP Phone registered to that LTPS card. The command provides information about the Echo Servers from the viewpoint of the LTPS on the card where you enter the command.

The command has one optional parameter, action; the only valid value is 99. When you enter **`echoServerShow 99`**, the counter values are reset after they appear. When you enter only**`echoServerShow`** , the counter values appear without the counter 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 parentheses. This is different from the Configured parameter only when the default address (0.0.0.0) is configured. The explanation in parentheses 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 leader.
  - (node IP, other card): the IP address used is the Node IP address, but another card is currently the Node leader; 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 indicate 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 prevent 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

A sample output is shown in Figure 29 "echoServerShow sample output" (page 117).

Figure 29
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

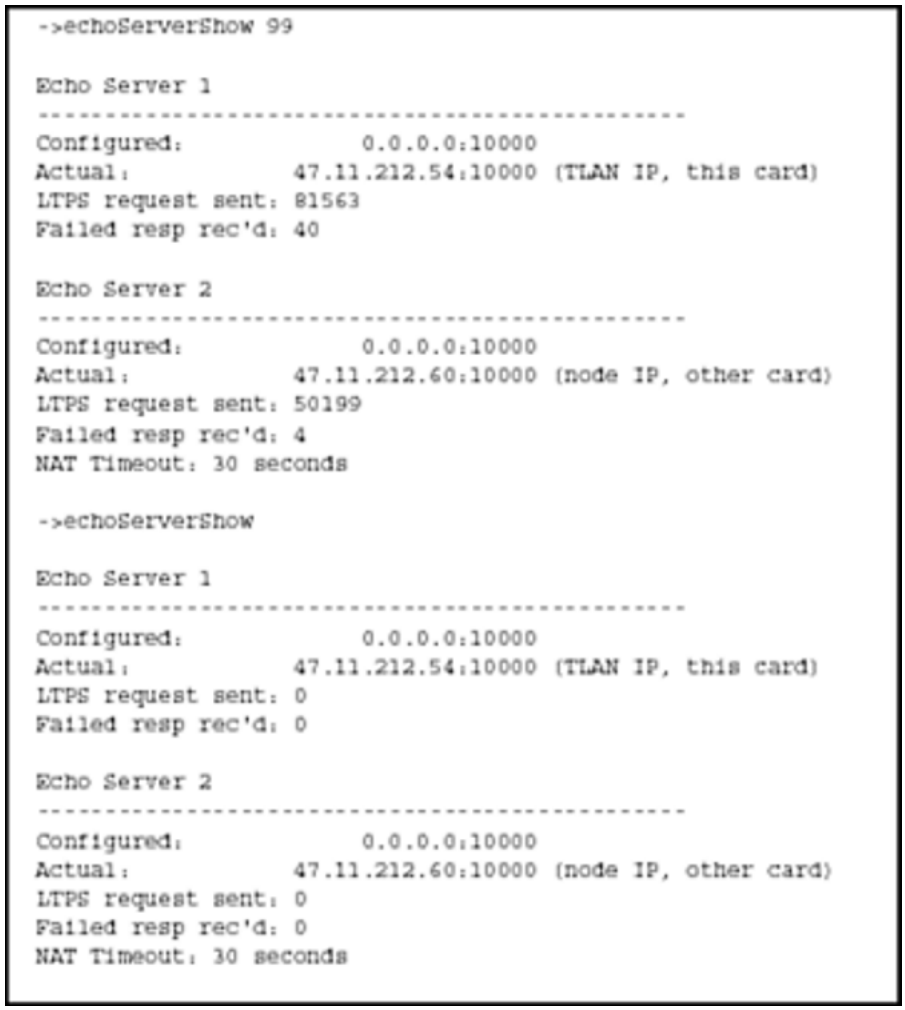
Echo Server 2
-----------------------------------------------
Configured:              0.0.0.0:10000
Actual:            47.11.212.60:10000 (node IP, other card)
LTPS request sent: 82201
Failed resp rec'd: 0
NAT Timeout: 30 seconds
```

When you enter the **`echoServerShow`** command with the reset parameter 99, the counter values appear and then reset. If you enter the **`echoServerShow`** command again and no subsequent requests, the counter values appear as 0.

A sample output is shown in Figure 30 "echoServerShow 99 sample output" (page 118).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 30
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 permits 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 can map to a single IP address. You can enter the public port number for an IP Phone.

vgwShow <"IPAddr">, <port>

If you enter no port number, the first entry found with the specified IP address on a Voice Gateway Media Card is returned. An example is shown in Figure 31 "vgwShow with IP address command output" (page 119).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 31
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 you entered the command, 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 more than one match occurs, the administrator can log on to that specific card and enter the **vgwShow** command without entering an IP address and port number. This command prints all the busy channels on the card. To quickly find an 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 4.0 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Corporate Directory is configured in LD 11. LD 11 accepts CRPA/CRPD CoS for the IP Phones (see Table 67 "Corporate Directory: LD 11 configuration" (page 280)).

For more information about the operation of the Corporate Directory feature, see*Telephony Manager 4.0 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 6.0.

Use the Personal Directory feature to enter or copy names into a personal directory, and to edit or delete all entries in the directory.

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 called. The user can dial a number from the Redial List.

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

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

For more information, see “Personal Directory application” (page 157).

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 the 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:

Copyright © 2010 Nortel Networks. All Rights Reserved.

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

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

- 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 monitors. These USM messages contain the IP address and port number 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 to capture and record 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, which provides the recording and playing function for the IP calls.

The following IP Phones support IP Call Recording: 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 Phone 1210, IP Phone 1220, and IP Phone 1230 do not support IP Call Recording.

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

- Bulk Call Recording: All calls are automatically recorded for an 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 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

Copyright © 2010 Nortel Networks. All Rights Reserved.

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:

- You can start or stop call recording at any time during a call.
- You can repeatedly pause and restart call recording during a call, to record excerpts from a conversation.
- You can retroactively begin call recording. At any time during the conversation, you can save the entire call. You need not start recording when the call begins.
- You can configure call recording to maintain ACD Emergency key functionality.

The CR initiates the IP Call Recording. A Start Recording Request message 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 CoS 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 126).

Warning tones

If you require a Recording Warning Tone, you can turn on and off this tone on the Call Server by using the existing UNIStim 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 K. As the IP Call Recorder uses two separate streams for the incoming and outgoing calls, there are four streams that require a total of 320 K for the voice packet data. In a typical 100 Mb/s LAN network environment, if 80 percent 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 you enable the IP Call Recording feature, the network is limited to a maximum of 250 calls.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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

Depending on the ability of the IP Call Recorder Server to handle the RTP stream, you might require more than one IP Call Recorder Server 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 servers.

Feature interactions

This section describes IP Call Recording feature interactions.

Mute key

When you press the Mute key, the IP Phone keeps both the primary and the duplicate audio stream open. When you press the Mute, the recording state remains active, but only the incoming conversation is recorded. Press the Mute key a second time to resume normal recording.

Hold key

When you press the Hold key, 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 you press the Transfer key and the transfer is 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 you forward a call, 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 if that IP Phone is part of the conference.

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

Copyright © 2010 Nortel Networks. All Rights Reserved.

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. A maximum of two associated (AST) keys exists for each TN.

In a Multiple Appearance DN Redirection Prime (MARP) configuration, the Call Server enables the association of MARP DNs on different TNs. A maximum of two associated (AST) keys exists for each TN.

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

Table 32
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, 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	

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 32
LD 11 AST configuration (cont'd.)

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

Administration

This section describes how to administer the IP Call Recording feature.

LD 17

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

The IPIE prompt enables or disables system-wide IP Call Recording. The functionality is disabled by default. When IP Call Recording is 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).

Table 33
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

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 33
LD 17 IP Call Recording (cont'd.)

Prompt	Response	Description
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

Use the CoS ICRD/ICRA responses to configure whether an IP Phone allows call recording.

Table 34
LD 11 Service change request for CoS 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, 1210, 1220, 1230, 1120, 1140, 1150, 2210, 2211, 2212, 6120, 6140
TN		Terminal Number of IP Phone
	l s c u	Where l = loop, s = shelf, c = card, u = unit
...		
CLS	ICRA (ICRD)	IP Call Recording allowed IP Call Recording denied
...		

If the ICRA CoS applies to a non-IP Phone, error SCH1599 message is generated.

If the CoS on an IP Phone changes during an active call, the Call Server tears down the call. If an IP Phone TN is deleted during an active call on the IP Phone, the Call Server tears down the call.

Copyright © 2010 Nortel Networks. All Rights Reserved.

LD 20

The CoS options ICRA/ICRD appear in LD 20 when you request 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 CoS ICRA or ICRD.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 35
LD 81 Count the IP Phones with CoS ICRA or ICRD

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

LD 83
In LD 83, the ICRA/ICRD CoS appears when the IP Phone TNB prints.

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
```


Copyright © 2010 Nortel Networks. All Rights Reserved.

```
IPCR Tx Path:  47.11.181.174:6000 IPCR Rx Path:  47.11.181.17
4:6001
(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:  47.11.181.17
4:6001
(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:  47.11.181.17
4:5001
(Italics indicate the IP Call Recording information)
```

pbxLink connection failure detection

The pbxLink Connection Failure Detection feature provides a way to detect the link status of registered elements. An alarm is generated if the pbxLink is not detected after the Call Server warm or cold starts.

The Call Server monitors the pbxLink.

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

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

If an unknown Signaling Server registers with the Call Server, an ELAN0029 alarm is generated.

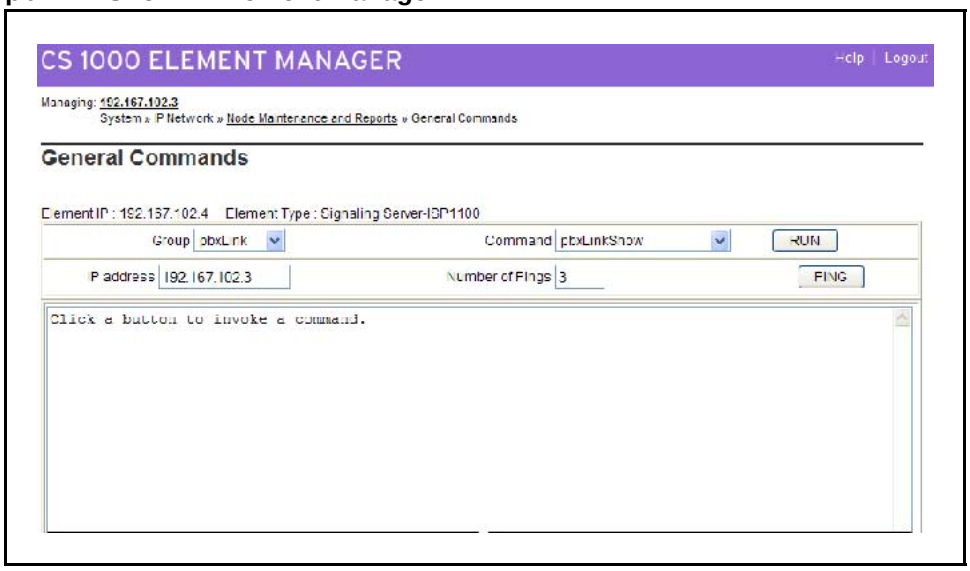
Copyright © 2010 Nortel Networks. All Rights Reserved.

Display pbxLink information by using Element Manager or LD 117. See the following sections for more information.

Display pbxLink information using 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 32 "pbxLinkShow in Element Manager" (page 130).

Figure 32
pbxLinkShow in Element Manager



Display pbxLink information using LD 117 STAT SERV

The suite of STAT SERV (Statistics Services) commands enables a technician to display link-status information for Signaling Servers 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

Copyright © 2010 Nortel Networks. All Rights Reserved.

- registered and unregistered endpoints, such as IP Phones
- information about the pbxLink and enabled applications
- Signaling Server resource count

The Signaling Server resource count helps to determine the number of virtual trunks that you can configure.

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 a connection
- the Signaling Server resource count

Application information

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

Table 36 "Queried information in STAT SERV" (page 131) lists the applications and describes the information provided by those applications.

Table 36
Queried information in STAT SERV

Application or 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.
Signaling Servers	Time that the element established the link with the Call Server. Elements that failed to register or lost the link.

Figure 33 "Sample LD 117 STAT SERV output" (page 132) shows an example of LD 117 STAT SERV output.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 33
Sample LD 117 STAT SERV output

```
=> stat serv

NODE ELANIP          LDR  SRV             PBXLINK
HOSTNAME
ID                                        STATE
3976 192.168.35.234  YES  Nortel CPPMv1   LINK UP
cppm-ss-4.asa.merann.ru
     APPS:     LTPS     VTRK
     PBXLINK DATE:   24/03/2009
     PBXLINK TIME:   16:19:18
     CONNECTID:      549b7b8
     Sets: [reg - 00000] [busy - 00000]
     VTRK: [reg - 00000] [busy - 00000]
     SIPL VTRK: [reg - 00000] [busy - 00000]
     SIGNALLING SERVER CAPACITY (SSRC): 2048
        Type: Nortel CPPMv1
        Location: 0 0 4
        Product Eng.Code: NTDW61BAE50003
        Serial Number: NNTMG19Y84B8CPPM
        Memory Size: 2048 MB
        Disk Size 37 GB


4250 192.168.35.30   YES  N/A             FAILED
hp8-e.asa.merann.ru
     APPS:     LTPS
     PBXLINK DATE:   20/03/2009
     PBXLINK TIME:   15:22:57
     CONNECTID:      0
```

Table 37 "STAT SERV response fields and description" (page 132) lists the descriptions for the fields in the STAT SERV response.

Table 37
STAT SERV response fields and description

STAT SERV response field	Description
NODE ID	Identifies the related node. Value is a number from 0–9 999.
HOSTNAME	Identifies the alias that the system gives the host. Value is a string.
ELANIP	Identifies the element IP connection to the Call Server. Value is an IP address.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 37
STAT SERV response fields and description (cont'd.)

STAT SERV response field	Description
LDR	Specifies if the element is the Leader for the related node. Value is Yes or No.
SRV	Specifies the element type: • SS:Signaling Server
APPS	Specifies the application running on the element: • LTPS • VTRK
PBXLINK STATE	Specifies the element current pbxLink state: • LINK UP • LOST • FAILED • INV CONN (element is connected, but the configuration is not on the Call Server, which indicates 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 as follows: • reg: the number of IP Phones registered to the element • busy: the number of IP Phones that are currently busy
VGWs	Values are as follows: • reg: the number of voice gateways (DSP resources) are configured on the element • busy: the number of voice gateways (DSP resources) active or busy on the element
VTRK	Values are as follows: • reg: the number of VTRK channels configured on the element • busy: the number of VTRK channels active or busy on the element
SSRC	Signaling Server capacity

Copyright © 2010 Nortel Networks. All Rights Reserved.

IP Phone support

The IP Line application supports the following IP Phones:

- IP Phone 2001. See*IP Phone 2001 User Guide*
- IP Phone 2002 Phase II. See *IP Phone 2002 User Guide*
- IP Phone 2004 Phase II. See *IP Phone 2004 User Guide*
- IP Phone 2007. See *IP Phone 2007 User Guide*
- IP Audio Conference Phone 2033. See *IP Audio Conference Phone 2033 User Guide*
- IP Phone 1110. See *IP Phone 1110 User Guide*
- IP Phone 1120E. See *IP Phone 1120E User Guide*
- IP Phone 1140E. See *IP Phone 1140E User Guide*
- IP Phone 1150E. See *IP Phone 1150E User Guide*
- IP Phone 1210. See *IP Phone 1210 User Guide*
- IP Phone 1220. See *IP Phone 1220 User Guide*
- IP Phone 1230. See *IP Phone 1230 User Guide*
- IP Softphone 2050. See *IP Softphone 2050 User Guide*
- Mobile Voice Client (MVC) 2050

  See *Mobile Voice Client 2050 User Guide*
- WLAN Handset 2210. See *WLAN Handset 2210 User Guide*
- WLAN Handset 2211. See *WLAN Handset 2211 User Guide*
- WLAN Handset 2212. See *WLAN Handset 2212 User Guide*
- WLAN Handset 6120; WLAN Handset 6140. See *WLAN Handset 6120/6140 User Guide*

For additional information, see the following documents:

- *Expansion Module for IP Phone 1100 Series User Guide* (NN43130-101)
- *IP Phone 1200 Series Key Expansion Module User Guide*
- *WLAN IP Telephony Installation and Commissioning* (NN43001-504)
- *IP Phones Fundamentals* (NN43001-368)

Element Manager support

Element Manager is installed using the Unified Communications Management (UCM) Common Services security framework on a Dell R300, IBM x306, IBM x3350, or an HP DL320 D4 commercial off the shelf

Copyright © 2010 Nortel Networks. All Rights Reserved.

(COTS) server, and Nortel CP PM servers. Element Manager is accessed through the UCM Common Services framework. The framework supports Single Sign-on so that the user can access multiple systems. Access the framework through Microsoft Internet Explorer 6.02600 or later. For information about how to log on to UCM Common Services, configure the UCM Common Services framework, and log on to Element Manager, see *Unified Communication Management Fundamentals* (NN43001-116).

Element Manager is a Web interface that provides an alternative to the traditional CLI and overlays. The interface is available if you use a Web browser on a PC. No special client software is required.

You can use Element Manager to configure an IP Telephony Node, check and upload loadware and firmware files, and retrieve the CONFIG.INI and BOOTP.TAB configuration files from the Call Server.

For more information, see *Element Manager System Reference—Admi nistration* (NN43001-632).

Call Statistics collection

You can collect statistics on the Quality of Service (QoS) of calls connected by the Call Server.

Commands in LD 32 and LD 117 print the number of IP Phones registered on a zone, node, or Signaling Server. Traffic printouts are available for each 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 you omit the MMMM parameter, the IP Phone Model Names and the associated mnemonics are listed.
- ECNT PEC <PEC>: count the number of IP Phones with a specified Product Engineering Code (PEC).

Copyright © 2010 Nortel Networks. All Rights Reserved.

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.

- ECNT CARD <Loop> <Shelf> <Card> <CustomerNumber>
- ECNT NODE <NodeNumber>
- ECNT SS <HostName>
- ECNT ZONE <ZoneNumber> <CustomerNumber>

Table 102 "LD 117 Count registered IP Phones" (page 361) describes these commands.

Error messages appear when you enter invalid data for these commands. The messages include information such as the correct ranges for the command parameters. See the following tables for the error messages:

- Table 38 "ECNT Card command error messages" (page 136).
- Table 39 "ECNT Zone command error messages" (page 136).
- Table 40 "ECNT Node command error messages" (page 137).
- Table 41 "ECNT SS command error message" (page 137).

Table 38
ECNT Card command error messages

Error	Error Message
Slot out of range error	Slot out of range. Range: [61–99]
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: [0–31]
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: [0–31]

Table 39
ECNT Zone command error messages

Error	Error Message
Zone out of range error	Zone out of range. Range: [0–255]
Zone not configured error	Zone not configured.
Customer out of range error	Customer out of range. Range: [0–31]

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 39
ECNT Zone command error messages (cont'd.)

Error	Error Message
Customer not configured error	Customer does not exist.
Combination of invalid zone and invalid customer error	Zone not configured. Customer out of range. Range: [0–31]

Table 40
ECNT Node command error messages

Error	Error Message
Node out of range error	Node out of range. Range: [0–9 999]
Node not configured error	Node not registered.

Table 41
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 prints for the following categories at the end of each collection period for each zone:

- Total inter and intrazone calls made
- Total inter and intrazone calls blocked
- Percent average inter and intrazone bandwidth used
- Percent maximum inter and intrazone bandwidth used
- Total inter and intrazone bandwidth threshold exceeded count

The counters are reset after the data prints.

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 to configure the system threshold use a value defined for the bandwidth threshold.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 42
System threshold commands

Command	Description
TTHS TH tv	Prints the current system thresholds.
STHS TH tv -- TV	Configures 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 example first configures the system bandwidth to 75 percent and then prints the actual value.

```
.STHS 5 750
.TTHS 5
```

Table 43 "IP Phone Zone Traffic Report 16 intrazone data output" (page 138) describes the intrazone IP Phone Zone Traffic Report 16 output data.

Table 43
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
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

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 43
IP Phone Zone Traffic Report 16 intrazone data output (cont'd.)

Data	Description
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 44 "IP Phone Zone Traffic Report 16 interzone data output" (page 139) describes the interzone IP Phone Zone Traffic Report 16 output data.

Table 44
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
ccnms	Calls completed without media security
cfnp	Calls failed by near end policy
cffr	Calls failed by incoming release
cosr	Outgoing calls switched to RTP

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 44
IP Phone Zone Traffic Report 16 interzone data output (cont'd.)

Data	Description
cisr	Incoming call switched to RTP
cfnr	Calls failed due to lack of resources (SRTP-capable DSPs)

Figure 34
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
INTERZONE       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
INTERZONE       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
INTERZONE       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
INTERZONE       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
INTERZONE       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 45 "SOPS, COPS, TOPS commands" (page 141) shows the SOPS, COPS, and TOPS commands:

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 45
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 print
`.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)

An IP Phone user can program the label on the feature key. This label change is saved and then displayed on the feature key.

Availability

Table 46 "Feature key availability on IP Phones" (page 141) describes the feature key availability on the IP Phones.

Table 46
Feature key availability on IP Phones

Model	Feature keys	Feature keys using Shift	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
IP Phone 1220	4	N/A	9
IP Phone 1230	10	20	9

The IP Phone 2001, IP Audio Conference Phone 2033, IP Phone 1110, and IP Phone 1210 do not support feature keys.

The feature key labels for each IP Phone 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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).

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.

For more information about zones and zone configuration, see *Converging the Data Network with VoIP Fundamentals* (NN43001-260).

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 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 are configured for that Private Zone. If the IP Phones require additional DSP resources than are available in the zone, DSP 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Resource-sharing for Shared and Private Zones

If a resource-critical IP Phone is configured for a Private Zone, and the zone has insufficient resources, 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 the search to the pool of shared DSP channels. The search does not extend into the Private Zones' channels.

When you configure the allocation of shared versus private resources, consider the required number of private resources. You must configure enough DSP resources to prevent the IP Phones in Shared Zones from running out of channels.



WARNING

Zones used for IP Media Gateway (IPMG) purposes must be configured as Shared so that other IP devices that are not in the same Zone can gain access to the IPMG devices.

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.

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 search algorithm within the pool.

If an available resource is not found, the overflow tone is given. For most installations, this approach works because all IP Phone users share the IP Line DSP resources. The DSP can be provisioned using a DSP-to-IP Phone ratio similar to trunk resources, because the DSP 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 use trunk resources to make calls, it becomes difficult to provision the system to guarantee 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 calls cannot be made. This occurs because all DSP channels are in one pool.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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.

You can configure a zone as shared or private.

Network wide Virtual Office

Network-wide virtual office allows a user to log on to 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 a user logs on, they can access their DN, autodial numbers, key layout, feature keys, and voice mail indication and access that are configured on their own home or office IP Phones. For example, if a user goes 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 the home or 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 system.

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 1210, IP Phone 1220, IP Phone 1230, 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.

For 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 “IP Phone type checking and blocking” (page 150).

Table 47 "Virtual Office logon from various IP Phones" (page 145) shows which users can log on to particular IP Phones.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 47
Virtual Office logon from various IP Phones

IP Phone User	Virtual Office logon
IP Phone 2001, IP Audio Conference Phone 2033, IP Phone 1110, or IP Phone 1210	Log on from another IP Phone 2001, IP Audio Conference Phone 2033, IP Phone 1110, IP Phone 1210, IP Phone 1230, IP Phone 1220, 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 "IP Phone type checking and blocking" (page 150).
IP Phone 2002, IP Phone 1120E, or IP Phone 1220	Log on from another IP Phone 2002, IP Phone 2004, IP Phone 1220, IP Phone 1230, IP Phone 2007, IP Softphone 2050, MVC 2050, WLAN Handset 2210/2211/2212/6120/6140, IP Phone 1120E, and IP Phone 1140E. Log on under certain conditions when they attempt a Virtual Office logon from an IP Phone 2001, IP Audio Conference Phone 2033, IP Phone 1110, and IP Phone 1210. See "IP Phone type checking and blocking" (page 150).
IP Phone 1230	Log on from another IP Phone 1230. Log on under certain conditions when they attempt a Virtual Office logon from an IP Phone 2001, IP Audio Conference Phone 2033, IP Phone 1110, IP Phone 1220, 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. See "IP Phone type checking and blocking" (page 150).
IP Phone 2004, IP Phone 2007, IP Phone 1140E	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. Log on under certain conditions when they attempt a Virtual Office logon from an IP Phone 2001, IP Phone 2002, IP Phone 1210, IP Phone 1220, IP Phone 1230 and IP Audio Conference Phone 2033. See "IP Phone type checking and blocking" (page 150).
IP Softphone 2050 or MVC 2050	Log on from another IP Softphone 2050, MVC 2050, IP Phone 2004, IP Phone 1230, IP Phone 2007, WLAN Handset 2210/2211/2212/6120/6140, IP Phone 1120E, and IP Phone 1140E. Log on under certain conditions when they attempt a Virtual Office logon from IP Phone 2002, IP Phone 1210, IP Phone 1220, IP Phone 1120E, and IP Phone 1140E. See "IP Phone type checking and blocking" (page 150).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 47
Virtual Office logon from various IP Phones (cont'd.)

IP Phone User	Virtual Office logon
	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	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 log on (destination) must have Virtual Office User Allowed (VOUA) configured.
- The IP Phone where the user wants to log on (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 a LD 32 command to disable and re-enable that TN. See *Communication Server 1000M and Meridian 1 Large System Maintenance* or *Software Input Output Reference — Maintenance* (NN43001-711).

Passwords and IP Phone Registration

An IP Phone registers using the TN (in the EEPROM). A valid user ID and password 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 occurs.

Virtual Office capabilities

Virtual Office provides the following capabilities:

- A network-wide connection server (Network Routing Server [NRS]) is provides addressing information of call servers, based on a user DN.
- 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

Copyright © 2010 Nortel Networks. All Rights Reserved.

in LD 11. If a SCPW is not configured, the Virtual Office feature is blocked.

- A user logs off on 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 use the Virtual Office feature to log on to their home IP Phones from various Call Servers within the network.

When an IP user moves from the home location to a location that has another Call Server and logs on to a Virtual Office from the home Call Server, the IP Phone used for Virtual Office registration obtains the following information:

- 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 changes only if the zone is reconfigured. The Current Zone field stores the current zone number. This value changes with each Virtual Office log on.

For more information about the Bandwidth Management for Network wide Virtual Office feature, see *Converging the Data Network with VoIP Fundamentals* (NN43001-260).

Branch Office and Media Gateway 1000B

The Media Gateway 1000B (MG 1000B) provides a way to extend CS 1000 Release 6.0 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.

At least one Signaling Server must be at the main office and each branch office.

ATTENTION
To provide NRS redundancy in a network with branch offices, Nortel recommends that you configure a Failsafe NRS at each branch office that is not otherwise configured with a Primary or Alternate NRS.

Copyright © 2010 Nortel Networks. All Rights Reserved.

For more information about MG 1000B, see *Branch Office Installation and Commissioning* (NN43001-314).

The total number of IP Phones in all offices can be no greater than the capacity of the main office, as specified in*Communication Server 1000E: Planning and Engineering* (NN43041-220) or *Communication Server 1000M and Meridian 1 Large System Planning and Engineering* (NN43021-220) .

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 1210
- IP Phone 1220
- IP Phone 1230
- 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 defines the virtual LAN (VLAN) 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 result.

Configuration of 802.1Q on IP Phones

The 802.1Q support for the IP Phones is configured 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 values:

- p bits
- VLAN ID

Copyright © 2010 Nortel Networks. All Rights Reserved.

For more information about manual or automatic IP Phone configuration, see *IP Phones Fundamentals* (NN43001-368).

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.

You can use CLI commands to use the Data Path Capture tool.

IP Phone firmware

See the ReadmeFirst documentation to determine the IP Phone minimum firmware (F/W) versions supported by IP Line.

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 /var/opt/nortel/tps/fw/ directory. Use Element Manager to load, remove and manage firmware files.

Hardware watchdog timer

A hardware watchdog timer is enabled on the Voice Gateway Media Cards. This feature enhances 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 returning it 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, which covers most normal operating conditions.

A reset reason is logged and saved when a card resets. The reset reason appears as a message during the startup 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

- 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 appear at any time by entering the CLI command **`lastResetReason`**.

Linux servers also have hardware watchdog timers. For more information, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

Codecs

Codec refers to the voice coding and compression algorithm used by the DSP on the 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.

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 177).

IP Phone type checking and blocking

If the registration is a regular request (as opposed to 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 occur:

- If the TN has Flexible Registration Denied (FRD) CoS configured, the Call Server checks the IP Phone type against the TN type. If the types do not match, the registration attempt is rejected and registration in Emulation Mode is blocked.
- If the TN has the default Flexible Registration Allowed (FRA) CoS configured, the Call Server checks the IP Phone type against the TN

Copyright © 2010 Nortel Networks. All Rights Reserved.

type. If the types are compatible, the TN is converted and the IP Phone registers.

- If the TN has Flexible Registration on Upgrade CoS configured, 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 CoS is configured to FRD and registration in Emulation Mode is blocked.

However, if the registration request is a virtual logon, this check does not occur. All IP Phones can register on any IP TN type when the logon is through Virtual Office.

Special checking on the self-labeled line/programmable feature keys occurs when an IP Phone 2004, IP Phone 2007, IP Softphone 2050, IP Phone 1120E, or IP Phone 1140E user logs on from an IP Phone 2002 or IP Phone 1220, or when an IP Phone 2002, or IP Phone 1220, IP Phone 1230, 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, IP Phone 1210, or IP Phone 1110.

Special checking is required to prevent a user from logging on 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 is permitted, the IP Phone can ring without providing the user a way to answer the call. The configuration of the logging on 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 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, IP Phone 1220, and IP Phone 1120E logon restrictions

Because the IP Phone 2002, IP Phone 1220, 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, IP Phone 1230, and IP Phone 1140E TN when they log on using an IP Phone 2002, IP Phone 1220, or IP Phone 1120E.

Copyright © 2010 Nortel Networks. All Rights Reserved.

When the IP Phone 2004, IP Phone 2007, IP Softphone 2050, IP Phone 1230, or IP Phone 1140E user logs on from an IP Phone 2002, IP Phone 1220, 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 4 to 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, IP Phone 1210, and IP Phone 1110 logon restrictions

Because the IP Phone 2001, IP Audio Conference Phone 2033, IP Phone 1210, and IP Phone 1110 do not support feature keys, a restricted VO logon applies to IP Phone 2002, IP Phone 1220, IP Phone 1230, IP Phone 2004, IP Phone 2007, IP Softphone 2050, IP Phone 1120E, and IP Phone 1140E TN when the user logs on using an IP Phone 2001, IP Audio Conference Phone 2033, IP Phone 1210, or IP Phone 1110.

When an IP Phone 2002, IP Phone 1220, IP Phone 1230, 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, IP Phone 1210, 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 1 to 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 three-digit Node ID can register to a node configured with a four-digit Node ID. To enable the registration to be successful, the three-digit Node ID must match the first three digits of the node four-digit Node ID.

This feature enhances the IP Phone survivability in the case of network outages or equipment failure; 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 addresses of two nodes, and properly configuring the Node IDs, the IP Phone can register to another secondary node if it cannot register to the primary node.

Copyright © 2010 Nortel Networks. All Rights Reserved.

The rules are as follows:

- if the Node ID on the system has three digits or less, the Node ID from the IP Phone must match exactly
- if the Node ID on the system has four digits and
  - if the Node ID from the IP Phone has fewer than three digits, reject the registration.
  - if the Node ID from the IP Phone has only three digits and they match the first three digits of the four digit Node ID (left to right), then allow the IP Phone to register. If the first three digits do not match, reject the registration.
  - if the Node ID from the IP Phone has four digits, the Node ID must match exactly. If the four digits do not match, reject the registration.

Up to 10 nodes can be configured on a system (three-digit Node ID base plus 0 to 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:

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 presents one of the following Node IDs, it is 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 two- or four-digit Node ID retains the exact match requirement.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Patch Management

CS 1000 Release 6.0 introduces Patching Manager (PM) which is a centralized patch deployment application that supports all Linux elements.

Patching Manager supports patching for all Linux-based elements in Release 6.0. This includes patching of all Linux bases and applications on these elements (except for Call Server on the Co-resident Call Server and Signaling Server).

> ***Note:*** Patching for the Call Server (on VxWorks or Linux) and other VxWorks devices such as media cards is supported by Element Manager.

Linux patching involves the patching of a specific version of an RPM. The RPM is the base building block of the Linux patching process.

RPM patches are issued only as Serviceability Updates (SU) and each Serviceability Update can contain only one RPM. Serviceability Updates have the same filename as the RPM file it contains; however, the Serviceability Update has a different extension.

Binary patches are created and distributed against a specific RPM name and release. Patches are given a unique patch name, which are automatically generated by the Meridian Patch Library (MPL). Binary patches are linked to their RPM using the patch header.

All other patching on Linux, such as JAR, WAR, and BIN are treated in the same manner as binary patches and each is tied to a specific release of an RPM.

Some patches may be dependent on one or more patches to be in-service before the latest patch is activated.

For more information about the Patching Manager, see *Patching Fundamentals* (NN43001-407).

Migration from Solid database to MySQL

The Solid RPM package will be replaced by two groups of RPMs. One group will be the MySQL third-party RPM. The other group is the Nortel application RPM which is renamed from Solid to dbcom. The two groups of RPMs are part of the Nortel application image and are included in the Linux application load-build.

There will not be any impact on the user interface due to MySQL migration.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Note 1: When the Solid database is upgraded to MySQL, the database server TCP port is changed from 1313 to 3306.

Note 2: When the Solid database is upgraded to MySQL, all Solid database utilities are removed.

Database application creation and operation

The dbcom application creation is based on the original Solid RPM creation and follows the Linux base RPM guidelines. The current Linux base appinstall and appstart are used for the MySQL installation and operation. After the application is installed, the default database configuration, accounts and passwords will be loaded. These include:

- NRS/NRS Manager: the account name “nrs” with the default password from the Secret Manager (SM) has full privileges on the databases NRS_A, NRS_B, and NRS_D. The databases will be empty initially.
- PD: the account name “pd” with the default password from the Secret Manager (SM) has full privileges on the database pddb. The database will be empty initially.
- EM/BCC: the account name “mgmt” with the default password from the Secret Manager (SM) has full privileges and it can create the databases on the fly. The default empty databases are systemdatabase and template_database.

Similar to operation of the Solid database, the following commands are supported under the nortel account and should be used to start, stop, restart and check the status of the MySQL database engine:

- **`appstart dbcom start`**
- **`appstart dbcom stop`**
- **`appstart dbcom restart`**
- **`appstart dbcom status`**

Copyright © 2010 Nortel Networks. All Rights Reserved.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Personal Directory application

Contents

This section contains the following topics:

- “Introduction” (page 157)
- “Personal Directory” (page 159)
- “Callers List” (page 160)
- “Redial List” (page 162)
- “IP Phone Application Server configuration and administration” (page 163)
- “IP Phone Application Server database maintenance” (page 168)
- “Call Server configuration” (page 172)
- “Password administration” (page 172)
- “Unicode Name Directory” (page 174)

Introduction

The Personal Directory application supports the creation of a Personal Directory for IP Phone users.

Personal Directory, Callers List, and Redial List are supported on the IP Phone 2002, IP Phone 1220, IP Phone 1230, 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 IP Phone 1210, 2033, and IP Phone 1110.

Copyright © 2010 Nortel Networks. All Rights Reserved.

The IP Phone Application Server ELAN network interface IP address must be configured. See “IP Phone Application Server configuration and administration” (page 163).

ATTENTION
Calling Party Name Display (CPND) must be configured as a Class of Service (CoS) on the system to enable Personal Directory, Callers List, and Redial List.

An IP Phone user creates and manages the personal directory. The IP Phone user can enter or copy names to the personal directory and delete entries from the personal directory. 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 CoS 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 48 "Comparison of Personal Directory with Callers List and Redial List" (page 158) compares the Personal Directory with the Callers List and Redial List features.

Table 48
Comparison of Personal Directory with Callers List and Redial List

Operation	Personal Directory	Callers List and Redial List
Display 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, IP Phone 1220, IP Phone 1230, and IP Phone 1120E display either the name or DN. The phones cannot simultaneously display the name and DN.)	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)

Copyright © 2010 Nortel Networks. All Rights Reserved.

Virtual Office

Personal Directory, Callers List, and Redial List are available when you use 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 the 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) make up 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 for multiple customers.

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 specific Personal Directory, Callers List, and Redial List. If using Multiple Appearance DN (MADN) for a group of users and you must 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 has the following specifications:

- maximum entries = 100
- maximum characters in name = 24

Copyright © 2010 Nortel Networks. All Rights Reserved.

- 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
- 1-minute time-out

Personal Directory is deployed as part of the Signaling Server software package. You can stop and restart the Personal Directory without stopping and restarting other Signaling Server applications.

Note: To start Personal Directory on TPS it is not enough to provide TPS ELAN IP address in Element Manager, it is also necessary to enable Personal Directory service in Node configuration interface in Element Manager.

Callers List

Callers List has the following specifications:

- 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, and the number of times the caller calls this user
- Idle Display option: displays and counts all calls or only unanswered calls

Copyright © 2010 Nortel Networks. All Rights Reserved.

- displays caller name (Redial List only displays the caller DN)
- after the 100 entry limit is reached, the newest entry overwrites the oldest entry
- 1-minute time-out

Call log options

Use Call log options to configure the following preferences on the IP Phone:

- whether the Callers List logs all incoming calls or only unanswered calls
- whether Idle Set Display indicates when new calls are logged to the Callers List
- whether a name stored in the Personal Directory that is associated with the incoming call DN appears instead of the name transmitted by the Call Server
- the three area codes to display after the DN, rather than before it (for example, local area codes)

Follow the steps in Procedure 7 “Accessing the call log options” (page 161) to access the call log options for the IP Phone.

Procedure 7
Accessing the call log options

Step	Action
1	On the IP Phone, press the **Services** key. The **Telephone Options** menu appears.
2	Select **Telephone Options, Call Log Options** .
3	Select the desired options.

--End--

Table 49 "Call log options" (page 161) summarizes the call log options.

Table 49
Call log options

Call log option	Description	Default value
Log all or unanswered incoming calls	Configures the Callers List to log all incoming calls or only the unanswered incoming calls.	Log all calls

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 49
Call log options (cont'd.)

Call log option	Description	Default value
New Call Indication	When New Call Indication is on, a message appears on the IP Phone to inform the user of a new incoming call. If not configured, nothing appears.	On
Preferred Name Match	Configures whether the displayed caller name is the CPND from the Call Server or the name associated with the DN stored in the Personal Directory	CPND from the Call Server appears
Area code set-up	Configures how the incoming DN appears. If the area code of the incoming call matches a specified area code, the DN appears in the configured manner (for example, the area code can appear after the DN)	No area code
Name display format	Configures the format of the name display of the incoming call on the IP Phone <first name> <last name> <last name> <first name>	<first name> <last name>

The IP Phone 2002, IP Phone 1220, IP Phone 1230, and IP Phone 1120E do 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 has the following specifications:

- 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:

Copyright © 2010 Nortel Networks. All Rights Reserved.

- dial the DN of an entry
- edit the entry
- copy the entry
- delete the entry
- delete contents of a list

- 1-minute time-out

IP Phone Application Server configuration and administration

The IP Phone Application Server runs on the Signaling Server with the SS package deployed. For more information about deploying Signaling Server software, see “Signaling Server software installation using Deployment Manager” (page 193).

If less than 1 000 users are supported, then the IP Phone Application Server can run on the same Signaling Server as Element Manager. If more than 1 000 users are supported, then the IP Phone Application Server must run on another Signaling Server (preferably a Follower) with no co-located applications. Therefore, you must configure in Element Manager the ELAN network interface IP address of the Signaling Server where the IP Phone Application Server is installed. You must also enable the IP Phone Application Server in the IP Telephony node.

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

To configure the IP Phone Application Server in an existing IP Telephony node see Procedure 8 “Configuring the IP Phone Application Server in an existing node” (page 164).

To configure the IP Phone Application Server in a new node and if the IP Phone Application Server must support more than 1 000 users, see Procedure 9 “Configuring the IP Phone Application Server on a new node” (page 165).

In CS 1000 Release 6.0, the default transfer method is SFTP. If a backup was done in an earlier release than CS 1000 Release 6.0 to FTP server, then SFTP must be supported to do the restore. Otherwise, SFTP connect fails and PD restore will not be completed.

Copyright © 2010 Nortel Networks. All Rights Reserved.

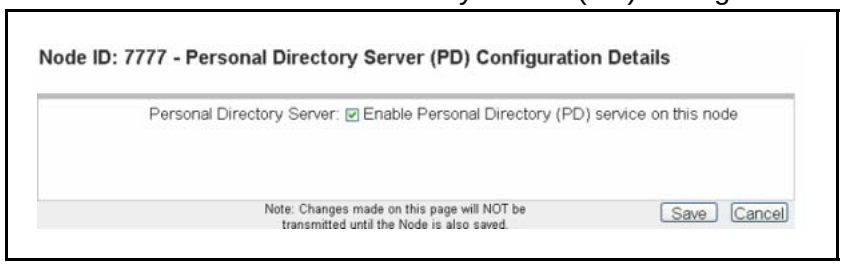
Procedure 8
Configuring the IP Phone Application Server in an existing node

Step	Action
1	In the Element Manager navigator, select **IP Network, Nodes: Servers, Media Cards**. The IP Telephony Nodes window appears.
2	Select the link for a Node ID. The Node Details window appears for that node.

Figure 35
Node Details



3	Click the **Personal Directories (PD)** link in the Applications (click to edit configuration) section of the window. The Personal Directory Server (PD) Configuration Details window appears.



4	Select the **Enable Personal Directory (PD) service on this node** check box.
5	Click **Save**. The Node Details window appears.
6	Click **Save**. The Node Saved window appears.
7	Click **Transfer Now**.

Copyright © 2010 Nortel Networks. All Rights Reserved.

The Synchronize Configuration Files window appears.

8 Select all servers and click **Start Sync** .

The Synchronization Status changes to Sync in progress and then to Synchronized.

9 Select all servers and click **Restart Applications**.

--End--

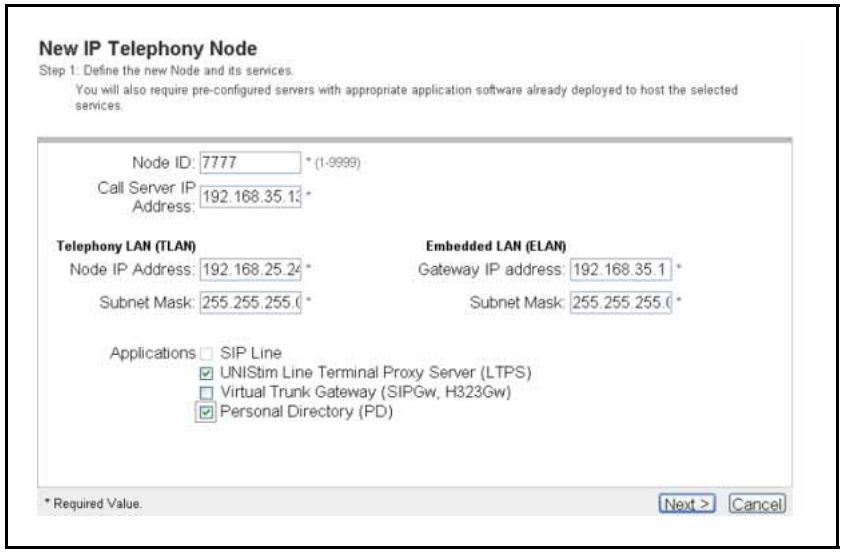
Perform the steps in the following procedure to configure IP Phone Application server on a new node.

Procedure 9
Configuring the IP Phone Application Server on a new node

Step	Action
1	In the Element Manager navigator, select **IP Network, Nodes: Servers, Media Cards** to configure a new node.
	The IP Telephony Nodes window appears.
2	Click **Add**.
	The Node Details window appears.
3	Enter a unique Node ID in the Node ID box.
4	Configure the IP addresses and subnet masks for the Signaling Server.
5	Select the necessary applications including Personal Directory (PD). If the IP Phone Application Server must support more than 1 000 users, choose only Personal Directory (PD).
6	Click **Next**.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 36
New IP Telephony Node - Personal Directory check box



7 Select from the list and click **Add** to associate servers with this node. If the IP Phone Application Server must support more than 1 000 users, select only one server with the SS package deployed.

8 Select one of the servers and click **Make Leader**.

9 Click **Next**.

10 Additional configuration windows appear for each selected application. Configure each of them and click **Next**.

11 The Confirm new Node details window appears. Click **Finish**.

The Node Saved window appears.

12 Click **Transfer Now** . The Synchronize Configuration Files window appears.

13 Select all servers and click **Start Sync**. The Synchronization Status changes to Sync in progress and then to Synchronized.

14 Select all servers and click **Restart Applications**.

--End--

Because you can back up and restore the IP Phone Application Server database, you must configure information to support the backup and restore feature. See Figure 37 "Personal Directories Server Configuration window" (page 167).

The following parameters are configured:

Copyright © 2010 Nortel Networks. All Rights Reserved.

- ELAN network interface IP address of the IP Phone Application Server where the database is located
- check box 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 and restore feature

Figure 37
Personal Directories Server Configuration window

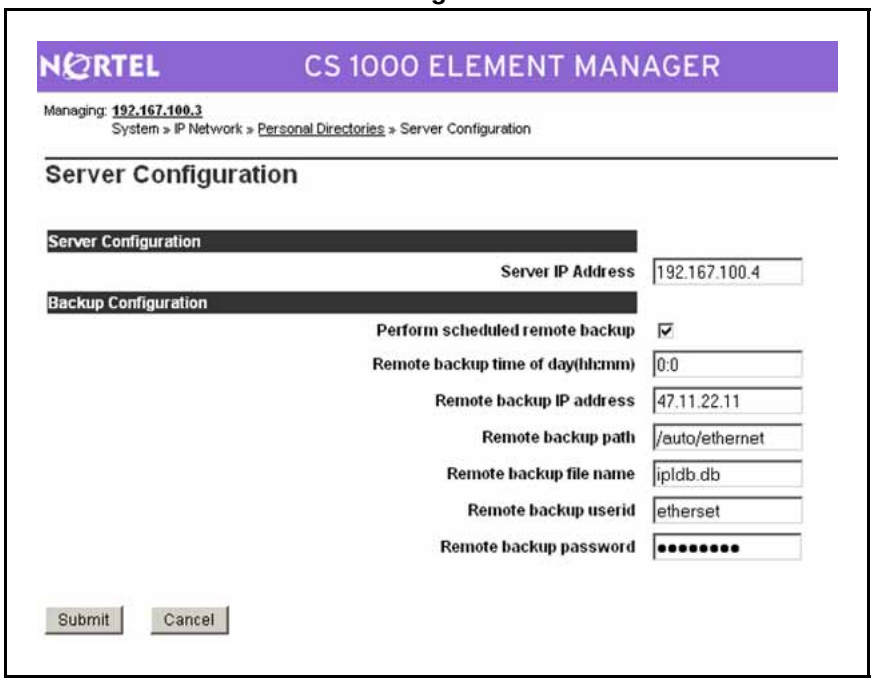


Table 50 "Sample IP Phone Application Server configuration" (page 167) provides a sample IP Phone Application Server configuration.

Table 50
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	Check box is selected	Select check box to enable scheduled remote backups.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 50
Sample IP Phone Application Server configuration (cont'd.)

Data field name	Example	Description
Remote backup time of day (hh:mm)	00:00	The time of day to perform the backup (default is 00:00 midnight).
Remote backup IP address	47.11.22.11	Remote backup server IP address.
Remote backup path	/auto/etherset	Remote path where the back up 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 features are available again only when contact with the Signaling Server is reestablished.

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 tracks 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

Use Element Manager to maintain the IP Phone Application Server database.

Configure a daily backup to occur at a scheduled time.

You can recover an IP Phone Application Server database for all users or for one user entries.

IP Phone Application Server database backup

Follow the steps in Procedure 10 "Backing up the IP Phone Application Server database server manually" (page 169) to manually back up the IP Phone Application Server database.

You can also schedule a backup of the database. See "Configure the IP Phone Application Server and remote backup" (page 163).

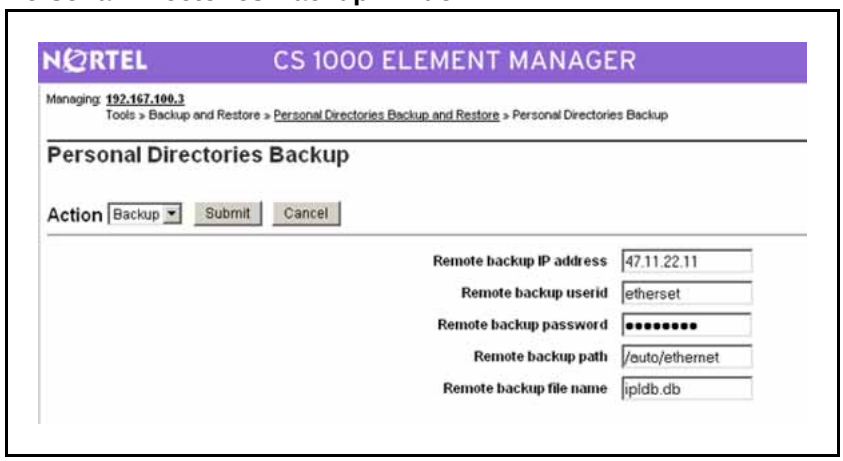
Copyright © 2010 Nortel Networks. All Rights Reserved.

Procedure 10
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 38 "Personal Directories Backup window" (page 169).
3	Enter the data for the **Remote backup IP address, Remote backup userid, Remote backup password, Remote backup path**, and **Remote backup file name** fields.
4	Click **Submit**.

--End--

Figure 38
Personal Directories Backup window



Full database recovery

Perform the steps in Procedure 11 “Performing a full database recovery” (page 169) to perform a full database backup for the IP Phone Application Server.

Procedure 11
Performing a full database recovery

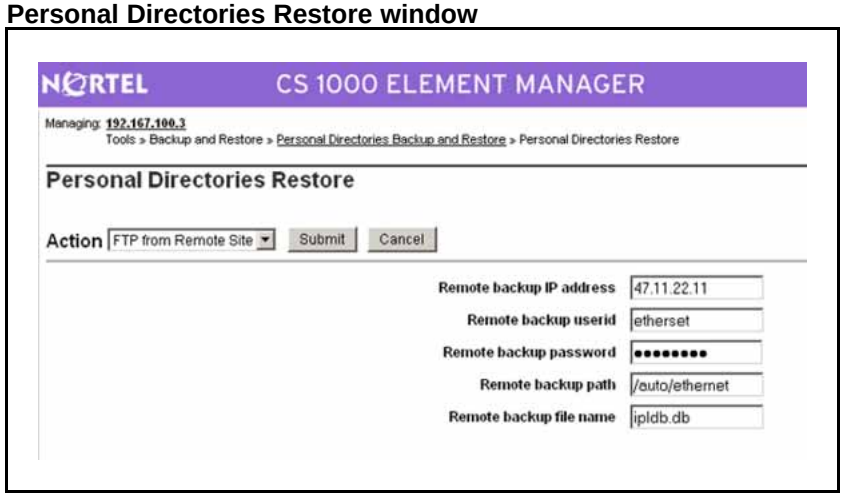
Step	Action
1	Select **Tools, Backup and Restore, Personal Directories**. The Personal Directories Backup and Restore window appears.

Copyright © 2010 Nortel Networks. All Rights Reserved.

2 Click **Personal Directories Restore**.

The Personal Directories Restore window appears. See Figure 39 "Personal Directories Restore window" (page 170).

Figure 39
Personal Directories Restore window



3 From the **Action** list, select **SFTP 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 to the local drive, an message appears indicating successful file transfer.

7 Click **OK**.

The file is transferred to the server but the database is not yet restored.

8 Reset all the IP Phones using **isetResetAll** on every LTPS in the system and allow the IP Phones to register.

9 From the Action list, select **Restore All Users**.

10 Click **Submit**.

11 Click **OK**.

The data for all users is restored and the existing data in the Personal Directories database is overwritten.

--End--

Copyright © 2010 Nortel Networks. All Rights Reserved.

ATTENTION
The length of time to restore a database depends on the number of records.

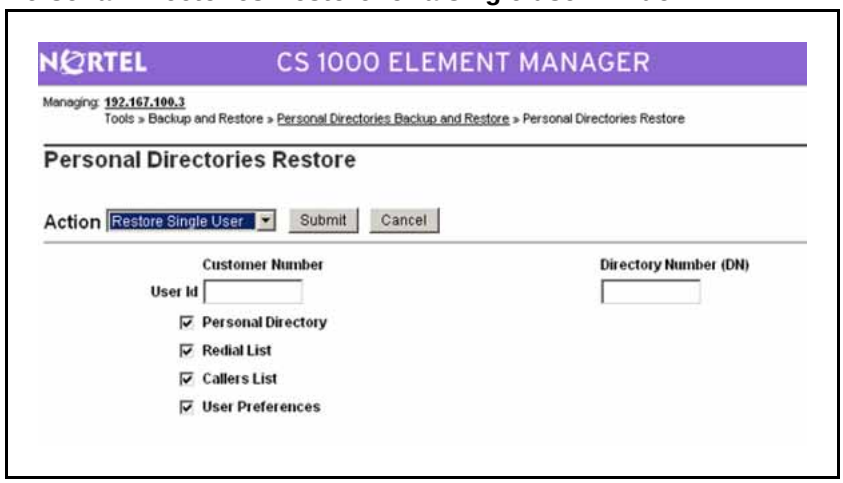
Selective database recovery for a single user

Follow the steps in Procedure 12 “Performing a selective database recovery” (page 171) to recover a database for a single user. A valid backup file is required to recover a database.

Procedure 12
Performing a selective database recovery

Step	Action
1	Select **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** list, select **Restore Single User**.
	The Personal Directories Restore window for a single user opens. See Figure 40 "Personal Directories Restore for a single user window" (page 171).

Figure 40
Personal Directories Restore for a single user window



4	Enter the **Customer Number** and **Directory Number (DN)** of the user.
5	Select the check boxes for the data that you want to restore.
6	Click **Submit**.

--End--

Copyright © 2010 Nortel Networks. All Rights Reserved.

Fault clearance

The database recovery clears any faults.

Recommendation
Nortel recommends that you install the IP Phone Application Server 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, is added to the Flexible Feature Code (FFC) parameters for the Call Server. When DFLT_SCPW is 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 Yes.

The new prompt DFLT_SCPW and the existing prompt Station Control Password Length (SCPL) are prompted for 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 changes, the change takes effect only after a data dump and then a sysload of the Call Server. The SCPL changes 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.

By default, when the IP Phone first registers to the system, the password protection is 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 51 "LD 15 Enable a default SCPW" (page 173).

Table 51
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.
...		
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 1 hour. This means that the Personal Directory, Callers List, and Redial List cannot be accessed and password administration cannot occur. A message appears on the IP Phone to indicate that access is locked.

After 1 hour, the retry counter is reset and access is unlocked. The retry counter also resets when the user correctly enters the password.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 the SCPW to access 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 the 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.

Unicode Name Directory

With the Unicode Name Directory System feature, the CS 1000 caller or called party name appears in up to seven other languages. This new feature enhances the functionality of IP Phones that can display Unicode. The Unicode Name Directory feature provides localized names on a subscriber base and generates the Calling Line IDs and URIs on a subscriber telephony account on a network level to serve the Unicode Name Directory server.

The Unicode Name Directory provides the following features:

- display of localized name in UTF-8 Unicode character encoding for incoming and outgoing calls
- storage for up to seven localized names in the database for a particular subscriber
- support for Korean, traditional and simplified Chinese, Japanese and other Unicode languages for called or caller party name display
- ability to work with 2007, 1120E, 1140E, 1150E, 2050V3, 1110, 1210, 1221, 1241 IP Phones
- a Web interface for Unicode Name Directory server configuration

Unicode Name Directory integrates with Personal Directory (PD) is part of the Personal Directory installation. The Unicode Name Directory is enabled in the Call Server only if Personal Directory is configured. For more information about configuring Unicode Name Directory, see *Element Manager System Reference—Administration* (NN43001-632).

Copyright © 2010 Nortel Networks. All Rights Reserved.

In CS 1000 Release 6.0, Personal Directory and Unicode Name Directory can be installed as a part of Local software deployment or Centralized software deployment. For more information about deployment options, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

Unicode Name Directory feature restrictions and limitations

The following is a list of restrictions and limitations that apply to the UND feature.

- UND is not supported by SIP terminals that support Unicode.
- UND inherits all limitations of CPND and Preferred Name Match features.
- Manual intervention is required to migrate from Release 5.5 where the patched solution exists: backup and export the Release 5.5 PD database and UND database XML files. Convert XML file into CSV file. Restore and import the Release 5.5 PD database and UND database CSV files into Release 6.0. Refer to *Subscriber Manager Fundamentals* (NN43001-120).
- UND is limited only for those user names and phone numbers which are propagated from Subscriber Manager to Unicode Name Directory database.
- Unicode name will not be displayed during a trunk call if the trunk side does not provide reliable Caller Line ID (CLID) and correct type of the call.
- Only characters supported by the IP Phone (including phone firmware and font files) can be used to display the name. If a system administrator enters for localized name Unicode characters not supported by the IP Phone, user name will be displayed incorrectly during the call.
- Cannot display Japanese, Chinese and Korean characters simultaneously. IP Phone 1110, IP Phone 1120E and IP Phone 12x0 can store only one downloadable font in the firmware. IP Phone 1140E, IP Phone 1150E and IP Phone 2007 can store four fonts simultaneously.
- The Primary and alternate redundancy model is not supported for the Unicode Name Directory application in Release 6.0.
- Unicode Name Directory application as a part of PD cannot serve multiple telephone nodes located on different Call Servers.
- Only half-width Japanese Katakana font is supported for name displaying.

Copyright © 2010 Nortel Networks. All Rights Reserved.

- Phone numbers entered in Subscriber Manager for a specific subscriber as ‘external’ should be unique . UND feature does not guarantee correct user name displaying in case the ‘external’ number is not unique.
- Signaling Server should have certificates signed by Primary Security server to establish secure LDAP connection with Subscriber Manager.
- UND service applies only to the primary Call Server system which provides calls under normal mode. When the Call Server system switches over to redundant systems (such as Geographic Redundant Call Server system and Branch Office Call Server system), UND service is not available.

IP Phones configuration

The following configuration of IP Phones must be in place before Unicode Name Directory can be properly used.

- CPND block configuration. To properly display names on an IP Phone, CPND block must be configured on the Call Server for each customer using UND.
- Class-of-Service configuration. The CNDA and DNDA classes of service must be enabled for each IP Phone that will use Unicode Name Directory.
- Language selection. For those IP Phones that support Unicode Name Directory, select the language through the Telephone Options, Language menu.

  Note: IP Phones that support Unicode require a special font file to display Asian languages. Download the font file to the IP Phone using TFTP server. For more information, see the installation guide for the specific IP Phone.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Codecs

Contents

This section contains the following topics:

- “Introduction” (page 177)
- “Codec configuration” (page 179)
- “Codec registration” (page 180)
- “Codec negotiation” (page 184)
- “Codec selection” (page 186)

Introduction

Codecs refers to the voice coding and compression algorithms used by the Digital Signal Processors (DSPs) on a Media Card. Codecs provide levels of audio quality and compression rates. IP Phones and Media Cards support different codecs. The codecs, and the order in which they are used, are configured on the LTPS and on the CS 1000 system. The CS 1000 system selects the appropriate codecs based on user-configurable parameters.

For instance, configure an IP Phone-to-IP Phone call in the same zone within a LAN using G.711 at 64 kb/s. Configure an IP Phone-to-IP Phone call over a WAN using G.729A or G.729AB at 8 kb/s. These data rates are for voice streams only. Packet overhead is not included.

Predefined codec table

The Line Terminal Proxy Server (LTPS) and the Voice Gateway Channel Server on a 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

When the Call Server sets up a Call Server connection between an IP Phone-to-IP Phone, 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 to select a codec that both endpoints support. As part of zone management, the system further selects the codec based on whether it tries 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.

Table 52 "Supported codecs" (page 178) shows which codecs the CS 1000 system supports.

ATTENTION
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.

ATTENTION
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.

Table 52
Supported codecs

Codec	Payload size
G.711 a-law, G.711 mu-law, NOVAD	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	30 ms
T.38	Supported for fax calls on gateway channels
G.711 Clear Channel	Supported for fax calls on gateway channels

The MVC 2050 supports only the G.711 codec with a 30-ms payload.

Copyright © 2010 Nortel Networks. All Rights Reserved.

If multiple nodes are 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.

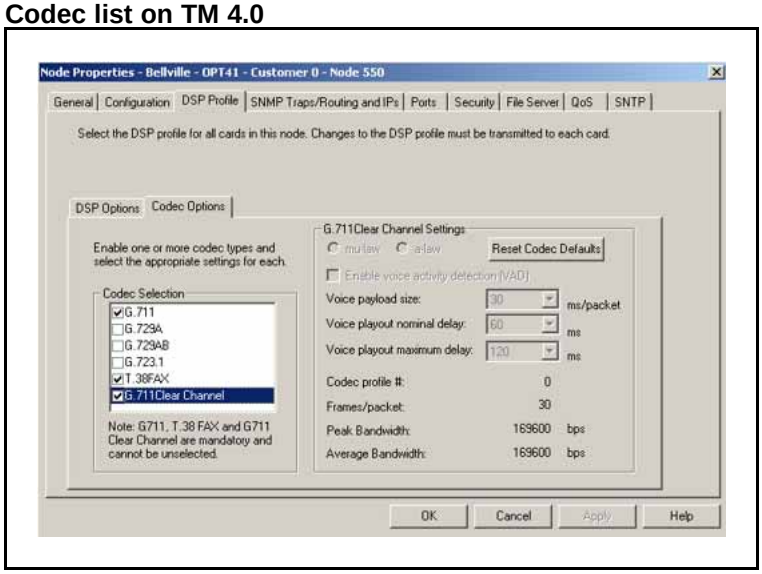
Codec configuration

Configure the codec in the DSP Profile sections of TM 4.0 and Element Manager.

Codec selection in TM 4.0

Figure 41 "Codec list on TM 4.0" (page 179) shows the list of codecs available on the DSP Profile tab within the TM 4.0 IP Line application. The Codec Options subtab presents a table of 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 41
Codec list on TM 4.0

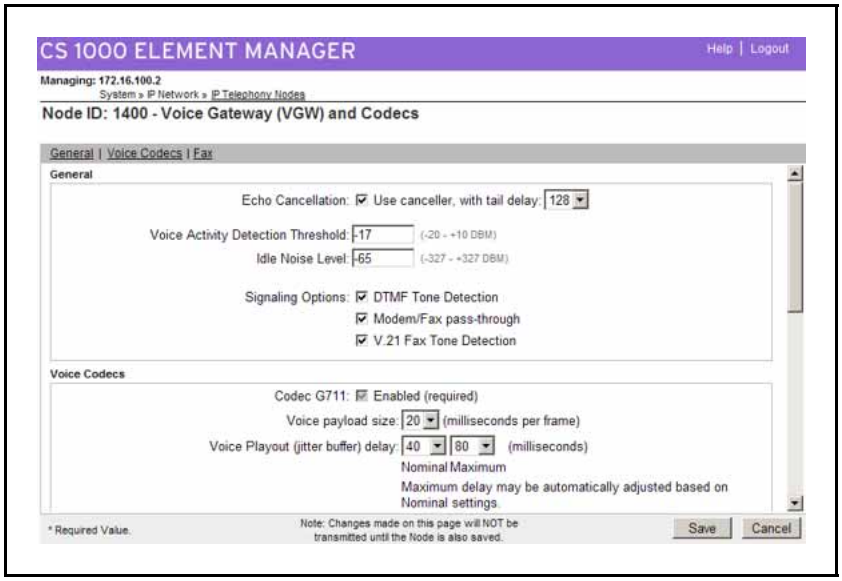


Codec selection in Element Manager

Figure 42 "Codec list in Element Manager" (page 180) shows the list of codec types that appear in Element Manager.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 42
Codec list in Element Manager



You cannot clear the automatically selected G.711 and T.38 Fax codecs. Even though you cannot clear these codecs, you can change the payload size and the jitter buffer for G.711. 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 ms.

For codec configuration in Element Manager, see “Configure Voice Gateway Profile data” (page 253).

Codec registration

After you configure the codecs, the IP Phones and DSPs must 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, and all user-configured codec. The codecs that the user can configure 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, G729A, G729AB, and G.723.1.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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-ms payload) and a G.723.1 codec (with a 30-ms payload).

The following three codecs are actually registered:

- G.711 mu-law (30 ms)
- G.711 a-law (30 ms)
- G.723.1 (30 ms)

Example 2

A user configures four codecs:

- G.711 a-law codec with a 10 ms payload
- G.729A codec with 50 ms payload
- G.729AB codec with 30 ms payload
- G.723.1 codec with a 30 ms payload

The following five codecs are actually registered:

- G.711 a-law (10 ms)
- G.711 mu-law (10 ms)
- G.729A (50 ms)
- G.729AB (30 ms)
- G.723.1 (30 ms)

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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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:

- G.711 a-law codec with a 10 ms payload
- G.729A codec with 50 ms payload
- G.729AB codec with 30 ms payload
- G.723.1 codec with a 30 ms payload

The following six codecs are registered:

- G.711 a-law (10 ms)
- G.711 mu-law (10 ms)
- G.729AB (30 ms)
- G.729A (50 ms)
- T.38
- G.711 Clear Channel

Copyright © 2010 Nortel Networks. All Rights Reserved.

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:

- G.711 mu-law codec with a 20 ms payload
- G.729A codec with 30 ms payload
- G.723.1 codec with a 30 ms payload

The following five codecs are actually registered:

- G.711 mu-law (20 ms)
- G.711 a-law (20 ms)
- G.729A (30 ms)
- T.38
- 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 is 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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

Codec refers to the voice coding and compression algorithm used by DSPs. Each codec has different QoS and compression properties. For every virtual trunk call, a common codec must be selected for the call. This is known as codec negotiation.

IP Peer Networking supports the per-call selection of codec standards, based on the type of call (interzone or intrazone). The codec preference sequence sent over SIP or H.323.

For more information about interzone and intrazone, see *Converging the Data Network with VoIP Fundamentals* (NN43001-260).

Codec sorting

The codec preference sequence sent over SIP or H.323 depends on the bandwidth policy selected for the Virtual Trunk zone and the involved IP Phones. For Best Quality, the list is sorted from best to worst voice quality. For Best Bandwidth, the list is sorted from best to worst bandwidth usage.

Codec sorting methods

Two methods are available to sort the codec list:

- 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.
- 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 53 "BQ and BB codec sorting lists" (page 185) 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 53
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_10 ms	G.711_a_law_10 ms	G.729AB_50 ms	G.729AB_50 ms
G.711_mu_law_20 ms	G.711_a_law_20 ms	G.729AB_40 ms	G.729AB_40 ms
G.711_mu_law_30 ms	G.711_a_law_30 ms	G.729AB_30 ms	G.729AB_30 ms
G.711_a_law_10 ms	G.711_mu_law_10 ms	G.729AB_20 ms	G.729AB_20 ms
G.711_a_law_20 ms	G.711_mu_law_20 ms	G.729AB_10 ms	G.729AB_10 ms
G.711_a_law_30 ms	G.711_mu_law_30 ms	G.729A_50 ms	G.729A_50 ms
G.729A_10 ms	G.729A_10 ms	G.729A_40 ms	G.729A_40 ms
G.729A_20 ms	G.729A_20 ms	G.729A_30 ms	G.729A_30 ms
G.729A_30 ms	G.729A_30 ms	G.729A_20 ms	G.729A_20 ms
G.729A_40 ms	G.729A_40 ms	G.729A_10 ms	G.729A_10 ms
G.729A_50 ms	G.729A_50 ms	G.723.1_5.3 kb/s_30 ms	G.723.1_5.3 kb/s_30 ms
G.729AB_10 ms	G.729AB_10 ms	G.723.1_6.4 kb/s_30 ms	G.723.1_6.4 kb/s_30 ms
G.729AB_20 ms	G.729AB_20 ms	G.711_mu_law_30 ms	G.711_a_law_30 ms
G.729AB_30 ms	G.729AB_30 ms	G.711_mu_law_20 ms	G.711_a_law_20 ms
G.729AB_40 ms	G.729AB_40 ms	G.711_mu_law_10 ms	G.711_a_law_10 ms
G.729AB_50 ms	G.729AB_50 ms	G.711_a_law_30 ms	G.711_mu_law_30 ms
G.723.1_5.3 kb/s_30 ms	G.723.1_5.3 kb/s_30 ms	G.711_a_law_20 ms	G.711_mu_law_20 ms
G.723.1_6.4 kb/s_30ms	G.723.1_6.4 kb/s_30 ms	G.711_a_law_10 ms	
T.38	T.38		
G.711CC	G.711CC		

Copyright © 2010 Nortel Networks. All Rights Reserved.

Best Quality (BQ) sorting		Best Bandwidth (BB) sorting	
For mu-law systems	For a-law systems	For mu-law systems	For a-law systems
		T.38 G.711CC	G.711_mu_law_10 ms T.38 G.711CC

Codec selection

For every Virtual Trunk call, a codec must be selected before the media path can be opened. When a call is setup or modified (that is, media redirection), one of two processes occurs:

- The terminating node selects a common codec and sends the selected codec to the originating node.
- 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. The following conditions are met before codec selection occurs:

- Each codec list contains more than one payload size for a given codec type (depending 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, the first codec in the far end list is the far end preferred codec).

Codec selection algorithm

When the codec lists meet the above conditions, one of the following codec selection algorithms selects the codec to be used:

- H.323 Master/Slave algorithm
- SIP Offer/Answer model
- Best Bandwidth codec selection algorithm

Copyright © 2010 Nortel Networks. All Rights Reserved.

H.323 Master/Slave algorithm

The H.323 Master/Slave algorithm operates in the following manner:

- The Master node uses its codec list as the preferred list and finds a common codec in the far end's list. For example, the Master finds the first codec in its list (for example, C1), checks the list at the far end and if the codec matches the Master (also C1) than that is the selected codec. Otherwise, it finds the second codec in its list and verifies it against the far end. The process continues until a common codec is found between the Master and far end.
- The Slave node uses the far end's list as the preferred list and finds in its own list the common codec.

SIP Offer/Answer model

The SIP codec negotiation is based on the Offer/Answer model with Session Description Protocol (SDP).

The following three cases of codec negotiation are supported:

- The calling user agent sends an SDP offer with its codec list in the invite message with a sendrecv attribute. In this case, the called user agent selects one codec and sends the selected codec in an SDP answer. The SDP answer is included in the 200 OK message (response to the INVITE) with the sendrecv attribute as the preferred method of operation.
- The calling user agent sends an SDP offer with its codec list in the invite message with a sendrecv attribute. The called user agent returns more than one codec in the SDP answer. In this case, that many codecs are included in the response, the calling user agent picks the first compatible codec from the called user agent list, and sends a new SDP offer with a single codec to lock it in.
- If the SDP of the calling user agent is not present in the INVITE message, then the called user agent sends its codec list in an SDP offer in the 200 OK message, with the sendrecv attribute. The calling user agent selects one codec and sends it in an SDP answer inside the ACK message, with a sendrecv attribute.

Best Bandwidth Codec Selection algorithm

The Best Bandwidth codec selection algorithm solves the issues caused by the H.323 Master/Slave algorithm. The Best Bandwidth algorithm selects one common codec based on two codec lists. Every time the selection is done with the same two lists, the selected codec matches. The Best Bandwidth codec decision is based on the codec type only. It

Copyright © 2010 Nortel Networks. All Rights Reserved.

does not consider the fact that some codecs, while generally using less bandwidth, can consume more bandwidth than others at certain payload sizes.

Best Bandwidth also applies to SIP.

Table 54 "Best Bandwidth codec Selection between any two codecs types" (page 188) 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 54
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.729AB	G.729AB	G.729AB
G.723.1	G.723.1	G.723.1	G.729A	G.729AB	G.723.1

For more information about codec selection and negotiation, see *Converging the Data Network with VoIP Fundamentals* (NN43001-260).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Installation task flow

Contents

This section contains the following topics:

- “Introduction” (page 189)
- “Before you begin” (page 189)
- “Installation summary” (page 189)
- Table 55 "IP Phone configuration data summary sheet" (page 192)

Introduction

Use the task flow information in this chapter to determine the proper steps for the installation or upgrade of the IP Line applications.

Read “Codecs” (page 177) before you install an IP Telephony node.

Before you begin

Ensure that the CS 1000 system runs CS 1000 Release 6.0.

Installation summary

Use the following summary of steps as a reference guide to install and configure an IP Telephony node. This summary is intended to serve as a pointer to the more detailed procedures in later chapters and to provide a sequential flow to the steps in the overall installation procedure.

Procedure 13
Preinstallation and configuration steps

Step	Action
1	Complete the IP Phone configuration data summary sheet. See Table 55 "IP Phone configuration data summary sheet" (page 192).
2	Install the hardware components:

Copyright © 2010 Nortel Networks. All Rights Reserved.

a Install the Voice Gateway Media Card. See Procedure 21 “Installing the Media Card” (page 219) for installing the Media Card 32-port cards.

b Cable the Voice Gateway Media Cards:

1. Install the Shielded 50-pin to Serial/ELAN/TLAN Adapter for the Media Card 32-port cards. See Procedure 23 “Installing the Shielded 50-pin to Serial/ELAN/TLAN Adapter onto the Media Card” (page 225).

3 Configure IP Line data on the system:

a Configure the IP address for the ELAN network interface. See Procedure 24 “Configuring the ELAN network interface IP address for the active ELNK” (page 226).

b Configure VoIP bandwidth management zones. See “Configure VoIP bandwidth management zones (LD 117)” (page 227).

c Configure IP Line physical TNs.

d Configure virtual superloops. See “Configure virtual superloops for IP Phones” (page 230).

e Configure IP Phone features. See “Configure IP Phone features in LD 11” (page 232).

4 Configure IP Line data using Element Manager:

a Manually add an IP Telephony node. See “Manually add an IP Telephony node” (page 246).

b Configure SNMP traps and community strings access for security. See “Configuring SNMP trap destinations and community strings” (page 252).

c Configure DiffServ CodePoint (DSCP) data, 802.1Q support, and NAT support. See “Configure Quality of Service” (page 257).

d Configure file server access. See “Configure file server access” (page 259).

e Configure the loss plan. See “Configure loss and level plan” (page 260).

f Configure Voice Gateway Media Card properties. See “Add card and configure the card properties of the Voice Gateway Media Card” (page 261).

5 Transmit Voice Gateway Media Card configuration data to the Voice Gateway Media Cards:

a Transmit node and card properties to the Leader. See Procedure 33 “Transmitting node properties to Leader” (page 263).

Copyright © 2010 Nortel Networks. All Rights Reserved.

6 Upgrade the card software and IP Phone firmware:

   a Verify card software version. See "Determine Voice Gateway Media Card software version" (page 266).

   b Verify the IP Phone firmware release.

   c Download software and firmware files from the Nortel Web site. See "Download the current loadware and IP Phone firmware" (page 266)

   d Upload the software and firmware files to the file server. See "Upload the loadware and firmware files to the Signaling Server" (page 266).

   e Upgrade the software on the Voice Gateway Media Card. See "Upgrade the Voice Gateway Media Card loadware" (page 268).

   f Restart the card. See "Restart the Voice Gateway Media Card" (page 269).

   g Upgrade the IP Phone firmware on the card. See "Upgrade the IP Phone firmware" (page 271).

7 Configure TM alarm notification feature to receive IP Line SNMP traps.

8 Assemble and install an IP Phone. See *IP Phones Fundamentals* (NN43001-368).

9 Configure the IP Phone Installer Passwords (see "IP Phone Installer Password" (page 288)).

   a Enable and configure the administrative IP Phone Installer Password. See Procedure 41 "Configuring the Administrative IP Phone Installer Password" (page 293).

   b If needed, enable and configure a temporary IP Phone Installer Password. See Procedure 42 "Configuring the temporary IP Phone Installer Password" (page 296).

--End--

Nortel recommends that you complete an IP Phone configuration data summary sheet as you install and configure IP Phones.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 55
IP Phone configuration data summary sheet

No DHCP								
			DHCP					
IP address	Sub-net mask	Gateway IP address	Connect Server IP address*	Node ID	VTN	DN	User Name	User Location
*Connect Server IP address is the Node IP address of the IP Telephony node.								

Copyright © 2010 Nortel Networks. All Rights Reserved.

Signaling Server software installation using Deployment Manager

Contents

This chapter contains the following information:

- “Introduction” (page 193)
- “Software Deployment Packages” (page 194)
- “Pre-installation checklist” (page 195)
- “Nortel Linux Base installation” (page 195)
- “Signaling Server application installation” (page 195)
- “Access UCM” (page 197)
- “Element Manager configuration” (page 198)

Introduction

This chapter explains how to deploy Signaling Server software and supported applications on the CS 1000 system.

When you install the Linux base platform, you deploy the Signaling Server software, which you can access through the Unified Communications Management (UCM) console. For more information about the Linux platform base install, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

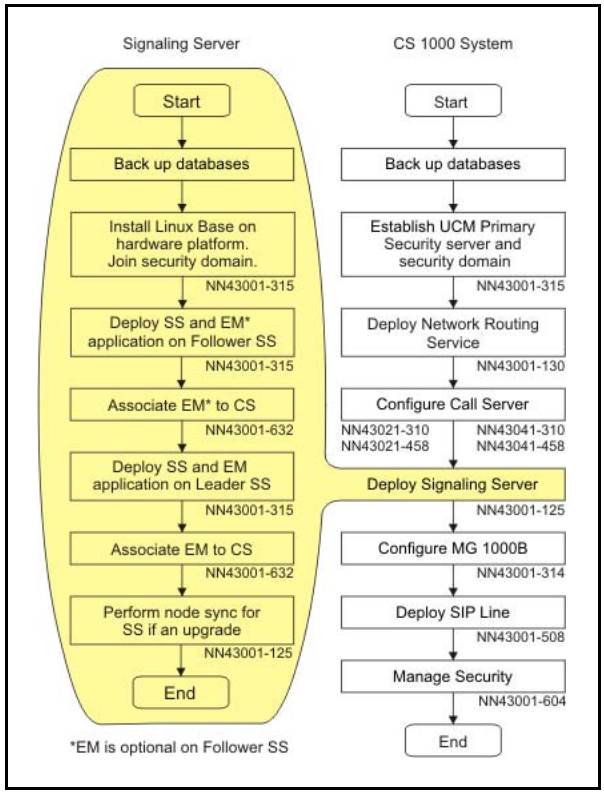
Installation Task Flow

This section provides a high-level task flow to install CS 1000 Release 6.0.

The task flow on the left side is for the Signaling Server software applications installation.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 43
Linux base and applications installation task flow



Software Deployment Packages

Install Nortel applications using Deployment Manager.

You can deploy the Signaling Server software from one of the following predefined deployment packages:

- Signaling Server (SS)
- Signaling Server and Network Routing Service
- Call Server (CS) and Signaling Server (basic stand-alone Co-resident system. For more information about the Co-resident system, see *CP PM Co-resident Call Server and Signaling Server Fundamentals* (NN43001-509).

After you deploy the Signaling Server software, configure the software applications through Element Manager. The software applications in CS 1000 Release. 6.0 include: LTPS, Vtrk (SIPgw and H.323GW), Personal Directory (PD). Voice Gateway Media Card loadware is also included as part of the Signaling Server software.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Pre-installation checklist

The CP PM Co-resident CS and Signaling Server requires a CP PM hardware platform with a 40 GB hard drive and 2 GB of memory. The CP PM BIOS version must be Release 18 or later. You must determine the CP PM BIOS version and upgrade the BIOS if necessary. For more information, see *CP PM Co-resident Call Server and Signaling Server Fundamentals* (NN43001-509).

For more information about BIOS versions for COTS platforms, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

Nortel Linux Base installation

Note: You must install the Nortel Linux base platform before you complete the procedures described in this section.

Perform the Linux Base installation from the command line interface (CLI) using a bootable CF installation media card. Configure the ELAN, TLAN IP address, gateway, subnet masks, and date and time settings during the Linux Base installation. A DVD install is available for COTS platforms.

For more information about the Linux Base installation, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

Note: After you complete the Linux base installation, you must configure the server as a primary, backup or member server in the UCM security framework. This configuration is completed using the default Nortel userID and password when logging on TO UCM to perform the security configuration. For more information, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

Signaling Server application installation

Use the Deployment Manager to install the Signaling Server application on the CP PM or COTS servers.

The Deployment Manager installs the Call Server, Signaling Server, and System Management applications as Linux Red Hat Package Manager (RPM) packages.

Deployment Manager access occurs through the Web-based CS 1000 UCM navigator.

The Deployment Manager can operate in two modes;

- Centralized Deployment Manager (Remote):

Copyright © 2010 Nortel Networks. All Rights Reserved.

The Deployment Manager runs on the UCM Primary Security Server. You must start the UCM navigator and log on to the UCM Primary Security Server. In this model, the Centralized Deployment Manager deploys application software to the target servers in the UCM security domain.

- Local Deployment Manager:

  The Deployment Manager runs on the target server. Accessing the Deployment Manager is similar to the Centralized Deployment option except you must log on to the local target server by using the default user ID and password. This mode is typically used when you want to install software on the target server before you configure it to join the UCM security framework.

In both Centralized and Local modes, the application software Nortel Application Image (NAI) on the software delivery media is uploaded from the client workstation to the server where Deployment Manager runs:

- For the Centralized Deployment Manager, the application software image is transferred to the hard disk of the UCM primary security server.
- For the Local Deployment Manager, the application software image is transferred to the hard disk on the target server.

  Note: For the Centralized Deployment Manager, you need to upload the application software only once. You can then deploy the software image to multiple target servers in the UCM security domain.

The Deployment Manager supports new installation and upgrades. Both processes are similar but contain the following differences:

- For the upgrade, you cannot remove or add any new type of application on the CP PM Co-res CS and SS; you must use the existing package configuration. You can upgrade only the existing applications to newer versions.
- For the upgrade, existing data is backed up and restored when you install the new version of the application software.

  Note: If you change the package configuration, you must manually back up data on the target by using the **`sysbackup`** command before you use the Deployment Manager to install a new package configuration on the CP PM Co-res CS and Signaling Server.

For detailed information, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Access UCM

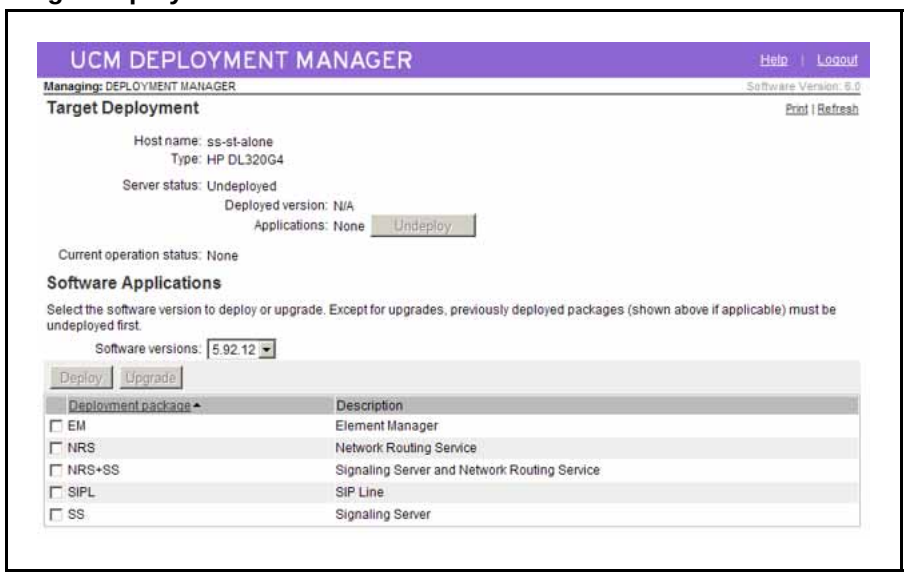
Centralized Deployment Manager allows software application deployment from the primary security server to other Linux servers in the same security domain. The primary security server is the central repository for the software application load and deployment occurs remotely, which eliminates the need to log on to each target server. For more information, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315)

You must access UCM to deploy software through the Deployment Manager.

Procedure 14
Deploying Signaling Server software to a COTS or CP PM server

Step	Action
1	Log on to the UCM Deployment Manager.
2	Select the **Software Deployment** link. The Target Deployment window appears.

Figure 44
Target Deployment window



3	Select a host name from the list, and click **Deploy**.
4	Select the check boxes for the software applications that you want to deploy to the server: EM, NRS, NRS+SS, SIPL, SS. When you select a check box, other check boxes might then be unavailable if the selected software cannot co-reside with the unavailable software.

Copyright © 2010 Nortel Networks. All Rights Reserved.

5 Click **Deploy** .

--End--

After you deploy the Signaling Server software, configure the VTRK (SIPgw and H.323gw) components. These features can be configured as part of IP Telephony node configuration. For more information, see "Manually add an IP Telephony node" (page 246).

IP Telephony nodes are configured through Element Manager. Ensure that Element Manager is deployed and configured. For more information, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

Element Manager configuration

The following sections provide information to set up the Internet Explorer browser.

Configuring the Internet Explorer browser

System requirements for Element Manager

Element Manager requires Microsoft Internet Explorer 6.0.2600 or later with Service Pack 1. Element Manager is not supported on the Netscape browser.

The Element Manager Virtual Terminal Environment requires the Java Runtime Environment (JRE).

Configuring the browser

Before you can use Element Manager, you must complete the following tasks:

- Enable pop-ups in the browsers search utility (mandatory)
- Configure the Internet Explorer browser settings (mandatory)
- Configure the Windows Display settings (highly recommended)

ATTENTION

Nortel discourages using the browser Back, Forward, and Refresh buttons.

Element Manager pages contain dynamic data content. Nortel does not recommend that you use the Back button. Element Manager provides a navigation path on the top of every page.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Nortel recommends that you use the navigation path to go to the previous page.

Note: The interface for the Internet Explorer browser settings and Windows Display settings can vary by browser version and by operating system.

If you use a browser search utility (such as the Google search engine or the Yahoo! search engine), ensure that pop-ups are enabled. Typically, you enable pop-up windows from the toolbar of the search utility.

ATTENTION
Do not block pop-ups if you use a search utility (such as Google or Yahoo!) in your browser.

Use the following procedure to configure the following Internet Explorer browser settings.

- Turn off Internet Explorer caching.

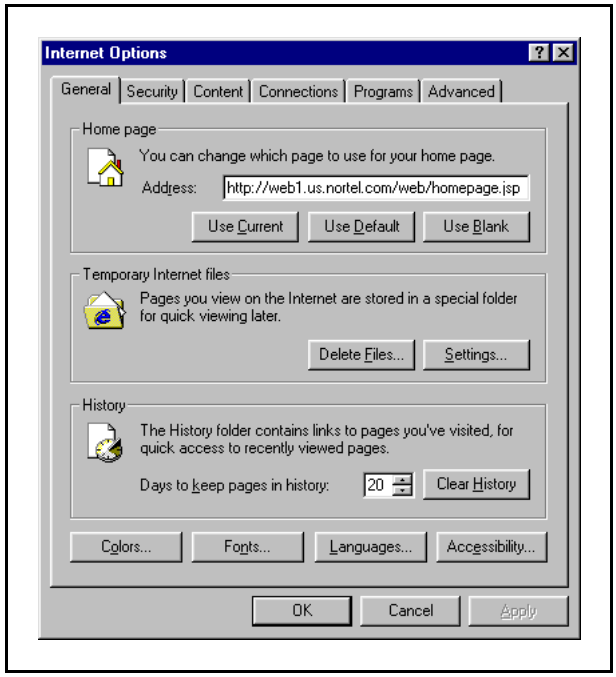
  Internet Explorer caching interferes with the Element Manager, so you cannot see real-time changes as they occur.
- Configure empty session information.
- Clear the AutoComplete options.

Procedure 15
Configure the Internet Explorer browser settings

Step	Action
1	Select **View, Text Size, Medium** to configure the text size in the browser.
2	Select **Tools, Internet Options** In the Internet Explorer browser window. The Internet Options window appears, as shown in Figure 45 "Internet Options window" (page 200).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 45
Internet Options window



3 Turn off Internet Explorer caching:

a On the **General** tab under the **Temporary Internet files** section, click **Settings**.

The Settings window appears.

b Under the **Check for newer versions of stored pages** section, select **Every visit to the page**.

c Click **OK**.

4 Configure empty session information:

a Select the **Advanced** tab.

The Advanced Settings window appears.

b Under **Security**, select **Empty Temporary Internet Files folder when browser is closed**.

5 Clear the AutoComplete options.

a Select the **Content** tab.

b Under **Personal Information**, click **AutoComplete**.

The AutoComplete Settings window appears.

c Under the **Use AutoComplete for** section, clear **Forms** and **User names and passwords on forms**.

6 (Optional) Configure the Windows display settings.

a Select **Start, Settings, Control Panel, Display**.

Copyright © 2010 Nortel Networks. All Rights Reserved.

The Display Settings window appears.

b Select the **Settings** tab.

c Select **True Color (32 bit)** from the **Colors** list.

d Under **Screen area**, select **1280 by 1024 pixels**.

e Click **OK**.

--End--

Copyright © 2010 Nortel Networks. All Rights Reserved.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Signaling Server Software upgrade

Contents

This chapter contains the following information:

- "Introduction" (page 203)
- "Overview" (page 204)
- "Before starting your upgrade" (page 204)
- "Upgrade paths" (page 205)
- "Upgrade procedures" (page 207)

Introduction

This chapter contains instructions to upgrade the software on your existing Signaling Server to CS 1000 Release 6.0. Support is available to upgrade from Succession 1000 Release 3.0, CS 1000 Release 4.0, Communication Server 1000 Release 4.5, Communication Server 1000 Release 5.0, and CS 1000 Release 5.5.

All Signaling Servers are subject to software upgrades in CS 1000 Release 6.0. Nortel CP PM, IBM X306m, and HP DL320-G4 Signaling Servers can not run software older than CS 1000 Release 5.0, so are subject to a software upgrade only from CS 1000 Release 5.0.

Note: You can contact Nortel Global Professional Services to assist you with your upgrade.

ATTENTION
The Upgrade procedure includes options to copy new IP Phone firmware and Voice Gateway Media Card loadware to the Signaling Server. If you use these options during the upgrade, ensure that you upgrade the firmware and loadware on all connected IP Phones and Voice Gateway Media Cards respectively.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Overview

In Succession 1000 Release 3.0, only H.323 signaling was supported on the Signaling Server. Session Initiation Protocol (SIP) signaling was introduced on the Signaling Server in CS 1000 Release 4.0. CS 1000 Release 4.0 also introduced Network Routing Service (NRS) functionality on the Signaling Server. When upgrading your Signaling Server from Succession 1000 Release 3.0 to a newer release, conversion of the H.323 signaling infrastructure to an NRS infrastructure is a critical component of the upgrade. For more information on an NRS upgrade, see *Network Routing Service Installation and Commissioning* (NN43001-130).

CS 1000 Release 6.0 Signaling Server software requires 2 GB of RAM to support operational requirements. Nortel CP PM, IBM X306m, and HP DL320-G4 Signaling Servers come with 1 or more GB of RAM already configured. For more information on system requirements, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

Before starting your upgrade

Read through the following important information before getting started with your CS 1000 Release 6.0 upgrade:

- The Signaling Server is out of service during a software upgrade.
- Ensure that you back up all data to a remote device or FTP server.

  ISP 1100 servers are not supported in CS 1000 Release 6.0; all saved data must be migrated to a supported hardware platform. For CP PM and COTS servers, all hard drives must be reformatted before an upgrade to CS 1000 Release 6.0.
- In earlier versions of CS 1000, there might be more than one database. For example, Signaling Server might be installed with IP Line and NRS. Ensure that you back up all databases that exist.

  All databases might not be restored to the same platform in CS 1000 Release 6.0. For example, Signaling Server applications and NRS can be deployed to different platforms in Release 6.0.

Signaling Server software upgrade task flow

The following is a high-level list of tasks that you go through to complete your upgrade to CS 1000 Release 6.0:

- Back up all databases to a remote device or FTP server. See the procedures in this chapter. For information about the NRS database,

Copyright © 2010 Nortel Networks. All Rights Reserved.

see *Network Routing Service Installation and Commissioning* (NN43001-130).

- Deploy the Linux base platform. For more information, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).
-
- Deploy and configure the Signaling Server package. For more information, see “Signaling Server application installation” (page 195)
- Log on to Unified Communications Manager (UCM). For more information, see “Access UCM” (page 197)
- Access Element Manager through UCM to restore your databases.

Upgrade paths

The following upgrade paths are available to upgrade your Signaling Server software:

- from Succession 1000 Release 3.0 to CS 1000 Release 6.0 (see “Upgrade from Succession 1000 Release 3.0” (page 205))
- from CS 1000 Release 4.0 to CS 1000 Release 6.0 (see “Upgrade from CS 1000 Release 4.0” (page 205))
- from CS 1000 Release 4.5 to CS 1000 Release 6.0 (see “Upgrade from Communication Server 1000 Release 4.5” (page 207))
- from CS 1000 Release 5.0 to CS 1000 Release 6.0 (see “Upgrade from Communication Server 1000 Release 5.0” (page 207))
- from CS 1000 Release 5.5 to CS 1000 Release 6.0 (see “Upgrade from Communication Server 1000 Release 5.5” (page 207)

Upgrade from Succession 1000 Release 3.0

The following task list contains all tasks necessary to upgrade your Signaling Server software from Succession 3.0 to CS 1000 Release 6.0.

1. Upgrade the Signaling Server software.

   For instructions, see Procedure 17 “Upgrading the Signaling Server software” (page 208).

Upgrade from CS 1000 Release 4.0

The following task list contains all of the tasks necessary to upgrade your Signaling Server software from CS 1000 Release 4.0 to CS 1000 Release 6.0.

1. Back up the IP Phone Application Server database (if present).

Copyright © 2010 Nortel Networks. All Rights Reserved.

For instructions, see Procedure 16 “Backing up the IP Phone Application Server database” (page 207)

2. Determine if an NRS database is present.

   For more information about upgrading the NRS application, see *Network Routing Service Installation and Commissioning* (NN43001-130).

3. Upgrade the Signaling Server software.

   For instructions, see Procedure 17 “Upgrading the Signaling Server software” (page 208).

4. Restore the IP Phone Application Server database (if present).

   For instructions, see Procedure 19 “Restoring the IP Phone Application Server database” (page 212).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Upgrade from Communication Server 1000 Release 4.5

The following task list contains the tasks necessary to upgrade your Signaling Server software from CS 1000 Release 4.5 to CS 1000 Release 6.0.

- Perform the instructions to upgrade Signaling Server software (see Procedure 17 “Upgrading the Signaling Server software” (page 208)).

Upgrade from Communication Server 1000 Release 5.0

The following task list contains the tasks necessary to upgrade your Signaling Server software from CS 1000 Release 5.0 to CS 1000 Release 6.0.

- Perform the instructions to upgrade Signaling Server software (see Procedure 17 “Upgrading the Signaling Server software” (page 208)).

Upgrade from Communication Server 1000 Release 5.5

The following task list contains the tasks necessary to upgrade your Signaling Server software from CS 1000 Release 5.5 to CS 1000 Release 6.0.

- Perform the instructions to upgrade Signaling Server software (see Procedure 17 “Upgrading the Signaling Server software” (page 208)).

Upgrade procedures

This section contains the procedures that you use during the Signaling Server software upgrade.

- Procedure 16 “Backing up the IP Phone Application Server database” (page 207)
- Procedure 17 “Upgrading the Signaling Server software” (page 208)
- Procedure 18 “Synchronize IP Telephony nodes” (page 210)
- Procedure 19 “Restoring the IP Phone Application Server database” (page 212)

Perform the following procedure to back up the IP Phone Application Server database.

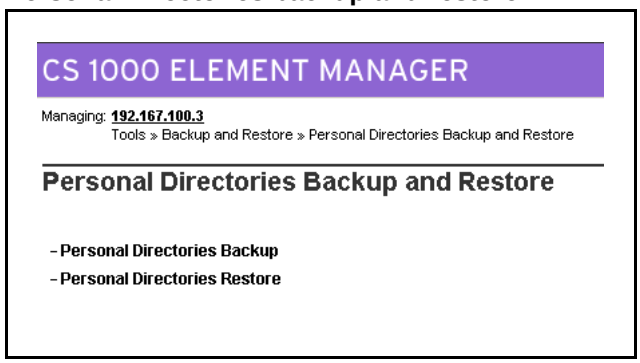
Procedure 16
Backing up the IP Phone Application Server database

Step	Action
1	In the Element Manager navigator, click **Tools, Backup and Restore, Personal Directories**.

Copyright © 2010 Nortel Networks. All Rights Reserved.

The Personal Directories Backup and Restore window appears.

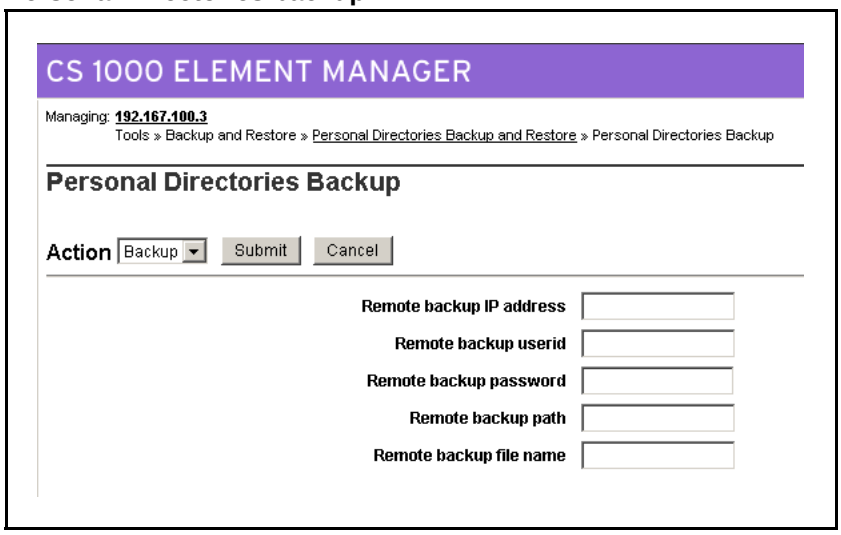
Figure 46
Personal Directories backup and restore



2 Click **Personal Directories Backup**.

The Personal Directories Backup window appears.

Figure 47
Personal Directories backup



3 Enter the data for the **Remote backup IP address**, **Remote backup userid**, **Remote backup password**, **Remote backup path**, and **Remote backup file name fields**.

4 Click **Submit**.

--End--

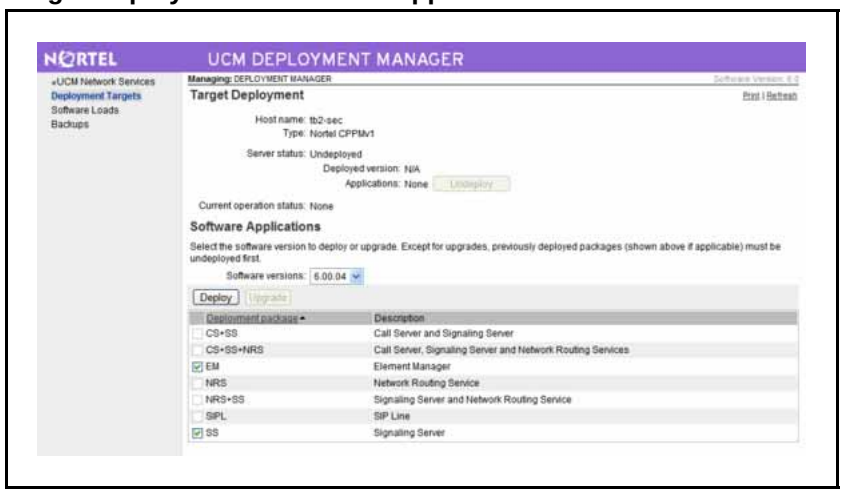
Perform the following procedure to upgrade the software on your Signaling Server.

Procedure 17
Upgrading the Signaling Server software

Copyright © 2010 Nortel Networks. All Rights Reserved.

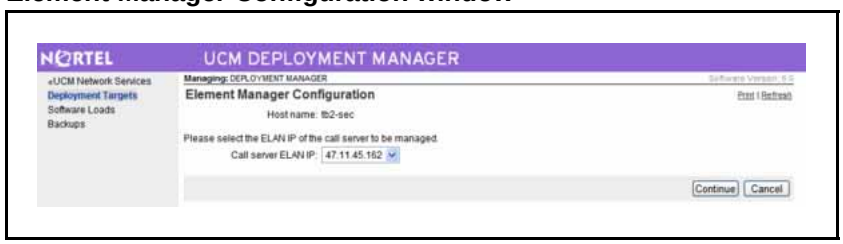
Step	Action
1	Log on to UCM using the Primary UCM Server ID and password credentials.
2	Select **Network, CS 1000 Servers, Software Deployment**. The Target Deployment window appears.
3	Select the target server and click **Deploy**.
4	Select the SS and EM applications.

Figure 48
Target Deployment - Software Applications window



Step	Action
5	On the Element Manager Configuration window, select the Call Server ELAN IP address and click **Continue**. The Call Server must be joined to the Security domain before you proceed with this step.

Figure 49
Element Manager Configuration window



The application deployment starts. Deploying applications might take a few minutes. When the deployment finishes, the Server Status is Deployed.

--End--

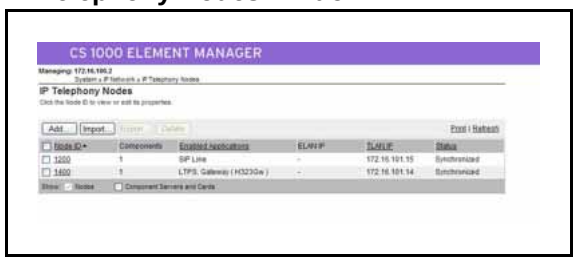
Perform the following procedure to synchronize the IP Telephony nodes using Element Manager.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Procedure 18
Synchronize IP Telephony nodes

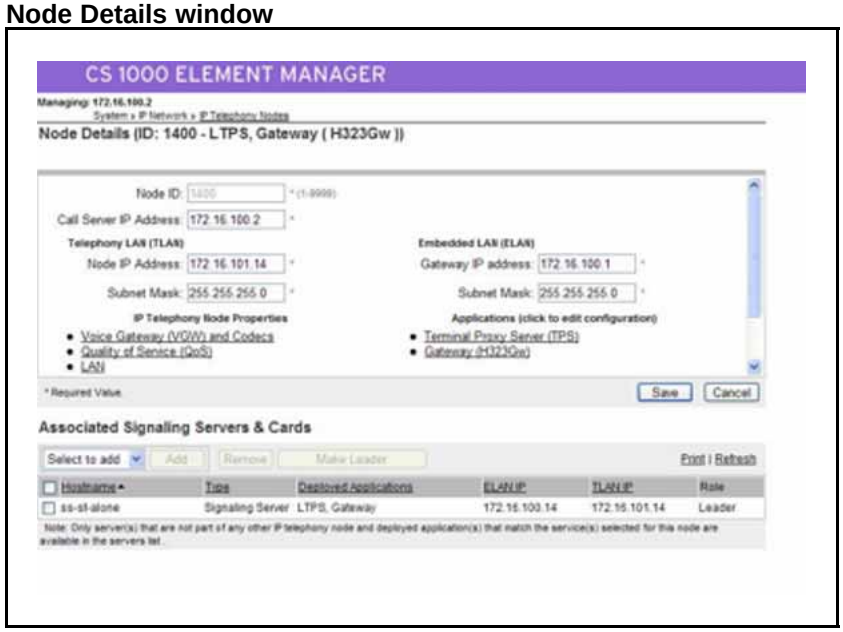
Step	Action
1	Log on to UCM using the Primary UCM Server ID and password credentials.
2	Log on to Element Manager.
3	Select **System, IP Network, Nodes: Server, Media Cards**. The IP Telephony Nodes window appears.

Figure 50
IP Telephony Nodes window



4	Select the link for a Node ID. The Node Details window appears.
5	On the Node Details window ensure the information is correct. Select the various links (TPS, Gateway) to ensure that information is correct.

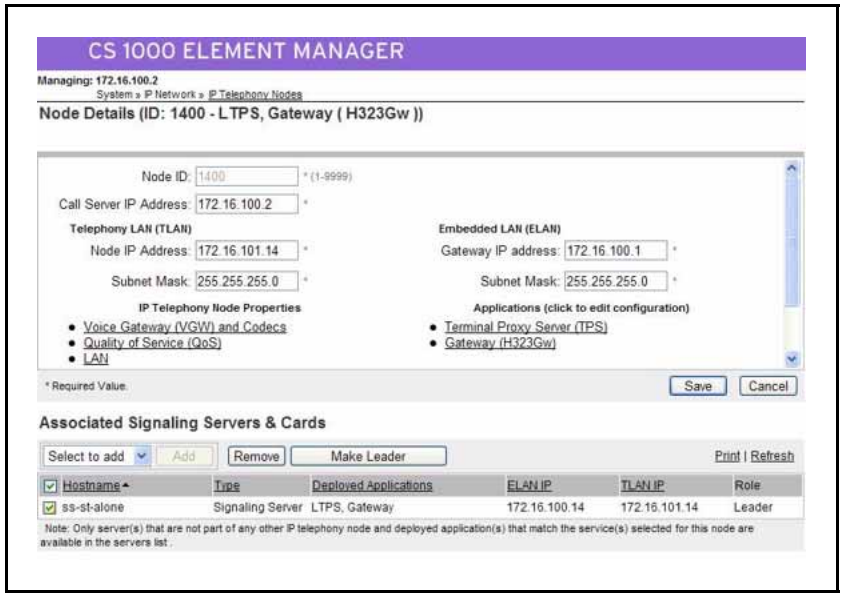
Figure 51
Node Details window



6	In the Associated Signaling Servers & Cards section of the window, select the Signaling Server from the Select to add list and click **Make Leader**.

Copyright © 2010 Nortel Networks. All Rights Reserved.

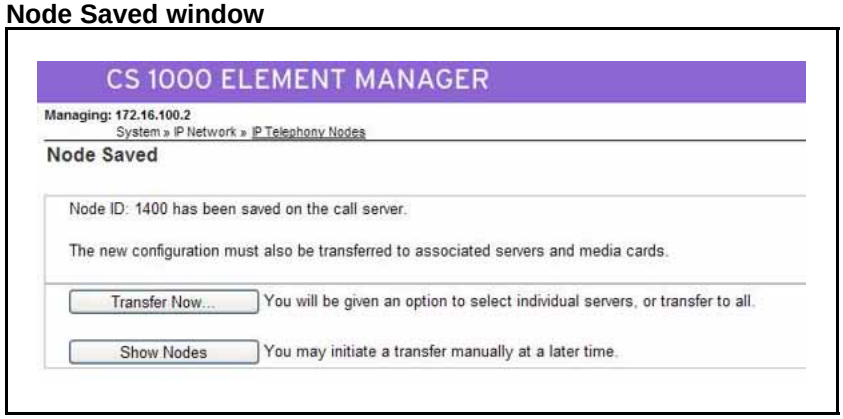
Figure 52
Node Details window - select Leader Signaling Server



7 Click **Save**.

8 Select the follower Signaling Server from the list and click **Add**. Click **Save**. The Node Saved window appears.

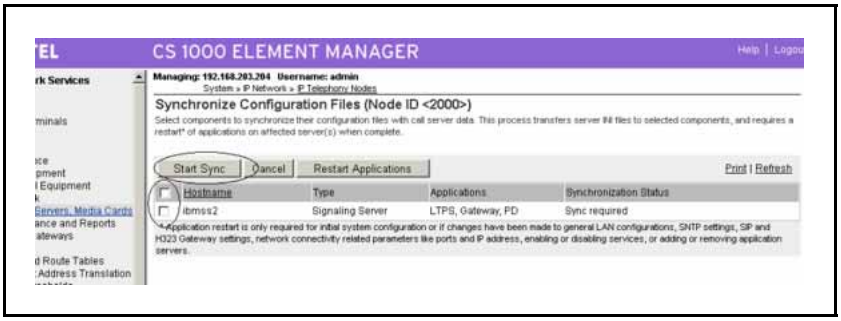
Figure 53
Node Saved window



9 Click **Transfer Now**. The Synchronize Configuration Files window appears.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 54
Synchronize Configuration Files window



10 Select the check boxes for the nodes to synchronize and select **Start Sync**. The Synchronization Status column displays Synchronized when the synchronization finishes.

11 Click **Restart Applications** to restart the Signaling Server applications. The LTPS, Gateway (SIP and H.323), and PD applications are now successfully deployed.

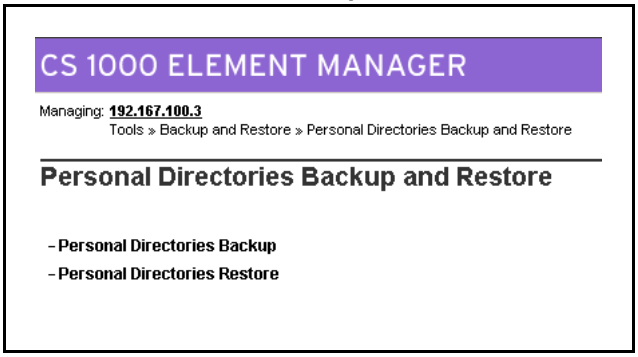
--End--

Perform the following procedure to restore the IP Phone Application Server database.

Procedure 19
Restoring the IP Phone Application Server database

Step	Action
1	In the Element Manager navigator, select **Tools, Backup and Restore, Personal Directories**. The Personal Directories Backup and Restore window appears.

Figure 55
Personal Directories backup and restore

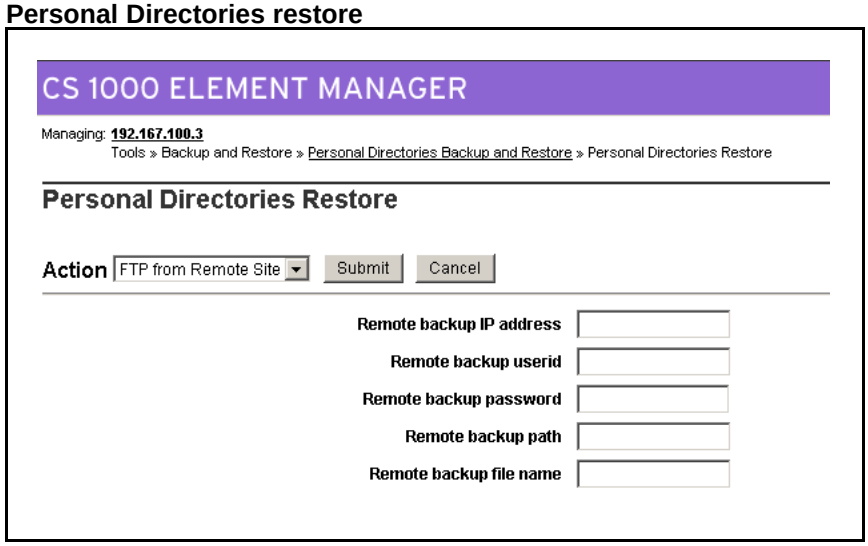


2 Click **Personal Directories Restore**.

The Personal Directories Restore window appears.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 56
Personal Directories restore



3 From the **Action** list, select **FTP from Remote Site** if you saved the backup on a remote server.

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.

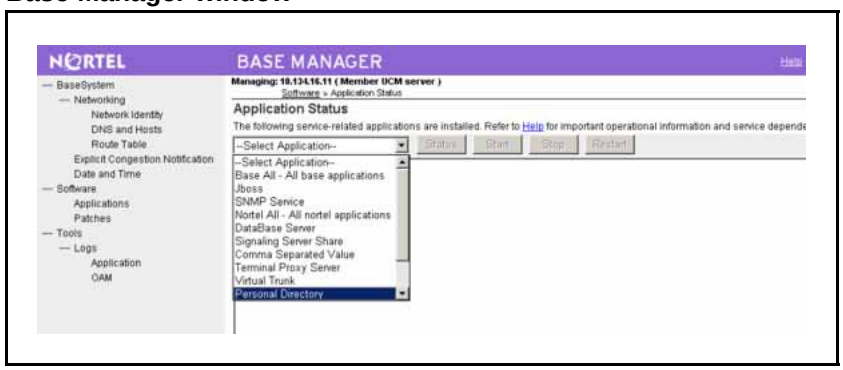
5 Click **Submit**.

6 Click **OK**.

7 Select **System, IP Networks, Maintenance and Reports**. The Node Maintenance and Reports window appears.

8 Click **Reset**. The Base Manager window for the server appears.

Figure 57
Base Manager window



9 Select **Personal Directory** and click **Restart**.

Copyright © 2010 Nortel Networks. All Rights Reserved.

10 Click **OK** to confirm that you want to restart the application. The status of the Personal Directory restart updates when the restart finishes.

--End--

ATTENTION
The length of time to restore an IP Phone Application Server database depends on the number of records.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Installation and initial configuration of an IP Telephony node

Contents

This section contains the following topics:

- "Introduction" (page 215)
- "Equipment considerations" (page 216)
- "Install the hardware components" (page 217)
- "Initial configuration of IP Line data" (page 226)
- "Node election rules" (page 243)

Introduction

This chapter explains how to install and initially configure a new IP Telephony nodes, Voice Gateway Media Cards (Media Card line cards), and associated cables.

Before you install an IP Telephony node, see *Converging the Data Network with VoIP Fundamentals* (NN43001-260) for information about IP network engineering guidelines.

Before configuring an IP Telephony node, you must:

- Install the COTS server or CP PM card and deploy the Linux platform base. For more information, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).
- Deploy the Signaling Server package. For more information, see "Signaling Server software installation using Deployment Manager" (page 193).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Installation and configuration procedures

This chapter contains the following procedures:

- Procedure 20 “Installing the CompactFlash card on the Media Card” (page 218)
- Procedure 21 “Installing the Media Card” (page 219)
- Procedure 22 “Replacing the existing I/O Panel Filter Connector” (page 221)
- Procedure 23 “Installing the Shielded 50-pin to Serial/ELAN/TLAN Adapter onto the Media Card” (page 225)
- Procedure 24 “Configuring the ELAN network interface IP address for the active ELNK” (page 226)

Equipment considerations

This section lists the required and optional equipment to install, configure, and maintain the Voice Gateway Media Cards and IP Phones.

Required equipment

The required equipment includes the following:

- a PC to manage IP Line, with Internet Explorer 6.0.2600 or later to run Element Manager for CS 1000 systems
- local TTY or terminal in a switch room (to configure a Leader)
- 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 a remote dial-up connection to the ELAN subnet for technical support (Nortel RM356 modem router is recommended)

Copyright © 2010 Nortel Networks. All Rights Reserved.

Install the hardware components

For Media Card 32-port card installation instructions, see Procedure 21 “Installing the Media Card” (page 219).

Voice Gateway Media Card

The Media Card 32-port card and the MC 32S card are known as Voice Gateway Media Cards.

Summary of installation steps

The following table summarizes the steps to install each Voice Gateway Media Card.

Table 56
Installation summary

Step	Media Card line cards
Unpack the card.	Remove all contents from the packaging box.
Install the CompactFlash Card.	Procedure 20 “Installing the CompactFlash card on the Media Card” (page 218).
Install the Media Cards.	Procedure 21 “Installing the Media Card” (page 219).
Install NTCW84JA ITG-specific I/O Panel Filter Connector for Option 51C/61C/81/81C.	Procedure 22 “Replacing the existing I/O Panel Filter Connector” (page 221).
Install the A0852632 Shielded 50-pin to Serial/ ELAN/TLAN Adapter.	Procedure 23 “Installing the Shielded 50-pin to Serial/ELAN/TLAN Adapter onto the Media Card” (page 225).
Add the card and configure the card properties.	In Element Manager: Procedure 32 “Adding a card and configuring Voice Gateway Media Card properties” (page 261).
Transmit and transfer properties.	In Element Manager: Procedure 33 “Transmitting node properties to Leader” (page 263).

Installing and cabling the Media Card 32-port card

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 you handle 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 you install the Media Card in the system. Perform the steps in Procedure 20 “Installing the CompactFlash card on the Media Card” (page 218) to install the CompactFlash card.

If it is necessary to remove the CompactFlash card, perform the steps in Procedure 55 “Removing the CompactFlash” (page 377).

Procedure 20
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 precautions for handling ESD-sensitive devices. Wear a properly connected antistatic wrist strap while you remove the cards from the packaging and work on a static-dissipating surface.

2	Locate the CompactFlash card socket in the lower left corner of the Media Card. See Figure 58 "CompactFlash card socket on Media Card" (page 218).

Figure 58
CompactFlash card socket on Media Card



3	Position the CompactFlash card with the label facing up, the metal clip pulled up, and the contact pins toward the socket as shown in Figure 59 "Position the CompactFlash in socket" (page 219).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 59
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 you insert it.

5 Gently insert the CompactFlash card, so that it is fully in contact with the connectors on the drive.

6 Push down the metal clip so that the CompactFlash card is locked in.

--End--

Install the Media Card

To install a Media Card, perform the steps in Procedure 21 “Installing the Media Card” (page 219).

Procedure 21
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 Table 57 "Media Card installation by module type" (page 220).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 57
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 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 contacts the backplane connector. Hook the locking devices.

The red LED on the faceplate remains lit until you configure and enable the card in the software, at which point the LED turns off.

The card faceplate window displays startup self-test results (T:xx) and status messages. A display F:xx indicates that a self-test failed. Some failures indicate that you must replace the card.

See “Transfer node configuration from Element Manager to the Voice Gateway Media Cards” (page 263). See Table 105 "Media Card 32-port card faceplate maintenance display codes" (page 369) 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, you must replace the standard I/O filter connector with the NTCW84JA ITG Line-specific I/O filter connector for the slot occupied by the Media Card.

To replace an existing I/O Panel Filter Connector, perform the steps in Procedure 22 “Replacing the existing I/O Panel Filter Connector” (page 221).

Copyright © 2010 Nortel Networks. All Rights Reserved.

CAUTION
For Large systems manufactured from 1998 to 1999 and shipped in North America, the IPE modules have the NT8D81BA Backplane to I/O Panel ribbon cable assembly with a nonremovable 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 nonremovable filter connector.

Replace existing I/O panel filter connector

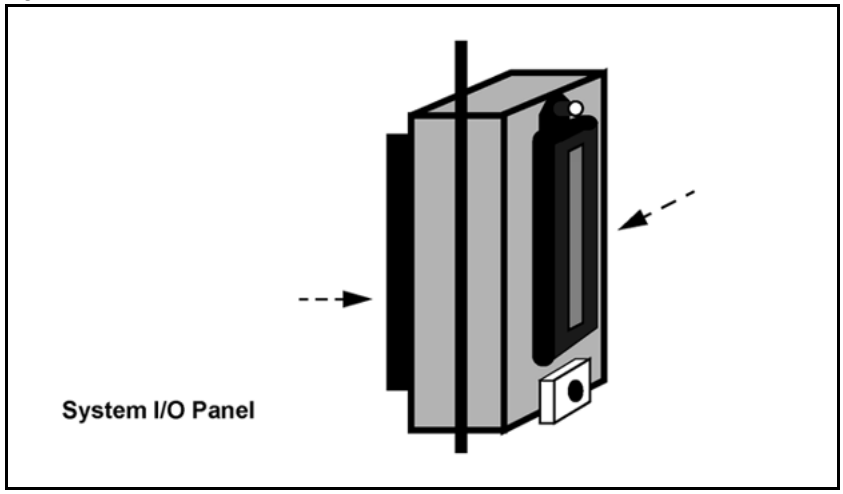
The standard I/O filter connector is shielded metal with a black plastic insert connector. The NTCW84JA connector uses yellow warning labels to indicate EMC filtering modifications and which MDF connection points can support 100BaseT connections.

Procedure 22
Replacing the existing I/O Panel Filter Connector

Step	Action
1	Remove the ITG pack, or any other IPE pack, from the IPE shelf card slot that correspond to the I/O Panel connector to remove.
	ATTENTION Make sure to use the I/O Panel Filter Connector that 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. One screw is on the lower front of the connector and one screw is 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 60 "NTCW84JA 50 pin ITG-specific I/O Panel filter connector for Large Systems" (page 222).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 60
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 the respective solutions are in Table 58 "I/O filter connector" (page 222).

Table 58
I/O filter connector

Scenario	Solution
You forget 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.
You install 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 58
I/O filter connector (cont'd.)

Scenario	Solution
You encounter 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 with interchangeable I/O filter connectors if you must 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 A0852632 Shielded 50-pin to Serial/ELAN/TLAN Adapter (see Figure 61 "Shielded 50-pin to Serial/ELAN/TLAN Adapter" (page 224))

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, which replace the standard connectors 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 (less than 100 meters) are recommended to attach the LAN ports to the local network.

Install the Shielded 50-pin to Serial/ELAN/TLAN Adapter

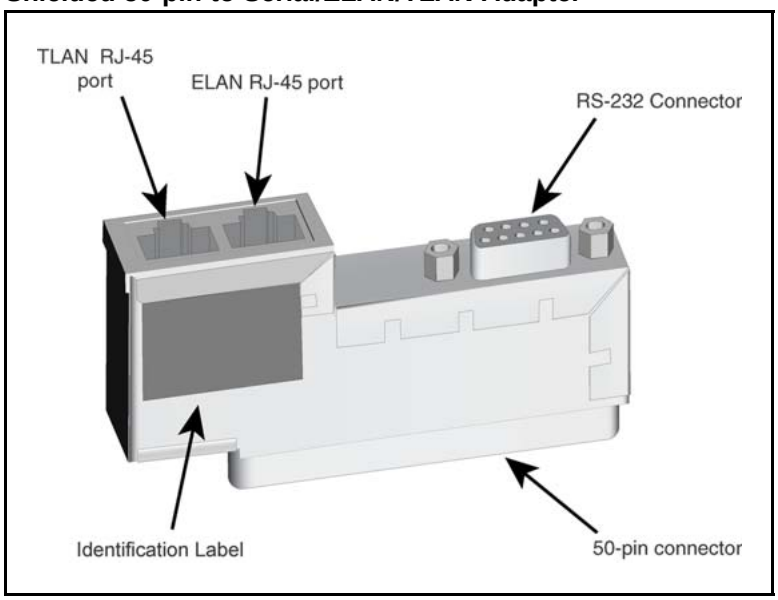
The Media Card can support a single connector solution to access the TLAN and ELAN network interfaces. This connector (see Figure 61 "Shielded 50-pin to Serial/ELAN/TLAN Adapter" (page 224)) is called the A0852632 Shielded 50-pin to Serial/ELAN/TLAN Adapter. It replaces the single NTMF94EA ELAN, TLAN, RS-232 Serial Maintenance I/O interface cable (octopus cable).

Copyright © 2010 Nortel Networks. All Rights Reserved.

The adapter breaks out the signals from the I/O connector to the following components:

- ELAN network interface
- TLAN network interface
- one RS-232 (local console) port

Figure 61
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 61 "Shielded 50-pin to Serial/ELAN/TLAN Adapter" (page 224).

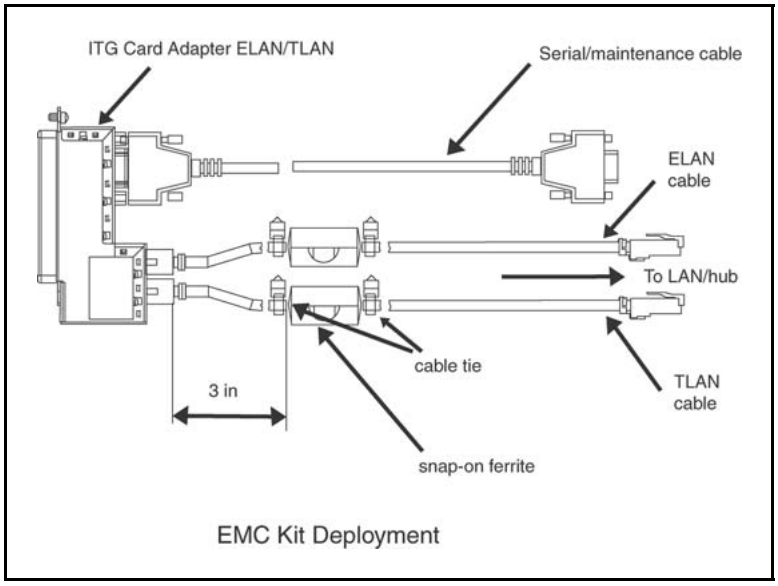
To ensure proper connection, install the adapter securely; otherwise, connectivity can be lost.

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 62 "ITG EMC Shielding Kit Deployment" (page 225), 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 62
ITG EMC Shielding Kit Deployment



Perform the steps in Procedure 23 “Installing the Shielded 50-pin to Serial/ELAN/TLAN Adapter onto the Media Card” (page 225) to install the ITG EMC shielding kit (NTVQ83AA) on the ELAN and TLAN network interface cables.

Procedure 23
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 ships from the factory with a blank compact flash card. When the card first powers up, it starts from a Gold Control and Signaling Processor (CSP) image. The Gold CSP image is a scaled-down version

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 at 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 ships from the factory.

Initial configuration of IP Line data

Before you start the configuration:

- Ensure the system is running CS 1000 Release 6.0 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 31) for more information.

Summary of procedures

This section contains the following procedures:

- "Configuring IP address for the system active ELNK Ethernet network interface (LD 117)" (page 226).
- "Configure VoIP bandwidth management zones (LD 117)" (page 227).
- "Configure virtual superloops for IP Phones" (page 230).
- "Configure IP Phone features in LD 11" (page 232).

Configuring IP address for the system active ELNK Ethernet network interface (LD 117)

To configure the Call Server ELAN network interface IP address (active ELNK), perform the steps in Procedure 24 "Configuring the ELAN network interface IP address for the active ELNK" (page 226).

Procedure 24
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`

Copyright © 2010 Nortel Networks. All Rights Reserved.

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)

You can define up to 256 zones using 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 zones.

Table 59 "LD 117 bandwidth management zone configuration" (page 228) 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). Best Quality (BQ) provides the best voice quality but uses the most bandwidth. Best 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 “Zones” (page 142).

LD 117 also includes the DIS and ENL commands to disable or enable a zone. When a zone is created, the default state is enabled.

Copyright © 2010 Nortel Networks. All Rights Reserved.



CAUTION
You must first configure zone 0 in LD 117 before you configure other zones or all calls associated with zone 0 are blocked.

Table 59
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) – 100 000 (kb/s) p2: intrazone preferred strategy = (BQ – Best Quality) or BB – Best Bandwidth p3: interzone available bandwidth = 0 – (10 000) – 100 000 (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 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 zone parameters. You must reenter all parameters, even those that are unchanged.
OUT ZONE xxx	Remove a zone.
DIS ZONE xxx	Disable a zone. No new calls are established inside, from, or toward a disabled zone.
ENL ZONE xxx	Enable a zone.
PRT ZONE xxx PRT ZONE ALL	Print zone and bandwidth information; xxx specifies a zone. If no zone is specified, information for all zones is printed. PRT ZONE ALL also prints information for all zones.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Element Manager for Zone Configuration

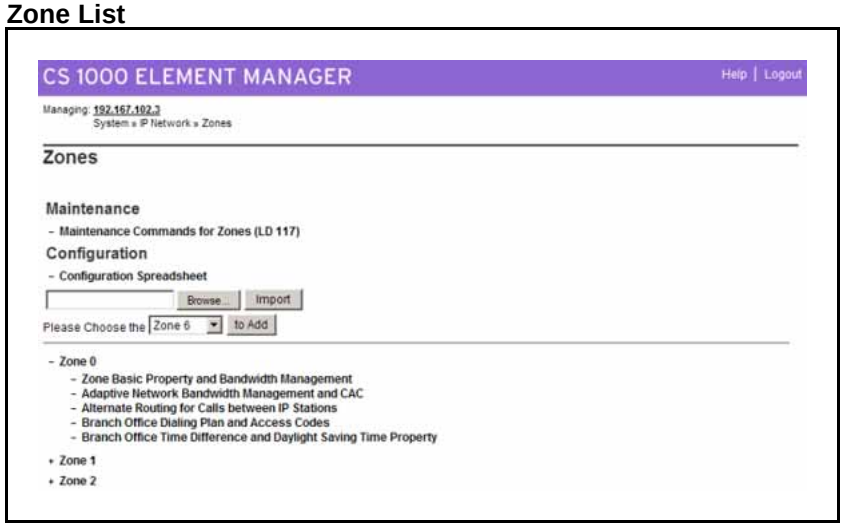
Optionally, you can configure zones for CS 1000 systems using Element Manager instead of LD 117.

To view Element Manager for zone configuration, perform the steps in Procedure 25 “Viewing Element Manager for Zone Configuration” (page 229)

Procedure 25
Viewing Element Manager for Zone Configuration

Step	Action
1	Log on to UCM and access Element Manager.
2	In the navigator, select **IP Network, Zones**. The Zones window appears. See Figure 63 "Zone List" (page 229).

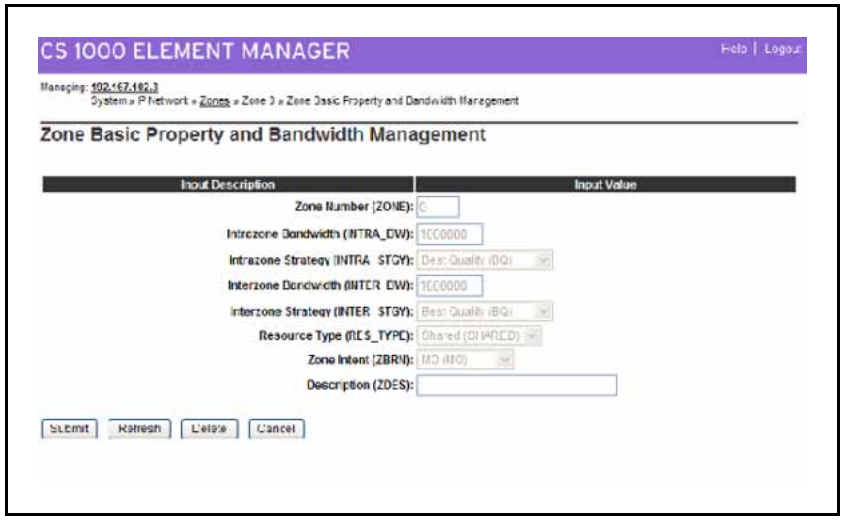
Figure 63
Zone List



3	Under **Configuration**, click **to Add** to add a new zone. The Zone Basic Property and Bandwidth Management window appears. See Figure 64 "Zone Basic Property and Bandwidth Management window" (page 230).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 64
Zone Basic Property and Bandwidth Management window



--End--

Configure virtual superloops for IP Phones

You must configure one or more virtual superloops to support IP Phone Virtual TN (VTN) in LD 97 or in Element Manager.

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 Fiber Network (FIBN) Package 365, a maximum of five network groups is available, 0 to 4. With Package 365, a maximum of eight network groups is available, 0 to 7.

For normal traffic engineering, provision up to 1024 VTN on a single virtual superloop for a Large System/CS 1000E. For nonblocking, do not exceed 120 VTN on a single virtual superloop for a Large System/CS 1000E.

Nortel recommends that configure virtual superloops starting in the highest non physically equipped group available. Table 60 "LD 97 Virtual superloop configuration for Large Systems/CS 1000E" (page 231) lists the prompts and responses required to configure virtual superloops in LD 97.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 60
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: • 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

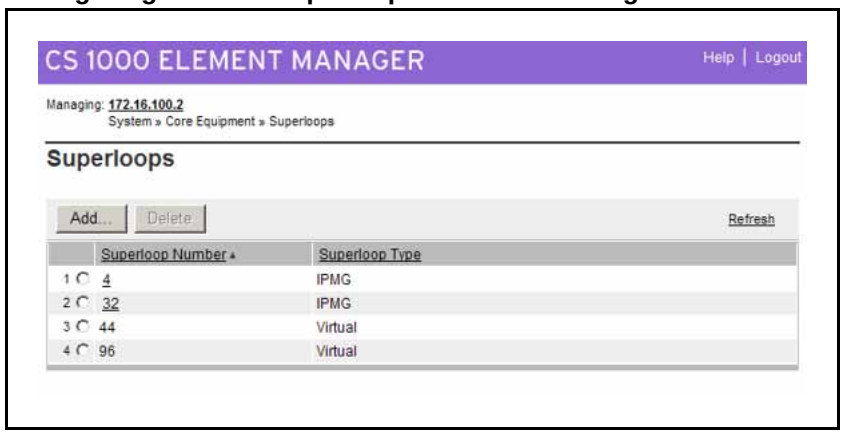
Configuring virtual superloops in Element Manager

To configure a virtual superloop in Element Manager, perform the steps in Procedure 26 “Configuring a virtual Superloop in Element Manager” (page 231).

Procedure 26
Configuring a virtual Superloop in Element Manager

Step	Action
1	In the Element Manager navigator, select **System, Core Equipment, Superloops**. The Superloops window appears. See Figure 65 "Configuring a virtual superloop in Element Manager" (page 231).
2	Select the superloop number from the **Choose a Superloop Number** list.
3	Select **Virtual** from the **type** list.

Figure 65
Configuring a virtual superloop in Element Manager



Copyright © 2010 Nortel Networks. All Rights Reserved.

4 Click **to Add**.

--End--

Configure IP Phone features in LD 11

The existing License header that prints at the start of LD 11 includes the new License limit for the IP Phone. See Table 55 "IP Phone configuration data summary sheet" (page 192).

Table 61
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 :	2001P2, 2002P1, 2002 P2, 2004P1, 2004P2, 2033, 2007, 2050PC, 2050MC, 1110, 1120, 1140, 1150, 2210, 1210, 1220, 1230, 2211, 2212, 6120, 6140	For IP Phone 2001, IP Phone 2002, IP Phone 2004, IP Audio Conference Phone 2033, IP Phone 2007, IP Phone 1210, IP Phone 1220, IP Phone 1230, 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	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 *Software Input Output — Administration* (NN43001-611).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 61
LD 11 Configure an IP Phone (cont'd.)

Prompt	Response	Description
KEY	xx aaa yy zz...zz	IP Phone function key assignments: xx: keys 0 to 5 xx: keys 6 to 11, using either the Shift key for IP Phone 2004, IP Phone 2007, IP Phone 1140E, IP Phone 1150E, WLAN Handsets 2210/2211/2212/6120, or Second Page functionality for IP Phone 1220 and IP Phone 1230 xx: keys 0 to 3 for the IP Phone 2002, IP Phone 1220, IP Phone 1230 and IP Phone 1120E These keys are self-labeled physical keys that you can program with any feature. For the WLAN Handset 2210, 2211, 2212, 6120, the keys are self-labeled virtual keys that you can program with any feature. xx: 0 for the IP Phone 2001, IP Audio Conference Phone 2033, IP Phone 1210, and IP Phone 1110; any other key number entered returns an error message. aaa: key name or function yyy, zzz: additional information required for the key. Keys 16 to 26 are reserved for dedicated IP Phone context-sensitive soft keys. Table 66 "LD 11 IP Phone dedicated context-sensitive soft key assignment" (page 242) lists the dedicated IP Phone key name values (aaa). Other key name values are in *Software Input Output — Administration* (NN43001-611).

Configure the IP Phone Key Expansion Module

Configure the optional IP Phone Key Expansion Module (KEM) in LD 11.

The IP Phone 2002 and IP Phone 2004 support the IP Phone KEM.

Table 62
LD 11 Configure the IP Phone KEM

Prompt	Response	Description
REQ :	NEW CHG	Add new data. Change existing data.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 62
LD 11 Configure the IP Phone KEM (cont'd.)

Prompt	Response	Description
TYPE : ...	2002P1, 2002P2, 2004P1, 2004P2	IP Phone 2002 (Phase I and Phase II) 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. Press **Enter**without entering a number to leave the value unchanged.
...		
	xx aaa yyyy (cccc or D) zz..z	
KEY		IP Phone function key assignments The following key assignments determine calling options and features available to a telephone. The KEY prompt repeats until you press **Enter**. xx: key number For IP Phone 2002: 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: 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

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 62
LD 11 Configure the IP Phone KEM (cont'd.)

Prompt	Response	Description
		The cccc or D entry deals specifically with the Calling Line Identification feature: cccc: CLID table entry of (0)-N; 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 you enter the character D, 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 is used. The position of the (cccc or D) field varies depending on the key name or function.
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) Enter <CR> to keep the current setting.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 62
LD 11 Configure the IP Phone KEM (cont'd.)

Prompt	Response	Description
KEMOFST	<KEM> <KeyOffset>	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 appears, 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: 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 IP Phone 1120E, IP Phone 1140E, and IP Phone 1150E support the Expansion Module.

Table 63
LD 11 Configure the Expansion Module

Prompt	Response	Description
REQ	NEW/CHG	Add new or change existing data.
TYPE	1120, 1140, 1150	For IP Phone1120E, IP Phone 1140E, and IP Phone 1150E
…	…	…
KEM	(0) - 3/ <CR>	Number of attached Expansion Modules (0). Up to three Expansion Modules are supported.

Copyright © 2010 Nortel Networks. All Rights Reserved.

…	…	…
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: 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: 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 configuration <CR> or just <CR>.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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>.

Configure the IP Phone 1200 Series Key Expansion Module

Configure the optional IP Phone 1200 Series Key Expansion Module (KEM) in LD 11.

The IP Phone 1220 and IP Phone 1230 support the IP Phone 1200 Series KEM.

Table 64
Configure the IP Phone 1200 Series KEM

Prompt	Response	Description
REQ	NEW/CHG	Add new or change existing data.
TYPE	1220, 1230	For IP Phone 1220, IP Phone 1230
…	…	…
KEM	(0) - 4/ <CR>	Number of attached Expansion Modules (0). Supports up to four Expansion Modules.
…	…	…
KEY	0 - <see text>/ <CR>	Key number range depends on the number of IP Phone 1200 Series KEM modules specified by KEM prompt: xx: key number For the IP Phone 1230: xx: 0 to 31 when KEM: 0 xx: 0 to 55 when KEM: 1 xx: 0 to 79 when KEM: 2 xx: 0 to 67 when KEM: 3

Copyright © 2010 Nortel Networks. All Rights Reserved.

		xx: 0 to 79 when KEM: 4 For the IP Phone 1220: xx: 0 to 31 when KEM: 0 xx: 0 to 43 when KEM: 1 xx: 0 to 55 when KEM: 2 xx: 0 to 67 when KEM: 3 xx: 0 to 79 when KEM: 4
PAGEOFST	<Page> <KeyOff-set> <CR>	This prompt appears if one or two IP Phone 1200 Series KEM are specified at the KEM prompt, if <CR> is entered at the KEY prompt, and if attached to an IP Phone 1230. This prompt enables the administrator to enter: Page number: 0 for KEM 1 1 for KEM 1 when you configure 1 KEM and 2 KEM when you configure 2 KEMs 2 for KEM 1 3 for KEM 2 and a Key Offset number from 0 to 11.
KEY <key>	<keys conf data>	<key> is the key number for the Page + Key Offset entered at PAGEOFST. Enter the key configuration <CR> or just <CR>.
KEMOFST	<KEM> <Key-Off-set>/ <CR>	This prompt appears for the IP Phone 1220 or if three or four IP Phone 1200 Series KEMs are specified at the KEM prompt for the IP Phone 1230 and <CR> is entered for KEY prompt. This prompt enables the administrator to enter a KEM number of 1, 2, 3, or 4 and a Key Offset number from 0 to 11. After you enter the KEM number,

Copyright © 2010 Nortel Networks. All Rights Reserved.

		the KEY prompt appears 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 configuration <CR> or just <CR>.

Configure the Expansion Module 2050

Configure the optional Expansion Module 2050 in LD 11.

The IP Softphone 2050 support the Expansion Module 2050.

Table 65
Configure the Expansion Module 2050

Prompt	Response	Description
REQ	NEW/CHG	Add new or change existing data.
TYPE	2050	For Softphone 2050
…	…	…
KEM	(0) - 3/ <CR>	Number of attached Expansion Modules 2050 (0). Supports up to three Expansion Modules 2050.
…	…	…
KEY	0 - <see text>/ <CR>	Key number range expanded to support number of Expansion Modules 2050 specified by KEM prompt. The range on the IP Softphone 2050 is as follows: xx: key number xx: 0 to 31 when KEM: 0 xx: 32 to 49 when KEM: 1 xx: 50 to 67 when KEM: 2 xx: 68 to 85 when KEM: 3

Copyright © 2010 Nortel Networks. All Rights Reserved.

PAGEOFST	<Page> <KeyOff-set> <CR>	PAGEOFST is prompted if one Expansion Module 2050 is specified at the KEM prompt and <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 configuration <CR> or just <CR>.
KEMOFST	<KEM> <Key-Off-set>/ <CR>	KEMOFST is prompted if two or three Expansion Modules are specified at the KEM prompt and <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 configuration <CR> or just <CR>.

IP Phone dedicated context-sensitive soft keys

Table 66 "LD 11 IP Phone dedicated context-sensitive soft key assignment" (page 242) 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 1220, IP Phone 1230, 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 2210/2211/2212/6120/6140. Remove unused feature keys by configuring the dedicated context-sensitive soft keys to NUL. Some features depend on the CoS.

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).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 66
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
Key 18	A03, A06, 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

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 can 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 runs the VTRK application.

The rules for the node election process are as follows:

- A Leader always wins over a Follower.
- Within each class (Leader/Follower), the Signaling Server with the longest up time wins.
- If a tie for up time occurs, the Signaling Server with the lowest IP address wins.

The precedence of the rules is from 1 (highest) to 3 (lowest).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Configuration of IP Telephony nodes using Element Manager

Contents

This section contains the following topics:

- "Introduction" (page 245)
- "Configure IP Line data using Element Manager" (page 246)
- "Transfer node configuration from Element Manager to the Voice Gateway Media Cards" (page 263)
- "Upgrade the Voice Gateway Media Card and IP Phone firmware" (page 264)
- "Assemble and install an IP Phone" (page 275)
- "Change the default IPL CLI Shell password" (page 275)
- "Configure the IP Phone Installer Passwords" (page 275)
- "Import node configuration from an existing node" (page 276)

Introduction

This chapter explains how to configure IP Telephony nodes using Element Manager. Access Element Manager using a PC with Internet Explorer 6.0.2600 or later. The PC must connect 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 instructions for upgrading IP Phone firmware.

Read the IP network engineering guidelines in *Converging the Data Network with VoIP Fundamentals* (NN43001-260) before installing an IP Telephony node.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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. You can configure and manage more than one node using Element Manager.

Node definition

A node is defined as a collection of Signaling Servers. Each node in the network has a unique Node ID. This Node ID is an integer value. A node has only one Primary Signaling Server. All other Signaling Servers are defined as Followers.

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 "Subnet Mask Conversion from CIDR to Dotted Decimal Format" (page 403).

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; you cannot see real-time changes as they occur. For this reason, you must turn off Internet Explorer caching.

See "Configuring the Internet Explorer browser" (page 198)for more information.

Summary of procedures

The following is the summary of the steps required to configure a node using Element Manager:

1. "Manually add an IP Telephony node" (page 246)
2. "Configuring SNMP trap destinations and community strings" (page 252)
3. "Configure Voice Gateway Profile data" (page 253)
4. "Configure Quality of Service" (page 257)
5. "Configure file server access" (page 259)
6. "Configure loss and level plan" (page 260)

Manually add an IP Telephony node

Follow the steps in Procedure 27 "Adding an IP Telephony node manually" (page 247) to add an IP Telephony node using Element Manager.

Copyright © 2010 Nortel Networks. All Rights Reserved.

When you work in the IP Network, Node: Servers, Media Cards window, Element Manager times out after a period of inactivity. A warning appears 5 minutes before Element Manager times out. If you click OK within the warning time-out period, the timer is reset. If you do not respond, the session terminates and you must log on again. Any data that you change but do not submit is lost.

Procedure 27
Adding an IP Telephony node manually

Step	Action
1	Log on to UCM with appropriate credentials.
2	In Element Manager, select **IP Network, Node: Servers, Media Cards** . The IP Telephony Nodes window appears. See Figure 66 "Adding a new node" (page 247). **Figure 66** **Adding a new node**  If this is the first node to add, the No nodes are configured message appears. Two options are available: **Add**or **Import**. The IP Telephony Nodes window lists all configured nodes. To view a node and the elements, select the link for the Node ID.
3	Click **Add** . The New IP Telephony Node window appears. See New IP Telephony Node window - Step 1
4	Type an identifier for the node in the **Node ID** field. The Node ID can be a value between 0 and 9999. When you define the node number, determine if the Enhanced Redundancy for IP Line Nodes functionality is required. For more information on Enhanced Redundancy for IP Line Nodes, see “Enhanced Redundancy for IP Line nodes” (page 152). If it is required, factor the requirement into the node number assignment process.

Copyright © 2010 Nortel Networks. All Rights Reserved.

The Node ID field corresponds to the Node ID field in the IP Phone configuration. Note the node number used during the IP Phone configuration.

5 Type the IP address for the Call Server in the **Call server IP address** field.

6 Select the radio button corresponding to the required value in the **TLAN address type** field.

If the TLAN address type supports IPv4 only, select the value **IPv4 only**. If dual stack is supported, select the value**IPv4 and IPv6**.

7 Enter the details for the ELAN in the following fields:

a Type the ELAN subnet gateway IP address in dotted decimal format in the **Gateway IP address** field.

This is the IP address of the router interface on the ELAN subnet, if present. If there is no ELAN subnet gateway, type 0.0.0.0.

b Type the ELAN subnet mask address in dotted decimal format in the **Subnet mask** field.

8 Enter the details for the TLAN in the following fields:

a Type the TLAN node IPv4 address in the **Node IPv4 address** field.

b Type the TLAN subnet mask address in dotted decimal format in the **Subnet mask** field.

c Type the TLAN node IPv6 address in the **Node IPv6 address** field.

9 Select the check box corresponding to **SIP Line** to deploy the SIP Line software application to the element.

10 Select the check box corresponding to **UNIStim Line Terminal Proxy Server (LTPS)** to deploy the LTPS software application to the element.

11 Select the check box corresponding to **Virtual Trunk Gateway (SIPGw, H323Gw)** to deploy the Virtual Trunk Gateway software application.

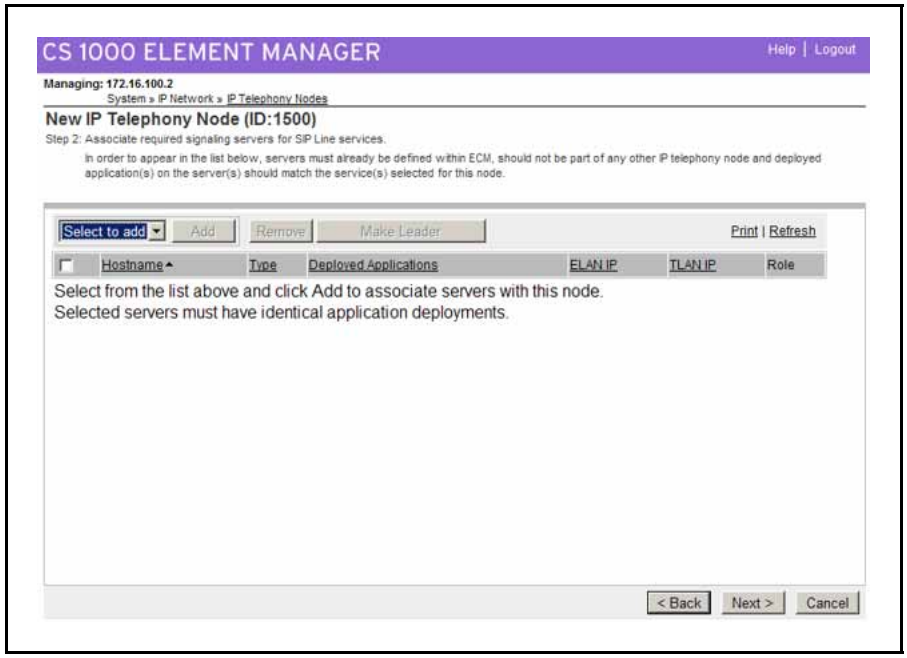
ATTENTION
Do not click **Save** until you enter all information for the node. If you click **Save** . You can click **Edit** to return to the IP Telephony Node window and continue the configuration.

12 Click **Next**.

The next page of the New IP Telephony Node window appears.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 67
New IP Telephony Node window - Step 2



13 Select the required Signaling Server from the **Select to add** field.

If you select **Media card**, the New Media Card window appears.

14 To make a node as the leader, perform the following steps:

a Select the check box corresponding to the signaling server.

b Click **Make Leader**.

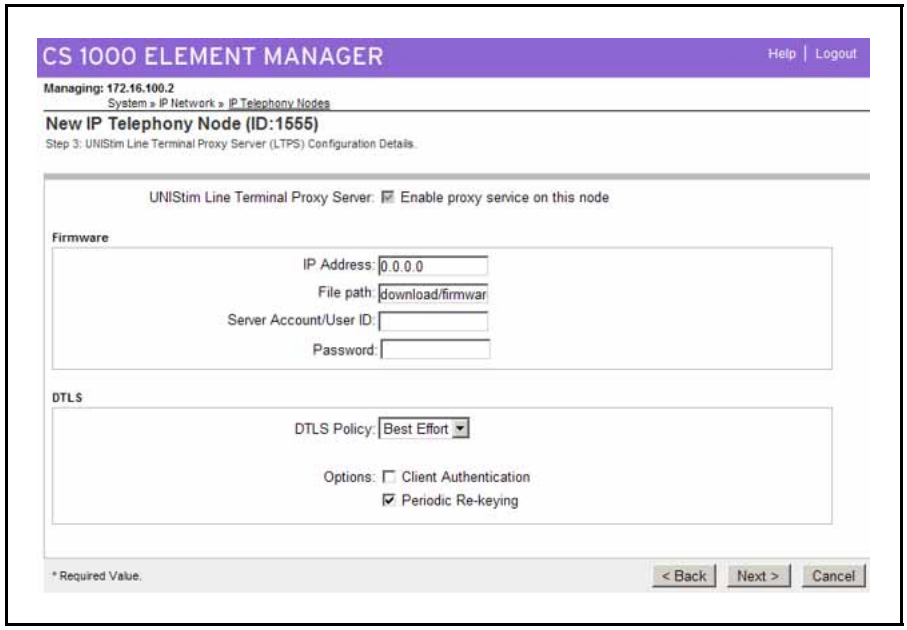
15 To associate servers with the node, click **Add**.

16 Click **Next** to proceed to the next window of the New IP Telephony node configuration.

17 If you selected the UNIStim Line Terminal Proxy Server (LTPS) check box in the page one of the configuration, provide the information for the UNIStim Line Terminal Proxy Server (LTPS).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 68
New IP Telephony Node window - Step 3



a **IP Address:** Type the IP address where the firmware for IP Phones are downloaded from.

b **File path:** Type the path where the files are located.

c **Server Account/User ID:** Type the server account name or user id.

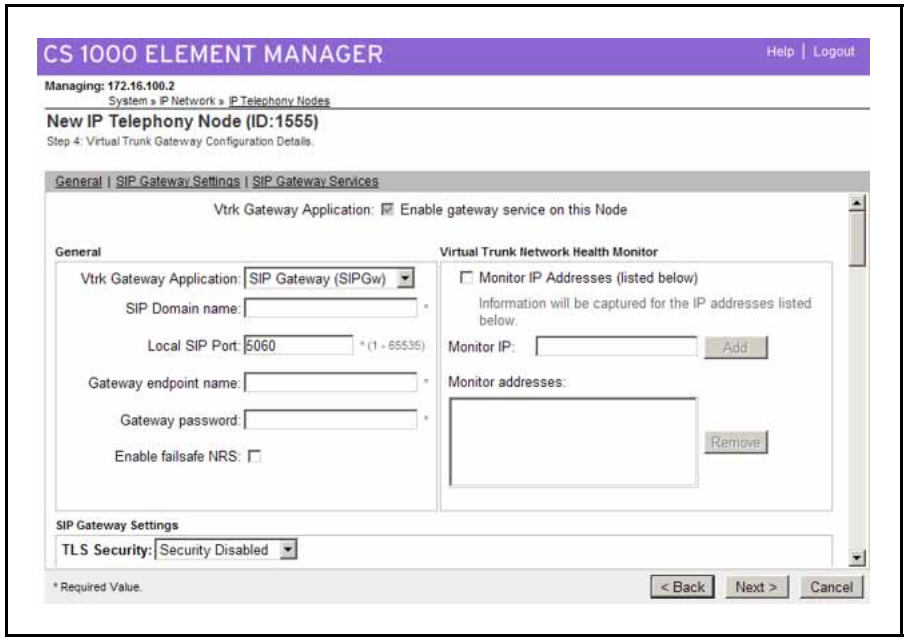
d **Password:** Type the password for the server account.

18 Click **Next** to proceed to the next window of the New IP Telephony node configuration.

In this page you can configure the settings for the Virtual Trunk Gateway.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 69
New IP Telephony Node window - Step 4



19 Provide the information corresponding to following parameters in the **General**tab of the window.

a **Vtrk gateway application**

b **SIP domain name**

c **Local SIP port**

d **Gateway endpoint name**

e **Gateway password**

f **H.323 ID**

g **Enable failsafe NRS**

h **SIP ANAT**

i **Monitor IP Addresses** Select the check box to enable the virtual trunk health monitor. Enter an IP address in the Monitor IP box and click **Add**.

20 Select the **SIP Gateway Settings** link to view all the parameters for the SIP gateway.

21 Click **Next** to proceed to the next window of the New IP Telephony node configuration.

22 On the last window of the new node configuration, review the information and click **Finish**.

--End--

Copyright © 2010 Nortel Networks. All Rights Reserved.

SNMP configuration

For more information about SNMP, see *Communication Server 1000 Fault Management—SNMP* (NN43001-519).

Configuring SNMP trap destinations and community strings

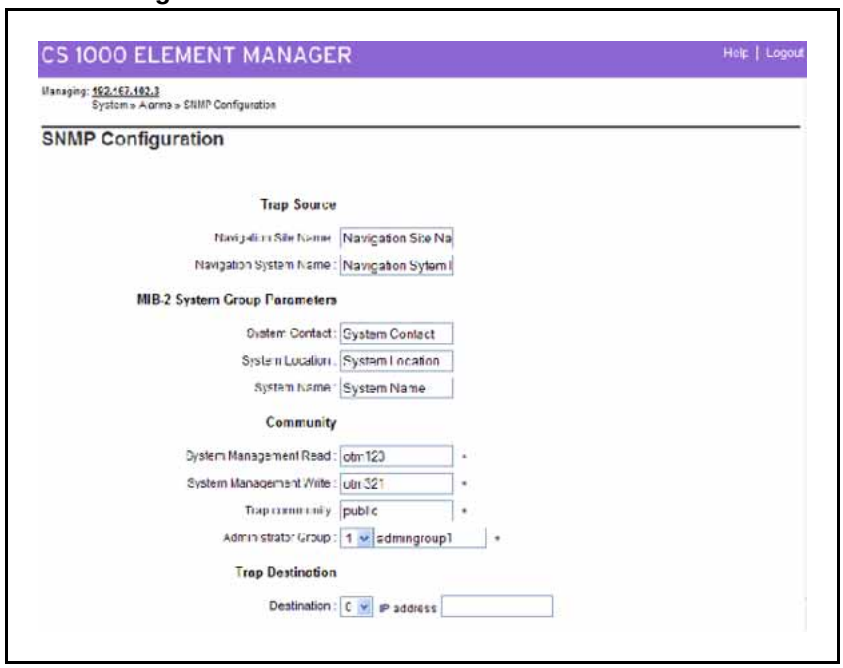
IP Line introduces single point configuration for SNMP traps. To configure the SNMP trap destinations and community strings for the Call Server, Signaling Server, and Media Gateway Controller in Element Manager, perform the steps in Procedure 28 “Configuring SNMP trap destinations” (page 252).

ATTENTION
You must perform a datadump to save the configuration information permanently whether the parameters are configured in Element Manager or in LD 117.

Procedure 28
Configuring SNMP trap destinations

Step	Action
1	In the Element Manager navigator, click **System, Alarms, SNMP**. The SNMP Configuration window appears. See Figure 70 " SNMP configuration window" (page 252).

Figure 70
SNMP configuration window



Step	Action
2	In the **Trap Source** section, enter the following parameters:

Copyright © 2010 Nortel Networks. All Rights Reserved.

- **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 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, 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

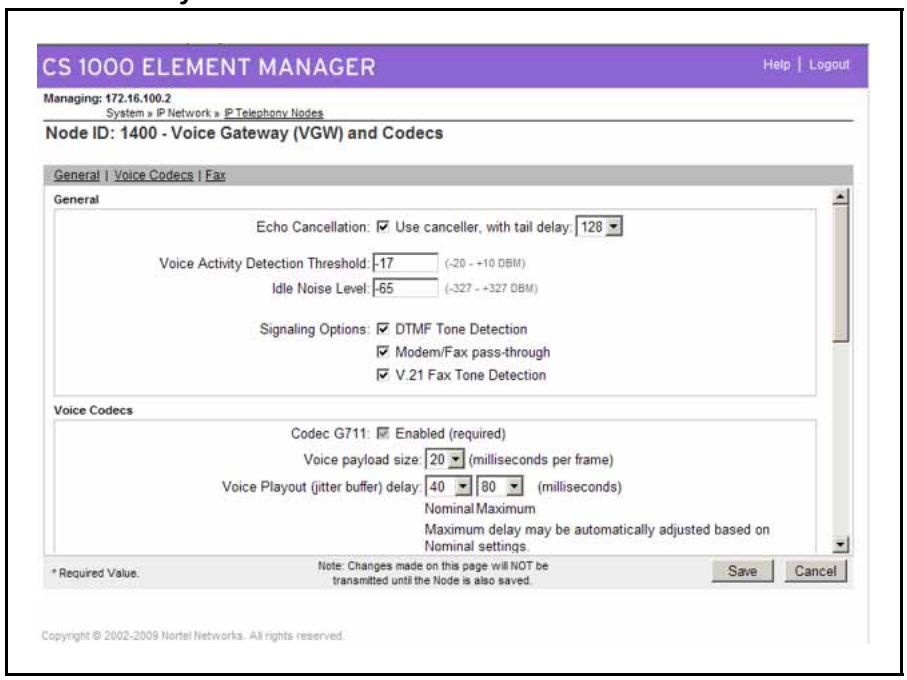
Perform the steps in Procedure 29 “Configuring DSP Profile data” (page 254) to configure the Voice Gateway Profile data.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Procedure 29
Configuring DSP Profile data

Step	Action
1	In Element Manager, select **System, IP Network, Nodes: Server, Media cards**. The IP Telephony Nodes window appears.
2	Select a link for a Node ID. The Node Details window appears.
3	Select the **Voice Gateway (VGW) and Codecs** link.
4	The Voice Gateway (VGW) and Codecs window appears. See Figure 71 "Voice Gateway and Codecs" (page 254). This window displays VGW information and a list of codecs. Leave the default values unless Nortel Field Support directs you to change them.

Figure 71
Voice Gateway and Codecs



To select a codec, scroll through the list, and click the corresponding **Select** check box. A maximum of four codecs can be selected.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Recommendation

Nortel recommends that you configure the system with both G.711 and G.729A if a possibility exists that an IP Softphone 2050 can be configured with the "I use a modem to connect to the network" check box checked. If the node does not have G.729A or G.723 configured, IP Softphone 2050 users with that check box selected will have calls blocked.

This does not apply to the MVC 2050 as it supports only G.711 capability; no dial-up capability is available.

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.

5 Provide information for the following parameters in the General section of the window.

a **Echo Cancellation:** Echo cancellation is enabled by default. Do not clear this check box. Never disable echo canceller unless directed by Nortel Field Support.

b **Echo Cancellation:** Echo cancellation is enabled by default. Do not clear this check box. Never disable echo canceller unless directed by Nortel Field Support.

c **Use canceller, with tail delay:** Select the maximum value available. The default value is 128 ms. Never reduce the echo cancellation value unless directed by Nortel Field Support.

d **Voice activity detection threshold:** The default value is –17 db. The range is –20 db to +10 db.

e **Idle noise level:** The default value is –65 db. The range is –327 db to +327 db.

f **DTMF Tone detection:** Select to enable DTMF tone detection. This is enabled by default.

g **Enable V.21 FAX tone detection:** Select to enable V.21 FAX tone detection. This is enabled by default.

6 By default, the G.711, G711 Clear Channel, and T.38 FAX codecs are selected; you cannot clear them. However, you can change the following:

- The payload size, jitter buffer setting, and companding law for the G.711 codec. The default is G.711 mu-law.
- Only the jitter buffer can change for the G.711 Clear Channel codec.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Up to three additional codecs can be optionally selected: G.729A, G.729AB, or G.723.1 codecs.

- If the G.729A or G.729AB codec are selected, the payload and jitter buffer can change. The payload defaults are the maximum supported payload.
- If the G.723.1 codec is selected, only the jitter buffer can change. The payload size of 30 ms is the only supported payload.

The supported G.723.1 codec has bit rates of 5.3 kb/s and 6.3 kb/s.

Element Manager enables some jitter buffer adjustments on the browser side:

- A change of payload resets the Nominal Voice Playout (NVP) and Maximum Voice Playout (MVP) values to the default recommended values:
  NVP = 2 * payload
  MVP = NVP + 2 * payload
- A change of NVP value changes the MVP value to the default (MVP = NVP + 2 * payload) and changes the values listed in the MVP list so the minimum value does not violate the requirement of NVP + 2 * payload.
- The MVP value can be changed. The values range from the minimum recommended value to the maximum allowed value for the selected codec type.

7 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 uses the default maximum value: 30 ms or G.711 (a-law and mu-law), 50 ms for G.729A, 50 ms for G.729AB, and 30 ms 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:** Configure the nominal value to the highest setting that the device allows. The range is 20 to 200 ms and depends on the codec. Changing this value can automatically adjust the other settings for this codec. For more information, see *Converging the Data Network with VoIP Fundamentals* (NN43001-260).

Copyright © 2010 Nortel Networks. All Rights Reserved.

d **Voice playout (jitter buffer) maximum delay:** The maximum delay has a range of 60 to 500 ms and depends on the codec. Changing this value can automatically adjust the other settings for this codec.

e **Voice Activity Detection (VAD)** Select this check box to enable Voice Activity Detection.

Because CS 1000 Release 6.0 does not support VAD for G723.1 codec, Element Manager does not support configuration of VAD for G723.1.

8 Select parameters for the fax codecs.

a **FAX maximum rate:** The FAX maximum rate is one of the following values: 2400, 4800, 7 200, 9 600, 12 000, or 14 400. The default value is 14 400 bps.

b **FAX playout nominal delay:** The default value is 100 ms. The range is 0 ms to 300 ms.

c **FAX no activity timeout:** The default value is 20 seconds. The range is from 10 seconds to 32 000 seconds.

d **FAX packet size:** Select the desired FAX packet size. The default value is 30 bytes. The range is from 20 to 48 bytes.

9 Repeat step 5 for each selected codec.

--End--

Configure Quality of Service

The Quality of Service (QoS) section includes the settings for the following:

- DiffServ CodePoint (DSCP)
- 802.1Q support

Perform the steps in Procedure 30 “Configuring QoS” (page 257) to configure QoS.

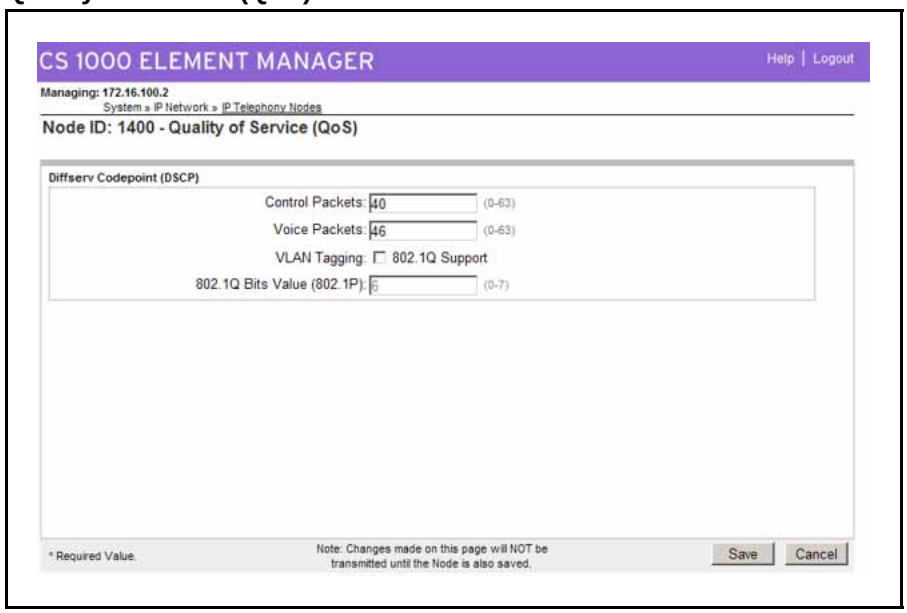
Procedure 30
Configuring QoS

Step	Action
1	In Element Manager, select **System, IP Network, Nodes: Server, Media cards**.
2	Select a link for a Node ID. The Node Details window appears.
3	Select the **Quality of Service (QoS)** link.

Copyright © 2010 Nortel Networks. All Rights Reserved.

The Quality of Service (QoS) window appears. See Figure 72 "Quality of Service (QoS) window" (page 258).

Figure 72
Quality of Service (QoS) window



4 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.

Modify the Control packets priority and Voice packets priority values only if directed by the IP network administrator.

The recommended configuration values are as follows:

a **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 **Voice packets:** A value of 46 Control DSCP - Expedited Forwarding (EF). The range is 0 to 63.

5 802.1Q 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 **VLAN Tagging:** 802.1Q support is disabled by default.

Copyright © 2010 Nortel Networks. All Rights Reserved.

b **802.1Q Bits value (802.1p):** The priority field is a three-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, which improves network throughput for IP telephony data.

6 Click **Save**.

--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 restarts, IP Phone firmware files are retrieved from the Leader Signaling Server. You can configure the Leader Signaling Server to retrieve the IP Phone firmware files from an external sFTP site server during startup. All files, which match xFF.fw naming convention are retrieved and registered.

Note: When you use the FTP Server to upload an IP Phone firmware version on the Signaling Server, any previous IP Phone firmware that was uploaded through the FTP Server will not be saved. To downgrade the firmware on IP Phone to the previous IP Phone firmware, repeat the process again by uploading the previous IP Phone firmware through the FTP Server.

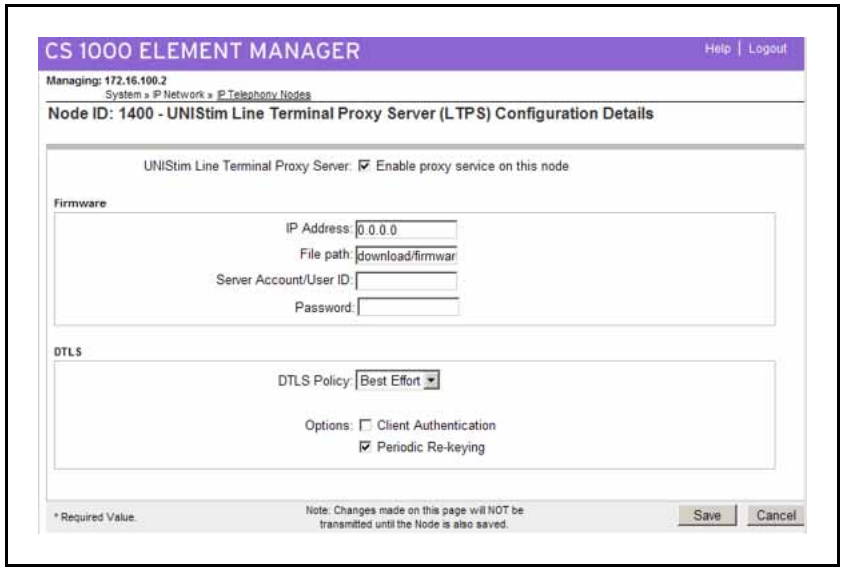
To configure the file server, perform the steps in Procedure 31 “Configuring access to the file server” (page 259).

Procedure 31
Configuring access to the file server

Step	Action
1	Log on to UCM with appropriate credentials.
2	In Element Manager, select **IP Network, Nodes: Servers, Media Cards**. The IP Telephony window appears. See Figure 73 " UNIStim Line Terminal Proxy (LTPS) Configuration Details window" (page 260).
3	Select the link for a Node ID. The Node Details window appears.
4	Select the **Terminal Proxy Server (TPS)** link. The UNIStim Line Terminal Proxy (LTPS) Configuration Details window appears.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 73
UNIStim Line Terminal Proxy (LTPS) Configuration Details window



5 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.

> ***Note:*** You can point to another IP Telephony Node that already has firmware updated. If the Firmware download server IP Address is an existing IP Telephony Node, specify the Firmware File Path as /var/opt/nortel/tps/fw/.

c **User ID:** Enter the User ID required to access the file server.

d **Password:** Enter the Password required to access the file server.

For information about the Enhanced UNIStim Firmware Download for IP Phones, see "Enhanced UNIStim Firmware Download for IP Phones" (page 70).

--End--

Configure loss and level plan

The loss and level plan determines parameters, such as transmission gain, that vary from country to country.

Default values

The default values in the system are for the North American loss plan.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Non-North American countries

Installing IP Line in any other country requires that you configure the pad values in Table 15 to that country loss plan. If you install the system 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.

For more information, see *Transmission Parameters Reference* (NN43001-282) .

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 “Subnet Mask Conversion from CIDR to Dotted Decimal Format” (page 403).

In the Cards section, cards can be added, changed, or removed in the node one at a time.

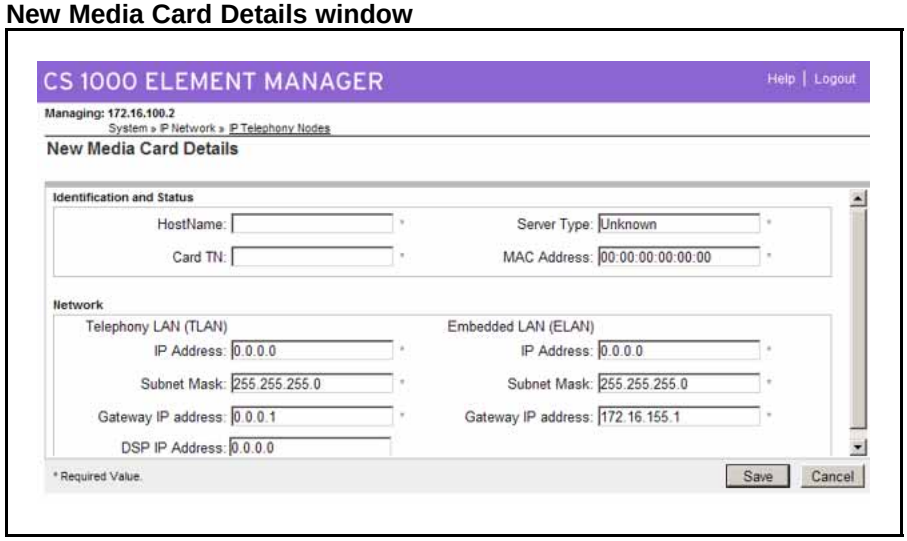
Perform the steps in Procedure 32 “Adding a card and configuring Voice Gateway Media Card properties” (page 261) to add a Voice Gateway Media Card and configure the properties or to configure the properties of an existing Voice Gateway Media Card.

Procedure 32
Adding a card and configuring Voice Gateway Media Card properties

Step	Action
1	In Element Manager, select **System, IP Network, Nodes: Server, Media Cards**. The IP Telephony Nodes window appears.
2	Select the link for a Node ID.
3	In the **Associated Signaling Servers & Cards** section of the window, select **Media Cards** from the Select to add menu.
4	Click **Add** . The New Media Card Details window appears. See Figure 74 "New Media Card Details window" (page 262).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 74
New Media Card Details window



5 In the **Identification and Status** section of the window, enter the following information.

a **HostName:** This is the Host name.

b **Card TN:** Enter the card slot number from 1 to 50.

c **Server Type:**

d **MAC Address:** This is the motherboard Ethernet address.

6 In the Network section of the window, enter the TLAN and ELAN network information.

a **Telephony LAN (TLAN) IP address:** This is the TLAN network interface IP address for the card.

b **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.

7 Click **Save** to transfer the changes to the Call Server.

8 To add additional cards to the node, click **Add** again and enter the card information. Repeat this step for each card that you add to the node.

9 To edit the properties of a Voice Gateway Media Card, select the link for the card to display the card properties.

--End--

Copyright © 2010 Nortel Networks. All Rights Reserved.

Transfer node configuration from Element Manager to the Voice Gateway Media Cards

Before you start the node configuration transfer, ensure the following:

- The Voice Gateway Media Cards and cables are 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 **Save** 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.

Transmit node properties

To transmit the node properties to the Leader, perform the steps in Procedure 33 “Transmitting node properties to Leader” (page 263).

Procedure 33
Transmitting node properties to Leader

Step	Action
1	If you change the node or card configuration data, in the Node Details window, click **Save** to save the data to the Call Server . A confirmation dialog box appears.
2	Click **OK** to confirm the save of the node data. The Node Details window closes, and the Node Configuration window appears.
3	In the Node Configuration window, click **Transfer/Status** 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 appears.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 Voice Gateway Media Card 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 Restart the Signaling Server if any IP address information changes.



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--

Upgrade the Voice Gateway Media Card and IP Phone firmware



WARNING
Before you start the upgrade, ensure that you configure a PWD1 user name and password on the Call Server. If no PWD1 user name and password exists, configure them in LD 17. This is necessary to enable logon to the Signaling Server.

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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 266).
2. Determine the version of the IP Phone firmware.
3. Obtain the most recent software from the Signaling Server. See "Download the current loadware and IP Phone firmware" (page 266).
4. Upload the software and firmware files using the File Upload system utility in Element Manager. See Procedure 34 "Uploading loadware and firmware files" (page 267).
5. Upgrade the Voice Gateway Media Card software. See Procedure 36 "Upgrading the card loadware" (page 268).
6. Restart the Voice Gateway Media Card. See Procedure 37 "Restarting the Voice Gateway Media Card" (page 269).

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 be necessary to upgrade only 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.
3. Upgrade only the IP Phone firmware.

   Restart all the IP Phones. Select a test IP Phone and reset the firmware only on that test IP Phone before you upgrade all IP Phones. If the upgrade works properly, use the **`umsUpgradeAll`** command to upgrade all the IP Phones.

For more information, see "Enhanced UNIStim Firmware Download for IP Phones" (page 70).

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 1210, IP Phone 1220, IP Phone 1230, IP Phone 1120E, IP Phone 1140E, and IP Phone 1150E firmware can be upgraded in the field.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 you distribute the telephone.

Determine Voice Gateway Media Card software version

To determine the software version on the Voice Gateway Media Card, log on to the Voice Gateway Media Card. At the command line, enter swVersionShow to retrieve information as shown in the following example.

swVersionShow example

```
pdt> swVersionShow unixbld3's loadbuild - basedon
ipl-5.92.22 (MC32S) was built on Tue Feb 10 07:39:49 EST
2009
Additional Modules:
mainos.sym
BOOTCODE: ipl-5.92.22
HOST MSP: MAA05
DB2 MSP: 2AB01
FPGA: V007
```

Download the current loadware and IP Phone firmware

You must download the file of Product Category: VOIP & Multimedia Communications, Product Name: Signaling Server and IP Peer Networking, Content type: Releases. Obtain the precise Release, Status, and Title of the file from your next level of support. See www.nortel.com/downloadingcontent for download instructions.

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. Use the Centralized File Upload window to upload and store software and firmware 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 34 “Uploading loadware and firmware files” (page 267).

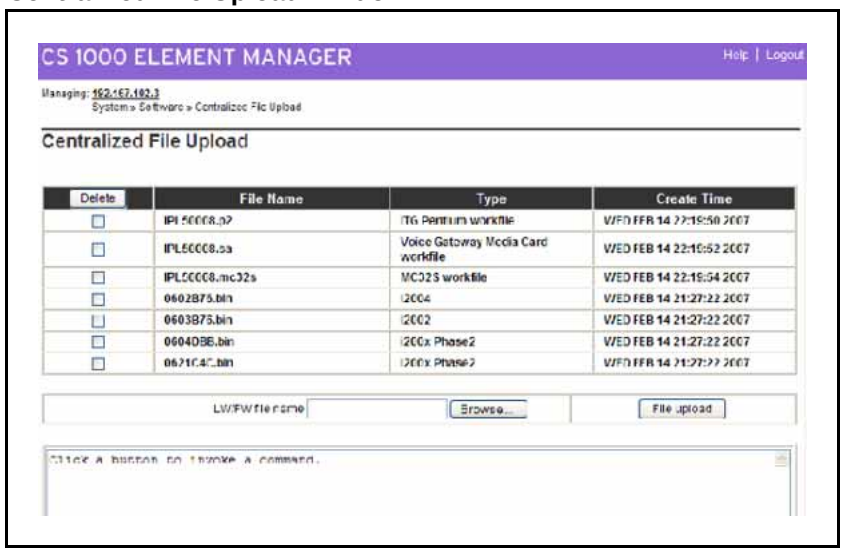
For patches, Element Manager need not to upload to the Signaling Server first. The Signaling Server obtains the patch file directly from the Element Manager PC.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Procedure 34
Uploading loadware and firmware files

Step	Action
1	In the Element Manager navigator, click **Software, File Upload**. The File Upload window appears. See Figure 75 "Centralized File Upload window" (page 267).

Figure 75
Centralized File Upload window



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 upload. Only one loadware or firmware file can be uploaded at a time. Once selected, the path and file name appear in the box to the left of the Browse button.
3	Click **File Upload**. The uploaded file appears in the list at the top of the window. To delete older versions of the firmware and loadware files, select the corresponding check box and click **Delete** at the top of the column of check boxes.

--End--

Copyright © 2010 Nortel Networks. All Rights Reserved.

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, perform the steps in Procedure 36 “Upgrading the card loadware” (page 268).



WARNING
When upgrading a CS 1000 system from 4.5 to 6.0, remember to install the MPLR 24008 patch on the 4.5 system before upgrading. The patch ensures that the VGMC card upgrades properly.

Files in the /fw folder on the MC 32 VGMC card are read-only. You must remove this protection and delete the files in the /fw folder before you try to upgrade the loadware. You must perform these steps to remove the read-only attribute and delete the existing files from the /fw folder.

Procedure 35
Removing the read-only protection and delete existing files in the /fw folder

Step	Action
1	Remove the flash memory card from the VGMC card.
2	Insert the flash memory card into your laptop or into the card reader on your computer.
3	Delete the files in the /fw folder on the flash memory card.
4	Reinstall the flash memory card in the VGMC.
5	Perform the steps in Procedure 36 “Upgrading the card loadware” (page 268).

--End--

Procedure 36
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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Element Manager supports upgrading the software on up to four cards at the same time.

4 In the lower part of the window, select the most current software version.

If the card receiving the upgrade is a Media Card 32S card, select 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 upgrade status appears for each card selected to receive the upgrade. The upgrade status can be Work in progress, Upgrading, Fail, or Finished.

7 Click **OK**.

8 Repeat steps 3 to 7 to upgrade the other card.

--End--

Restart the Voice Gateway Media Card

Perform the steps in Procedure 37 “Restarting the Voice Gateway Media Card” (page 269) to restart a Voice Gateway Media Card.

Procedure 37
Restarting the Voice Gateway Media Card

Step	Action
1	Disable the Voice Gateway Media Card.
2	Click the Element Manager navigator, select **IP Network, Maintenance and Reports**. The Node Maintenance and Reports window appears.
3	To expand the node containing the card to restart, click the plus sign (+) to the left of the node.
4	Click the Voice Gateway Media Card associated **Reset** button to restart the card. The cards remain in the Disabled state after the upgrade, so a Reset command can be used. You can also reset the card by using a pointed object to press the Reset button on the card faceplate.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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--

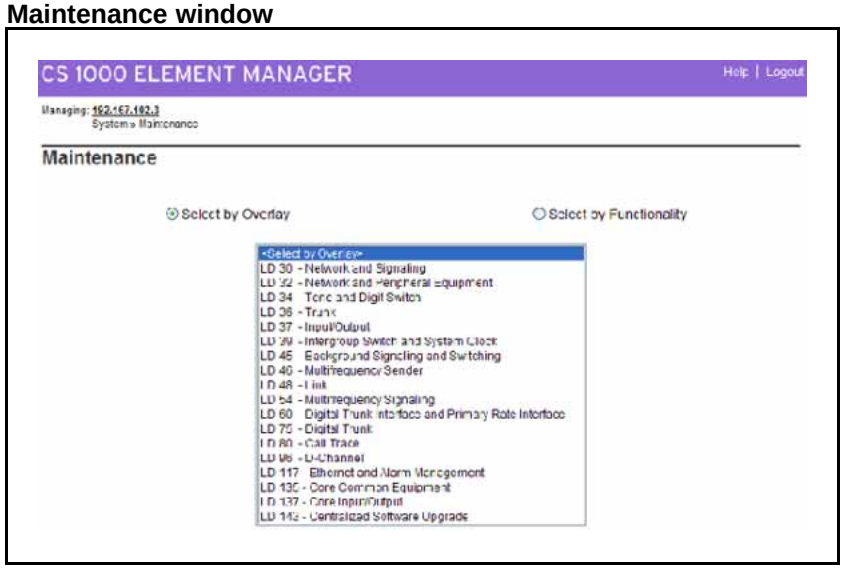
Re-enable the Voice Gateway Media Card

Perform the steps in Procedure 38 “Re-enabling the Voice Gateway Media Card” (page 270) to re-enable the Voice Gateway Media Card.

Procedure 38
Re-enabling the Voice Gateway Media Card

Step	Action
1	In the Element Manager navigator, click **System, Maintenance**. The Maintenance window appears. See Figure 76 "Maintenance window" (page 270).

Figure 76
Maintenance window



2 From the **Select by Overlay** list, select **LD 32 - Network and Peripheral Equipment**.

The Network and Peripheral Diagnostics window appears.

3 From the **Card Commands** list, select **ENLC - Enable and reset card**.

4 Under **Command Parameters**, enter **card number**.

Copyright © 2010 Nortel Networks. All Rights Reserved.

5 Click **Submit**.

6 Repeat steps 3 to 5 for each Voice Gateway Media Card to re-enable.

--End--

Upgrade the IP Phone firmware

After you upgrade the the IP Line software on the Signaling Server, determine if you must also upgrade the IP Phone firmware. If an upgrade is required, you must upgrade the Signaling Server to the newest IP Phone firmware version.

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 occurs 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 upgrade occurs after the user logs off. If the Virtual Office logon is between Call Servers, then the IP Phone registers to the home LTPS and follows the normal firmware rules for regular registration.

When the **`umsUpgradeAll`** command runs, 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.

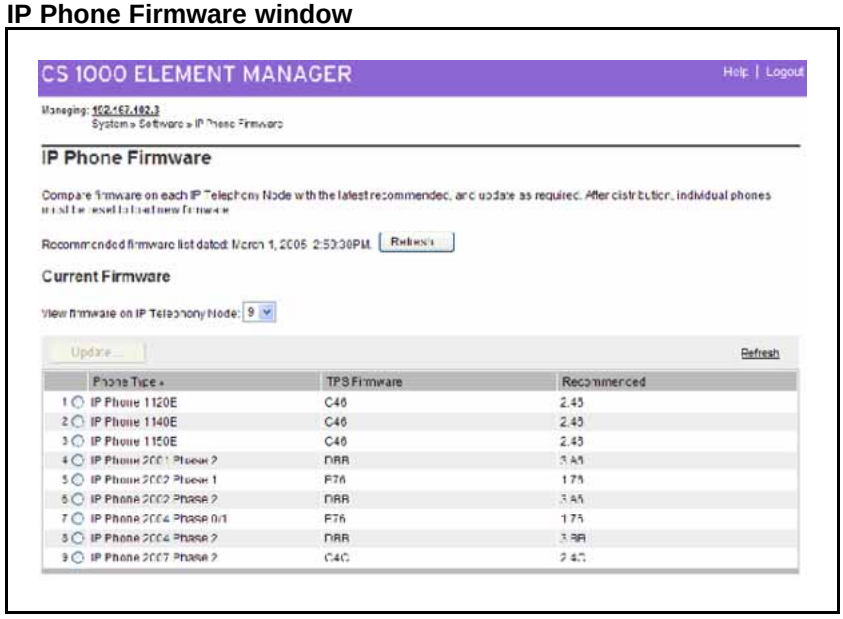
Perform the steps in Procedure 39 “Upgrading the IP Phone firmware” (page 271) to upgrade IP Phone firmware.

Procedure 39
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 77 "IP Phone Firmware window" (page 272).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 77
IP Phone Firmware window



2 Select the IP Telephony Node from the list to view the firmware on the Leader Terminal Proxy Server (TPS) of each Telephony Node configured on the Call Server.

3 Select the IP Phone type to update the firmware for the current IP Telephony node.

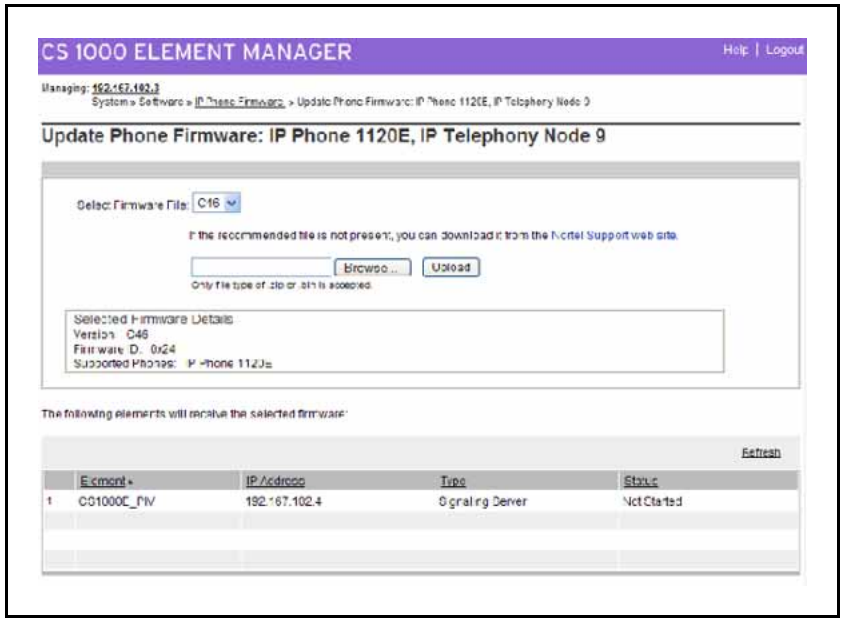
The phones in the Phone Type column are the phones listed in the Currency file.

4 Click **Update**.

The Update Phone Firmware opens for the selected IP Phone type. See Figure 78 "Update Phone Firmware window" (page 273).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 78
Update Phone Firmware window



5 Click **Browse** to locate the firmware file on the PC.

6 Click **Upload** to upload the firmware to the Leader TPS of the selected IP Telephony node.

Check the status column to ensure the server placed the new file in service.

7 Click **Update** to distribute the firmware.

Check the updated status message, which indicates that the file is in service.

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.

8 Repeat the preceding steps for all the card that have to be upgraded.

Commands are available from the Linux shell to immediately upgrade a single IP Phone, all IP Phones immediately, or to schedule all IP Phones for an upgrade. Before you upgrade, verify that the Signaling Server has the correct IP Phone firmware version.

9 Select an IP Phone for test purposes.

10 SSH to the Signaling Server and then log on to the Linux shell, and enter the following:

```
isetReset "xxx.xxx.xxx.xxx"
```

xxx.xxx.xxx.xxx is the IP Address of the selected IP Phone.

Copyright © 2010 Nortel Networks. All Rights Reserved.

11 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 receives the upgrade.

12 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.

13 Lift the IP Phone handset and make a call to verify the IP Phone works.

14 Enable and schedule Firmware Download Maintenance Mode to ensure that the Signaling Server uses the processing power for the firmware upgrade. For more information, see "Enhanced UNIStim Firmware Download for IP Phones" (page 70).

15 Before you proceed, ensure the time on the Signaling Server is configured correctly. Telnet to the Signaling Server and log on to the Linux shell, enter the following:

```
umsUpgradeAll "hh:mma/p"
```

hh:mma/p specifies the time when the upgrade occurs, 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 IP Phones registered to the Signaling Server go out of service. This can take several minutes.

After the firmware upgrade, the IP Phones are brought online as they complete the firmware upgrade.



CAUTION

If you use the **umsUpgradeAll** command without the time parameter, all IP Phones registered that are logged on are immediately removed from service. Use the time parameter with the command to prevent this.

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.

16 Inspect the list to ensure all IP Phones have the correct firmware version.

Copyright © 2010 Nortel Networks. All Rights Reserved.

17 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 failed on any IP Phone, the cause is probably one of the following:

- The Signaling Server did not upgrade the software successfully.
- An IP Phone firmware version was unable to be upgraded by the Signaling Server in the normal manner.
- The **`umsUpgradeAll`** command was not issued.

If the upgrade failed, redo the appropriate procedure. If the upgrade fails again, contact a technical support representative for further assistance.

--End--

For more 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 **`admin1`** and a default password of **`0000`**.

The default user name and password will be changed as a preventative security measure to PWD1 after synchronization with CS.

Configure the IP Phone Installer Passwords

The IP Phone Installer Password, used to change the TN on the telephone, controls registration with a virtual line TN on the Call Server. See “IP Phone Installer Password” (page 288) for more information about the IP Phone Installer Passwords.

Copyright © 2010 Nortel Networks. All Rights Reserved.

To enable and configure the administrative IP Phone Installer Password, see Procedure 41 “Configuring the Administrative IP Phone Installer Password” (page 293).

If required, enable and configure a temporary IP Phone Installer Password. See Procedure 42 “Configuring the temporary IP Phone Installer Password” (page 296).

You can also use Element Manager to configure the IP Phone Installer Passwords. See “Setting the IP Phone Installer Password” (page 352).

Import node configuration from an existing node

You can import a node and the configuration data from an existing node into Element Manager.

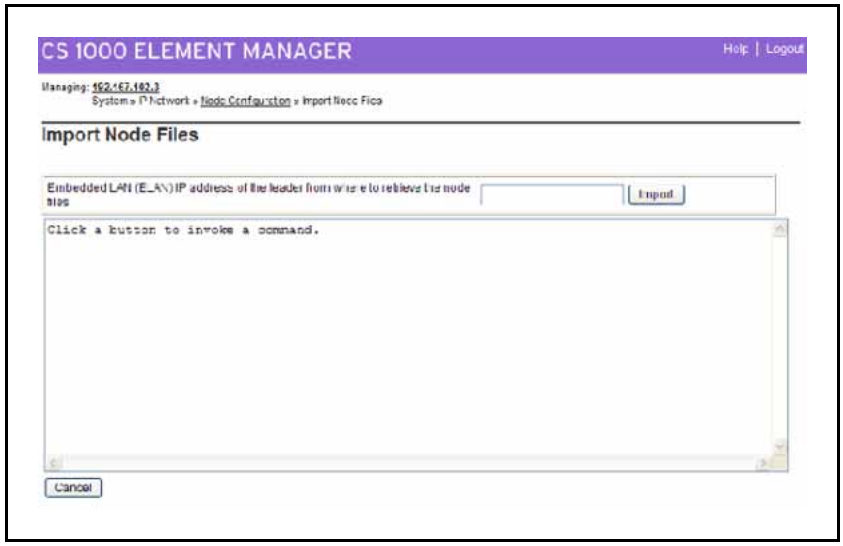
For example, if Node 151 exists, but does not exist on the Call Server, then Node 151 can be imported into Element Manager. After you import a node, you can update and edit the configuration data.

Procedure 40
Importing node files

Step	Action
1	In the Element Manager navigator, select **IP Network, Nodes: Servers, Media Cards**. The IP Telephony Nodes window appears.
2	Click **Import Node Files**. The Import Node Files window appears. See Figure 79 "Import Node Files window" (page 277).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 79
Import Node Files window



3 Enter the Embedded LAN (ELAN) network interface IP address of the Leader card in the box. This address is used to retrieve the node files.

4 Click **Import** .

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 appears indicating the import was successful. If Element Manager cannot write the configuration to the Call Server, the reason appears in the text area of the Import Node Files window.

In the message box, click **OK** 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 box area.

--End--

Copyright © 2010 Nortel Networks. All Rights Reserved.

Copyright © 2010 Nortel Networks. All Rights Reserved.

IP Line administration

Contents

This chapter contains the following topics:

- "Introduction" (page 279)
- "IP Line feature administration" (page 280)
- "Password security" (page 285)
- "IP configuration commands" (page 298)
- "TLAN network interface configuration commands" (page 298)
- "Display the number of DSPs" (page 299)
- "Display IP Telephony node properties" (page 299)
- "Display Voice Gateway Media Card parameters" (page 300)
- "Packet loss monitor" (page 302)
- "Transfer files using the CLI" (page 303)
- "Reset the Operational Measurements file" (page 304)

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.

The Voice Gateway Media Card provides four administration interfaces:

- Telephony Manager (TM) 4.0

  TM IP Line application provides a GUI to the Voice Gateway Media Card. TM 4.0 provides OM reports.

- Element Manager

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 debugging. The prompt for the CLI on the 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 (CoS) CRPA/CRPD for IP Phones.

Note: Corporate Directory is not supported on the IP Phone 2001P2, IP Audio Conference Phone 2033, IP Phone 1210, and IP Phone 1110.

Table 67
Corporate Directory: LD 11 configuration

Prompt	Response	Description
REQ	NEW CHG	Add new data or change existing data.
TYPE:	2001P2, 2002 P1, 2002P2, 2004P1, 2004 P2, 2050PC, 2050MC, 2033, 2007, 1110, 1210, 1220, 1230,1120, 1140, 1150, 2210, 2211, 2212	Enter terminal type.
TN	l s c u	Enter IP Phone TN.
…	…	…
CLS	CRPA CRPD	Enable or Disable the Corporate Directory feature for this TN.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 CoS as CPRD, then the current display and key handling remain unaffected. The changed CoS 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 4.0 System Administration* (NN43050-601)

Private Zone configuration

DSP channels and IP Phones are Shared or Private based on zone configuration. Use the parameter zoneResourceType in the zone configuration commands in LD 117 to configure this setting.

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> <interZoneStrat
egy>
CHG ZONE <zoneNumber> [<intraZoneBandwidth>
<zoneResourceType>]<intraZoneStrategy> <interZoneBandwi
dth> <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 error message appears to indicate to 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 CoS VOLA (Virtual Office logon Allowed). The TN associated with the User ID for the logon must be configured with the CoS VOUA (Virtual Office User Allowed).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Two CoSs restrict Virtual Office usage:

- VOLA/VOLD: defines whether this TN (physical IP Phone) allows or disallows a Virtual Office logon option.
- VOUA/VOUD: defines if a specific remote user can log on to this TN (allows or disallows a particular user to logon using Virtual Office).

Table 68 "LD 11 Virtual Office logon for IP Phones" (page 282) shows the CoS for LD 11.

Table 68
LD 11 Virtual Office logon for IP Phones

Prompt	Responses	Description
REQ:	NEW CHG	Add new data or change existing data.
TYPE:	2001P2, 2002 P1, 2002P2, 2004P1, 2004 P2, 2050PC, 2050MC, 2033, 2007, 1110, 1120, 1140, 1150, 1210, 1220, 1230, 2210, 2211, 2212	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 1210, IP Phone 1220, IP Phone 1230, 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.
...	...	...
CLS	(VOLA) VOLD	Virtual Office logon operation is allowed or denied on this TN.
CLS	(VOUA) VOUD	Allow/Deny Virtual Office user on this TN using other IP Phone.

Emergency Services Access while logged in to Virtual Office

If an IP Phone user dials 911 while logged on to Virtual Office, the LTPS redirects the 911 call to the local area 911 service (PSAP), not the remote Call Server 911 service. Table 69 "e911 process for IP Phones logged on to Virtual Office" (page 282) describes the process.

Table 69
e911 process for IP Phones logged on to Virtual Office

Step	Description
1	The LTPS terminates the call on the remote Call Server.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 69
e911 process for IP Phones logged on to Virtual Office (cont'd.)

Step	Description
2	The LTPS displays Emergency Call on the IP Phone.
3	The LTPS logs the IP Phone off 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 calls back the originator of the emergency call. After the IP Phone is redirected to the Home Site, it cannot initiate a new operation for 5 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 no emergency exists). If the IP Phone immediately resumes a Virtual Office logon to another site, it cannot receive the call back. If the local TN has another IP Phone Virtual Office logged on when it comes back, the nonemergency IP Phone is pre-empted. If this occurs, ESAxxx messages are generated on the system TTY.

Emergency Services Access while logged off Virtual Office

If an IP Phone user dials 911 while logged off 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 70 "e911 process for IP Phones while logged out of Virtual Office" (page 283).

Table 70
e911 process for IP Phones while logged out of Virtual Office

Step	Description
1	The LTPS terminates the call on the remote Call Server.
2	The LTPS displays Emergency Call Only on the IP Phone.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 off IP Phone Primary DN. A 60-second timer is created for the logged off 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 off 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 calls back 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 off state and the IP Phone ESTN becomes available for other ESA calls from any other logged off IP Phone.

Configuration

You must configure Emergency Services Access (ESA) on all nodes participating in Virtual Office logons. Enter the ESTN range in LD 24, and configure ESA in LD 11.

For more information, see *Emergency Services Access Fundamentals* (NN43001-613) and *Branch Office Installation and Commissioning* (NN43001-314)

802.1Q

You can use the telephone user interface or DHCP to configure the 802.1Q support for IP Phones. Using DHCP eliminates the need to manually configure the VLAN ID as part of the installation. The configuration comprises two items: setting the p bits and setting the VLAN ID.

TM 4.0 and Element Manager have two fields for configuring 802.1Q support:

- 802.1Q Support: Select this check box to activate 802.1Q support. The priority bits value is specified in the 802.1Q Bits value box. If the check box is not selected, the IP Phone sends out the default priority of 6.
- 802.1Q Bits value (802.1p): Enter a value in the box. The range is 0 to 7.

For more information, see “Configure Quality of Service” (page 257).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Password security

The following password security features should be configured to work with the IP Line application:

- SNMP community strings
- IPL> or oam> CLI Shell password
- Call Server Level 1 Password (PWD1)
- 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 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Password guessing protection

Password guessing protection helps to block a hacker from attempting to log on to the Voice Gateway Media Card shell by repeatedly trying to guess the shell user ID and password.

The password guessing protection applies 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 three and a lockout period of 10 minutes. This is not user-configurable.
- 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 log on. The user is not informed that logon blocking was 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 appears 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Node password synchronization

The BOOTP.TAB and CONFIG.INI must be the same on all cards in the system. The cards that can be in the system are the Media Card 32-port line card, the 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.

For the FTP process to work correctly, all cards in a node must be synchronized with the same user ID and password. After the Voice Gateway Media Cards synchronize with the Call Server, the user logon synchronizes 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 the user ID and password when it tries to access another card to send files using an FTP session. Sending data using an FTP session 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. You need not 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 occurs 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 on. 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

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 (change the password once on the Call Server). When the password changes at the Call Server, the password is automatically sent to all the Voice Gateway Media Cards.

If the PWD1 changes and an EDD operation does not occur, the cards can contain a mixture of old and new passwords. This can happen if a new card is plugged in, an existing card restarts or loses and reestablishes the ELAN subnet connection. Nortel recommends that you perform an EDD when the PWD1 password changes on the Call Server to ensure 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 five seconds as the IP Phone starts. 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 352).

For more information about password protection support on an IP Phone, see *IP Phones Fundamentals* (NN43001-368)

Administrator IP Phone Installer Password

The administrator password 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.

When the password is configured, the IP Phone 2004, IP Phone 2007, IP Phone 1140E, IP Phone 1150E, or WLAN Handset 2210/2211/2212/6120/6140 screen shows the following information:

- The four-digit Node ID and a Password prompt instead of the Node ID and TN fields. For example, see Figure 82 "IP Phone registration

Copyright © 2010 Nortel Networks. All Rights Reserved.

with no password checking" (page 292) and Figure 83 "IP Phone registration with password checking" (page 292)

- During password entry, an asterisk (*) appears for each digit entered. The password does not appear.
- After the Node ID and Password are entered, the user presses OK. If the password passes the Connect Server authentication, a screen appears with the TN field. For example, see Figure 83 "IP Phone registration with password checking" (page 292)

When the password is configured, the IP Phone 2001, IP Phone 2002, IP Audio Conference Phone 2033, IP Phone 1110, IP Phone 1210, IP Phone 1220, IP Phone 1230, and IP Phone 1120E screen shows:

- The four digit Node ID screen appears first. For example, see Figure 81 "IP Phone registration with password checking" (page 291).
- The user is then prompted with the Password screen instead of the TN field screen. For example, see Figure 83 "IP Phone registration with password checking" (page 292) and Figure 80 "IP Phone registration with no password checking" (page 291)
- During password entry, an asterisk (*) appears for each digit entered. The password does not appear.
- After the Password is entered, the user presses OK. If the password passes the Connect Server authentication, a screen appears with the TN field. For example, see Figure 83 "IP Phone registration with password checking" (page 292).

If the Node ID and Password are not entered, the registration continues after 5 seconds and the TN does not appear.

For an invalid Node ID password, the Node ID and Password screen appears again a maximum of two times to give the technician three chances to enter the password. After three failed attempts, the registration continues as if no password were entered. Restart 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 do not appear on the IP Phone during the registration process. This provides maximum security by preventing entry of passwords or TN 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 is 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 installs an IP Softphone 2050. The technician creates a temporary password, configures an appropriate number of uses (such as allowing two logons for each IP Softphone 2050 in case a problem occurs the first time) and configures 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 must 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 does not appear as part of the Set Info item on 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, rlmShow.

Registration screens with TN password feature

The IP Phone type and password protection determines the registration screen with the TN password feature.

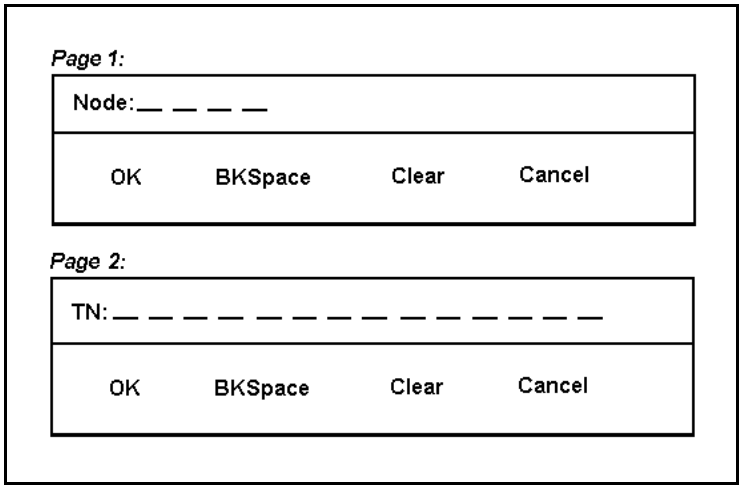
For IP Phone 2001, IP Phone 2002, IP Audio Conference Phone 2033, IP Phone 1210, IP Phone 1220, IP Phone 1230, IP Phone 1120E and IP Phone 1110, see “For IP Phones 2001/2002/2033/1210/1220/1230/1120E/1110” (page 290)

For IP Phone 2004, IP Phone 2007, IP Phone 1140E, IP Phone 1150E, and WLAN Handset 2210/2211/2212/6120/6140, see “IP Phones 2004/2007/1140E/1150E and WLAN Handset 2210/2211/2212/6120/6140 ” (page 291)

For IP Phones 2001/2002/2033/1210/1220/1230/1120E/1110 When you do not configure or enable password protection, the Password entry does not appear. The IP Phone displays the Node ID and TN. See Figure 80 "IP Phone registration with no password checking" (page 291).

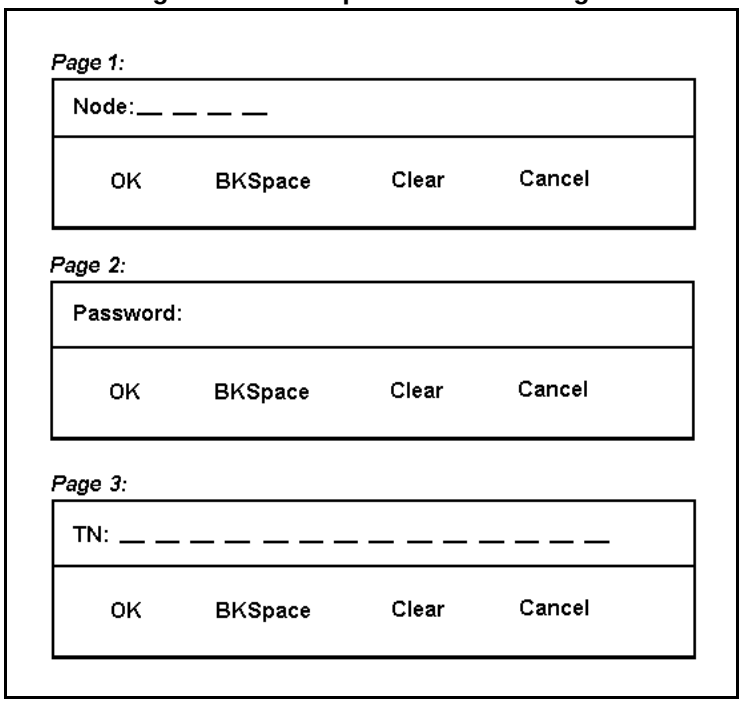
Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 80
IP Phone registration with no password checking



When you configure and enable password protection, the IP Phone displays the Node ID and password. The Password entry input field is blank (underscores do not appear). Therefore, the maximum length of the password is hidden. If you enter the correct password, the TN appears. See Figure 81 "IP Phone registration with password checking" (page 291).

Figure 81
IP Phone registration with password checking

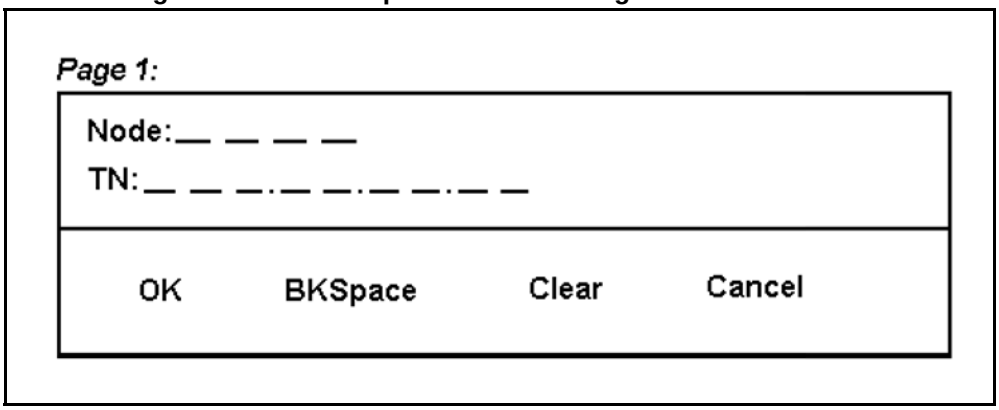


IP Phones 2004/2007/1140E/1150E and WLAN Handset 2210/2211/2212/6120/6140 When you do not configure or enable

Copyright © 2010 Nortel Networks. All Rights Reserved.

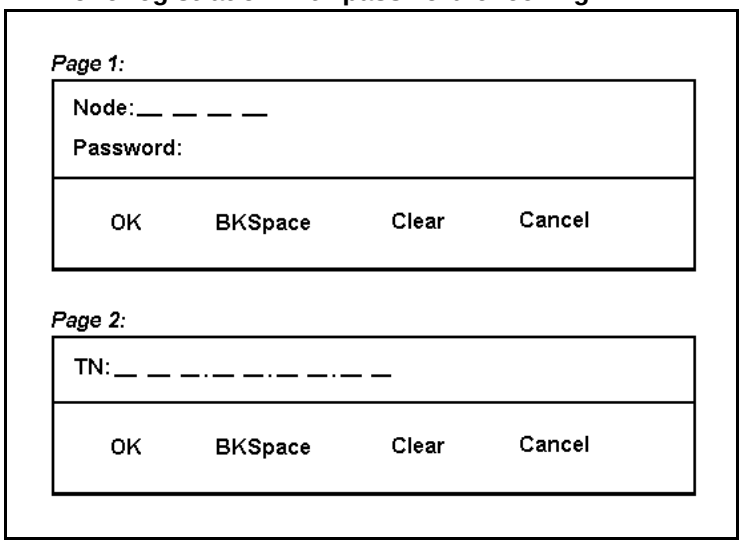
password protection, the Password entry does not appear. The IP Phone displays the Node ID and TN. See Figure 82 "IP Phone registration with no password checking" (page 292).

Figure 82
IP Phone registration with no password checking



When you configure and enable password protection, the IP Phone displays the Node ID and password. The Password entry input field is blank (underscores are do not appear). Therefore, the maximum length of the password is hidden. If you enter the correct password, the TN appears. See Figure 83 "IP Phone registration with password checking" (page 292).

Figure 83
IP Phone registration with password checking



Configure the IP Phone Installer Passwords

The IP Phone Installer Passwords are configured on a Signaling Server in the node. The passwords then apply to all Signaling Servers in the node.

Copyright © 2010 Nortel Networks. All Rights Reserved.

If the IP Phone Installer Password is configured on the Signaling Server, the IP Phone 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, perform the steps in Procedure 41 “Configuring the Administrative IP Phone Installer Password” (page 293).

Procedure 41
Configuring the Administrative IP Phone Installer Password

Step	Action
1	Log on to a Signaling Server using the SecurityAdmin credentials.
2	In the Linux shell 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 was never assigned. 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 Signaling Servers 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

Copyright © 2010 Nortel Networks. All Rights Reserved.

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: the number of Uses becomes zero or the Time expires. 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, asterisk (*), and number sign (#). This command can be entered at any time. The new password overwrites the previous password.

Configure the password, first with a null password and then with a password specified.



WARNING

By default, the **nodePwdSet** command with no parameter enables the administrator password and assigns 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

4 Type **nodePwdSet** at the prompt to specify no password parameter.

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 you specify no <"password"> parameter, the administrator password is null. A null password causes the node ID and Password screen to be skipped during a restart.

5 Type **nodePwdSet <"password">** at the prompt; the password parameter is 6 to 14 digits in length.

The valid character are 0 to 9, asterisk (*), and number sign (#). 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, appears.

Always specify the <password> parameter when you enter 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 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

Copyright © 2010 Nortel Networks. All Rights Reserved.

To configure a temporary IP Phone Installer Password, perform the steps in Procedure 42 “Configuring the temporary IP Phone Installer Password” (page 296).

Procedure 42
Configuring the temporary IP Phone Installer Password

Step	Action
1	At the Linux shell, type **nodeTempPwdSet <"password">, <uses>, <time>** ; password is the temporary password string 6 to 14 digits in length, uses is a value from 0 to 1 000, and time is from 0 to 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 is used the defined number of times (Uses) or when the duration expires (Timeout), whichever comes first. To delete the temporary password before the number of uses or time expires, type the **nodeTempPwdClear** command at the prompt.
3	Type **nodePwdShow** to verify that the temporary password is 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 will be changed as a preventative security measure to PWD1 after synchronization with the Call Server.

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).

Copyright © 2010 Nortel Networks. All Rights Reserved.

To reset the IPL> CLI shell user name and password, perform the steps in Procedure 43 “Resetting the user name and password to default” (page 297). This procedure requires a connection to the local maintenance port on the Voice Gateway Media Card and requires restarting the card, which interrupts services.

Procedure 43
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: • 9600 bps • 8 data bits • no parity • 1 stop bit
2	Press the **Enter** key on the keyboard. The `logon:` prompt appears.
3	Restart the card by pressing the **RESET** button on the faceplate of the card with a pointed object, such as a ball-point pen.
4	Start up messages are displayed on the terminal. Type `jkl` on the terminal keyboard when the prompt appears. `jkl` runs from BIOS or the boot ROM, which is printed early in the bootup process. You have 6 seconds to enter `jkl` at the prompt. If the prompt is missed, restart the card and repeat the above step.
5	After the card restarts 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 restart the card.
7	Wait for the card to completely restart into the IP Line application. The password synchronization feature automatically changes the password on the 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.

--End--

Copyright © 2010 Nortel Networks. All Rights Reserved.

IP configuration commands

Table 71 "IP configuration commands" (page 298) describes the IP configuration commands.

Table 71
IP configuration commands

IP configuration command	Function
setLeader	Performs all the necessary actions to configure 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 IP Phones default to half-duplex mode when no autonegotiation signaling occurs. The result is that the IP Phones 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 and 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 startup. The parameter speed is set to the following:

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 the speed is fixed to 10 Mb/s (or 10BaseT mode). The duplex mode is saved in NVRAM and read at startup. 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 interoperate 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 operates only with full-duplex at the far end.

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 prompt, type: **IPInfoShow**

The following IP Telephony node information appears 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:

Copyright © 2010 Nortel Networks. All Rights Reserved.

```
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
```

Table 72
ROUTE NET TABLE

destination	gateway	flags	Refcnt	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

Table 73
ROUTE HOST TABLE

destination	gateway	flags	Refcnt	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

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:

Copyright © 2010 Nortel Networks. All Rights Reserved.

```
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
```

Registered cards

The following information appears for each card currently registered:

- platform
- TN
- ELAN network interface MAC
- TLAN network interface IP Address
- ELAN network interface IP Address
- the length of time the card has been registered
- the number of IP Phones registered to the card
- number of Time Outs

Unregistered cards

The following information appears 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:

```
electShow
```


Copyright © 2010 Nortel Networks. All Rights Reserved.

```
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
====== 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 ======
```

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, the default) logs a message if packet loss during 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

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 from 1 to 1 000, and represents the threshold in 0.1 percent increments. Packet loss that 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 percent).

Transfer files using the CLI

A number of special file transfer commands are available to Put and 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.

The commands in Table 74 " File transfer" (page 303), are for 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.

The commands in Table 75 "File transfer for the MC 32S card" (page 304)are for the MC 32S card.

Table 74
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>

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 75
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 loc alDirPath 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 loca lDirPath localfile name]

All commands are case-sensitive. The parameters after the command must each be enclosed in quotation marks, and between parameters must be a comma with no spaces.

Host name 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

Reset the Operational Measurements file

Reset the Operational Measurements (OM) file if incorrect statistics are collected.

At the IPL> or oam> prompt, type: **resetOM**.

The resetOM command resets all operational measurement parameters that are collected since the last log dump. The statistics start from zero.

Copyright © 2010 Nortel Networks. All Rights Reserved.

IP Line administration using Element Manager

Contents

This section contains the following topics:

- “Introduction” (page 279)
- “Element Manager administration procedures” (page 305)
- “Backup and restore data” (page 338)
- “Update IP Telephony node properties” (page 341)
- “Update other node properties” (page 348)
- “Telnet to a Voice Gateway Media Card using Virtual Terminal” (page 350)
- “Check the Voice Gateway Channels” (page 351)
- “Setting the IP Phone Installer Password” (page 352)

Introduction

This chapter explains how to administer IP Line and the Voice Gateway Media Card on CS 1000 systems using by Element Manager.

Element Manager administration procedures

This section describes the administration procedures that can be performed by 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 you turn off Internet Explorer caching before you use Element Manager.

Perform the steps in “Configuring the browser” (page 198) to turn of caching in the Internet Explorer browser.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 from Element Manager. This OM report is a view of the LTPS and Voice Gateway channel activity on the card. Use this procedure to view the 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

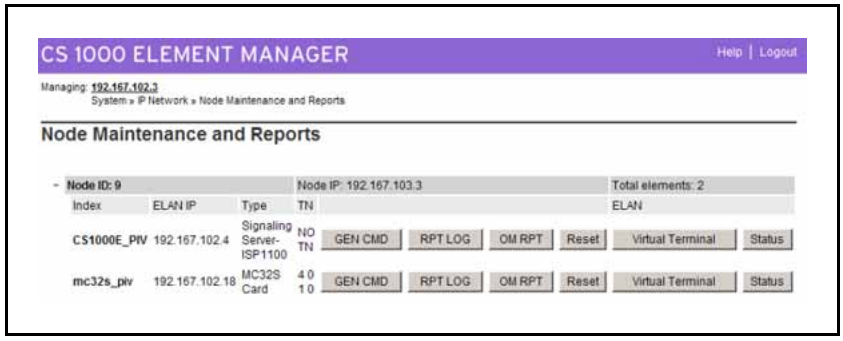
To view a Voice Gateway Media Card OM file from Element Manager, perform the steps in Procedure 44 “Retrieving the current OM file from the Voice Gateway Media Card using Element Manager” (page 306).

Procedure 44
Retrieving the current OM file from the Voice Gateway Media Card using Element Manager

Step	Action
1	In the Element Manager navigator, select **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 84 "Node Maintenance and Reports window" (page 307).

Copyright © 2010 Nortel Networks. All Rights Reserved.

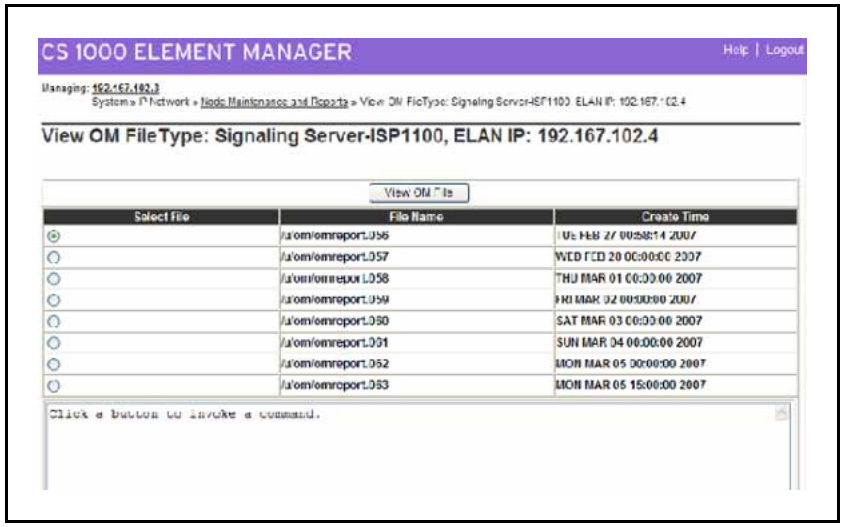
Figure 84
Node Maintenance and Reports window



3 Click **OM RPT** associated with the Voice Gateway Media Card.

The View OM File window appears. See Figure 85 "View OM File window" (page 307).

Figure 85
View OM File window



The eight most recent OM Report files appear in chronological order for that Voice Gateway Media Card.

4 To view a OM file, select the file to view 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 ran.

Copyright © 2010 Nortel Networks. All Rights Reserved.

The collection periods start with the hour from midnight to 1:00 a.m. As each hour passes, a collection period is added to the OM file; therefore, a maximum of 24 collection periods are available each day.

Output

The OM report output tracks the statistics for each IP Phone type.

Data is first written 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
```


Copyright © 2010 Nortel Networks. All Rights Reserved.

```
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
```


Copyright © 2010 Nortel Networks. All Rights Reserved.

```
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
```


Copyright © 2010 Nortel Networks. All Rights Reserved.

```
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
```


Copyright © 2010 Nortel Networks. All Rights Reserved.

```
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
1145Reg_Att:  0
1145Reg_Fail:  0
1145Unreg_Att:  0
1145Aud_Setup:  0
1145Jitter_Avg:  0.0
1145Jitter_Max:  0
1145Latency_Avg:  0.0
1145Latency_Max:  0
1145Pkt_Lost:  0.00
1145Listen_RFactor:  0.0
1145Voice_Time:  0 mins 0 secs
1210Reg_Att:  0
1210Reg_Fail:  0
```


Copyright © 2010 Nortel Networks. All Rights Reserved.

```
1210Unreg_Att:  0
1210Aud_Setup:  0
1210Jitter_Avg:  0.0
1210Latency_Avg:  0.0
1210Jitter_Max:  0
1210Latency_Max:  0
1210Pkt_Lost:  0.00
1210Listen_RFactor:  0.0
1210Voice_Time:  0 mins 0 secs
1220Reg_Att:  0
1220Reg_Fail:  0
1220Unreg_Att:  0
1220Aud_Setup:  0
1220Jitter_Avg:  0.0
1220Latency_Avg:  0.0
1220Jitter_Max:  0
1220Latency_Max:  0
1220Pkt_Lost:  0.00
1220Listen_RFactor:  0.0
1220Voice_Time:  0 mins 0 secs
1230Reg_Att:  0
1230Reg_Fail:  0
1230Unreg_Att:  0
1230Aud_Setup:  0
1230Jitter_Avg:  0.0
1230Latency_Avg:  0.0
1230Jitter_Max:  0
1230Latency_Max:  0
1230Pkt_Lost:  0.00
1230Listen_RFactor:  0.0
1230Voice_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
```


Copyright © 2010 Nortel Networks. All Rights Reserved.

```
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
```


Copyright © 2010 Nortel Networks. All Rights Reserved.

```
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
```


Copyright © 2010 Nortel Networks. All Rights Reserved.

```
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 hour.
- Voice Gateway channel information accumulated during the hour. The Voice Gateway data is prefixed by Chan.
- Notes indicating whether the equipment restarted during the hour.
- Virtual Trunk statistics display only for a Signaling Server that ran 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.

You can view OM files in Element Manager. You can use TM to support other Operational Measurements tasks such as scheduling reports, generating reports, opening reports, and viewing reports.

View Traffic reports

You can view system traffic and customer traffic reports in Element Manager.

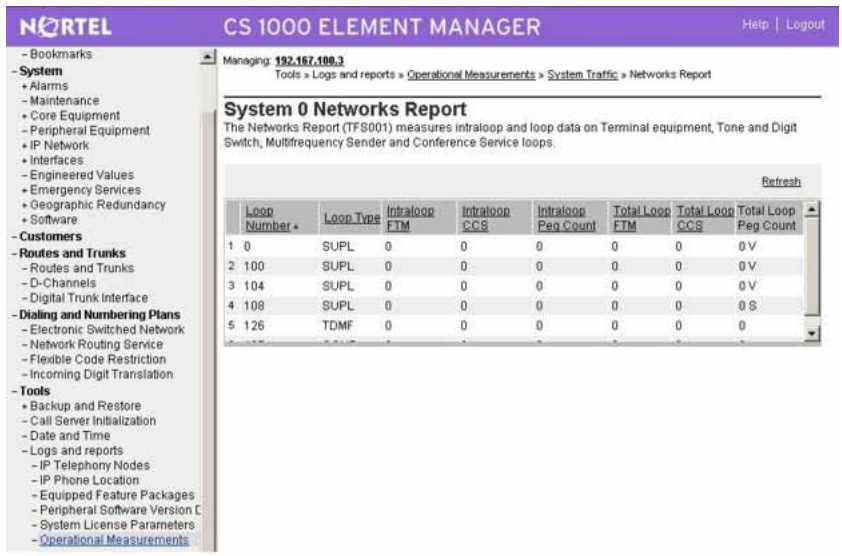
System reports

To view system traffic reports in the Element Manager navigator, click **Tools, Logs and Reports, Operational Measurements, System Traffic**.

Click **Network** in the table to view the Networks report.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 86
Networks report



Service loops report (TFS002)

Click Service loops in the table to view the page title, report description, and the parameters measured in the Service Loops report.

Table 76
TFS002

Title	System xxx Service Loops Report
Description	System xxx Service Loops Report (TFS002) measures service loops and tone detectors.
Parameters Measured	
1	Service number.
2	Service type.
3	Service FTM.
4	Service usage.
5	Service request peg count.

Dial tone delay report (TFS003)

Click Dial tone delay in the table to view the page title, report description, and the parameters measured in the Dial tone delay report.

Copyright © 2010 Nortel Networks. All Rights Reserved.

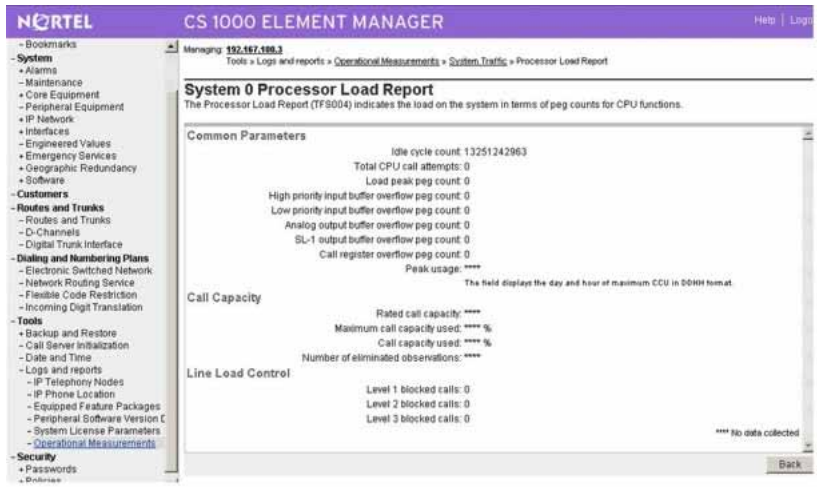
Table 77
TFS003

Title	System xxx Dial Tone Delay Report
Description	Dial Tone Delay Report (TFS003) shows the number of times users waited for dial tone for longer than 1 second.
Parameters Measured	
1	Number of times a user waited longer than 1 second
2	Number of times a user waited longer than 10 second
3	Total time delay

Processor load report

Click Processor load in the table to view the Processor Load report.

Figure 87
Processor load report



Selected terminals Report (TFS005)

Click Selected terminals in the table to view the page title, report description, and the parameters measured in the Selected terminals report.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 78
TFS005

Title	System xxx Selected Terminals Report
Description	Selected Terminals Report (TFS005) measures the output for individual terminals and terminal loops.
Parameters Measured	
1	Loop number
2	Line usage
3	Line peg count

Junctor group report (TFS007)

Click Junctor group report in the table to view the page title, report description, and the parameters measured in the Junctor group report.

Table 79
TFS007

Title	System xxx Junctor Report
Description	Junctor Report (TFS007) displays measurements related to paths that connect network groups involving an intergroup junctor
Parameters Measured	
1	Junctor group
2	Failure to match
3	Total usage
4	Peg count

Command status links and application module report (TFS008) Click Command status links and application module links in the table to view the page title, report description, and the parameters measured in the Command status links and application module links group report.

Table 80
TFS008

Title	System xxx Command Status Link and Application Module Link measurements Report
Description	Command Status Link (CSL) and Application Module Link (AML) measurements Report (TFS008) captures traffic data related to Command Status Links and Application Module Links.
Parameters Measured	
System	

Copyright © 2010 Nortel Networks. All Rights Reserved.

1	Input queue overflow
2	Output queue overflow
3	System resource not available
4	Input queue size for system messages
5	Input queue size for call processing messages
5	Input queue size for administration messages
Command Status Link	
1	Port number
2	Value Added Server ID
3	CSL output failures
4	Number of link stops
5	Link down time
6	Average output queue size
7	Number of IOCHAR TTY buffer overflows
8	Packets with missing End of Block flag
9	Packets with premature End of Block flag
10	Packets with invalid priority
11	Packets with invalid length
Outgoing/Incoming message types	
1	Channel assignment request
2	Call connection
3	Present call
4	Call answered
5	Call disconnect
6	DN update
7	Dialed digits
8	Telset message
9	Telset status message
10	Message waiting indication change
11	Mpdate terminal status
12	TN maintenance mode
13	Confirmation
14	Administration data block
15	Software audit

Copyright © 2010 Nortel Networks. All Rights Reserved.

16	Change terminal status
17	Device state information
18	Network layer data
19	Terminal status
20	Requests acquired
22	Responses acquired
23	Statistics messages
24	Incoming call indication messages
25	Call detail recording state requests
26	Call detail recording state responses
27	De-acquire request
28	De-acquire response
29	ATB on/off for acquire route
30	Error indications sent
31	Error indications received
32	Incoming calls accepted
33	System initialization indication messages
34	Acquired devices removed
35	Queue requests
36	Queue request response messages
37	Query request
38	Query request responses
39	Startup or shutdown indications
40	Startup or shutdown indication response messages
41	Statistics requests
42	Statistics response messages
43	Treatment completed messages
44	Treatment requests
45	Return to queue
46	Treatment response messages
47	Filter Bitmap request
48	Filter Bitmap response
49	Monitor make set busy
50	Make set in service
51	Message waiting indication change

Copyright © 2010 Nortel Networks. All Rights Reserved.

52	Not ready
53	Off-hook
54	Operator revert
55	Override
56	Present call
57	Query
58	Ready
59	Call disconnect request
60	Request terminal status change
61	Set feature message
62	Set feature notification
63	Set feature
64	Timestamp
65	Unsolicited status message
66	Update terminal status
Message Priority	
1	Priority 1 messages
2	Priority 2 messages
3	Priority 3 messages
4	Priority 4 messages
Traffic	
1	Average incoming usage
2	Peak incoming usage
3	Average outgoing usage
4	Peak outgoing usage
5	Time since last query
Flow Control	
1	First flow control
2	Second flow control
3	Third flow control
4	Fourth flow control
5	Outgoing SSD failure count
6	AML reset count
Packets	

Copyright © 2010 Nortel Networks. All Rights Reserved.

1	Incoming packets
2	Outgoing packets

D-channel report (TFS009)

Click D-channel report in the table to view the page title, report description, and the parameters measured in the D-channel report group.

Table 81
TFS009

Title	System xxx D-channel Report
Description	D-channel Report (TFS009) captures traffic activity on D-channels.
Parameters Measured	
System	
1	D-channel number
2	Incoming messages received
3	Outgoing messages sent
4	Input queue size for system messages
5	Input queue size for call processing messages
6	Input queue size for administration messages
7	Incoming call processing messages
8	Outgoing call processing messages
9	Incoming management messages
10	Outgoing management messages
11	Incoming maintenance messages
12	Outgoing maintenance messages
13	Average number of incoming bytes for each message
14	Average number of outgoing bytes for each message
15	Total transfer time for incoming messages
16	Total transfer time for outgoing messages
17	Requests in output message buffer
18	Output message buffer idle count
19	No End of Message mark message count
20	PRA Layer-3 protocol errors
21	D-channel down instances
22	Attempted anti-tromboning operations

Copyright © 2010 Nortel Networks. All Rights Reserved.

23	Successful anti-tromboning operations
24	First flow control
25	Second flow control
26	Third flow control
27	Fourth flow control
MSDL data	
1	Average incoming link usage
2	Peak incoming link usage
3	Average outgoing link usage
4	Peak outgoing link usage
5	Number of connected calls
6	Time since MSDL D-channel traffic was cleared
Optimization data	
1	Optimization requests with the diversion trigger
2	Successful optimizations with the diversion trigger
3	Successful optimizations retaining the old path with the diversion trigger
4	Optimization requests with the congestion trigger
5	Successful optimizations with the congestion trigger
6	Successful optimizations retaining the old path with the congestion trigger
7	Optimization requests with the connected trigger
8	Successful optimizations with the connected trigger
9	Successful optimizations retaining the old path with the connected trigger

ISDN GF transport report (TFS010)

Click ISDN GF transport in the table to view the page title, report description, and the parameters measured in the ISDN GF transport report group.

Table 82
TFS0010

Title	System xxx ISDN Generic Functional Report
Description	ISDN Generic Functional Report (TFS010) counts the number of times supplementary services or the ISDN transport cannot find an idle call register.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Parameters Measured	
1	GF/SS call register overflow peg count

Multi purpose ISDN signaling processor traffic report (TFS011) Click Multipurpose ISDN signaling processor traffic in the table to view the report.

Multi-purpose ISDN signaling processor DCH management report (TFS012) Click Multi-purpose ISDN signaling processor DCH management in the table to view the report.

Table 83
TFS012

Title	System xxx Multipurpose ISDN Signaling Processor D-channel Report
Description	Multipurpose ISDN Signaling Processor D-channel Report (TFS012) displays the traffic management activity for each DSL based on the exchange of signaling messages between the MISP and the terminals over the D-channels.
Parameters Measured	
MISP information	
1	Loop number
2	1 to 10 bytes
3	11 to 20 bytes
4	More than 20 bytes
BRSC information	
1	D-channel
2	1 to 10 bytes
3	11 to 20 bytes
4	More than 20 bytes

Multi-purpose ISDN signaling processor messages report (TFS013) Click Multipurpose ISDN signaling processor messages in the table to view the report.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 84
TFS013

Title	System xxx Multipurpose ISDN Signaling Processor messages Report
Description	Multipurpose ISDN Signaling Processor messages Report (TFS013) shows the total number of call processing, maintenance, and management messages sent through each MISP in the system grouped by message size.
Parameters Measured	
MISP information	
1	MISP loop number
2	MISP link initializations
3	Terminal link initializations
4	MISP management messages
5	Terminal management messages
6	Incomplete calls Link errors
BRSC information	
1	D-channel
2	BRSC link initializations
3	Terminal link initializations
4	BRSC management messages
5	Terminal management messages
6	Incomplete calls Link errors

ISDN BRI trunk DSL system report (TFS014) Click ISDN BRI trunk DSL system in the table to view the report.

Table 85
TFS014

Title	System xxx ISDN BRI Trunk DSL Report
Description	ISDN BRI Trunk DSL Report (TFS014) shows the total number of maintenance, administrative and protocol messages sent through each Digital Subscriber Loop in the system.
Parameters Measured	
MISP information	
1	MISP ID
2	Outgoing maintenance messages
3	Incoming maintenance messages

Copyright © 2010 Nortel Networks. All Rights Reserved.

4	Outgoing administration messages
5	Incoming administration messages
6	Outgoing protocol messages
7	Layer 3 protocol messages
8	Layer 2 protocol messages
9	Layer 1 protocol messages
10	Connected calls

Meridian packet handler report (TFS015) Click Meridian packet handler in the table to view the page title, report description, and the parameters measured in the Meridian packet handler report group.

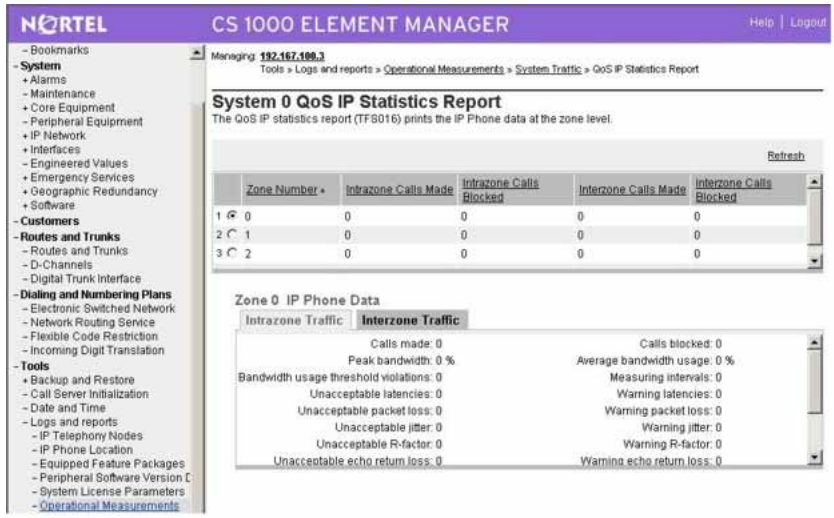
Table 86
TFS015

Title	System xxx Meridian Packet Handler Report
Description	Meridian Packet Handler Report (TFS015) provides specific information about incoming and outgoing calls and data packets. This report is particularly useful for analyzing the flow of data over network links.
Parameters Measured	
1	MPH number
2	Link interface type
3	Link time slot number
4	Layer 2 link initializations
5	Attempted incoming calls
6	Completed incoming calls
7	Attempted outgoing calls
8	Duration of a data call
9	Incoming data packets
10	Outgoing data packets

QoS IP statistics (TFS016) Click QoS IP statistics in the table to view the report.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 88
QoS IP statistics report



Customer traffic reports

To view customer traffic reports in the Element Manager navigator, click **Tools, Logs and Reports, Operational Measurements, Customer Traffic**.

Network report (TFC001) Click Networks in the table to view the page title, report description, and the parameters measured in the Networks report group.

Table 87
TFC001

Title	System xxx Customer yy Networks Report
Description	Networks Report (TFC001) describes traffic details for each customer call.
Parameters Measured	
Incoming Traffic Data	
1	Failure to match
2	Usage
3	Peg count
1	Failure to match
2	Usage
3	Peg count

Copyright © 2010 Nortel Networks. All Rights Reserved.

Outgoing Traffic Data	
1	Failure to match
2	Usage
3	Peg count
Intracustomer Traffic Data	
1	Failure to match
2	Usage
3	Peg count
Tandem Traffic Data	
1	Failure to match
2	Usage
3	Peg count
Miscellaneous	
1	Permanent signal
2	Abandon
3	Partial dial

Trunks report (TFC002) Click Trunks in the table to view the page title, report description, and the parameters measured in the Trunks report group.

Table 88
TFC002

Title	System xxx Customer yy Trunks Report
Description	Trunks Report (TFC002) displays trunk usage. The report prints when the All Trunks Busy (ATB) condition occurs during the reporting period.
Parameters Measured	
1	Route number
2	Trunk type
3	Equipped trunks
4	Working trunks
5	Incoming usage
6	Incoming peg count
7	Outgoing usage
8	Outgoing peg count
9	Outgoing overflow

Copyright © 2010 Nortel Networks. All Rights Reserved.

10	All Trunks Busy
11	Toll peg count
12	All Trunks Busy for nonpriority users

Console queue report (TFC003) Click Console queue in the table to view the page title, report description, and the parameters measured in the Console queue report group.

Table 89
TFC003

Title	System xxx Customer yy Console Queue Report
Description	Console Queue Report (TFC003) examines the treatment of calls in customer queues.
Parameters Measured	
Attendant Response	
1	Average speed of answer
2	Average attendant response
3	Calls delayed peg count
4	Average time in queue
Abandoned Calls	
1	Abandoned calls peg count
2	Average wait time

Individual console measurement report (TFC004) Click Individual console measurement in the table to view the page title, report description, and the parameters measured in the Console queue report group.

Feature key usage report (TFC005) Click Feature key usage in the table to view the page title, report description, and the parameters measured in the Feature key usage report group.

Table 90
TFC005

Title	System xxx Feature Key Usage Report
Description	Feature Key Usage Report (TFC005) looks at patterns of customer usage.
Parameters Measured	
1	Feature number
2	Peg count

Copyright © 2010 Nortel Networks. All Rights Reserved.

Radio paging report (TFC006) Click Radio paging in the table to view the page title, report description, and the parameters measured in the Radio paging report group.

Table 91
TFC006

Title	System xxx Customer yy Radio Paging Report
Description	Radio Paging Report (TFC006) shows the number of calls processed by Radio Paging.
Parameters Measured	
1	RPA system number
2	Request peg count
3	Blocked requests peg count
4	Requests abandoned by caller
Radio Paging	
1	Preselection peg count
2	Post selection peg count
3	Automatic mode peg count
4	Manual mode peg count
5	Diversion peg count
Paging Modes	
1	Mode 1 peg count
2	Mode 2 peg count
3	Mode 3 peg count
4	Mode 4 peg count
5	Mode 5 peg count
Average time	
1	Paging time out
2	Average answer time
3	Recall count
4	Average paging trunk use

Call Park report (TFC007) Click Call Park in the table to view the page title, report description, and the parameters measured in the Call Park report group.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 92
TFC007

Title	System xxx Customer yy Call Park Report
Description	Call Park Report (TFC007) shows the call parking data across a System park and Station park DN.
Parameters Measured	
1	System park peg count
2	System Park overflow peg count
3	Station Park peg count
4	Parked call access peg count
5	Parked call recall peg count
6	Average park wait time

Messaging and auxiliary processor links report (TFC008) Click Messaging and auxiliary processor links in the table to view the page title, report description, and the parameters measured in the Messaging and auxiliary processor links report group.

Table 93
TFC008

Title	System xxx Customer yy Messaging and Auxiliary Processor Links Report
Description	Messaging and Auxiliary Processor Links Report (TFC008) provides data on Messaging and Auxiliary Processor links.
Parameters Measured	
Auxiliary Processor Link	
1	APL number
2	Output queue overflow
3	Input queue overflow
4	Average output queue size
5	Average input queue size
6	Down time
7	Unavailable input message call register
8	Four second time out count
9	Negative acknowledgments
10	Input characters not synchronized
OMSG	
IMSG	

Copyright © 2010 Nortel Networks. All Rights Reserved.

Packets	
1	Output packet messages
Message Attendant Queue	
1	Automatic Call Distribution DN
2	Value Added Server ID
3	Auxiliary Processor Link number
4	Calls in message attendant queue
5	Direct calls to message attendant
6	Indirect calls
7	Time overflow calls
8	Abandoned calls
9	Average waiting time for abandoned calls
10	Average delay
11	Direct call processing time
12	Post call processing time
Telephone Status	
1	Automatic Call Distribution DN
2	Value Added Server ID
3	Auxiliary Processor Link number
4	Total calls
5	Special prefix access calls
6	Call forward access calls
7	User key access calls
8	Unsuccessful calls
Telephone Messaging	
1	Automatic Call Distribution DN
2	Value Added Server ID
3	Auxiliary Processor Link number
4	Total calls
5	Successful telephone messaging calls
6	Abandoned calls
7	Unsuccessful calls
8	Telephone messaging processing time
9	Calls requesting message attendant

Copyright © 2010 Nortel Networks. All Rights Reserved.

Network attendant service report (TFC009) Click Network attendant service in the table to view the page title, report description, and the parameters measured in the Network attendant service report group.

Table 94
TFC009

Title	System xxx Customer yy Network Attendant Service Report
Description	Network Attendant Service Report (TFC009) shows the attempts to route to NAS.
Parameters Measured	
Alternate Routes	
1	Attempts to route to NAS across route 1
2	Attempts to route to NAS across route 2
3	Attempts to route to NAS across route 3
4	Attempts to route to NAS across route 4
Drop Backs	
1	Drop back busies over route 1
2	Drop back busies over route 2
3	Drop back busies over route 3
4	Drop back busies over route 4

DSP peg count report (TFC012) Click Call blocking due to lack of DSP resource in the table to view the page title, report description, and the parameters measured in the DSP peg count report group.

Table 95
TFC0012

Title	System xxx Customer yy DSP Peg Count Report
Description	DSP Peg Count Report (TFC012) shows the number of times calls were blocked on an IP Media Gateway (IPMG) due to insufficient Digital Signal Processor (DSP) resources or a lack of bandwidth.
Parameters Measured	
Alternate Routes	
1	IPMG loop number
2	Attempts to allocate DSP resources
3	Lack of DSP resources
4	Lack of bandwidth

Copyright © 2010 Nortel Networks. All Rights Reserved.

ISPC link establishment report (TFC105) Click ISPC link establishment in the table to view the page title, report description, and the parameters measured in the ISPC link establishment report group.

Table 96
TFC105

Title	System xxx Customer yy ISPC Link Establishment Report
Description	ISPC Link Establishment Report (TFC105) provides a peg count of the number of ISPC links established by an Australian Central office for each Phantom loop for each defined trunk.
Parameters Measured	
Alternate Routes	
1	Loop Number
2	Peg Count

Broadcasting routes report (TFC111) Click Use of broadcasting routes set in the table to view the page title, report description, and the parameters measured in the Broadcasting routes report group.

Table 97
TFC111

Title	System xxx Customer yy Broadcasting Routes Report
Description	Broadcasting Routes Report (TFC111) provides traffic data broadcasting route usage.
Parameters Measured	
1	Route Number
2	Trunk Type
3	Successful connections
4	Average call duration
5	Average waiting duration
6	Maximum waiting time
7	Waiting time threshold peg count
8	Waiting parties threshold peg count
9	Lowest usage trunk connections
10	Next to lowest usage trunk connections
11	Next to next lowest usage trunk connections

Route list measurement report (TFN001) Click Route list measurement in the table to view the page title, report description, and the parameters measured in the Route list measurement report group.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 98
TFN001

Title	System xxx Customer yy Route List Measurement Report
Description	Route List Measurement Report (TFN001) shows how often a route list was accessed, which list entries were used, and whether the call was successfully performed a selection or connection.
Parameters Measured	
Route List	
1	Route list number
2	Number of requests
3	Requests served without delay
4	Expensive route acceptances
5	Requests blocked
6	VNS trunks reuse count
7	VNS trunks total idle time
Route List Entry	
1	Route list number
2	Number of calls
Off-hook Queuing	
1	Number of calls
2	Time elapsed in queue
3	Abandoned calls
Call Back Queuing	
1	Number of calls
2	Time elapsed in queue
3	Calls offered
4	User cancellations
Remote Virtual Queuing	
1	Number of calls
2	Time elapsed in queue
3	Calls offered
4	User cancellations

Network Class of Service Report (TFN002) Click Network Class of Service measurement in the table to view the page title, report description, and the parameters measured in the Network Class of Service report group.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 99
TFN002

Title	System xxx Customer yy Network Class of Service Report
Description	Network Class of Service Report (TFN002) shows the grade of service in terms of blocking and queuing delay.
Parameters Measured	
1	NCOS group number
2	Calls attempted
3	Expensive route acceptances
4	Requests served without delay
5	Requests blocked
6	Calls refusing expensive routes
Off-hook Queuing	
1	Number of calls
2	Time elapsed in queue
Call Back Queuing	
1	Number of calls
2	Time elapsed in queue
Remote Virtual Queuing	
1	Number of calls
2	Time elapsed in queue

Incoming trunk group report (TFN003) Click Incoming trunk group measurements in the table to view the page title, report description, and the parameters measured in the Incoming trunk group report group.

Table 100
TFN003

Title	System xxx Customer yy Incoming Trunk Group Report
Description	Incoming Trunk Group Report (TFN003) shows incremental traffic that network queuing features impose on incoming trunk groups.
Parameters Measured:	
1	Incoming trunk group
2	Calls in off-hook queuing
3	Time elapsed in off-hook queuing
Call Back Queuing	
1	Calls offered
2	Calls accepted

Copyright © 2010 Nortel Networks. All Rights Reserved.

3	Time elapsed in queue
4	Calls blocked in call back
5	Unsuccessful call back attempts
Remote Virtual Queuing	
1	Calls offered
2	Calls accepted
3	Time elapsed in queue
4	Calls blocked in call back
5	Unsuccessful call back attempts

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.

You need to back up no Element Manager data. All data is retrieved from the Call Server and elements.

The c:/u/db/node directory is populated on the Call Server when you save node configuration data. 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; xxxx is the node ID:

- nodexxxx.btp is the BOOTP.TAB file
- nodexxxx.cfg is the CONFIG.INI.

If you remove a node, the associated files are also removed. For every node you create, a nodeyyyy.btp and nodeyyyy.cfg file are created in the C:/u/db/node directory.



WARNING
To prevent Element Manager corruption, do not manually edit or delete the node files.

Backup

The Backup feature starts the Equipment Data Dump (EDD) on the Call Server to back up all Call Server data. Within Element Manager, the Call Server Backup feature starts a data dump and writes the Call Server data to the primary and internal backup drives.

Copyright © 2010 Nortel Networks. All Rights Reserved.

The backup includes all Call Server data and 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.

You can also back up the Call Server by entering the **EDD** CLI command using LD 43.

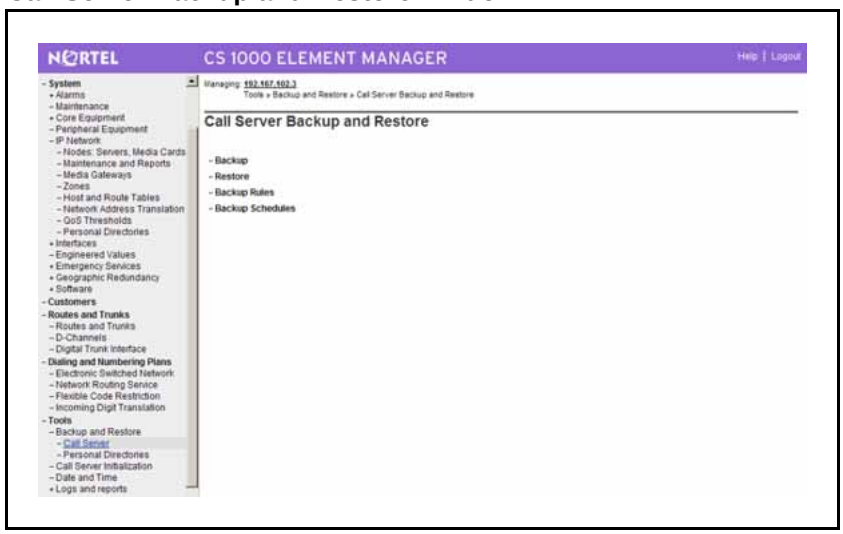
During a backup, the BOOTP.TAB and CONFIG.INI files of all registered nodes are copied so you can restore them if the system fails.

Perform the steps in Procedure 45 “Backing up the Call Server data” (page 339) to back up the Call Server.

Procedure 45
Backing up the Call Server data

Step	Action
1	In the Element Manager navigator, select **Tools, Backup and Restore, Call Server Backup and Restore**. See Figure 89 "Call Server Backup and Restore window" (page 339).
2	Click **Backup**. The Call Server Backup window appears. See Figure 90 "Call Server Backup window" (page 340).

Figure 89
Call Server Backup and Restore window



Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 90
Call Server Backup window



3 Select **Backup** from the **Action** list.

4 Click **Submit** or click **Cancel** to cancel the backup.

The window displays the message "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 occurred.

--End--

Restore the backed up files

The Call Server Restore function restores the backup 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.

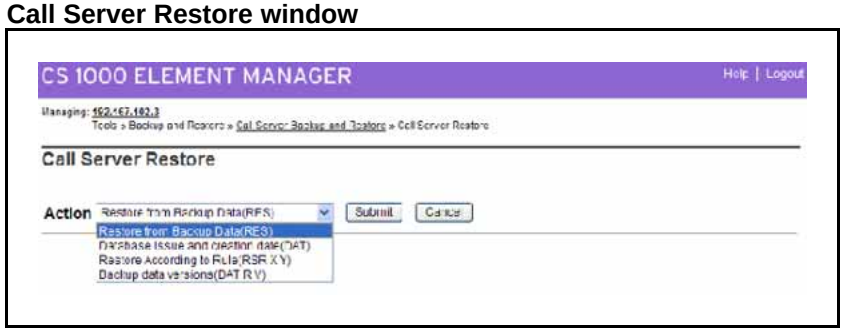
To restore the Call Server data, perform the steps in Procedure 46 "Restoring the Call Server data" (page 340).

Procedure 46
Restoring the Call Server data

Step	Action
1	In the Element Manager navigator, select **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 91 "Call Server Restore window" (page 341).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 91
Call Server Restore window



3 Select **Restore from Backup Data (RES)** from the **Action** list.

4 Click **Submit** .

If the Restore is successful, the message "Restore was done successfully" appears.

--End--

Update IP Telephony node properties

To update the node properties, perform the steps in Procedure 47 “Updating the IP Telephony node properties” (page 341).

Procedure 47
Updating the IP Telephony node properties

Step	Action
1	In the Element Manager navigator, select **IP Networks, Nodes: Servers, Media Cards**. The IP Telephony Nodes window appears.
2	Select the link for a Node ID. The Node Details window appears. See Node Details window.
3	Update the parameters in the appropriate sections as required. For more information, see Procedure 32 “Adding a card and configuring Voice Gateway Media Card properties” (page 261).
4	Click **Save**.

--End--

Add a Voice Gateway Media Card to the node

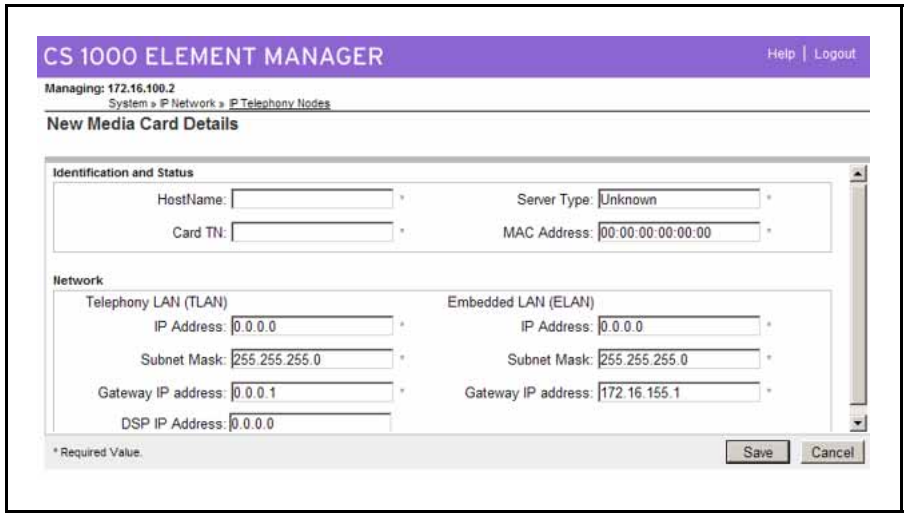
To add a Voice Gateway Media Card to the node, perform the steps in Procedure 48 “Adding a Voice Gateway Media Card to the node” (page 342).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Procedure 48
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, select **IP Network, Nodes: Servers, Media Cards**. The IP Telephony Nodes window appears.
5	Click the link for the Node ID where the card will be added. The Node Details window appears.
6	Select **Media Card** from the **Select to add** menu.
7	Click **Add**. The New Media Card Details window appears. See Figure 92 "New Media Card Details window" (page 342).

Figure 92
New Media Card Details window



8	In the Identification and Status section of the window, enter the following information. **a** **HostName:** This is the host name. **b** **Card TN:** Enter the card slot number from 1 to 50. **c** **Server Type:** **d** **MAC Address:** This is the motherboard Ethernet address.
9	In the Network section of the window, enter the TLAN and ELAN network information.

Copyright © 2010 Nortel Networks. All Rights Reserved.

a **Telephony LAN (TLAN) IP address:** This is the TLAN network interface IP address for the card.

b **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.

10 To add additional cards to the node, click **Add** again and enter the new card information. Repeat this step for each card that you add to the node.

11 Click **Save** after you add and configure a card.

12 Click **Save** on the Node Details window to save the data to the Call Server.

13 Click **OK** to confirm.

If you click **Cancel** all configured information is discarded.

14 Click **Transfer/Status** associated with the node where the new card was added.

15 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 Card retrieves the CONFIG.INI and BOOTP.TAB files from the Call Server. A check mark is added to each field as the card receives the CONFIG.INI and BOOTP.TAB files.

16 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.

17 Insert the new card.

The card starts and obtains the IP configuration from the node leader. This process takes several minutes.

The Maintenance faceplate shows an alarm of T:21 or S009.

- T:21 appears if the card is new and there is no CONFIG.INI file.
- S009 appears if the card was used before and has a CONFIG.INI file that contains an IP address for the Call Server that is no longer correct.

18 In the Element Manager navigator, select **IP Network, Maintenance and Reports**.

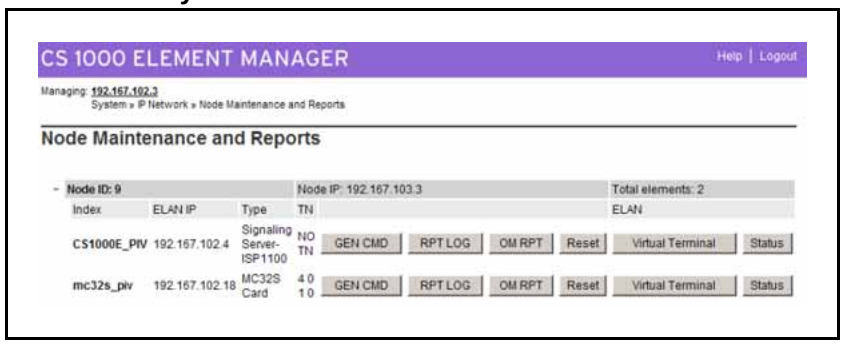
Copyright © 2010 Nortel Networks. All Rights Reserved.

The Node Maintenance and Reports window appears.

19 Expand the node containing the Voice Gateway Media Card by clicking the plus sign (+) to the left of the Node ID.

20 Click **GEN CMD** associated with the Voice Gateway Media Card. See Figure 93 "Voice Gateway Media Card and GEN CMD button" (page 344).

Figure 93
Voice Gateway Media Card and GEN CMD button



The General Commands window appears.

21 From the Group list, select **Misc**.

22 In the Element Manager navigator, select **IP Network, Nodes: Servers, Media Cards**.

The IP Telephony Nodes window appears.

23 Click **Transfer/Status** to download the node information to the card.

24 In the Element Manager navigator, select **IP Network, Maintenance and Reports**.

The Node Maintenance and Reports window appears.

25 Expand the node containing the new card by clicking the plus sign (+) to the left of the Node ID.

26 Click **Status** for each Voice Gateway Media Card that was added.

The card status is Enabled or Disabled. If the status message "Web3003: Destination IP address cannot be reached; initial RPC failure" appears, then verify the network connection and the proper configuration of network equipment.

--End--

Change the IP addresses of an IP Telephony node in Element Manager

Before you change any IP address understand “Codecs” (page 177), and consult with the system administrator.

Copyright © 2010 Nortel Networks. All Rights Reserved.

To change the IP address of an IP Telephony node, perform the steps in Procedure 49 “Changing the IP addresses of an IP Telephony node in Element Manager” (page 345).

Procedure 49
Changing the IP addresses of an IP Telephony node in Element Manager

Step	Action
1	In the Element manager navigator, select **IP Network, Nodes: Servers, Media Cards**. The IP Telephony Nodes window appears.
2	Select the link for the Node ID. The Node Details window appears.
3	Change the IP addresses as required. **a** **Node ID:** The Node ID appears but you cannot change it. **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 TLAN subnet. If the node IP address changes, this affects the configuration of the Connect Server IP address in the DHCP Server for the IP Phones. **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 router interface on the ELAN subnet, if present. If the subnet does not have an Embedded LAN gateway, enter 0.0.0.0. • When an 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 (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. When you change these subnet masks, consider the possible conflict between the ELAN and TLAN network interface IP addresses. Consult with the network administrator before you change subnets.

Copyright © 2010 Nortel Networks. All Rights Reserved.

When you change the Embedded LAN (ELAN) network interface IP address, coordinate it 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
- other devices on the ELAN subnet and customer enterprise network subnet that need to communicate with IP Line
- devices that receive SNMP traps

4 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 to 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 control transmitting and retrieving 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 entered IP address. A maximum of eight IP addresses can be configured.

e Click **Save**.

Copyright © 2010 Nortel Networks. All Rights Reserved.

The parameters are automatically synchronized with the Call Server, Signaling Server, and Media Gateway Controller.

ATTENTION
Perform an Equipment Data Dump (EDD) to permanently save the configured information.

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.

5 In the Element manager navigator, select **IP Network, Nodes: Servers, Media Cards**.

The IP Telephony Nodes window appears.

6 Select the link for the Node ID where the IP address is being changed.

The Edit window appears.

7 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 **Signaling port**: The default value is 15 000. The range is 1 024 to 65 535.

c **Broadcast port**: The default value is 15 001. The range is 1 024 to 65 535.

8 If entries must be made to the card routing table, click the **LAN** link on the Node Details window.

The LAN window .

9 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. Click **Add**.

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

Copyright © 2010 Nortel Networks. All Rights Reserved.

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.



CAUTION
Use caution when you assign 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 routes, click **Add** again and enter the route information. Repeat this step for each new route.

10 Click **Save** , and then click **OK**.

11 In the Node Configuration window, click **Save** associated with the node that had the IP address changes.

--End--

Update other node properties

You can update the following node properties on the Node Details window.

- DSP Profile section: see Procedure 29 “Configuring DSP Profile data” (page 254)
- QoS section: see Procedure 30 “Configuring QoS” (page 257)

Import or Export an IP Node Configuration File

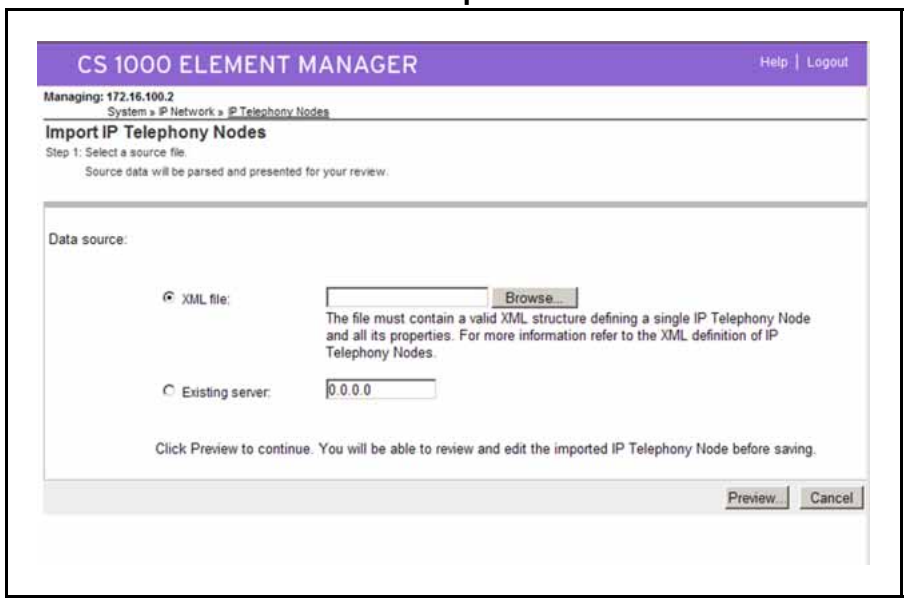
Using Element Manager, import or export an XML file that contains the parameters for IP Telephony node data.

Using the Import feature, import a standard XML file from a local workstation. The file contains node properties data. Configuration parameters must be entered in the file in a standard template model. The template follows the same model as the config.ini file format. You can import, edit, and save the file to the Call Server. To import a file, perform the steps in Procedure 50 “Importing an IP Node Configuration File” (page 349)

Copyright © 2010 Nortel Networks. All Rights Reserved.

Procedure 50
Importing an IP Node Configuration File

Step	Action
1	In Element Manager, select **System, IP Network, Nodes: Server, Media Cards**. The IP Telephony Nodes window appears.
2	Click **Import** .



3	To use an existing XML file that contains the configuration data for the IP Telephony node, click **Browse** . Search for the file on the local workstation, and click **Open** to add the file to the box.
4	To review and edit the configuration data, click **Preview** . If the data in the imported file is invalid, an error message appears. The import fails. If the data in the imported file is valid, the Node Details window appears.
5	Change the configuration data for the IP Node if required.
6	Click **Save** to save the changes to the Call Server. If the configuration data is invalid an error message . The data is not updated to the Call Server.

--End--

Copyright © 2010 Nortel Networks. All Rights Reserved.

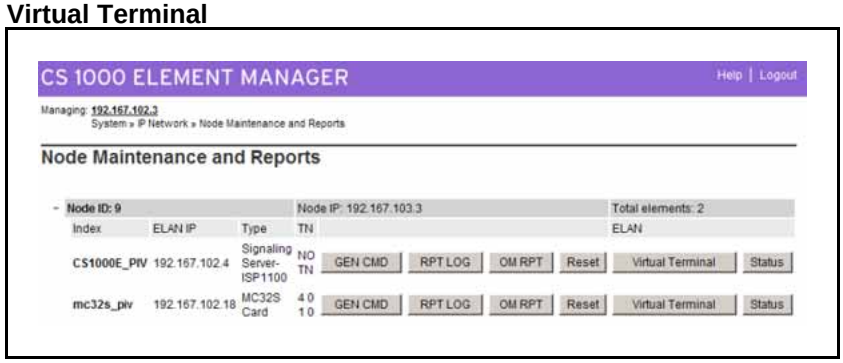
Telnet to a Voice Gateway Media Card using Virtual Terminal

To access the CLI on a Voice Gateway Media Card using Virtual Terminal from Element Manager, perform the steps in Procedure 51 “Accessing a Voice Gateway Media Card using Telnet” (page 350).

Procedure 51
Accessing a Voice Gateway Media Card using Telnet

Step	Action
1	In the Element Manager navigator, select **IP Network, Maintenance and Reports**. The Node Maintenance and Reports window appears.
2	Expand the node containing the Voice Gateway Media Card.
3	Click **Virtual Terminal** associated with the Voice Gateway Media Card. See Figure 94 "Virtual Terminal" (page 350).

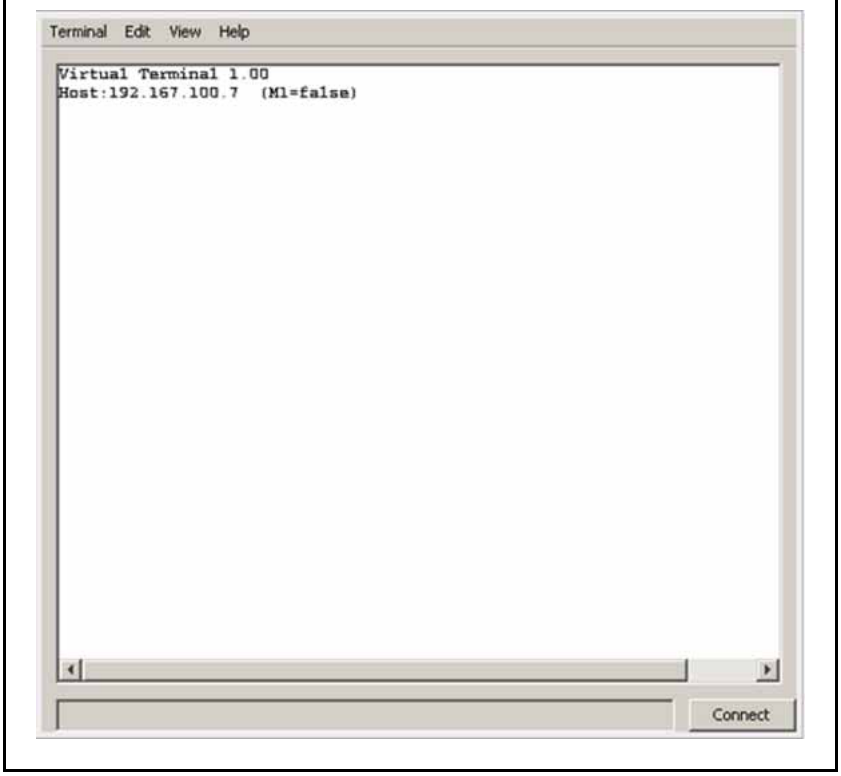
Figure 94
Virtual Terminal



The Virtual Terminal window appears and automatically connects to the Voice Gateway Media Card by using the TLAN or ELAN network interface IP address. See Figure 95 "Virtual Terminal window" (page 351).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 95
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 logon is successful.

5 Type a question mark (?) 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 366) for a list of commands.

--End--

Check the Voice Gateway Channels

To check the Voice Gateway Channels on a Voice Gateway Media Card, perform the steps in Procedure 52 "Checking the Voice Gateway Channels" (page 351).

Procedure 52
Checking the Voice Gateway Channels

Copyright © 2010 Nortel Networks. All Rights Reserved.

Step	Action
1	In the navigation tree, select **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 **GEN CMD** associated with the Voice Gateway Media Card. The General Commands window appears.
4	From the **Group** list, select **Vgw**.
5	From the **Command** list, select **vgwShowAll**.
6	Click **RUN**. The output of the `vgwShowAll` command appears in the text area at the bottom of the window.
7	To view the VGW Channel configuration, from the **Command** list, select **Print VGW Channels** and click **RUN** .
	--End--

Setting the IP Phone Installer Password

Element Manager includes the CLI commands to configure the administrative and temporary IP Phone Installer Password. For more information about the IP Phone Installer Password, see “IP Phone Installer Password” (page 288).

To configure the IP Phone Installer Password in Element Manager, perform the steps in Procedure 53 “Setting the administrative and temporary IP Phone Installer Passwords” (page 352).

Procedure 53
Setting the administrative and temporary IP Phone Installer Passwords

Step	Action
1	Select **IP Network, Maintenance and Reports**. The Node Maintenance and Reports window appears.
2	Expand the node to show all elements.
3	Click **GEN CMD** associated with the Voice Gateway Media Card. The General Commands windows appears.
4	From the **Group** list, select **NodePwd**.

Copyright © 2010 Nortel Networks. All Rights Reserved.

5 From the **Command** list, select **nodePwdShow** and click **RUN** .

The output from the **nodePwdShow** command appears in the text area at the bottom of the window. If in the default state, the IP Phone Installer Password was never assigned. 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

Copyright © 2010 Nortel Networks. All Rights Reserved.

```
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: the number of Uses becomes zero or the Timeout expires. If both the Uses and Timeout parameters are entered and are zero, it is the same as not setting the temporary password.

6 From the **Group** list, select **NodePwd**.

7 From the Command list, select **nodePwdSet** and click **RUN** .

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 **RUN** .

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, asterisk (*), and number sign (#). 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 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 you click **RUN** in the Node Password field and no password is entered in the 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 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** list, select **nodePwdShow** from the list box and click **RUN**.

The text area data output is similar to the following:

Copyright © 2010 Nortel Networks. All Rights Reserved.

```
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 list and click **RUN**.

14 Confirm that the temporary password is cleared.

From the **Command** 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--

Copyright © 2010 Nortel Networks. All Rights Reserved.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Maintenance

Contents

This chapter contains the following topics:

- “Introduction” (page 357)
- “IP Line and IP Phone maintenance and diagnostics” (page 357)
- “IP Line CLI commands” (page 366)
- “Lamp Audit function” (page 368)
- “Troubleshoot an IP Phone installation” (page 368)
- “Maintenance telephone” (page 368)
- “Faceplate maintenance display codes” (page 369)
- “System error messages” (page 371)
- “Voice Gateway Media Card self-tests” (page 376)
- “Replace the Media Card CompactFlash” (page 376)

Introduction

This chapter describes maintenance functions for the Voice Gateway Media Card, IP Line and IP Phones.

Check the Nortel Web site for information about the most recent software, firmware, and application releases.

IP Line and IP Phone maintenance and diagnostics

This section describes the commands in LD 32 and LD 117.

LD 32

Table 101 "LD 32 Maintenance commands for the Voice Gateway Media Card" (page 358) summarizes the system maintenance commands available in LD 32.

Copyright © 2010 Nortel Networks. All Rights Reserved.

The following ECNT commands are available in LD 117 and LD 32:

- ECNT CARD
- ECNT NODE
- ECNT SS
- ECNT ZONE

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 135) and "LD 117" (page 360).

Table 101
LD 32 Maintenance commands for the Voice Gateway Media Card

Command	Description
DISC l s c	Disables the specified card, l = loop, s = shelf, c = card.
DISI l s c	Disables the specified card when idle, l = loop, s = shelf, c = card Use the DISI command to disable the Voice Gateway Media Card instead of the DISC command. The NPR0011 message indicates the disabled state of the Voice Gateway Media Card.
DISU l s c u	Disables the specified unit; l = loop, s = shelf, c = card, u = unit
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 according to that parameter. A customer cannot be specified in this case. Example:

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 101
LD 32 Maintenance commands for the Voice Gateway Media Card (cont'd.)

Command	Description
	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 logged on 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: 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: 1 000

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 101
LD 32 Maintenance commands for the Voice Gateway Media Card (cont'd.)

Command	Description
	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; l = loop, s = shelf, c = card
ENLU l s c u	Enable the specified unit; l = loop, s = shelf, c = card, u = unit
IDC l s c	Print the Card ID information for the specified card, 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, l = loop, s = shelf, c = card
STAT l s c u	Print the CS 1000 software status of the specified unit, l = loop, s = shelf, c = card, u = unit

LD 117

Table 102 "LD 117 Count registered IP Phones" (page 361) 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 135).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 102
LD 117 Count registered IP Phones

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 appears, as an underscore is an invalid character.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 102
LD 117 Count registered IP Phones (cont'd.)

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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 102
LD 117 Count registered IP Phones (cont'd.)

Command	Description
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.

TN

For Nortel IP Phones, consider two kinds of TN:

- 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 TN

Physical TN, that are seen as trunk units, are managed using existing LD 32 commands.

Virtual TN

Because virtual TN 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 103 "LD 32 maintenance commands for IP Phones" (page 364) contains the maintenance commands in LD 32 for the IP Phone. For more information about commands, see *Software Input Output Reference — Maintenance* (NN43001-711).

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 103
LD 32 maintenance commands for IP Phones

Command	Description
STAT l s c u	Displays 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 configured in the system but not yet registered. • REGISTERED identifies a registered IP Phone.
DISU l s c u	Change the IP Phone state to DSBL. UNREGISTERED or REGISTERED state is not modified.
ENLU l s c u	Change the IP Phone state to IDLE. UNREGISTERED or 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 that you can use to test the end-to-end IP connectivity of the IP Phone.

See Figure 96 "IDU command output" (page 365)for an example of IDU command output.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 96
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 also appears.

In the example in Figure 96 "IDU command output" (page 365), 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 parentheses.

This format applies only for IP Phone Virtual TNs.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 generates an NPR0053 message. 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 supplement Overlay commands and introduce features specific to the Signaling Server platform.

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

Note 1: CS 1000 Release 6.0 does not support VxWorks-based **`deplist`** CLI commands.

Note 2: Use the **`appinstall`** command only if you are directed by Nortel support.

Use SSH to access the CLI. These IP Line CLI commands are entered at the command prompt. Instructions to connect to the maintenance port of the Signaling Server are described in *Communication Server 1000M and Meridian 1 Small System Installation and Commissioning* (NN43011-310).

Protocol trace tool commands for the Network Connection Service

ATTENTION
A system warm start causes all tracing to cease. Traces must be reentered after the system restarts.

Table 104 "Protocol trace tool CLI commands for the NCS" (page 366) includes the protocol trace tool commands for the Network Connection Service (NCS). You must be assigned to the OAM role to run these commands.

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

Table 104
Protocol trace tool CLI commands for the NCS

CLI Command	Description	Signaling Server
`tpsARTrace` **`IP <IP Address>`** **`ID <user ID>`** **`ALL`**	Traces the tpsAR protocol, which is used to determine where an IP Phone registers. • IP Address: a string containing the IP Phone IP address	X

Copyright © 2010 Nortel Networks. All Rights Reserved.

CLI Command	Description	Signaling Server
	• user UID: the ID of the IP Phone to trace (the DN used to log on) or the H323_Alias of where the IP Phone tries to register • ALL: all IP Phones are to be monitored	
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. • Output_Destination specifies where all the trace messages for the tpsARTraceSet are to be directed. If the command runs from the Voice Gateway Media Card or the Linux shell prompt: The values are as follows: 1 = TTY 2 = RPTLOG 3 = File 4 =TTY + File If the command runs from the OAM prompt or Linux prompt on the Signaling Server: The values are the actual word, not a number: TTY RPTLOG FILE TTY+FILE • File Pathname is a string enclosed in quotation marks. It specifies the file to write to if you select option 3 or 4.	X
tpsARTraceSettings	Displays the trace tool settings, which endpoints are traced, and where the trace output is directed.	X
tpsARTraceHelp	Displays a list of all CLIs used for tracing tpsAR protocol messages, including usage and parameters.	X

Copyright © 2010 Nortel Networks. All Rights Reserved.

Lamp Audit function

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 a reliable UDP connection exists from the core through to the IP Phones, any failure of the IP Phone 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).

Troubleshoot an IP Phone installation

If an IP Phone cannot be installed because the prompt for the node ID or TN does not appear, perform the steps in Procedure 54 “Troubleshooting an IP Phone installation” (page 368).

Procedure 54
Troubleshooting an IP Phone installation

Step	Action
1	Log on to a Signaling Server in the node.
2	Type the **`nodePwdShow`** command at the prompt.
3	Use the **`nodePwdSet "password"`** command to configure the administrative password and to enable IP Phone installation. Ensure the password parameter is included.

--End--

Maintenance telephone

An IP Phone functions as a maintenance telephone when the CoS 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, you can enter only a subset of commands from a system terminal. 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, press 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

The previous 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.

Faceplate maintenance display codes

The Voice Gateway Media Card maintenance display provides the diagnostic status of the card during powerup, the operational state when in service, and error information about the functional state of the card.

- Table 105 "Media Card 32-port card faceplate maintenance display codes" (page 369) lists the normal and fault display codes for the Media Card 32-port line card.
- Table 107 "Media Card 32 card diagnostic information" (page 370) and Table 108 "Messages displayed on the LED during Media Card 32S card normal operation" (page 371) lists the messages on the faceplate for the Media Card 32S card.

Table 105
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 ISPDI FPGA
T:11	F:11	Testing host dual port RAM
T:12	F:12	Testing DS-30 dual port RAM
T:13	F:13	Testing SEEPROM
T:14	F:14	Booting Host processor, waiting for response with self-test information
T:15	F:15	Not used
T:16	F:16	Not used
T:17	F:17	Not used
T:18	F:18	Not used

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 105
Media Card 32-port card faceplate maintenance display codes (cont'd.)

Normal code	Fault code	Message
T:19	F:19	Not used
T:20	F:20	Waiting for application startup message from Host processor
T:21	F:21	CardLAN enabled, waiting for request configuration message
T:22	F:22	CardLAN operational, A07 enabled, display now under host control

Table 106
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 or EEPROM interface failure
H:80	PCM connector failure

Table 107
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 performs hardware system tests during system powerup.
PASS	Appears when POST passes.
EXXX	Appears if a serious system error is detected. Error code where XXX is a numeric value.
LOAD	Appears when application software loads.

Copyright © 2010 Nortel Networks. All Rights Reserved.

During powerup, the card performs multiple self-tests, including an internal RAM test, a ALU test, address mode test, a boot ROM test, a timer test, and an external RAM test. If a test test fails, the card enters a maintenance loop, and no further processing is possible. A failure message appears to indicate which test failed.

If the other tests fail (up to and including the EEPROM test), a message appears for three seconds. If more than one test fails, the message indicates the first failure. If you select verbose mode (by the test input pin on the backplane), the 3-second failure message does not appear.

If a test fails on the Media Card, F:XX appears on the hexidecimal display for 3 seconds after the T:13 message (Testing SEEPROM). For example, if the 8051 coprocessor test fails, F:05 appears on the Media Card faceplate. If more that one test fails, the message indicates the first failure.

If the IXP encounters failures during initialization, an H:XX error code appears. Table 106 "List of error codes for the Media Card 32-port card" (page 370) shows the list of error codes.

When the Media Card 32S card starts, diagnostic information, such as boot status, appears on the faceplate.

In normal operation, the messages appear in the following order:

- BOOT
- POST
- PASS
- LOAD

If a self-test error occurs, an error code appears.

Table 108
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.
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 an error log file.

Copyright © 2010 Nortel Networks. All Rights Reserved.

View the error log in TM 4.0 IP Line by clicking Open Log File on the Maintenance tab of the ITG Card Properties. Alternatively, view the log file in any text browser after you upload 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; xxx is the last three digits of the ITG or ITS message. The Signaling Server has no display. Alarms appear in the Signaling Server report log or by way of SNMP on an Alarm browser.

Table 109 "Critical ITG Error messages" (page 372) lists the critical ITG messages and Table 110 "Critical ITS Error messages" (page 375) lists the critical ITS messages.

A Voice Gateway Media Card can send all listed alarms. Any alarm that can be sent by the Signaling Server has an X in the Signaling Server column.

For a complete list of other error messages, see *Software Input Output Reference—System Messages* (NN43001-712).

Table 109
Critical ITG Error messages

Maintenance display	Corresponding critical error message	Signaling Server	Description
G000	ITG1000	X	Card (re)started.
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>.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 109
Critical ITG Error messages (cont'd.)

Maintenance display	Corresponding critical error message	Signaling Server	Description
G005	ITG1005	X	Message queue error <operation> <object> <errno> <errtext>.
G006	ITG1006	X	Unexpected state encountered <file> <line> <state>.
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>

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 109
Critical ITG Error messages (cont'd.)

Maintenance display	Corresponding critical error message	Signaling Server	Description
G026	ITG1026	—	DSP download retry succeeded <dsp>
G027	ITG1027	—	DSP memory test: <dsp> <reason>
G028	ITG1028	X	Voice packet loss: <channel> <%packetLoss> <direction> <dstAddr>
G029	ITG1029	—	Error in DSP task <file> <line> <errno> <errtext>.
G030	ITG1030	—	Allocation failure in DSP memory pool.
G031	ITG1031	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 or 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

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 109
Critical ITG Error messages (cont'd.)

Maintenance display	Corresponding critical error message	Signaling Server	Description
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 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 110
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	Corrupt node ID/TN field <ip> <hwid>.
S006	ITS1006	X	Received corrupt UNIStim message <message dump>.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 110
Critical ITS Error messages (cont'd.)

Maintenance Display	Corresponding Critical Error Message	Signaling Server	Description
S007	ITS1007	X	Received unknown UNIStim 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>)
S012	ITS1012	X	User entered the wrong IP Phone Installer Password three times during Branch User Config. The IP Phone is locked out from User Configuration for one hour. Action: Wait for the IP Phone to unlock in 1 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.

Voice Gateway Media Card self-tests

During powerup, 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 the serial port to provide Card LAN communication and connects the processor with the external RS-232 port.

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 you use the Media Card.

Copyright © 2010 Nortel Networks. All Rights Reserved.

If you must remove the CompactFlash card, perform the steps in Procedure 55 “Removing the CompactFlash” (page 377). To reinstall a CompactFlash card, see Procedure 20 “Installing the CompactFlash card on the Media Card” (page 218).

Procedure 55
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 from the socket and carefully remove the CompactFlash card.
3	Return the CompactFlash card to an antistatic package.

--End--

Copyright © 2010 Nortel Networks. All Rights Reserved.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Voice Gateway Media Card maintenance using Element Manager

Contents

This chapter contains the following topics:

- “Introduction” (page 379)
- “Replace a Voice Gateway Media Card” (page 379)
- “Add another Voice Gateway Media Card” (page 380)
- “Access CLI commands from Element Manager” (page 381)

Introduction

This chapter provides information about the maintenance functions for the Voice Gateway Media Card that you perform 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 restart. 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 failed. This is indicated by failing to show a link pulse on the voice IP interface status LED or on the switch. The maintenance port can also continuously print "lnIsa0 Carrier Failure" messages after determining that the hub or switch port and ELAN cable are valid.
- 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Verify Voice Gateway Media Card loadware

Perform the following steps to verify and upgrade the card loadware.

Step	Action
1	Verify the version of the loadware currently installed on the Voice Gateway Media Card. See "Determine Voice Gateway Media Card software version" (page 266).
2	Obtain the latest files from the Nortel Web site. See "Software delivery" (page 14).
3	Upload the loadware files using the File Upload system utility in Element Manager. See Procedure 34 "Uploading loadware and firmware files" (page 267).
4	Upgrade the Voice Gateway Media Card software. See Procedure 36 "Upgrading the card loadware" (page 268).
5	Restart the Voice Gateway Media Card. See Procedure 37 "Restarting the Voice Gateway Media Card" (page 269).

--End--

Add another Voice Gateway Media Card

Perform the steps in Procedure 56 "Add another Voice Gateway Media Card to the system" (page 380) to add another Voice Gateway Media Card to the system.

Procedure 56
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 217).
2	In the Element Manager navigator, select **IP Network, Nodes: Servers, Media Cards**. The IP Telephony Nodes window appears.
3	Select the link for a Node ID. The Node Details window appears.
4	Select **Media Card** from the **Select to add** menu and then click **Add** . The New Media Card window appears.
5	Enter the card information. **a** **Hostname:** This is the host name.

Copyright © 2010 Nortel Networks. All Rights Reserved.

b **Card TN:** Enter the card slot number from 1 to 50.

c **MAC Address:** The MAC address is the Motherboard Ethernet address labeled on the faceplate of the Voice Gateway Media Card.

d **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.

e **Telephony LAN (TLAN) IP address:** This is the TLAN network interface IP address for the card.

f **Telephony LAN (TLAN) DSP IP address**

Note: The DSP daughterboard is a device that is fixed on the main board of the MC32S card. The device requires a TLAN IP address.

6 Click **Save**.

The Node Details window appears.

7 Click **Save** on the Node Details window.

8 On the IP Telephony Nodes window, click the **Status** link associated with the node containing the Voice Gateway Media Card.

9 After the transfer is complete, restart the new card.

Restart the card to obtain the BOOTP parameters from the Leader and to establish ELAN and TLAN subnet connectivity.

10 Perform the steps in Procedure 36 “Upgrading the card loadware” (page 268) to download the most recent software to the Voice Gateway Media Card.

11 Perform the steps in Procedure 37 “Restarting the Voice Gateway Media Card” (page 269) to restart the card and run the new software.

12 Perform the steps in Procedure 39 “Upgrading the IP Phone firmware” (page 271) to update the card firmware.

--End--

Access CLI commands from Element Manager

To access CLI commands in Element Manager, perform the steps in “Access CLI commands from Element Manager” (page 381).

Copyright © 2010 Nortel Networks. All Rights Reserved.

CS 1000 Release 6.0 supports the following command groups for the Media Card 32S:

- General
- System
- Voice Gateway
- Special
- Security

Accessing CLI commands for the Media Card 32S

Step	Action
1	In the Element Manager navigator, select **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 **GEN CMD** associated with the MC 32S 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 MC 32S card.
4	Select one of the following CLI command groups from the **Group** list box: • General • System • Voice Gateway • Special • Security
5	Select the CLI command from the **Command** list, and click **RUN**. The output of the command appears in the text area at the bottom of the General Commands window. For information about the CLI commands, see *Software Input Output Reference — Maintenance* (NN43001-711).

--End--

Copyright © 2010 Nortel Networks. All Rights Reserved.

Appendix NAT router requirements for NAT Traversal feature

Contents

This section contains the following topics:

- "Description" (page 383)
- "Requirements" (page 384)
- "Natcheck output" (page 386)

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:

- Use a cone NAT.
- Configure a long time-out period for the Private-to-Public mapping.
- If multiple IP Phones are behind the same NAT router, support hairpinning.
- Keep alive the Private-to-Public mapping created by a NAT router by packets in only one direction (standard in most NAT routers).
- The IP Phone run the correct minimum firmware version (not a NAT device requirement, but still important).

You can confirm most of the issues encountered by using either an IP Phone behind the NAT device or a PC running the third-party natcheck tool.

Copyright © 2010 Nortel Networks. All Rights Reserved.

ATTENTION
Nortel is not affiliated in any manner with the natcheck tool, and, therefore is not liable or responsible for problems that you might encounter.

The natcheck tool can be downloaded at no cost from //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 appears, then the NAT router uses a cone NAT.

Confirm using IP Phone

The NAT router uses a cone NAT if no error message appears 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 restarts, use LD 117 to lower the NAT Keep Alive Timer value on the Call Server. The restarts can indicate that the NAT device address or port mapping is cleared because no message traffic arrives from the IP Phone. By lowering the NAT Keep Alive Timer value in the Call Server, keepalive 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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.

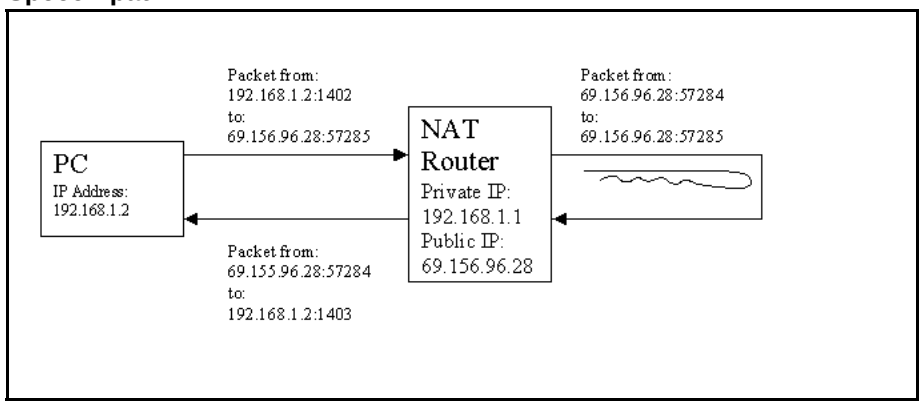
Confirm using natcheck

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 97 "Speech path" (page 385).

Figure 97
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 registration, and continues to have a two-way speech path 2 to 30 minutes later, then the NAT device address or port mapping is kept alive by the packets. If a one-way speech path occurs after this time

Copyright © 2010 Nortel Networks. All Rights Reserved.

period, ensure that the IP Phone has the latest firmware version. If the IP Phone has the most recent 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 restarting 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 most recent firmware version (previous firmware versions can be a possible source of problems for the one-way speech path).

Firmware versions

The IP Phone must have the correct minimum firmware version.

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 as follows:

- IP Phone 2002 and IP Phone 2004: xxxxB64
- Phase II IP Phone 2002 and IP Phone 2004: xxxxD41
- IP Softphone 2050: xxxx375

Previous firmware versions do not correctly support the NAT Traversal feature.

Natcheck output

A NAT router using CONE NAT produces 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
```


Copyright © 2010 Nortel Networks. All Rights Reserved.

```
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
```


Copyright © 2010 Nortel Networks. All Rights Reserved.

```
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)
```

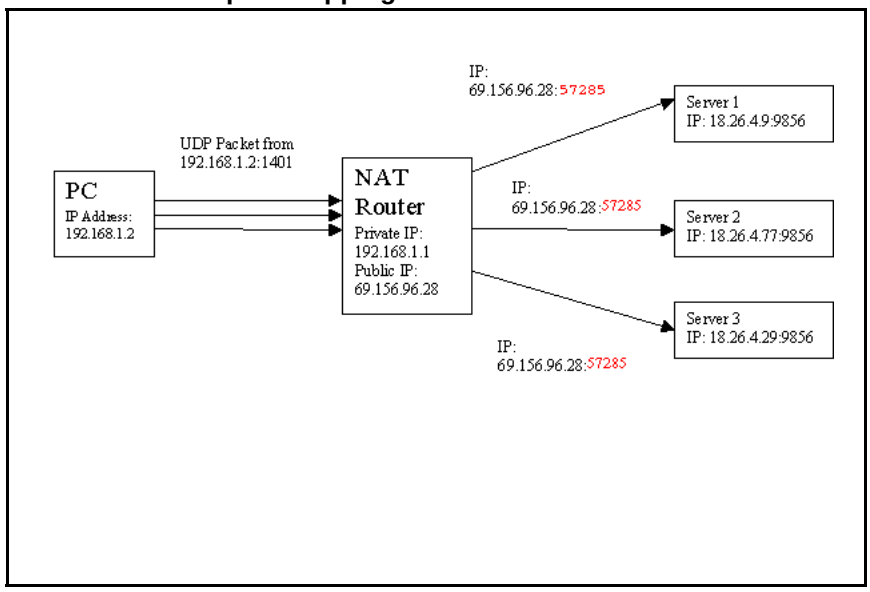
For the NAT router to support the NAT Traversal feature, natcheck must display the following:

```
UDP consistent translation:  YES (GOOD for peer-to-peer)
```

Ye indicates that Cone NAT is used. No indicates that Symmetric NAT is present. Symmetric NAT is not supported.

Near the beginning of the output, the PUBLIC port seen by various servers appears. In this case, all three servers receive the packets from the same PUBLIC port of 57283. Figure 98 "Private-to-Public port mapping" (page 388)shows this Private-to-Public port mapping.

Figure 98
Private-to-Public port mapping



Because all three servers see the same PUBLIC port, the NAT router uses Cone NAT.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Appendix I/O, maintenance, and extender cable description

Contents

This section contains the following topics:

- “Introduction” (page 389)
- “NTMF94EA I/O cable” (page 389)
- “Connector pin assignments” (page 390)
- “NTAG81CA maintenance cable description” (page 393)
- “NTAG81BA maintenance extender cable” (page 394)
- “Replace the NT8D81BA cable” (page 395)

Introduction

This appendix describes the NTMF94EA, NTAG81CA, and NTAG81BA cables and explains how to replace the NT8D81BA backplane ribbon cable and 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 has one DB9 serial port that provides serial connection between the card and the customer PC or TTY. See Figure 99 "NTMF94EA ELAN, TLAN and RS-232 serial maintenance I/O cable" (page 390).

You must use the mounting screw 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.

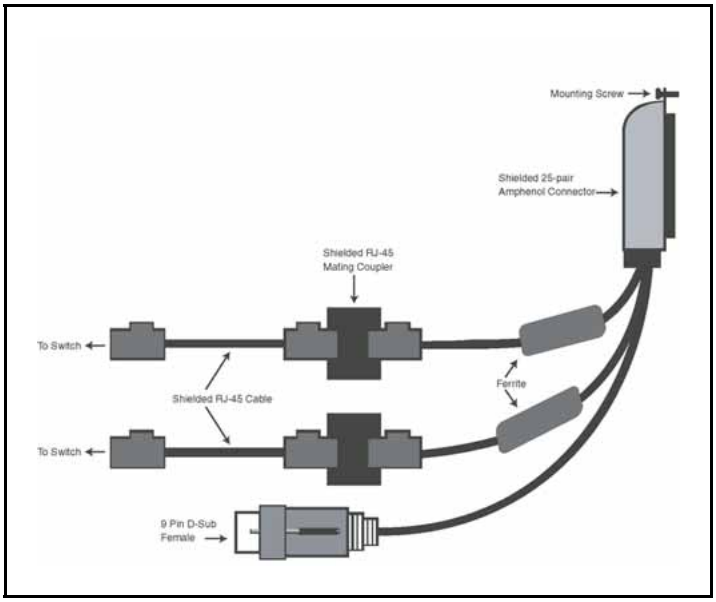
Copyright © 2010 Nortel Networks. All Rights Reserved.

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 prevents ground loops (if required). See “Prevent ground loops on connection to external customer LAN equipment” (page 392)to determine if you use the unshielded coupler. 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 from the system.

ATTENTION
To avoid damage to CAT5 cable, do not overtighten cable ties.

Figure 99
NTMF94EA ELAN, TLAN and RS-232 serial maintenance I/O cable



Connector pin assignments

Table 111 "Voice Gateway Media Card I/O Panel Pinout" (page 390) shows the I/O connector pin designations for the Voice Gateway Media Card.

Table 111
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

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 111
Voice Gateway Media Card I/O Panel Pinout (cont'd.)

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 112
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

Copyright © 2010 Nortel Networks. All Rights Reserved.

P1-46	BDCDB-	P2-1	Orange
P1-47	BDSRB-	P2-6	Yellow
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. Perform the steps in Procedure 57 “Preventing ground loops” (page 392) to prevent ground loops when you connect to external customer LAN equipment.

Follow the steps in Procedure 57 “Preventing ground loops” (page 392) to prevent ground loops.

Procedure 57
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 you plug it into the shielded RJ-45 coupler on the end of the NTMF94EA.

Copyright © 2010 Nortel Networks. All Rights Reserved.

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 100 "NTAG81CA Maintenance cable" (page 393).

Figure 100
NTAG81CA Maintenance cable

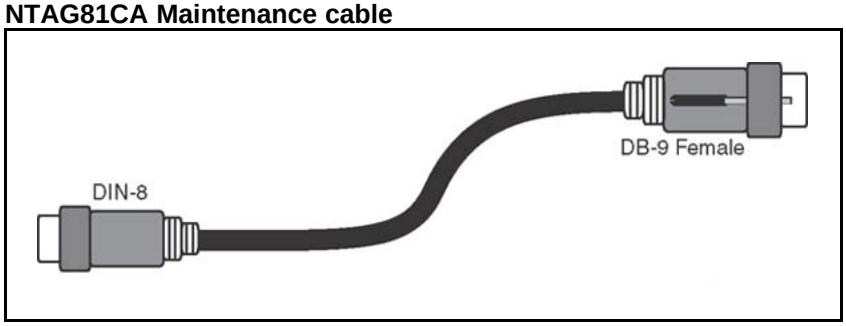


Table 113 "NTAG81CA maintenance cable pin description" (page 393)describes the NTAG91CA cable pin description.

Table 113
NTAG81CA maintenance cable pin description

Signals (MIX Side)	Eight-pin Mini-DIN (MIX Side) Male	Nine-pin D-Sub (PC Side) Female	Signals (PC Side)
DTRB-	1	6	DSR-
SOUTB-	2	2	SIN-
SINB-	3	3	SOUT-
GND	4	5	GND
SINA-	5	nc	nc

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 113
NTAG81CA maintenance cable pin description (cont'd.)

Signals (MIX Side)	Eight-pin Mini-DIN (MIX Side) Male	Nine-pin D-Sub (PC Side) Female	Signals (PC Side)
CTSA-	6	nc	nc
SOUTA-	7	nc	nc
DTRA-	8	nc	nc

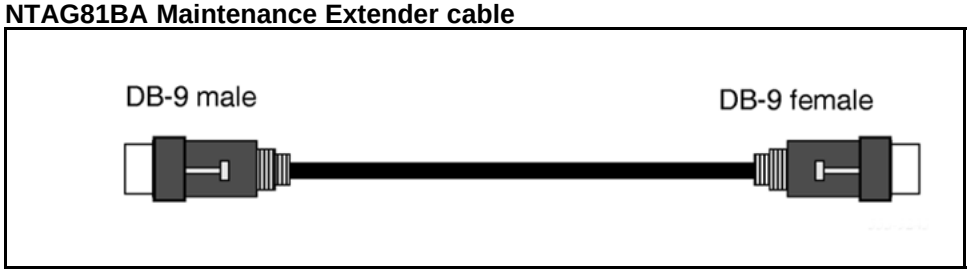
NTAG81BA maintenance extender cable

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 114 "NTAG81BA Maintenance cable pin description" (page 394). The cable can also extend the serial port presented by the NTMF94EA I/O panel cable. The extender cable is shown in Figure 101 "NTAG81BA Maintenance Extender cable" (page 394).

Table 114
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 101
NTAG81BA Maintenance Extender cable



Copyright © 2010 Nortel Networks. All Rights Reserved.

Replace the NT8D81BA cable

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) IPE Modules, all 16 IPE card slots support 24-pair cable connections. Table 115 "NT8D37 cable connections" (page 395) shows the cable connections from the backplane to the inside of the I/O panel.

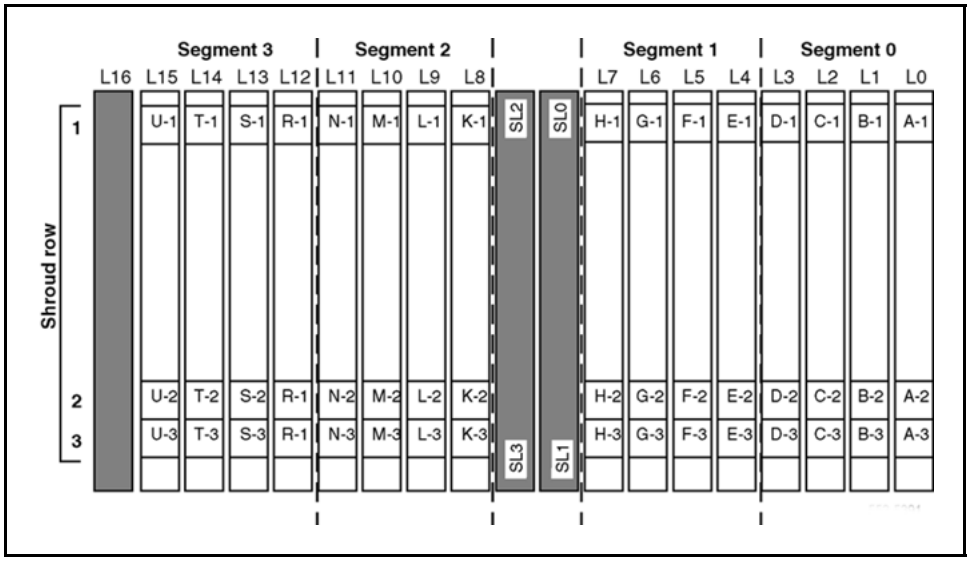
Table 115
NT8D37 cable connections

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 102 "Backplane slot designations" (page 396) 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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Figure 102
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

Perform the steps in Procedure 58 “Removing an NT8D81BA cable” (page 396) to remove the NT8D81BA cable.

Procedure 58
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.

Copyright © 2010 Nortel Networks. All Rights Reserved.

5 To remove the ribbon cables from the IPE backplane, apply gentle pressure on the tab on the right side of the shroud while you pull the connector 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

Perform the steps in Procedure 59 “Installing an NTCW84JA filter and NT8D81AA cable” (page 397) to install the NTCW84JA filter and NT8D81AA cable.

Procedure 59
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 you install the connector so the label faces right with the arrow pointing up and the connector 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 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--

Copyright © 2010 Nortel Networks. All Rights Reserved.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Appendix Product integrity

Contents

This section contains the following topics:

- “Introduction” (page 399)
- “Reliability” (page 399)
- “Environmental specifications” (page 400)

Introduction

This chapter presents information about the Voice Gateway Media Card reliability, environmental specifications, and electrical regulatory standards.

For more information about COTS and CP PM servers, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

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 for every 106 hours of operation are 2.483, based on 40 degrees Celcius (140 degrees Fahrenheit).

Voice Gateway Media Card power consumption

Table 116 "Voice Gateway Media Card power consumption" (page 400) shows the worst case current drawn by the Voice Gateway Media Cards from each Backplane voltage supply.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 116
Voice Gateway Media Card power consumption

Card Type	Power Consumption
Media Card	+ 15 volt = 6 watts => 0.2 amps +5 volt = 7.25 watts => 1.45amps

Environmental specifications

Table 117 "Environmental specifications (maximum)" (page 400) 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 117
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 regarding temperature and shock were made under test conditions. Table 118 "Environmental specifications (recommended)" (page 400) shows recommended temperature and humidity ranges for the Voice Gateway Media Card based on results from this test.

Table 118
Environmental specifications (recommended)

Specification	Minimum	Maximum
Normal Operation		
Recommended Relative humidity	15°C 20%	30°C 55% (non condensing)
Absolute Relative humidity	10°C 20%	45°C 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

Copyright © 2010 Nortel Networks. All Rights Reserved.

Table 118
Environmental specifications (recommended) (cont'd.)

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	

Copyright © 2010 Nortel Networks. All Rights Reserved.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Appendix 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. You must convert the subnet mask from CIDR format to dotted decimal format 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 /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.

Perform the steps in Procedure 60 “Converting a subnet mask from CIDR format to dotted decimal format” (page 403) to convert a subnet mask from CIDR format to dotted decimal format.

Procedure 60
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 8 divides into the CIDR format value) equals the number of dotted decimal fields containing 255. In the example 10.1.1.1/20, the subnet mask is expressed as /20. A value of 20 divided by 8 equals a quotient of 2, with a remainder of 4. Therefore, the first two fields of the subnet mask in dotted decimal format are 255.255.
2	If a remainder exists, see Table 119 "CIDR format remainders" (page 404) to obtain the dotted decimal value for the field following the last field containing 255. In the example of

Copyright © 2010 Nortel Networks. All Rights Reserved.

/20 above, the remainder is 4. In Table 119 "CIDR format remainders" (page 404), a remainder of 4 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 remaining fields exist 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 119
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

Copyright © 2010 Nortel Networks. All Rights Reserved.

Index

802.1Q Support 148
911 282

A

add additional cards to the node 262, 343
Automatic IP Phone TN conversion 47

B

Back up an IP Phone Application Server database 207
backplanes
  connectors 395
  I/O panel connections 395
backup 338
bandwidth used 135
Basic IP User License 31
blocked calls 135
BOOTP parameters 381
Branch Office 147

C

call attempts and completions 135
Call Statistics 135
Card TN 262, 342
CHG ES1 112
CHG ES2 112
CHG NKT 112
CLI commands, informational 381
Codec 150
community string 252
CompactFlash 218
Configuring a virtual Superloop in Element Manager 231
connector pin assignments
  NT8D02 Digital Line Card 390
connectors 395
Corporate Directory 119, 280
CRPA/CRPD 280

D

Data Path Capture tool 149
Digital Signaling Processor (DSP) 70
Digital Signaling Processor daughterboards 19
DSP daughterboards 19

E

e911 282
Echo Server 111
echoServerShow 115
echoServerShow 99 116
EDD 288
Element Manager 134
Emergency Services Access 282
Emulation Mode 46
environmental specs 400
existing Voice Gateway Media Card properties 262

F

F
  10 code 379
  xx 379
FIBN 230
FIBN, Package 365 230
Firmware
  IP Phone 149

G

GEN CMD button 382
Group maximums 230

Copyright © 2010 Nortel Networks. All Rights Reserved.

H

hardware 216
Hardware Watchdog Timer 149
Hold 109
Hostname 262, 342

I

I/O panels
backplane connections 395
informational CLI commands available from Element Manager 381
Internet Explorer 216, 245–246
Internet Options dialog box 200
Internet Telephone Firmware 149
IP client cookies 44
IP Phone configuration data summary sheet 191
IP Phone Types 45
IP User License 31
IPE modules
cable connections 395
isetGet 115
isetReset 114–115
isetScpwModify 115
isetScpwQuery 115
isetScpwVerify 115

K

Keep Alive Time-out setting 112

L

Language synchronization 40
LD 97 230
License 31
Live Dialpad 38
lnIsa0 Carrier Failure 379

M

Manual IP Phone TN conversion 48
Mapping 106
mean time between failures 399
Media Card 32 card 26
Media Card 32S card 26
Mute 108
MVC 2050 36, 38, 134, 144, 241, 255, 282

N

NAT 106, 108
NAT Keep Alive timeout setting 111
NAT Mapping Keep Alive 108
NAT Mapping Keep Alive Time-out setting 112
Network Address Translation 105
NT8D02 Digital Line Card
connector pin assignments 390
NT8D37 IPE Modules
cable connections 395
NT8D37BA IPE Modules 395
NT8D37EC IPE Modules 395
NT8D81BA cable 395
NTCW84JW special IPE filter 395

O

operational parameters 304
operational report 306

P

Package 365 230
port 5200 107
Private Zone 142
PRT ES1 112
PRT ES2 112
PRT ESS 112
PRT ZONE 228
PRT ZONE ALL 228
PUBLIC RTCP port number 110
PWD1 288

Q

QoS 135
Quality of Service 135

R

reliability 399
Restore the IP Phone Application Server database 212

S

Security Device is missing 379
Software Deployment Packages 194
superloop 30

Copyright © 2010 Nortel Networks. All Rights Reserved.

T

temperature specifications 400
Temporary IP User License 31
Traffic printouts 135

U

Unicode support 39
unrecoverable hardware failure 379
Upgrade Signaling Server software 208

V

Virtual Office 144
virtual superloop 30, 230
virtual Superloop in Element Manager 231
Virtual Superloops 230
virtual superloops for IP Phones 230
VLAN ID 110
VLANs 110
Voice Gateway Media Card 26
VTNs 30

W

WLAN Handset 2210 31, 36
WLAN Handset 2210/2211/2212 145
WLAN Handset 2211 31, 36
WLAN Handset 2212 31, 36
WLAN Handset 6120 31, 36
WLAN Handset 6140 31, 36

Copyright © 2010 Nortel Networks. All Rights Reserved.

Copyright © 2010 Nortel Networks. All Rights Reserved.

Nortel Communication Server 1000

Signaling Server IP Line Applications Fundamentals

Release: 6.0
Publication: NN43001-125
Document revision: 01.04
Document release date: 19 February 2010

Copyright © 2010 Nortel Networks. All Rights Reserved.

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

Nortel, Nortel Networks, the Nortel logo, and the Globemark are trademarks of Nortel Networks.

All other trademarks are the property of their respective owners.

To provide feedback or to report a problem in this document, go to www.nortel.com/documentfeedback.

www.nortel.com

