297-5231-021

DMS-100 Family

Centrex IP

Service Implementation Guide

CIPL0001 Standard 02.07 October 2000

NORTEL NETWORKS™

DMS-100 Family

Centrex IP

Service Implementation Guide

Publication number: 297-5231-021
Product release: CIPL0001
Document release: Standard 02.07
Date: October 2000

United States of America

NORTEL NETWORKS CONFIDENTIAL: The information contained herein is the property of Nortel Networks and is strictly confidential. Except as expressly authorized in writing by Nortel Networks, the holder shall keep all information contained herein confidential, shall disclose the information only to its employees with a need to know, and shall protect the information, in whole or in part, from disclosure and dissemination to third parties with the same degree of care it uses to protect its own confidential information, but with no less than reasonable care. Except as expressly authorized in writing by Nortel Networks, the holder is granted no rights to use the information contained herein.

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

Publication history

October 2000

Standard, release 02.07. The following changes were made in this release:

- deleted MADN PDN information from the “DMS maintenance” chapter
- clarified the SNMP values for the PTM port and the Microsoft port in the “Gatekeeper” and “Packet Telephony Manager” chapters.
- revised information about i2004 port usage with regards to TFTP in the “System engineering” chapter
- revised NAT intraswitching information in the “System engineering” chapter
- added power requirements to the “Gateway” chapter
- added technical specifications to the “Gatekeeper” chapter

August 2000

Standard, release 02.06. The following changes were made in this release:

- revised the “Gateway” chapter in accordance with BTAC findings
- added UFTP information to the “DHCP and load servers” chapter
- added NAT information to the “System engineering” chapter
- added limitations and restrictions for options NO WAIT and ALL to the “DMS Maintenance” chapter
- revised figures in the “Terminal Proxy Server” chapter
- added “Appendix B: Changing the vocoder”

June 2000

Standard, release 02.05. The following changes were made in this release:

- revised QPIN limitations and restrictions in the “DMS Maintenance” chapter
- added the “Terminal Proxy Server” chapter

May 2000

Standard, release 02.04. The following changes were made in this release:

- added i2004 and TPS troubleshooting information to the “Troubleshooting” chapter
- added additional Gatekeeper security engineering rules to the “System engineering” chapter
- added provisioning information for the i2004 phone to the “DMS maintenance” chapter

April 2000

Standard, release 02.03. The following changes were made in this release:

- removed installation procedures that are now documented in either the *Centrex IP Upgrade Guide*, 297-5231-590, or the *3rd Party Integrator Preconfiguration Guide*, Installation Method 26-0332
- added troubleshooting information for Gatekeeper alarms, traps, and logs in the “Troubleshooting” chapter
- added the DHCP server configuration procedure for the DHCP server serving the i2004 telephones in the “DHCP and load servers” chapter
- added a list of trap explanations and Release Call limitations to the “Packet Telephony Manager” chapter

March 2000

Standard, release 02.02. The following changes were made in this release:

- incorporated all designated chapters in accordance with BTAC findings
- enhanced List of terms chapter
- incorporated editorial comments
- incorporated design review comments

February 2000

Preliminary, release 02.01. The following changes were made in this release:

- revised all chapters for Release 2 content
- added chapters “CO LAN and CO LAN edge device” and “Logs”

October 1999

Standard, release 01.03. The following changes were made in this release:

- incorporated review comments in “Gateway,” “Gatekeeper,” “System engineering,” “DMS maintenance,” and “Card replacement” chapters
- incorporated editorial comments in all chapters
- added FTP information to the “DHCP and FTP load server” chapter

September 1999

Preliminary, release 01.02. The following changes were made in this release:

- incorporated review comments in “Overview,” “Gateway,” and “Packet Telephony Manager” chapters
- revised “Gatekeeper” chapter to include additional and updated information
- added “System engineering” chapter

August 1999

Preliminary, release 01.01

Contents

Part III Planning and engineering III-1

Part IV Operations and maintenance IV-1

Figures

Tables

About this document

When to use this document

This document describes the technical requirements, functionality, and implementation guidelines for Release 2 of the Nortel Networks' Centrex IP product. This document covers the Centrex IP load CIPL0001, which requires the DMS-100 NA012 or NA013 software load and the NT7X07AA card in an ISDN line trunk controller (LTCI).

ATTENTION
This document is written for the DMS-100 market. For MSL-100 information, see Appendix A in this document.

How to use this document

Use this document to implement and support the Centrex IP network and its components. The following groups can use this document:

- Operating company personnel in network management centers, support centers and end offices
- Nortel personnel in support centers, engineering groups, and installation groups

This document consists of the following chapters:

- “Product overview” describes the Centrex IP central office and its components.
- “Gatekeeper” describes the operation of the Centrex IP Gatekeeper.
- “Gateway” describes the installation and operation of the Centrex IP Gateway card.
- “Packet Telephony Manager” describes how to manage the Centrex IP network and its components.
- “DHCP and load servers” describes the configuration and operation of the DHCP and load servers.

- “CO LAN and CO LAN edge device” describes the configuration and operation of the central office (CO) local area network (LAN).
- “System engineering” describes how to engineer the central office, access network, and enterprise network for acceptable quality of service.
- “DMS maintenance” describes the operation, administration, and maintenance functions that the DMS-100 switch provides for Centrex IP.
- “Card replacement” describes the NT7X077AA card replacement procedure.
- “Logs” describes the Centrex IP logs for the Gateway card.
- “Terminal Proxy Server” describes the terminal proxy server (TPS) software application and the TPS Config Tool.
- “Troubleshooting” describes some of the common troubleshooting procedures for the Gateway and the Gatekeeper.
- “Appendix A, MSL100 Internet Protocol” describes the application of Centrex IP on the MSL100 switch.

How to check the version and issue of this document

The version and issue of the document are indicated by numbers, for example, 01.01.

The first two digits indicate the version. The version number increases each time the document is updated to support a new software release. For example, the first release of a document is 01.01. In the *next* software release cycle, the first release of the same document is 02.01.

The second two digits indicate the issue. The issue number increases each time the document is revised but rereleased in the *same* software release cycle. For example, the second release of a document in the same software release cycle is 01.02.

To determine which version of this document applies to the software in your office and how documentation for your product is organized, check the release information in *Product Documentation Directory*, 297-8991-001.

References in this document

This section lists the documents that are referred in this document.

Nortel Networks documents

This document refers to the Nortel Networks documents that follow:

- Installation Method 26-0325, *Gatekeeper Installation and Configuration for Centrex IP*
- Installation Method 26-0332, *3rd party Integrator Preconfiguration Guide*

- Nortel Networks technical publication (NTP) *Card Replacement Procedures*, 297-8001-547
- NTP *DMS-100 Family Maintenance and Operations Manual*, 297-8991-500
- NTP *National ISDN BRI Service Implementation Guide*, 297-2401-201
- NTP *Log Reports Reference Manual*, 297-8001-840
- NTP *Product Documentation Directory*, 297-8991-001
- NTP *Translations Guide*, 297-8001-350
- NTP *SERVORD Reference Manual*, 297-8001-808
- Nortel Networks Engineering Change Memorandum (ECM) 590, Issue 05 and 06, *DMS-100 Family Traffic Tables*
- Nortel Networks ECM-497, Issue 13, *Simplified Traffic Provisioning*
- NTP *Centrex IP Upgrade Guide*, 297-5231-590

Other documents

This document refers to the other documents that follow:

- Alexander, Steve. *DHCP Options and BOOTP Vendor Extensions*, RFC 2132, Silicon Graphics, Inc., March 1997.
- Droms, R. *Dynamic Host Configuration Protocol*, RFC 2131, Bucknell University, March 1997.
- Sollins, Karen R. *The TFTP Protocol (Revision 2)*, RFC 1350, Massachusetts Institute of Technology Laboratory for Computer Science, July 1992.

What precautionary messages mean

The types of precautionary messages used in Nortel Networks documents include attention boxes and danger, warning, and caution messages.

An attention box identifies information that is necessary for the proper performance of a procedure or task or the correct interpretation of information or data. Danger, warning, and caution messages indicate possible risks.

Examples of the precautionary messages follow.

ATTENTION - Information needed to perform a task

ATTENTION

If the unused DS-3 ports are not deprovisioned before a DS-1/VT Mapper is installed, the DS-1 traffic will not be carried through the DS-1/VT Mapper, even though the DS-1/VT Mapper is properly provisioned.

DANGER - Possibility of personal injury

DANGER

Risk of electrocution

Do not open the front panel of the inverter unless fuses F1, F2, and F3 have been removed. The inverter contains high-voltage lines. Until the fuses are removed, the high-voltage lines are active, and you risk being electrocuted.

WARNING - Possibility of equipment damage

WARNING

Damage to the backplane connector pins

Align the card before seating it, to avoid bending the backplane connector pins. Use light thumb pressure to align the card with the connectors. Next, use the levers on the card to seat the card into the connectors.

CAUTION - Possibility of service interruption or degradation

CAUTION

Possible loss of service

Before continuing, confirm that you are removing the card from the inactive unit of the peripheral module. Subscriber service will be lost if you remove a card from the active unit.

How commands, parameters, and responses are represented

Commands, parameters, and responses in this document conform to the following conventions.

Input prompt (>)

An input prompt (>) indicates that the information that follows is a command:

```
>BSY
```

Commands and fixed parameters

Commands and fixed parameters that are entered at a MAP terminal are shown in uppercase letters:

```
>BSY CTRL
```

Variables

Variables are shown in lowercase letters:

```
>BSY CTRL ctrl_no
```

The letters or numbers that the variable represents must be entered. Each variable is explained in a list that follows the command string.

Responses

Responses correspond to the MAP display and are shown in a different type:

```
FP 3 Busy CTRL 0: Command request has been submitted.

FP 3 Busy CTRL 0: Command passed.
```

How measurements are described

The following table lists measurement abbreviations used in this document.

Table 1 Measurement abbreviations (Sheet 1 of 2)

Abbreviation	Description
Gbyte	gigabyte
Hz	hertz
kbit/s	kilobit per second
kbyte	kilobyte
kHz	kilohertz
Mbit/s	megabit per second
Mbyte	megabyte
MHz	megahertz
ms	milliseconds

Table 1 Measurement abbreviations (Sheet 2 of 2)

Abbreviation	Description
V	volt
V dc	volt dc

Part I Introduction

This part contains the “Product overview” chapter.

1 Product overview

Introduction

Centrex IP is an Internet Protocol (IP) telephony service that serves small and large businesses and the mobile work force. With the increase in data network usage, small and large businesses require high-performance data access technology for all their communications needs. Centrex IP integrates seamlessly with existing corporate networks to unify the delivery of voice and data over IP connections. It allows voice and data traffic to travel over a variety of carrier grade, cost-efficient packet networks. With Centrex IP, service providers can offer the same feature-rich capabilities of Centrex over an IP network, and still have the quality, security, and reliability of the public switched telephone network (PSTN). Business travelers and telecommuters can access the same business services they have in the office by using a dial-up connection.

Centrex IP uses two of Nortel Networks' most successful telecommunications services, Integrated Services Digital Network (ISDN) Basic Rate Interface (BRI) and Meridian Digital Centrex (MDC). MDC or Centrex is a robust, full-featured telecommunications service that has been serving the telecommunications needs of corporate enterprises for more than 20 years. Centrex IP uses the ISDN BRI call processing platform to deliver the DMS-100 Centrex features to the IP terminals.

Centrex IP benefits to users

Centrex IP coexists within current Centrex groups and can share dialing plans, line features, group features, and network access. This allows service providers to retain and grow their existing Centrex markets. Additional benefits to service providers are listed as follows:

- Leverages DMS-100 investment by extending DMS-100 Centrex onto the growing IP market
- Allows smooth migration of DMS-100 customers to managed IP networks
- Provides seamless integration with existing IP networks, eliminating network duplication
- Provides migration strategy to next generation data services

Centrex IP offers the following benefits to end users:

- Provides same features and benefits as DMS-100 Centrex
- Offers scalability in level of adopting new services
- Allows one network for voice and data, reducing network administration and expense
- Provides the platform for advanced services deployment while utilizing existing infrastructure
- Extends business communication services to the mobile work force

Packet switching versus circuit switching

Centrex IP uses packet switching to deliver voice over an IP network. In a packet-switched network, messages are divided into chunks of information called packets. Each packet contains a destination address that is used to route the packet. IP networks are considered *connectionless* because there is no established connection between the endpoints that are communicating. The individual packets for a given message may take different routes over the network. IP networks depend on the Transmission Control Protocol (TCP) to keep track of the packet sequence of a message. TCP is a connection protocol that puts the packets back in the proper order.

Some IP-based applications use User Datagram Protocol (UDP) instead of TCP. UDP uses IP to route packets, also called datagrams, across the network. UDP does not provide packet sequencing, but attempts to ensure that the packets arrive in the right order. Applications that exchange relatively small units of data use UDP to save processing time.

Circuit-switched networks differ from packet-switched networks in that a physical path is obtained and dedicated for the duration of a connection between endpoints. The dedicated connection makes resources unavailable to other users. The following table compares the features of a packet-switched network with those of a circuit-switched network.

Table 1-1 Network comparison (Sheet 1 of 2)

Packet-switched network	Circuit-switched network
Virtual line card	NTBX27 line card
Ethernet connection or coaxial cable	Copper twisted pair
Shared bandwidth	Dedicated bandwidth
No distance limitation	Maximum distance of 18k ft per loop

Table 1-1 Network comparison (Sheet 2 of 2)

Packet-switched network	Circuit-switched network
Q.931 and H.225 call control signaling	Q.931 call control signaling
Converts voice to IP packets	Converts voice to 64 kbit/s time division multiplex (TDM)

H.323 standard

The Centrex IP system components are based on a proprietary version of the International Telecommunications Union (ITU) Recommendation H.323. This recommendation provides standards for protocols used in packet-based multimedia communications systems. Compliance to the H.323 standard ensures multimedia products and applications from different vendors are compatible with each other. This section introduces some of the concepts and terms associated with the H.323 standard.

The H.323 standard defines four major components for a communications network:

- gatekeepers
- gateways
- terminals
- multipoint control units (MCU)

Note: Centrex IP does not contain MCUs.

The functions of the H.323 components are defined in the following sections.

H.323 gatekeeper

A gatekeeper performs call control functions and zone management. The collection of H.323 components that are managed by a single gatekeeper is referred to as the H.323 zone. The required functions that the gatekeeper performs for the terminals and gateways that have registered within its zone are as follows:

- address translation
- admissions control
- bandwidth control
- zone management

In addition, a gatekeeper can have the following optional functions:

- call control signaling
- call authorization

- bandwidth management
- call management

H.323 gateway

A gateway functions as an interface between two networks. If there is only one network, a gateway is not required. The gateways and terminals on the network are called endpoints in an H.323 system. An endpoint is a device that can initiate and receive calls. Two endpoints (terminals) can communicate directly with each other if they are on the same local area network (LAN). The gateway allows a terminal on a LAN to connect with a terminal on another LAN.

In addition, a gateway performs translations between the H.245 and Q.931 protocols used by the terminals. This allows the terminals on an Ethernet LAN and the terminals on the PSTN to talk to each other. The actual number of H.323 terminals that can communicate through a gateway is not defined in the H.323 standard. This, and other gateway functions, can be designed by the manufacturer.

H.323 terminal

A terminal is a device that allows real-time, two-way voice communication over a LAN. Terminals usually consist of PC-based telephony software or stand-alone IP-based phones. The H.323 standard specifies the requirements for audio, video, and data to operate on H.323 terminals. Video and data functionality is optional, but audio conferencing is required. All H.323 terminals must support H.245, which is a protocol used to negotiate channel usage. In addition, H.323 terminals must support the following protocols:

- Q.931 for call signaling and call setup
- H.225 protocol to communicate with the Gatekeeper
- real-time protocol/real-time control protocol (RTP/RTCP) for audio and video signal management

Multipoint control unit

The MCU is a device that allows three or more endpoints to have an audio or video conference.

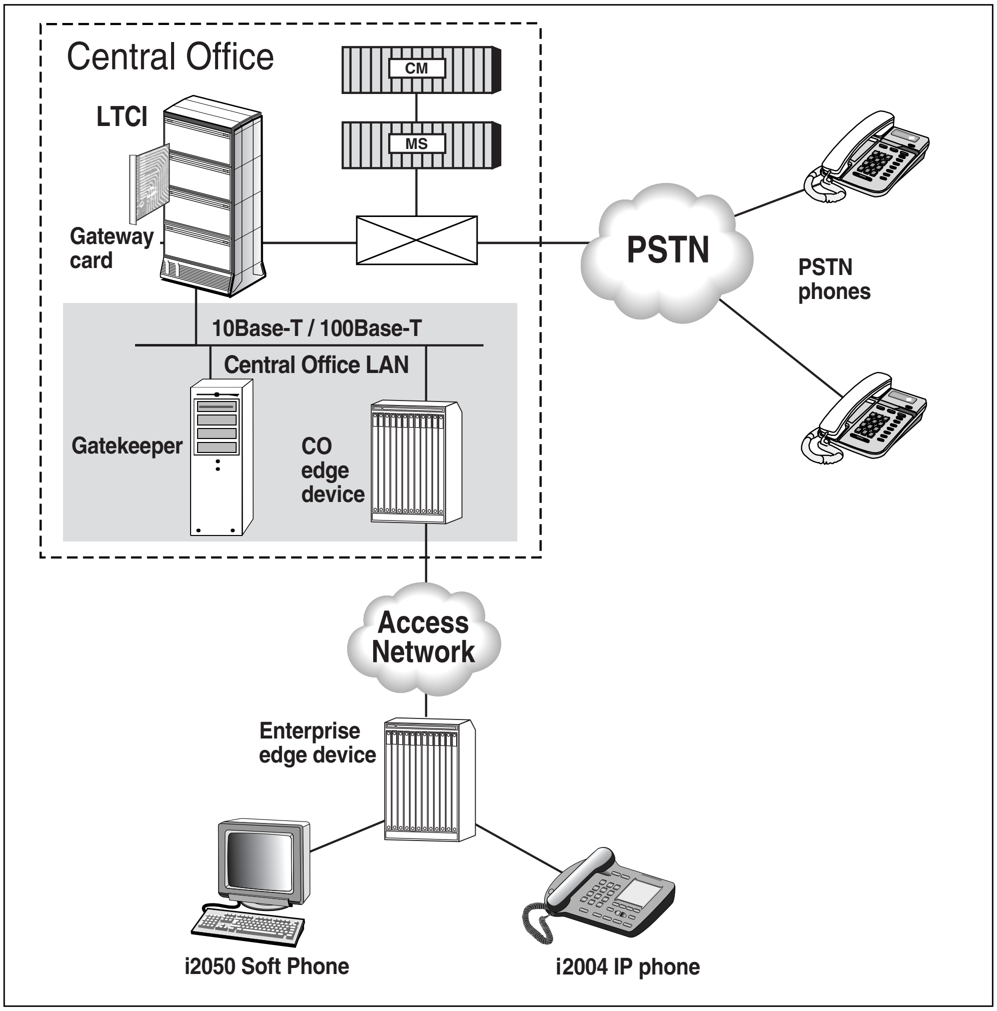
Codecs

A codec is a type of voice compression protocol. The H.323 standard uses several codecs, which use different voice compression algorithms. All H.323 endpoints must support the G.711 codec for voice compression. The other codecs are optional. The G.711 codec delivers toll quality speech at 56 or 64 kbit/s. This is the best codec for speech quality; however, it also requires the largest bandwidth. The G.711 codec was designed originally for continuous bit-rate networks. The G.723.1 and G.729A codecs operate at lower bit rates and are also predominant audio codecs in H.323-based systems.

Centrex IP components

The Centrex IP system components are shown in the following figure.

Figure 1-1 Centrex IP network diagram



The Centrex IP system has the following basic components:

- the IP-ready ISDN line trunk controller (LTCI)
- the integrated IP Gateway card in the LTCI
- a Gatekeeper that resides in the central office
- the Packet Telephony Manager
- the dynamic host configuration protocol (DHCP) servers, file transfer protocol (FTP) server, and trivial file transfer protocol (TFTP) server

- a central office (CO) LAN
- the i2004 and i2050 terminals on the customer LAN
- the Terminal Proxy Server (TPS)

The Centrex IP components are described in the sections that follow.

IP-ready LTCI

The IP-ready LTCI (NT6X01AF) is an XMS-based peripheral module (XPM) that has been enhanced to integrate the IP Gateway card as an IP interface. In addition to a new shelf and backplane, 16 pins are added to the backplane for each slot that accommodates the Gateway card. A backplane-to-bulkhead cable assembly and bulkhead personality plate accommodate the additional cables that connect the LTCI to the edge device on the LAN. The IP-ready LTCI supports the following DMS services:

- voice features
- directory number (DN) provisioning and billing
- static data download
- operations, administration, and maintenance (OAM)

Gateway card

The IP Gateway card (NT7X07AA) is an XPM circuit pack that resides in the P-side interface slots of an IP-ready LTCI. The Gateway card provides the primary interface between the PSTN and the IP terminals on the Ethernet LAN. The Gateway card also converts the voice data from the IP terminals to TDM voice data for the PSTN.

Gatekeeper

The Gatekeeper is the central call processing server of the Centrex IP network. It is a dual configuration PC and application that runs on a Windows NT platform. The Gatekeeper provides registration and admission control to the H.323-based terminals.

The Gatekeeper provides the following services:

- address translation—translates a DN to its transport address (IP and TCP port number)
- admissions control—allows or denies a terminal request to access the packet telephony network
- zone management—provides address translation and admission control for terminals and Gateways that have registered with the Gatekeeper

- call signaling—sends the calling party number in the setup message to the Gateway; forwards the rest of the call signaling messages to the terminals
- authentication—blocks calls from unauthorized users

Packet Telephony Manager

The Packet Telephony Manager (PTM) is a web-based subnetwork management system that allows you to remotely manage the Centrex IP components. In Release 2, the PTM manages the Gatekeeper, the Gateway, and the TPS. The PTM also provides information on terminals assigned to the Gatekeepers.

DHCP and FTP load server

The DHCP server runs on the Gatekeeper and provides configuration information to the Gateway cards. The FTP server runs on the same machine as the DHCP server and supplies the software load to the Gateway card.

CO LAN and CO LAN edge device

The CO LAN is an Ethernet device that connects the Gateway cards in the LTCI to the CO LAN edge device. The CO LAN can provide an Ethernet connection to the Gatekeeper.

The CO LAN edge device provides a WAN connection from the CO LAN through the access network to the enterprise network. The CO LAN edge device can be a router or data switch.

The CO LAN and the CO LAN edge device can reside within the CO or outside the CO. However, standard restrictions on Ethernet reach apply to all connections.

i2004 Internet Telephone

The i2004 Internet Telephone is Nortel Networks’ first offering in a family of IP-based telephone sets. This product family focuses on the integration of voice and data at the desktop in the local and wide area network environments. The i2004 telephone has embedded voice coding algorithms, called vocoders, for digitizing and compressing speech signals and provides excellent voice quality.

The i2004 telephone requires network intelligence to provide telephony and features to the end user. The i2004 telephone uses the Unified Network IP Stimulus (UNISTIM) protocol to communicate with the TPS. The TPS translates the stimulus messages and transmits them to the Gatekeeper and the Gateway for call processing.

The i2004 telephone has a familiar telephony dialpad plus a liquid crystal display (LCD) user interface for text and icon information. The i2004 user interface documentation is supplied with the i2004 equipment.

Terminal proxy server

The TPS is a mandatory component in the network whenever the i2004 telephone is present. The TPS software resides on the Gatekeeper. Its function is to perform call control services for the i2004 telephone. The TPS processes the stimulus messages received when the user presses a hard key or selects a softkey from the display. It then converts the stimulus messages to the appropriate signaling to access network services from the Gatekeeper. The TPS processes some of the stimulus messages locally to provide a set of specific i2004 services, such as the softkey options.

The TPS database stores the configuration data of the i2004 phones, such as the DNs assigned to the phones, the key assignments for voice features, and the IP address of the Gatekeeper. The TPS performs the following functions for the i2004 phone:

- makes call setup requests to the Gatekeeper
- processes and transmits Gatekeeper messages to the i2004 phone
- performs admission signaling for the i2004 phone
- performs call control signaling for the i2004 phone
- maintains the call state and the user interface

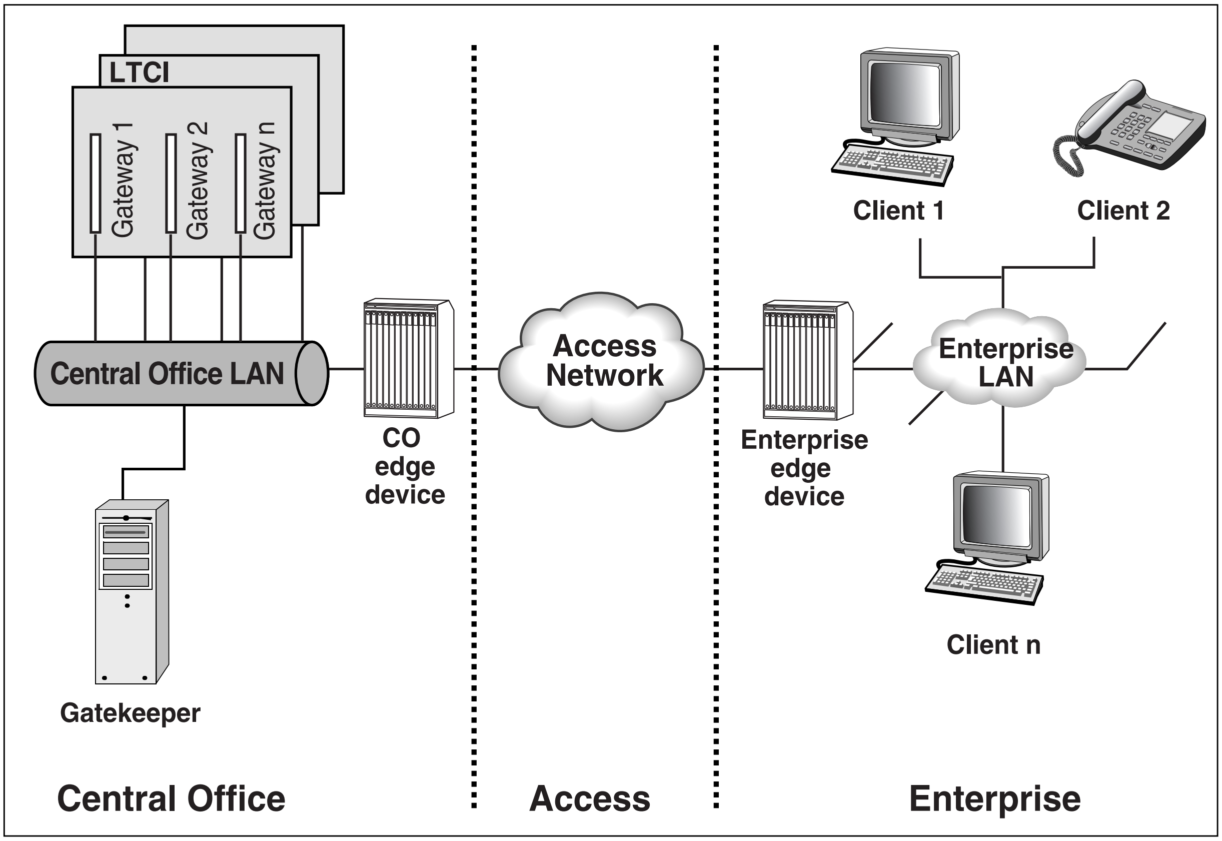
i2050 Soft Phone

The i2050 Soft Phone client is a PC telephony application that runs on the Windows 2000 operating system. The Soft Phone provides a graphical user interface (GUI) that allows users to originate and terminate calls to the PSTN from a multimedia PC. The Soft Phone, like the i2004 Internet Telephone, is directed by the TPS. The features implemented in the TPS are downloaded to the i2050 Soft Phone. The Soft Phone is available with a post-GA release of Centrex IP.

The Centrex IP network

The Centrex IP network consists of the CO LAN, the access network, and the enterprise network. These three networks work together to deliver Centrex IP to the end-user. The figure that follows shows a high-level view of the three networks and how they are connected.

Figure 1-2 Centrex IP network



Central office network

The Centrex IP CO must contain the following:

- IP-ready LTCI
- Gatekeeper
- CO LAN

The DHCP server, FTP server, and PTM may exist outside the CO.

Access network

The access network provides connectivity between the Centrex IP CO LAN and an enterprise network. The access network is also referred to as the transport network or a wide-area network (WAN) because it consists mainly of the transmission facilities that connect two LANs over a geographical area. Network topologies can include the following:

- point-to-point connections, such as T1 links
- a virtual private network (VPN)
- a public data network (PDN)

> ***Note:*** The Centrex IP system does not require a particular access network implementation, but certain performance and bandwidth requirements must be met in order to provide acceptable quality of service.

Enterprise network

The enterprise network is the private data network on the customer premises. The components for this network are as follows:

- the enterprise LAN, usually an Ethernet LAN configuration, with routing connectivity to the access network

  > ***Note:*** The Centrex IP system does not require a particular enterprise LAN implementation, but certain performance parameters must be met to ensure acceptable quality of service.

- i2050 Soft Phone clients and/or i2004 telephones
- an edge device, for connectivity and traffic control between networks
- an optional DHCP server for dynamic configuration of an i2004 terminal

ISDN base service

Centrex IP requires two software loads, the LAN software load CIPL0001, and the DMS software load CIP00001, which includes the ISDN basic call processing functionality and the Centrex features. Centrex IP terminals appear to the DMS switch as BRI terminals and are provisioned using the standard BRI Service Order System (SERVORD).

ISDN base service uses logical terminal identifiers (LTID) to provision the BRI terminals. Centrex IP also uses LTIDs to uniquely identify the service profile of each terminal. LTID parameters identify the terminal, its associated features, and the type of service it provides. These are the first parameters defined for the base service capability. Defining LTID parameters for base service involves entering data for logical terminal group names in table LTGRP, and defining individual terminals in table LTDEF using SERVORD.

The following tables require datafill to create service profiles on Centrex IP terminals. Tables with an asterisk (*) are automatically datafilled using SERVORD.

- LTGRP—defines the LTID group
- LTDEF—defines the LTID
- KSETINV*—defines the number of feature activators on an LTID
- KSETLINE*—defines the DNs for keys on an LTID
- KSETFEAT*—defines the feature keys
- LTMAP*—maps the LTID to a line equipment number (LEN)

A detailed description of the SERVORD commands used to build an LTID can be found in the “SERVORD procedures” chapter of the *National ISDN BRI Service Implementation Guide*, 297-2401-201. For more information about SERVORD commands, see the *SERVORD Reference Manual*, 297-8001-808.

In addition, Centrex IP requires the following tables to define the hardware interface profiles:

- LTCINV—defines the LTCI
- LTCPSINV—defines the P-side links on the LTCI
- IPINV—defines the Gateway node
- LNINV—defines the LEN

Centrex voice features

Centrex IP offers most of the high priority Centrex voice features. These features function essentially like the DMS Centrex features with some possible variations. See the *SERVORD Reference Manual* for a description of how to assign these options using SERVORD.

Station features

The Centrex IP feature offering for Release 2 includes the following:

- Automatic Call Back (ACB)
- Automatic Line (AUL)
- Automatic Line and MADN (AUL)
- Automatic Recall (AR)
- BRI in RES (SLBRI)
- Call Forward Busy (CFB)
- Call Forward Busy Unrestricted (CBU)
- Call Forward Don’t Answer (CFD)
- Call Forward Don’t Answer Unrestricted (CDU)
- Call Forward Don’t Answer Validation Timer (CFVDT)
- Call Forward Optional Call Forward Links
- Call Forward Time Busy (CFTB)
- Call Forward Time Don’t Answer (CFTD)
- Call Forwarding Fixed (CFF)
- Call Forward Universal (CFU)
- Call Hold (HLD)
- Call Park (PRK)

- Call Pickup (CPU)
- Calling Identity Delivery (CIDSDLV)
- Calling Identity Suppression (CIDSSUP)
- Calling Line Identification (CLI)
- Calling Name Delivery
- Calling Number Delivery (CND)
- Control Multiple Call Forwards (CMCF)
- Customer Data Change Enhancement for ISDN (CDC)
- Customer-Dialed Account Recording
- Customer-Originated Trace (COT)
- Denied Incoming (DIN)
- Denied Termination (DTM)
- Deny Call Forward Busy of External Calls (CBE)
- Deny Call Forward Busy of Intragroup Calls (CBI)
- Deny Call Forward Don’t Answer of Incoming Calls (CDE)
- Deny Call Forward Don’t Answer of Intragroup Calls (CDI)
- Directory Number Hunt (DNH)
- Distributed Line Hunt (DLH)
- Do Not Disturb (DND)
- Electronic Key Telephone Set (EKTS) Key Short Hunt (KSH)
- EKTS Multiple Appearance Directory Number-Single Call Arrangement (MADN-SCA)
- EKTS Secondary MADN Member Call Forward Programming (CFMDN)
- Feature Code Access
- Feature Group (FTRCRP)
- Feature Key Template (FTRKEYS)
- Flex Call Interworking with Attendant Console
- Flex Call Transfer to Uniform Call Distribution (UCD)
- Flexible Calling Conference Drop (DROP)
- Flexible Calling 6/30 Port Conferencing (FC)
- Free Number Terminating (FNT)
- Individual Business Line

- IntraLATA Primary Interexchange Carrier (LPIC)
- ISDN Call Forwarding Uniformity (CFXDNCT)
- ISDN Calling Name/Number Privacy
- ISDN TCAP Name Delivery (CNAMD)
- Keyset Music on Hold (KSMOH)
- Last Number Redial (LNR)
- Last Number Redial Associated with Set (LNRA)
- Line Overflow to DN (LOD)
- Line Overflow to Route (LOR)
- Line Study (SDY)
- Make Busy Key (MBK)
- Make Set Busy (MSB)
- Make Set Busy Intragroup (MSBI)
- MDC Feature Activation Operational Measurements
- MDC Queuing Operational Measurements
- MDC Operational Measurements
- Meet-Me Conference
- Meet-Me Conference Large
- Message Waiting Indication (Lamp Only)
- Multiline Hunt
- Multiple Appearance Directory Number EKTS (MDN)
- Multiple Directory Numbers on an IP Terminal
- NI-2 Call Forwarding Processing
- Operational Measurements MDC Enhanced
- Preset Conference
- Preset Conference Large
- Private Business Line (PBL)
- Privacy Change Allowed (PCA)
- Reason Display (REASDSP)
- Release (RLS)
- Selective Call Acceptance (SCA)
- Selective Call Forwarding (SCF)

- Selective Call Rejection (SCRJ)
- Semi-Restricted Service Line (SL)
- Simultaneous Provisioning of FC3 and FC6
- Speed Calling Long (SCL)
- Speed Calling Short (SCS)
- Storing of 24 Dialed Digits
- Subscriber Line Usage (SLU)
- Suppress Name Display (SUPPRESS)
- Suspended Service
- Terminating Billing Option
- Time-of-Day Network Class-of-Service Routing
- Toll Essential
- Transfer of Non-Conference Related Call

Centrex group features

Centrex IP also supports Centrex group features. These features are not assigned to individual DNs, but are provisioned for the customer group. A customer group provides a common set of features to an enterprise customer. The Centrex IP group features for Release 2 are listed as follows:

- Access Feature Grouping
- Audio Table Expansion
- Automatic Message Accounting Test Call (AMATEST)
- Automatic Number Identification (ANI) Information in the Station Message Detail Recording (SMDR) Output
- Automatic Route Selection (ARS)
- Bellcore Automatic Message Accounting (AMA)
- Call Forward Exempt (DCF)
- Call Forward Validation (CFXVAL)
- Centrex Group Dial Plan
- Class 5 MDC Inward Wide Area Telephone Service (INWATS)
- Class 5 MDC Outward Wide Area Telephone Service (OUTWATS)
- Code Restrictions
- Customer Group Transparency
- Denied Origination

- Direct Inward Dialing (DID)
- Direct Inward System Access (DISA)
- Direct Outward Dialing (DOD)
- DISA Call Prompting Default Destination
- DISA Remove Authorization Code Timeout
- DISA Third Dial Tone
- Electronic Tandem Network (ETN)
- Enhanced MDC WATS
- Extension Dialing
- Fully Restriced Service
- Functional Signaling Access to MDC Features
- International Direct Distance Dialing (IDDD)
- ISDN Translation and Routing Compliance (TR-488)
- ISDN User Part and MDC Interworking
- ISUP BRI Interworking Enhancements (TR-444)
- MDC Outpulsing to POTS trunks
- MDC Primary Interexchange Carrier (PIC) using SERVORD
- Multicustomer Operation
- Multiline Variety Package Dial Plan
- Network Class of Service
- Provide Charge Number for Calling Number
- Random Conditional Routing
- Service Order Enhancements for BRI Functional Signaling
- Service Order System (SERVORD)
- Simplified Dialing
- Simplified Message-Desk Interface (SMDI)
- Station Message Detailed Recording (SMDR)
    - SMDR Derived from Bellcore AMA Records
    - SMDR Output Files for ISDN SMDR and AMA
    - Separate SMDR Output Files for Customer Group
- Special Billing Requirements
- Station-to-Station Calling

- Time-of-Day Routing
- Toll-Restricted Service
- Uniform Numbering-Plan Capability
- Unrestricted Service
- Variable Speed-Call Access Code
- Warm Line (WML)
- 800 Calling, Credit Card

Centrex IP system features

Release 2 of Centrex IP offers the following system-wide features:

- Security and authentication
- Failover
- LAN redundancy
- Quality of service
- Capacity
- Parameter downloading
- LAN-routed speech

Security and authentication

The edge device can provide firewall routing to ensure IP connections to the Centrex IP network are not made illegally. Firewall routing prohibits connections except to the Gatekeeper for call control signaling and to the associated Gateway card for speech connections. Firewall routing is an optional feature in Centrex IP.

The authentication capability also protects the network from unauthorized users on different subnets. During client registration, an encrypted key is sent to the Gatekeeper for authentication. The Gatekeeper unlocks the key and admits the client. Without authentication, the terminals cannot register with the Gatekeeper to process calls.

Failover

The reliability target for Centrex IP is 99.9%. This translates into approximately 8 hours of total downtime for each system yearly. To meet this objective, the Centrex IP LAN is configured with hardware redundancy. The Gatekeeper provides failover capability with a dual-processor configuration. If one processor fails, the failover capability transfers all Gatekeeper resource control to the standby node. Failover then restarts the Gatekeeper application in the standby node. The former standby node becomes the active node.

The Centrex IP Gatekeeper also preserves stable calls between endpoints during and after a failover interval. Failover gracefully terminates calls when one of the endpoints (parties) in the call goes on hook.

> ***Note:*** During Failover, in which the Gatekeeper switches activity from its main processor to its standby processor, transient calls do not survive.

CO LAN redundancy

The Ethernet links on the CO LAN switch are also configured for redundancy. The two Ethernet ports on the Gateway card are connected to two Ethernet modules in the LAN switch. The Gatekeeper also connects to the same switch modules with redundant links. If a cable, switch, or card failure occurs, all traffic is shifted over to the available link. Optionally, multiple WAN connections can be provisioned on the edge device to provide redundant routes from the CO to the enterprise.

Quality of service

The Centrex IP system offers near toll-grade voice quality. Centrex IP is designed to minimize conditions that affect voice quality on data networks, such as latency, jitter, and packet loss. Latency is the delay between speaking and being heard on an established call. Jitter is a condition that affects voice quality when there are variations in the arrival rates of voice packets. Packet loss refers to the voice packets that are sent by one party but not received by the other party. The Centrex IP system quality of service (QoS) targets are as follows:

- latency (less than 200 ms, one way)
- jitter (4 ms)
- packet loss (2% or less)
- dial tone delay (1000 ms)
- post dial delay (600 ms)
- blocking (1%)

Quality of service can be affected by many things external to the system itself, such as background traffic, file transfers, or any network activity that affects bandwidth.

Capacity

The Gatekeeper manages the call processing capacity of the H.323 zone. The call processing capacity of the Centrex IP Gatekeeper is as follows:

- supports up to 2000 users
- supports 3 calls each second (high-day busy-hour [HDBH] call volume)
- supports 400 maximum simultaneous calls

Parameter downloading

The Centrex IP system supports DMS parameter downloading to i2004 phones on the IP network.

To support BRI parameter downloading, the TPS acts as a BRI agent through the Gatekeeper and Gateway to the XPM. The Q.931 protocol messaging between the XPM and the Gateway and Gatekeeper passes the Q.931 messages to the TPS, and adds the user-user information element (UUIE).

For information on the use of the QPIN command, see the “DMS maintenance” chapter in this document.

LAN-routed speech

LAN-routed speech allows two IP clients to establish a direct speech path between each other on a CO LAN. A direct speech path eliminates the need for the IP clients to route speech calls through the DMS switch. A direct speech path has the following benefits:

- decreases latency in a client-to-client IP basic call. Latency can occur due to additional transcoding in the Gateway of each leg of the call, since each call half must pass through a digital signaling processor (DSP) in the Gateway
- conserves links between remote locations and the host for the speech path, because the speech path does not use the Gateway or the DMS switch

Call flow

In order to process a call in the LAN environment, the terminals and the Gateway must register with the Gatekeeper. The following sections describe a typical call processing scenario.

Gateway registration

The Gateway registers with the Gatekeeper during its initialization sequence, as follows:

- The Gateway receives its IP address and the load server’s IP address from the DHCP server.
- The Gateway downloads its software load from the load server.
- The Gateway initiates its boot and load sequence.
- A technician applies the return to service (RTS) or PMRESET command at the MAP display, which brings the Gateway card into service.

- The Gateway checks the status of the Gatekeeper. If the Gatekeeper is up, the Gateway sends an identification message to the Gatekeeper to register itself.
- The Gatekeeper stores the registration data in a mapping table used for call processing. The mapping table contains the terminal identifiers (TID) of all registered endpoints.

Static data download

When an end user orders Centrex IP service, a DN and service profile are stored in the DMS-100 switch. The DMS switch downloads the information as static data when the Gateway registers with the Gatekeeper. The Gateway forwards the static data to the Gatekeeper.

- At subscription, a DN is provisioned through SERVORD.
- The DN is assigned an LTID and mapped to a Gateway's TID instead of a LEN.
- The Gateway receives the static data when it registers with the Gatekeeper.
- Whenever the terminal data on a Gateway is changed, the DMS switch resends the static data.

Terminal registration

When an IP terminal registers with the Gatekeeper, the following occurs:

- The end user enters their directory number key (DNkey) into the i2004 phone. The i2004 phone checks the Gatekeeper's static data to verify that the terminal DN, node number, and terminal ID (TID) match the static data. If the static data matches, the terminal automatically registers with the Gatekeeper.
- The Gatekeeper updates the mapping table with the terminal's registration data. This information is necessary for the Gatekeeper to process calls between terminals.
- Terminal registration contains an encrypted key for authentication with the Gatekeeper. The Gatekeeper unlocks the key and admits the terminal. This protects the system from unauthorized users on different subnets.

Call setup

When an IP terminal user originates a call to the PSTN, the following occurs:

- The end user dials the destination phone number and the Gatekeeper receives an H.323 call request. A call set-up message goes through the Gatekeeper and checks to see if the user is registered.
- The Gatekeeper looks up the home gateway address and routes the call request using H.225, the call control signaling protocol.

- The Gateway converts the H.225 (IP) signal to a Q.931 (circuit switched) signal and sends the call request to the DMS-100 switch.
- The DMS switch routes the call as if the end user was using a local PSTN phone.

Call types

The call types and voice paths are described as follows.

IP to PSTN

When an IP terminal originates a call to a PSTN terminal, the following occurs:

- The call signaling path is routed through the Gatekeeper to the Gateway on the DMS switch for call and feature control.
- The voice path is established directly between the IP terminal and the Gateway.

IP to IP

When an IP terminal originates a call to another IP terminal, the following occurs:

- The call signaling path is routed through the Gatekeeper to the Gateway on the DMS switch for call and feature control.
- The voice path is established directly between the two terminals by way of the Gateway card.

System limitations and restrictions

The following restrictions apply to Release 2 of the Centrex IP system:

- The system is limited to 2000 users per Gatekeeper.
- The LTCIs supporting the Gateway cards must have the NTSX05AA processor card.
- Each Gateway card supports up to 128 terminal identifiers (TID) for offices with the NA012 software load. For offices with the NA013 load, a Gateway card supports up to 512 TIDs.
- The default codec for Centrex IP is G.729. All incoming and outgoing calls from a Centrex IP terminal use the G.729 codec. If the customer requires a different default codec, contact Nortel Networks for support.
- Silence suppression is not implemented for G.711 encoding.
- No voice service prioritization for the enterprise is implemented. The required quality of service is achieved through end-to-end bandwidth management.
- Active Centrex IP calls survive an XPM warm switch of activity (SWACT). However, calls in a transient state, such as ringing or dialing, are not guaranteed to survive.

Part II
Functional description

This part contains the following chapters:

- Gatekeeper
- Gateway
- Packet Telephony Manager
- DHCP and load servers
- CO LAN and CO LAN edge device

2 Gatekeeper

Overview

The Centrex IP Gatekeeper platform consists of a high-availability binary cluster PC with an external shared-disk array. The Gatekeeper software runs on a Windows NT operating system using the Microsoft Cluster Server (MSCS) and Compaq Proliant cluster software.

The Gatekeeper software handles call control functions for the H.323-based terminals and acts as a security mechanism in the network. The Gatekeeper software provides the following call-control functions:

- registration, admission, and status (RAS) messages— communicates with H.323-based endpoints
- admission control—allows or denies a terminal request to access the packet telephony network
- authentication—blocks calls from unauthorized terminals
- address translation—translates a directory number (DN) to its transport address (IP and transmission control protocol [TCP] port number)
- zone management—provides address translation and admission control for terminals and Gateways that have registered with the Gatekeeper
- call processing—uses provisioned data for call completion and signaling
- call preservation—preserves stable calls and gracefully terminates calls when one of the parties goes on hook

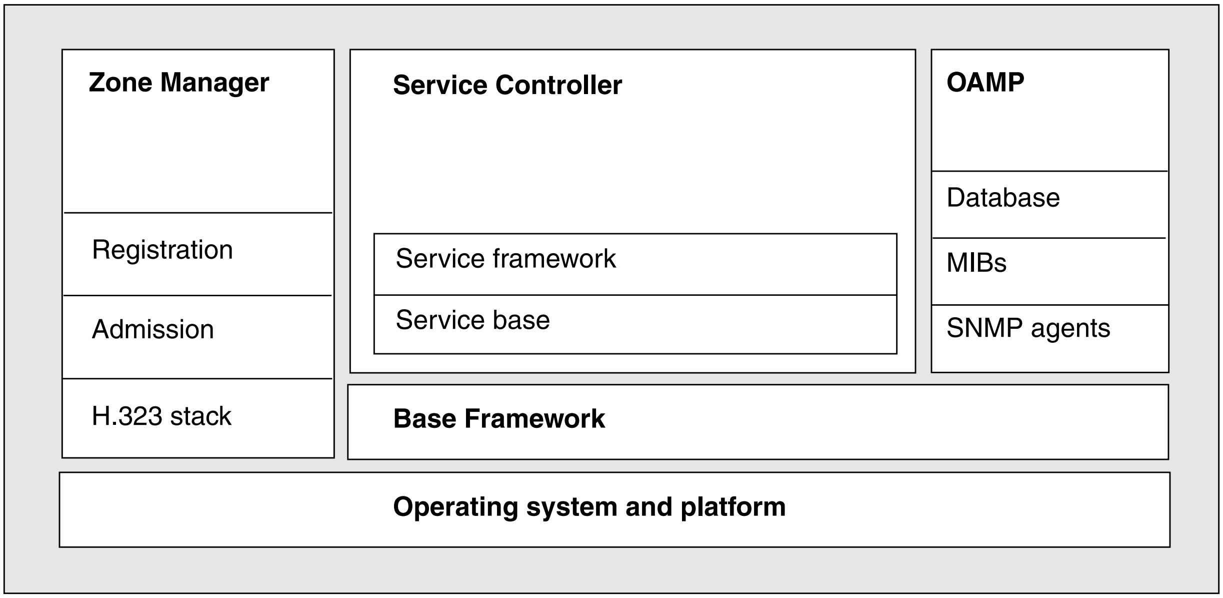
In addition to call-control functions, the Centrex IP Gatekeeper supports the following services:

- persistent database—stores terminal information downloaded from the DMS switch and registration information from the terminals
- element management interface—supports the interface to the Packet Telephony Manager (PTM)
- error, warning, and info logs—stores error information in a persistent manner; displays logs with a log viewer utility

Functionality

The following figure shows the functional layers of the Gatekeeper software.

Figure 2-1 Gatekeeper functional layers



Zone Manager

The Zone Manager is the interface for providing RAS message functions. RAS is a type of message protocol defined by the International Telecommunications Union (ITU) standard H.323. The RAS message protocol allows the Gatekeeper to communicate with the endpoints in a zone. A zone is defined as a group of H.323 entities that are managed by a single Gatekeeper. The Gatekeeper also uses RAS messages to perform bandwidth management and authentication under H.323.

The Zone Manager contains the H.323 stack from RAD Vision, which is based on the H.225 protocol. The H.225 protocol defines the call control messages in the H.323 standard. As Zone Manager, the Gatekeeper responds to various requests from endpoints using RAS messages.

The Zone Manager supports the following RAS messages:

- **Gatekeeper discovery** (GRQ, GCF, GRJ) is the process an endpoint uses to determine which Gatekeeper to register with. The Gatekeeper responds to a Gatekeeper Request (GRQ) message with a Gatekeeper Confirm (GCF) or a Gatekeeper Reject (GRJ). The Gatekeeper's response depends on whether or not the endpoint has been provisioned in the Gatekeeper.
- **Endpoint registration** (RRQ, RCF, RRJ) is the process by which an endpoint joins a zone and informs the Gatekeeper of its transport address and alias addresses. All endpoints register with the Gatekeeper identified

through the discovery process. The Gatekeeper responds to a Registration Request (RRQ) with a Registration Confirm (RCF) or a Registration Reject (RRJ). The Gatekeeper's response depends on whether or not the registration parameters are valid.

- **Endpoint Unregistration** (URQ, UCF, URJ) is the process by which the association between a terminal and a Gatekeeper is broken. The Unregistration Request (URQ) can be initiated either by the Gatekeeper or by the endpoint (terminal or Gateway). The Unregistration Confirm (UCF) response confirms the request and the Unregistration Reject (URJ) response rejects it.
- **Admission** (ARQ, ACF, ARJ) is the first step in setting up a call. The Gatekeeper allows admission with an Admissions Confirm (ACF) message or disallows admission with an Admission Reject (ARJ) message. Admission cannot be granted based on the following conditions:

  — if the required resource (for example, the Gateway) is not available

  — if the user is not authorized for network access
- **Gatekeeper Failover** (DRQ) occurs when the Gatekeeper restarts due to an irrecoverable application error or switches from its main processor to its standby processor. During and after a failover, the Gateway sends a Disengage Request (DRQ) message to the Gatekeeper. The Gatekeeper sends the DRQ message to the Terminal Proxy Server (TPS).

  Also during and after a failover interval, the i2004 telephone begins a call termination when the TPS sends a DRQ message to the Gatekeeper. The Gatekeeper returns a Disengage Confirmation (DCF) message to the TPS.

Authentication

RAS messages also handle the Authentication capability. Authentication uses an encryption and decryption algorithm to exchange RAS messages between the Gatekeeper and the terminals. Authentication protects the system from unauthorized users. The Authentication capability generates an encrypted key when the terminal registers with the Gatekeeper. Only the Gatekeeper can unlock the key to admit terminals into the zone for calling privileges. Authentication is required for successful transactions (registration and admission) within the H.323 zone. The Gatekeeper only performs authentication with registration (RRQ, RCF, RRJ) and admission (ARQ, ACF, ARJ) messages. The Gatekeeper does not perform authentication for components that are configured within the trusted network, such as the PTM, the Gateway, and the TPS.

Layer interactions

The Zone Manager interacts with the other functional layers. The Zone Manager uses the services of the operating system and the Base Framework. It uses the Windows Sockets (WinSock) to send RAS messages over the local area network (LAN). The Zone Manager collaborates with the Service

Controller and Operation, Administration, Maintenance, and Provisioning (OAMP) layers because these layers contain the objects required for registration and admission functions. For example, when registration is successful, an endpoint object is created that contains a reference to the endpoint profile in the OAMP database.

Service Controller

The Service Controller consists of the service framework and the service base. The service framework supports a number of service applications and protocols. An example is basic call service, which uses Q.931 protocol for call processing. The service framework inserts the terminal ID (TID) in messages going to the Gateway and routes the Q.931 messages. The service framework supports interaction with the installed base of distributed telephony services. The service base provides the run-time environment for service processing and manages the service processing resources.

OAMP

The OAMP layer handles the operation, administration, maintenance, and provisioning functions in the Gatekeeper. The OAMP layer provides access to a real-time database for persistent storage of terminal profiles and other provisioning data. The OAMP layer also contains the management information bases (MIB) and simple network management protocol (SNMP) agents for interfacing with the element management system for Centrex IP, the PTM.

Persistent data

Centrex IP provides the capability to preserve data after a failover or system restart. This capability is referred to as persistent data. The Gatekeeper maintains a proprietary database that functions as a persistence facility. This database contains the data the Gatekeeper receives from static data download, registrations, and authentication. The Failover capability uses the persistence facility to preserve endpoint and registration data across a Gatekeeper process or node failure. The standby node or restarted Gatekeeper process receives all the data from the persistence facility after a failover.

Static data download

The static data download mechanism is part of the OAMP layer. The Gateway sends static data download to the Gatekeeper to communicate which DNs correspond to associated TIDs. The Gatekeeper processes the static data and stores it in the database in a DN-to-TID mapping table.

The Gatekeeper uses the DN-to-TID mapping table during call setup. When the terminal registers to make a call, the Gatekeeper compares the terminal’s configured DN with the DN the Gateway sent in static data. If the Gatekeeper can match this information, the terminal can proceed with the call. If the Gatekeeper cannot match the information, the terminal is not allowed to register and does not receive dialtone.

> ***Note:*** See the chapter “Gateway” for additional information on static data download.

Gatekeeper alarms

The Gatekeeper sends SNMP notifications to the PTM’s Alarm Manager for tracking and clearing alarms. For a description of the Gatekeeper alarms and their causes, see the “Troubleshooting” chapter.

Base Framework

The Base Framework consists of a TCP connection server for handling TCP/IP connections and an object management framework for maintenance of system processes. These subsystems are used by the other functional layers.

Failover

To ensure 99.9% reliability, the Gatekeeper component provides a failover capability. The Failover capability preserves zone management dynamic data during a Gatekeeper process or computing node failure.

The more common type of failover is Gatekeeper failure. Gatekeeper failure can occur when the Gatekeeper exits under duress. The cluster service restarts the Gatekeeper on the same node.

If the cluster service on the standby node detects a fatal error on the active node, Failover transfers all Gatekeeper resource control to the standby node. It then restarts the Gatekeeper application in the standby node. The former standby node becomes the active node. The former active node becomes the standby node. This type of failover is called node failure.

The active node always controls the Gatekeeper resource group. Failover shuts down all resources in the active node and restarts them on the standby node. Resource group components have dependencies that can affect the shutdown and startup order of the resource group. Failover supports automatic failback (reversing the move) at the resource group level.

The resource group functions as a single entity. The Gatekeeper resource group contains the following items:

- Gatekeeper IP address
- Gatekeeper virtual server name

- Gatekeeper service
- Redundant array of inexpensive disks (RAID) array access

> ***Note:*** RAID is a storage device that uses two or more magnetic or optical disks. These disks operate together to increase performance and provide error recovery and fault tolerance.

Failover includes the following advantages over a manual reboot:

- Failover protects against a hardware failure, which prevents extended outages while waiting for a hardware diagnosis or replacement.
- Failover eliminates the delay associated with bringing down and restarting the operating system.
- Failover does not require manual intervention.

Call preservation

The Centrex IP Gatekeeper also preserves stable calls between endpoints during and after a failover interval. A failover interval is the length of time between the beginning of a Gatekeeper failover and when the Gatekeeper is again in operation. A stable call is a call that involves two talking parties. Therefore, during a Gatekeeper failover, the talking parties remain connected. The preserved calls do not respond to feature activations (such as, conferencing), but clear when either of the parties releases the call.

> ***Note:*** Failover does not preserve transient calls. A transient call refers to a call in the dialing or alerting state.

A media channel (that is, a call) exists between the Gateway and the Centrex IP system. A fatal fault (such as a hardware error) does not interrupt an established call. The Gatekeeper is unavailable briefly, but returns to service. Since the fatal fault breaks the TCP signaling channel between the Gatekeeper and the endpoints, RAS messaging completes call clearing.

The following paragraphs describe the RAS messaging sequences that occur when the Gateway and the i2004 telephone affect a preserved call.

Gateway terminates the call

During and after a failover interval, the Gateway sends a DRQ message to the Gatekeeper. The Gatekeeper sends the DRQ message to the TPS.

If a failover has occurred and the Gatekeeper is not available, the Gateway resends the request for 90 seconds. The Gateway stops sending the DRQ message if the Gatekeeper does not respond within the 90-second time limit.

When the Gatekeeper receives the DRQ message, it returns a DCF message to the Gateway and sends the DRQ message to the TPS. The TPS then sends a message to the i2004 telephone to terminate the call. The TPS returns a DCF message to the Gatekeeper.

The DRQ message from the Gateway contains the calling identifier and its endpoint identifier. To forward the DRQ message to the TPS, the Gatekeeper must identify the call signal transport address (CSTA) of the destination TPS. If the Gatekeeper receives a second DRQ message from the same endpoint, it does not send another DCF message.

i2004 telephone terminates the call

During and after a failover interval, the i2004 telephone begins a call termination when the TPS sends a DRQ message to the Gatekeeper. The Gatekeeper returns a DCF message to the TPS.

If a failover has occurred and the Gatekeeper is not available, the TPS resends the request for 90 seconds. The TPS stops sending the DRQ message if the Gatekeeper does not respond within the 90-second time limit.

When the Gatekeeper receives the DRQ message, it forwards it to the Gateway. The Gateway returns a DCF message to the Gatekeeper.

The DRQ message from the TPS contains the calling identifier and its endpoint identifier. To forward the DRQ message to the Gateway, the TPS must identify the CSTA of the destination Gatekeeper. If the Gatekeeper receives a second DRQ message from the same endpoint, it does not send another DCF.

Endpoint unregistration message

If an endpoint sends a URQ message to the Gatekeeper during a failover, the endpoint resends the request for the next 90 seconds. When the Gatekeeper receives the URQ message, it sends DRQ messages to all endpoints involved in a call with the endpoint that originated the URQ.

The Gatekeeper considers a URQ message to be an implicit DRQ message for each active call under the following conditions:

- when it has received the message from an endpoint with active calls
- the signaling channel runs through the Gatekeeper

TPS failover limitations

The following failover limitations apply to the TPS:

- During a failover, if the user presses any key during the time it takes for the TPS to come back online (30 to 90 s), the call will drop. A key press initiates communication with the TPS, but during the takeover interval, the TPS is unavailable.
- After the TPS fails over to the standby node, if the user presses any key to invoke a feature (such as “Confer”), the key press will result in the phone

producing a beep (indicating the keypress was denied). The call will stay up but the feature will not work for that call.

- A TPS reset means that the TPS application was terminated and then restarted. If a TPS reset occurs during an active call, the user cannot receive any new calls until the user releases the call.

Gateway sparing on the Gatekeeper

A Gateway takeover event occurs when a primary Gateway encounters a fault that forces the Gateway to transfer control to a secondary Gateway. A Gateway takeover does not change the IP address of other components in the Centrex IP network, including the Gatekeeper.

The occurrence of a Gateway takeover event affects the Gatekeeper in the following ways:

- A takeover event breaks the TCP signaling connections with the Gatekeeper. However, the Gatekeeper allows the affected calls to stay up.
- After a Gateway takeover on a call release from the public switched telephone network (PSTN), the Gateway sends the Gatekeeper a disengage request (DRQ) message. The Gatekeeper forwards the message to the other endpoints in the call.

  If the Gateway does not receive a reply from the Gatekeeper, the Gateway resends the request for 90 seconds. The Gateway stops sending the message if the Gatekeeper does not respond within the 90-second time limit. When the Gatekeeper receives the message, disconnect processing (including call clean-up) begins.

Hardware requirements

The Gatekeeper platform consists of the Compaq Proliant 19-inch, rack-mountable, high-availability PC, which runs the Windows NT Enterprise Server operating system. The Gatekeeper hardware requirements are listed in the following table.

Table 2-1 Gatekeeper hardware (Sheet 1 of 2)

Description	Quantity
Compaq Proliant Pentium III dual 550-MHz PC	2 base PCs
6/550 Pentium III 512k processor option kit	2
128 Meg SDRAM memory kit (512 Meg for each PC)	2
9.1 gigabytes wide Ultra-2 SCSI drive (9.1 redundant gigabytes for each PC)	8
Rack internal trackball keyboard	1

Table 2-1 Gatekeeper hardware (Sheet 2 of 2)

Description	Quantity
Dual 10/100 TX PCI network interface card (NIC)	2
Shared storage RAID controller	1
19-inch monitor	1
256 Meg SDRAM memory kit	2
Hot plug redundant power supply (2 for each PC)	4
100-foot CAT5 cable	4

The following section describes the Gatekeeper hardware configuration.

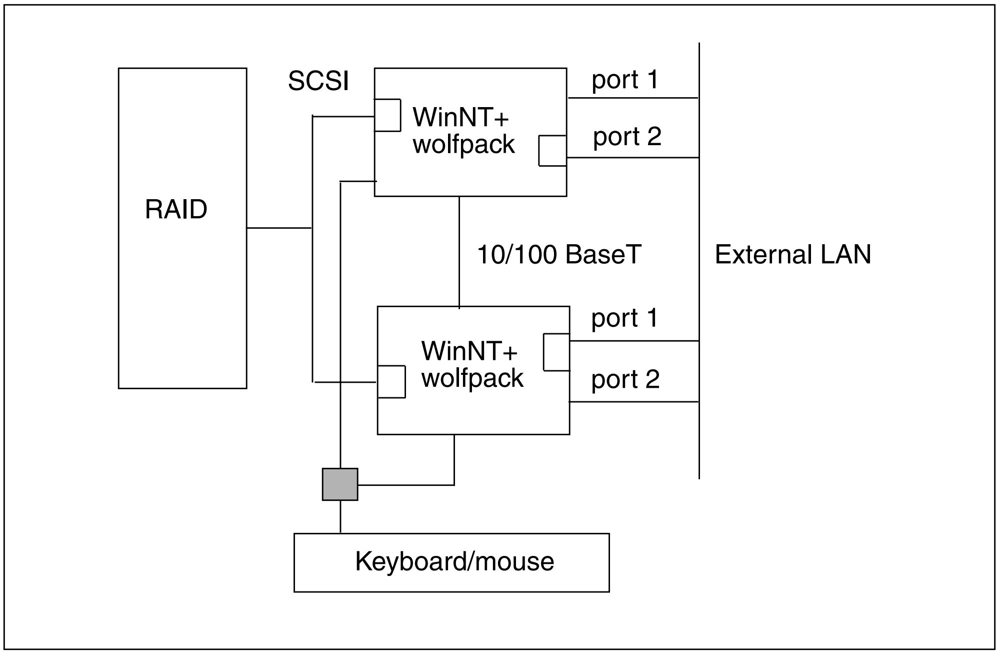
Cluster hardware configuration

The Gatekeeper hardware configuration is a binary cluster, also referred to as a wolfpack cluster. The two nodes of the cluster can function independently as separate computers. The cluster nodes cooperate to provide one or more virtual servers that offer high availability services to network clients. The cluster provides high availability by the ability of either physical server to host the virtual servers. The cluster also provides high availability because both physical servers can serially access a shared disk storage unit. To ensure uninterrupted intra-cluster communication, the cluster includes a private Ethernet connection between the two server machines.

> ***Note:*** Refer to Installation Method (IM) 26-0325, *Gatekeeper Installation and Configuration for Centrex IP*, for the Gatekeeper hardware installation procedure.

The following figure shows the hardware architecture for the wolfpack cluster.

Figure 2-2 Wolfpack cluster



The addition of the cluster software enables the Gatekeeper to display one IP address for all external clients. Clients use this IP address to exchange messages with the online node (primary Gatekeeper) of the cluster.

Use the following procedure to verify the physical configuration of the wolfpack cluster. This procedure is a visual inspection of the physical connections and components of the wolfpack cluster.

> *Note:* Power down all hardware before performing this procedure.

Procedure 2-1 Verify physical configuration

At the Gatekeeper cluster

1 Ensure that Gatekeeper node 1 is connected to the upper small computer system interface (SCSI) connector on the shared disk array.

2 Ensure that Gatekeeper node 2 is connected to the lower SCSI connector on the shared disk array.

3 Ensure that both Gatekeepers are attached to the video/mouse shared array box.

4 Ensure that the shared disk array has four hard drives installed.

5 Ensure that both Gatekeepers have two hard drives installed.

6 Ensure that both Gatekeepers have the cross-connect Ethernet cable plugged into the main board.

7 Ensure that both Gatekeepers have a LAN drop Ethernet cable plugged into port 1 of the dual network interface card (NIC).

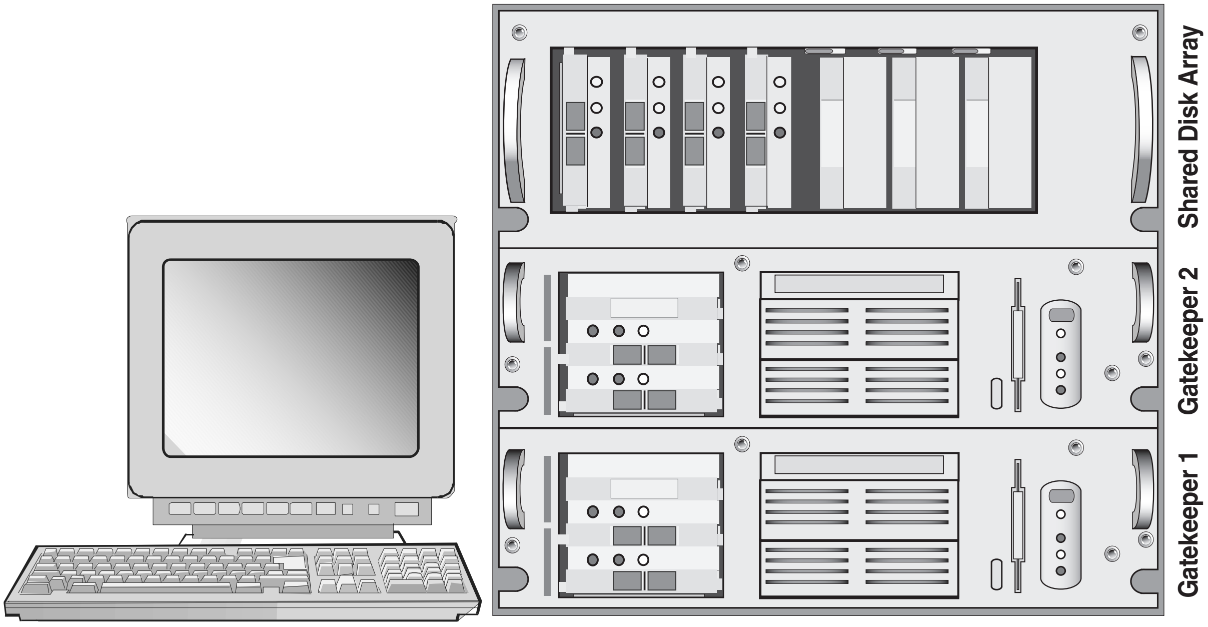
8 Turn on the Gatekeeper components in the following order:

  a Turn on the shared disk array.

  b Turn on Gatekeeper 1 and 2.

The following figure shows the Gatekeeper PCs with a shared disk array.

Figure 2-3 Dual Gatekeeper with disk array



Note: For Release 2, Gatekeeper 1 mounts above Gatekeeper 2.

Figure 2-4 shows the two nodes and the physical connections from the Gatekeeper to switch modules in the CO LAN.

Figure 2-4 Redundancy between Gatekeeper and switch modules

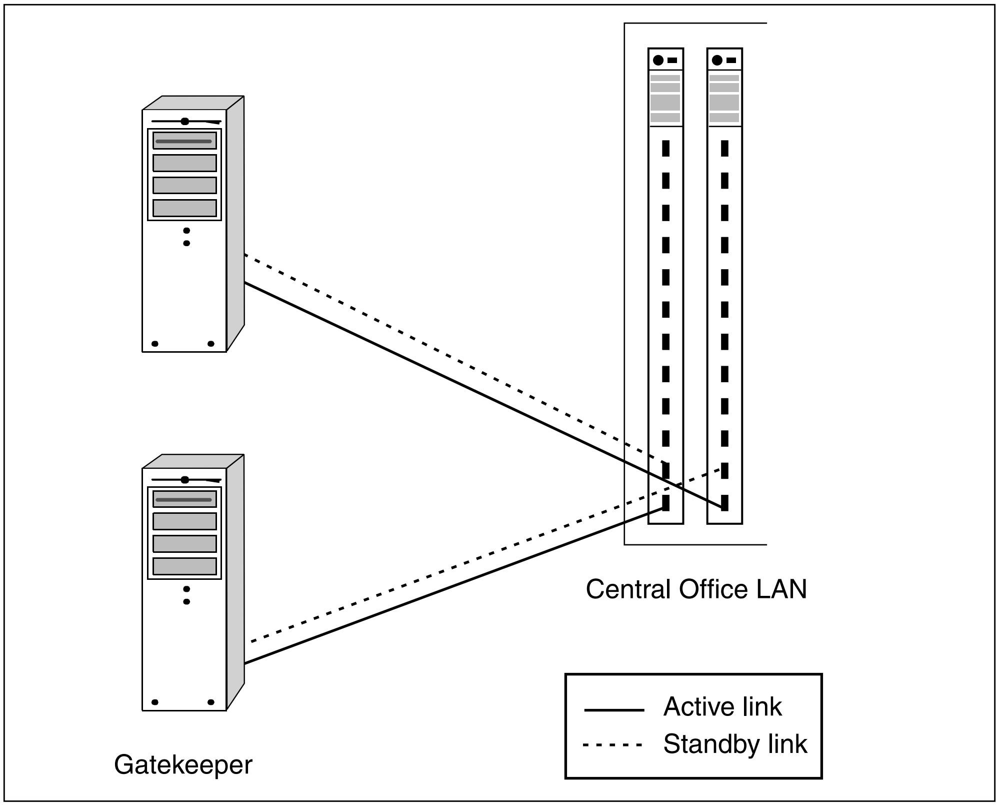


Table 2-2 lists the possible port assignments for this connection.

Table 2-2 Redundant port connections between Gatekeeper and switch modules

Gatekeeper	Switch modules
Gk1P1	Sw1P24
Gk1P2	Sw2P23
Gk2P1	Sw2P24
Gk2P2	Sw1P23

Software requirements

The following table lists the Gatekeeper platform and application software.

Table 2-3 Gatekeeper software

Description	Quantity
Windows NT 4.0 Server Enterprise Edition	2
Worldwide WNT SVR ENT 4.0 DOC kit	1
Additional Windows NT Server licenses	5
Microsoft Cluster Server 1.0	2
Compaq Insight Manager	1
Compaq Smartstart	1
Array Configuration Utility (ACU) with Smart Array Controllers Configuration Utility	1
WWf /Easy NT SVR ENT 4.0 SP6 w/boot CD	1
Sofpag SP12294	1
Timbuktu Pro	2
Gatekeeper load	2
TPS software	1
PTM software	2
NetID software	2

Note: Do not install Exceed software on the Gatekeeper. Exceed uses the same TCP/IP port as the Gatekeeper.

Cluster software

Use the following procedure to verify the cluster software configuration.

Procedure 2-2 Verify cluster software

At the Gatekeeper console

1 Check that the cluster software exists on each box.

Select Start->Control Panel->Services.

The Cluster Server program displays. The Status of the Cluster Server is "Started."

2 Open the Cluster Administrator program.

a Select Start->Programs->Administrative Tools->Cluster Administrator.

b Enter <cluster name> when prompted.

3 Check the network settings for the cluster. Select the cluster name and click the right mouse button. Select Properties.

4 Check the network settings against the IP addresses for the cross-connect and external LAN connections.

a Double-click on Network Neighborhood icon.

b Select Properties from the File Menu.

c Select the TCP/IP tab.

Note: If the network properties have changed or are inconsistent with the cluster network settings, the cluster software must be removed and reinstalled.

Cluster operation

Use this procedure to test the cluster's ability to move the Gatekeeper resource group from Gatekeeper 1 to Gatekeeper 2 or from Gatekeeper 2 to Gatekeeper 1.

> **CAUTION**
> **Loss of service**
> Do not perform this procedure when the Gatekeeper is in-service. This procedure will drop existing calls and cause a brief service outage.

Procedure 2-3 Verify cluster operation

At the Gatekeeper console

1 Start the Cluster Administrator utility on both Gatekeepers.

a Select Start->Programs->Administrative Tools->Cluster Administrator.

b When prompted, enter the cluster name.

2 Move the shared disk from Gatekeeper 1 to Gatekeeper 2 using the Cluster Administrator utility.

a Select DISK GROUP 1 (for Release 2) and click the right mouse button.

b Select Move group.

The Cluster Administrator freezes for approximately 1 minute.

The Cluster Administrator screen displays disk group 1 ownership for Gatekeeper 2. The status of all resources in the cluster group reads "Online."

3 Repeat the previous Cluster Administrator utility step, moving the shared disk from Gatekeeper 2 to Gatekeeper 1.

The Cluster Administrator freezes for approximately 1 minute.

The Cluster Administrator screen displays disk group 1 ownership for Gatekeeper 1. The status of all resources in the cluster group reads "Online."

Restart option for cluster

In a Gatekeeper cluster, an option in the cluster administration software can control restarts and switches of activity. If a node experiences a set number of restarts in a set period of time, activity automatically switches to the other node. The default number of restarts is three, and the default period of time is 15 minutes.

This cluster-level option can conflict with the actions available through the Remote maintenance menu. Use the following procedure to view the cluster-level option for restarts.

Procedure 2-4 View cluster-level option for restarts and switches of activity

At the Gatekeeper console

1 Under the Groups folder, select the Gatekeeper service.

2 Use the right mouse button to open the pop-up menu.

3 From the pop-up menu, select Properties.

4 Select the Advanced tab.

The Restart radio button turns the cluster-level restart option on or off.

The Affect the group field shows all the affected groups to be failed over to the other node.

The Threshold field shows the number of restarts that would trigger a switch of activity.

The Period field shows the period of time in seconds that the restarts would occur to trigger a switch of activity.

Installation

Before installing the Gatekeeper software, the system and cluster software must be installed and configured. Refer to Installation Method (IM) 26-0332, *3rd Party Integrator Preconfiguration Guide* and the *Centrex IP Upgrade Guide*, 297-5231-590, for complete Gatekeeper software installation procedures.

Pre-installation requirements

The user must have the following information for the Gatekeeper installation:

- Gatekeeper virtual and physical IP address
- Gatekeeper port number
- Packet Telephony Manager IP address
- SNMP port number

> ***Note:*** Ensure the SNMP values for the PTM port and the Microsoft port do not match. You must enter 161 for the PTM SNMP port. However, the Microsoft SNMP value for the Gatekeeper can be any unused port

number. The recommenced SNMP default value for the Gatekeeper is 8161.

The Gatekeeper application requires the following allocations for application memory:

- ~ 20 Mbyte RAM
- ~ 2.8 Mbyte program store
- ~ 1.2 Mbyte data store

Technical specifications

The table that follows shows the technical specifications for the Gatekeeper.

Table 2-4 Power, heating, and cooling requirements for Gatekeeper

Parameter	Sub-parameter	Specifications
Dimensions (HxWxD)	Rack form factor	17.35 x 17.50 X 22 in
	Tower form factor	19.75 x 17.50 x 22 in
Weight (two servers, one shared storage system, cabinet)		125
Input requirements	Range line voltage	115 VAC/230VAC
	Nominal line voltage	• 100 VAC • 120 VAC • 220 VAC • 240 VAC • 250 VAC
	Line frequency	50 to 60 Hz
	Input power	90 VAC/264 VAC
Heat	Operating	41^o to 122^oF/5^o to 50^oC
	Non-operating	-40^o to 185^oF/-40^o to 85^oC
Output power		225W
Temperature range	Operating	50^o to 93^oF/10^o to 35^oC
	Shipping	-22^o to 140^oF/-30^o to 60^oC
Relative humidity (non-condensing)	Operating	20% to 80%
	Non-operating	5% to 90%
Maximum wet bulb temperature		101.7^oF/38.7^oC
Acoustic noise	Idle (fixed disk drives spinning)	6.35 BELS/49.1 dBA
	Operating (random seeks to fixed disks)	6.43 BELS/49.8 dBA

Operation

The Gatekeeper application operates as described in the following sections.

Windows NT service

The Gatekeeper operates as a generic Windows NT service without a graphical user interface (GUI). A Windows NT service is an executable program that runs as a background task.

The use of the Gatekeeper as a generic Windows NT service with clustering software supplies the following advantages:

- Users can configure a Windows NT service to run under any user ID rather than just the user ID of the cluster administrator.
- Users can view and control the Gatekeeper service status both with the Cluster Administrator and the Windows NT Service Control Manager utilities.

Log viewer

The log viewer utility runs as a separate process from the Gatekeeper application. The log viewer continually displays the logs from the debug log file to a console window.

Gatekeeper application

Use the following procedure to start or stop the Gatekeeper application.

Procedure 2-5 Start the Gatekeeper application

At the Gatekeeper console

1 Open the Cluster Administrator program.

Select Start->Programs->Administrative Tools->Cluster Administrator.

2 Verify that CPC/S100 Group 1 (the Gatekeeper resource group) is online (that is, no red “X” exists next to its name).

> ***Note:*** If CPC/S100 Group 1 is not online, contact your next level of support for assistance.

3 Select CPC/S100 Group 1 in the left panel of the Cluster Administrator window. Check the right panel to determine which machine hosts the resources in the group.

4 Select the Gatekeeper Service resource listed in the right panel and click the right mouse button. Select “Bring Online” from the pull-down menu.

5 To stop the Gatekeeper program, select the Gatekeeper Service resource again and click the right mouse button. Select “Take Offline” from the pull-down menu.

Limitations and restrictions

The following limitations apply to the Gatekeeper:

- The Gatekeeper supports up to 2000 users.
- The Gatekeeper does not support bandwidth control messages.
- The Gatekeeper does not support status messages.
- A manual shutdown of the primary server may not result in failover to the standby server. Do not perform a manual shutdown of the primary server while the standby server is online.

The following are limitations for Release 1 of the Authentication capability:

- Authentication does not protect against the following security breaches:
  - — denial of service
  - — eavesdropping
  - — interference with call signaling
- The Gatekeeper does not perform authentication on DRQ messages.
- Authentication is not compliant with the H.235 protocol.

3 Gateway

Overview

The Centrex IP Gateway card (NT7X07AA) is an XPM circuit pack that resides in the DS-1 P-side interface slots of an ISDN line trunk controller (LTCI). The Gateway card integrates the call processing and voice functionality of the public switched telephone network (PSTN) with the internet protocol (IP) terminals on a local area network (LAN). The Gateway card allows ISDN Centrex features to be provisioned on the i2050 Soft Phone or the i2004 Internet Telephone. The Gateway card converts the IP voice data from the H.323 terminals to time division multiplexing (TDM) voice data for the PSTN.

The Gateway card's function as an H.323 interface to the Centrex IP network is based on the International Telecommunications Union (ITU) specification for gateways. The H.323 specification provides the industry standard for audio, video, and data communications across IP-based networks. Although the initial Centrex IP offering is IP-based, the Gateway card provides a generic packet network interface that supports Frame Relay and asynchronous transfer mode (ATM) networks in addition to IP networks.

The following list describes the functions of the Gateway in the Centrex IP network:

- supports H.225 registration, admission, and status (RAS) signaling to the Gatekeeper
- supports call setup and takedown on both the LAN side and the DMS side
- supports Q.931 call signaling
- supports circuit (TDM) to IP conversion
- provides call processing and voice features for H.323 clients
- provides transcoding between codecs
- provides 10/100Base-T connectivity to the central office (CO) LAN
- supports intraswitching - signaling routes through the DMS-100 switch, and speech routes through the IP.

Hardware and software

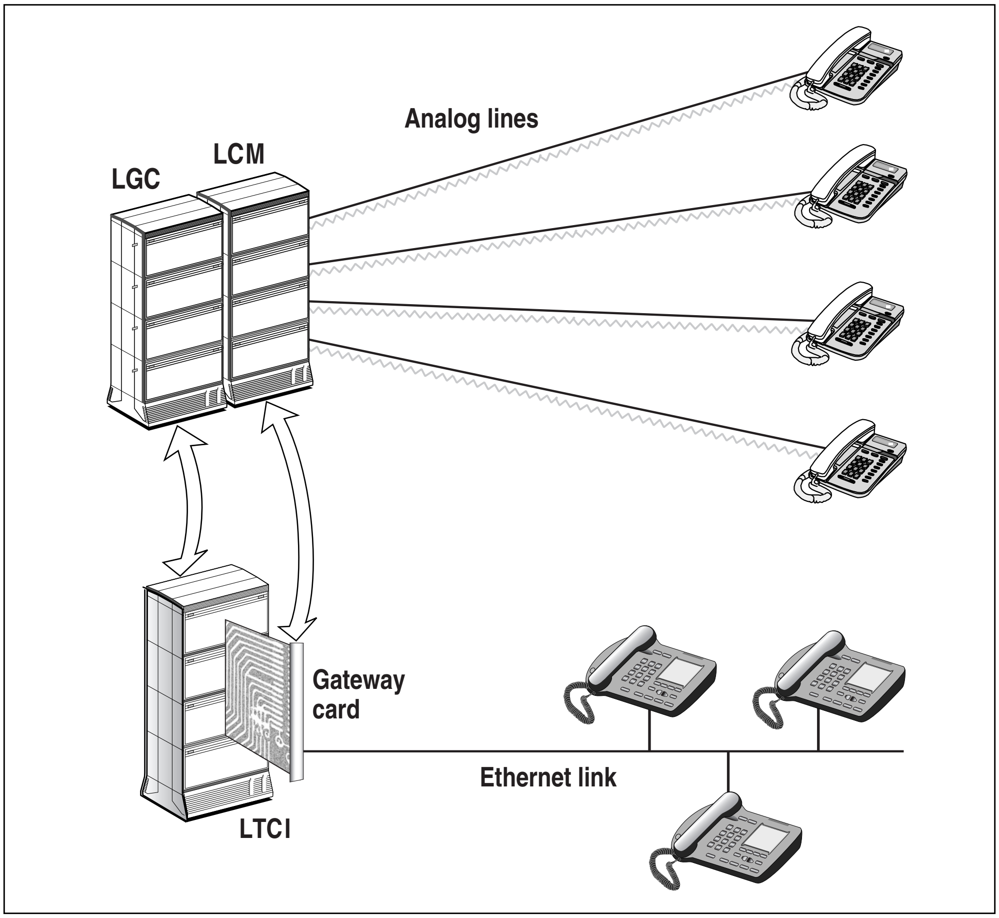
The Gateway circuit pack has a single, high-performance PowerPC processor for embedded applications. For a detailed description of the Gateway hardware, see the section “Physical description” in this chapter. The Gateway application and operating system are downloaded from the load server on the CO LAN. See the chapter “DHCP and FTP load server” for a description of the Gateway software load and boot process.

Node characteristics

The NT7X07 Gateway card has characteristics similar to a P-side node in the LTCI frame. It resides in a P-side slot and has a DS60 interface to the shelf backplane. The DS60 link connects the Gateway card to the XMS-based peripheral module (XPM). The Gateway card is considered a subtending node of the XPM, similar to a line concentrating module (LCM). The Gateway card also resembles a subtending node because of its on-board processing ability.

The following figure compares a packet-switched system with a Gateway card and shared bandwidth to a circuit-switched system and dedicated bandwidth.

Figure 3-1 Gateway card as a subtending node of the LTCI



DMS view of the Gateway node

The XPM Node Maintenance subsystem has IPGW as a new node type for the Gateway card. The IPGW MAP level displays the node state. The IPGW MAP level is a sublevel of the peripheral module (PM) MAP level. The commands available at the IPGW MAP level are similar to the commands for other PMs. See the chapter “DMS maintenance” for a detailed description of the IPGW MAP commands.

Limitations and restrictions

The following lists the limitations and restrictions of the Gateway card:

- One LTCI supports a maximum of 10 Gateway cards (8 active and 2 spares).
- The time switch card (NT6X44) on the LTCI shelf limits the active channels to 480. Therefore, only 8 Gateway cards can be active at one time since each card supports 60 channels (60 x 8 = 480).
- A single Gateway card supports up to 128 terminal identifiers (TID) or up to 60 simultaneous calls. The static data download mechanism supports up to 8 directory numbers (DN) on each TID.

  Note: With the NA013 load, a single Gateway card supports up to 512 TIDs or logical TIDs (LTID). Gateway cards provisioned before the NA013 one night process (ONP) support only 128 TIDs or LTIDs. To expand pre-NA013 Gateway cards to support 512 TIDs or LTIDs, refer to the Centrex IP Release Notes for Release 2.

- All Gateway cards within a single XPM must reside on the same subnet.
- Each Gateway card can serve only one H.323 zone.
- The LTCI that supports the Gateway must have an NTMX76 messaging card to support communication between the Gateway and the XPM processor.
- The LTCI that supports the Gateway must have an NTSX05 processor card. The MX77 processor card does not have enough memory to meet expanded capacity requirements that NA013 feature Centrex IP Capacity Enhancement provided.

  Note: An LTCI with an NTMX76 messaging card can use either an MX77 or an NTSX05 processor card.

- Per Telcordia Technology GR-1089-CORE intrabuilding surge requirements, the NT7X07 is suitable for connection to intrabuilding or nonexposed wiring or cable only.

Installation

The Gateway card is installed in the Centrex IP-ready cabinet or frame. Before installation, perform the following prerequisite actions:

- Ensure that the NetID software is configured to use the medium access control (MAC) address that is labeled on the Gateway card.

  Note: There are two MAC addresses labeled on the Gateway card faceplate. The first address, which is Ethernet 0, is entered in the NetID software.

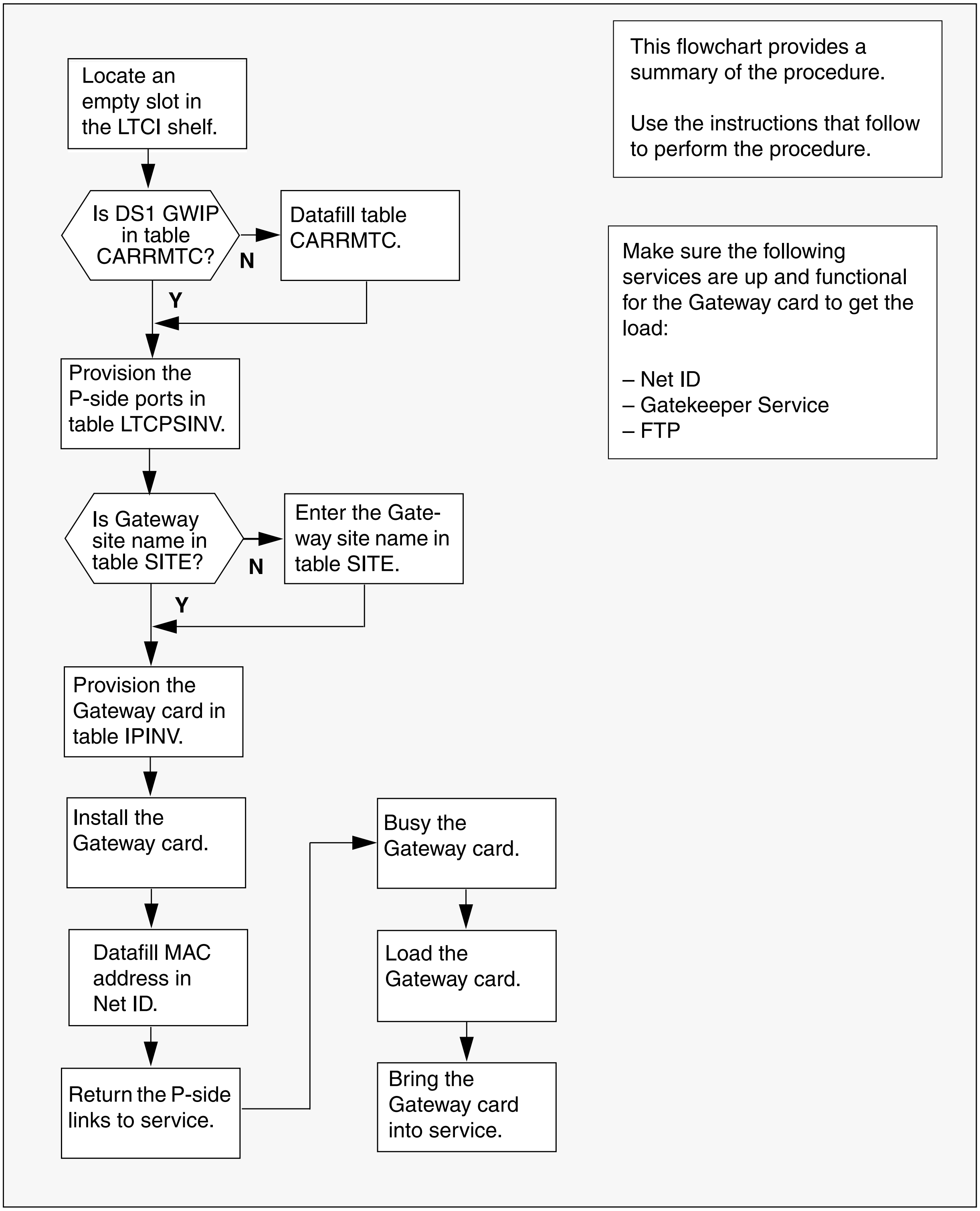
- Ensure that the current Gateway load file is in the correct directory for the DHCP server.

  Note: See the chapter "DHCP and load servers" for the procedure on configuring the DHCP server.

Installation summary of action

The flowchart that follows provides a summary of the "Installing an NT7X07 card in the LTCI" procedure. Use the instructions in the step-action procedure that follows the flowchart to install the Gateway card in a Centrex IP-ready LTCI frame or cabinet.

Figure 3-2 Summary of installing an NT7X07 card in an LTCI


This flowchart provides a summary of the procedure.
Use the instructions that follow to perform the procedure.
Locate an empty slot in the LTCI shelf.
Is DS1 GWIP in table CARRMTC?
N
Datafill table CARRMTC.
Y
Make sure the following services are up and functional for the Gateway card to get the load:
– Net ID
– Gatekeeper Service
– FTP
Provision the P-side ports in table LTCPSINV.
Is Gateway site name in table SITE?
N
Enter the Gateway site name in table SITE.
Y
Provision the Gateway card in table IPINV.
Install the Gateway card.
Busy the Gateway card.
Datafill MAC address in Net ID.
Load the Gateway card.
Return the P-side links to service.
Bring the Gateway card into service.

Procedure 3-1 Provisioning and installing the NT7X07 card in the LTCI

At the MAP terminal

1 Verity all patches listed in the release notes are applied.

2 Check table CARRMTC to ensure that the DS1 GWIP entry exists. Type

>TABLE CARRMTC

>POS LTC GWIP

and press the Enter key.

If the DS1 GWIP entry exists, go to the next step. If the DS1 GWIP entry does not exist, enter the DS1 GWIP entry in table CARRMTC. A datafill example for table CARRMTC follows.

Example of a MAP response

```
CSPMTYPE    TMPLTNM  RTSML  RTSOL                  ATTR
________________________________________________________________
LTC        GWIP 255  255 DS1 NT7X07AA MU_LAW SF ZCS
           BPV NILDL  N 250 1000 50 50 150 1000 3 6 864 100
            17 511 4 255
```

3 Check the P-side inventory of the LTCI. Type

>TABLE LTCPSINV

and press the Enter key.

4 Position on the desired LTCI in table LTCPSINV. For example, type

>POS LTC 0

and press the Enter key.

Example of table LTCPSINV

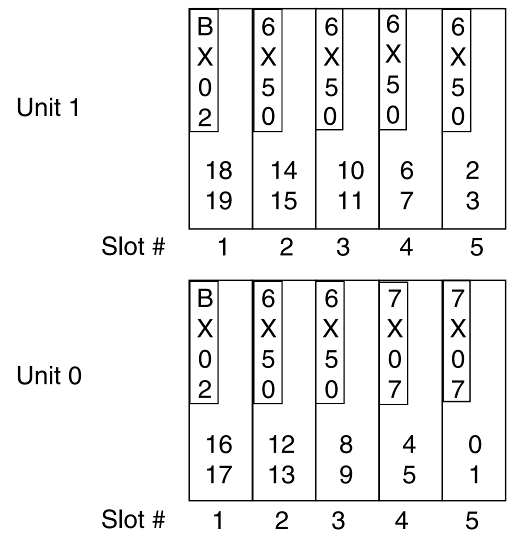
```
LTCNAME                                     PSLNKTAB
______________________________________________________

LTC   0
  N (0 DS1 GWIP N) (1 DS1 GWIP N)
   (2 DS1 GWIP N) (3 DS1 GWIP N)  (4 NILTYPE)
   (5 NILTYPE) (6 DS30A) (7 DS30A) (8 DS30A) (9 DS30A)
   (10 DS30A ) (11 DS30A) (12 DS30A) (13 DS1 DEFAULT N)
   (14 NILTYPE)  (15 DCH)  (16 NILTYPE)  (17 DCH)
   (18 NILTYPE )  (19 DCH) $
```

5 The Gateway card can be installed in slots 1 through 5 of either unit of the LTCI. These slots correspond to ports 0 through 19 in table LTCPSINV. Choose a slot that shows NILTYPE in both corresponding ports in table

LTCPSINV to ensure a slot is available. You can also check the physical slot of the LTCI and verify it is empty or contains a filler faceplate (PEC 0X50AA).

The following figure shows the assignment of ports to slots on the LTCI shelf.



6 Provision the DS-1 ports chosen in the step 5 in table LTCPSINV. In this example, the slot chosen for the Gateway card is slot 4 of unit 0. The ports were changed from NILTYPE to DS1 GWIP N. Type

```
>CHANGE
```

and press the Enter key until you reach the correct field

```
>4 DS1 GWIP N
>5 DS1 GWIP N
```

and press the Enter key until you reach the end of the tuple.

7 To confirm your selection and quit the table, type

```
>Y
>QUIT
```

and press the Enter key.

8 If this is the first time the Gateway card is being provisioned for an office, enter the Gateway site name in table SITE. In this example, the site name is GWIP. The site name can be any four characters. Type

```
>TABLE SITE
>ADD GWIP 0 0 VER90 $
```

and press the Enter key.

9 To confirm your selection and quit the table, type

```
>Y
>QUIT
```

and press the Enter key.

Proceed to one of the following steps (depending on the software load) to provision an NT7X07 card:

- Step 10 a with an NA012 load
- Step 10 b for a primary Gateway card with an NA013 load (which includes Gateway Sparing)
- Step 10 c for a spare Gateway card with an NA013 load (which includes Gateway Sparing)

10 Provision the NT7X07 card in table IPINV.

a To provision the NTX07 card in table IPINV with an **NA012** software load, type

```
>TABLE IPINV
```

```
>ADD <IPNO PMTYPE PMNO IPPEC LOAD PORT IPZONE GW_TYPE
INTRASW SPARE>
```

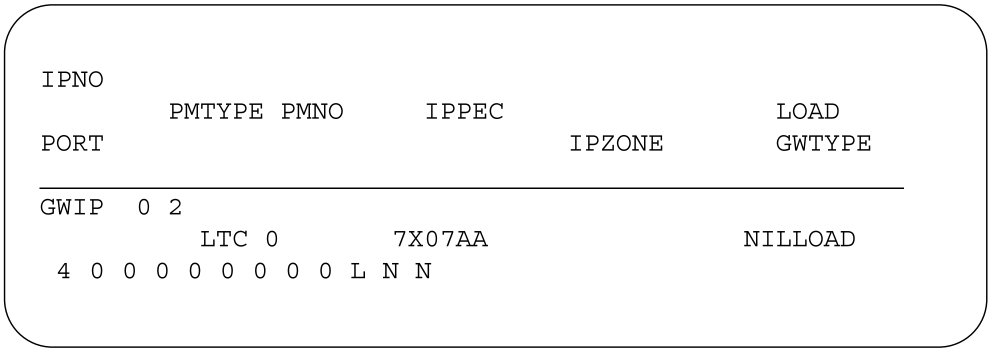
and press the Enter key.

Example of command

```
>ADD GWIP 0 2 LTC 0 7X07AA NILLOAD 4 0 0 0 0 0 0 0 0 L
N N
```

Note: The NT7X07 card uses the numbering convention `ltc_number port number_divided_by_2`. In the example, `GWIP 0 2`, `0` is the LTC number and `2` is the port number divided by 2.

Example of table IPINV (NA012)



```
IPNO
        PMTYPE PMNO     IPPEC                         LOAD
PORT                             IPZONE               GWTYPE
_____________________________________________________________________
GWIP  0 2
          LTC 0       7X07AA                       NILLOAD
 4  0  0  0  0  0  0  0  0  L  N  N
```

The following table describes the fields in table IPINV.

Table 3-1 Table IPINV field descriptions (Sheet 1 of 2)

Field	Description
IPNO	IP number. The site identifier, frame, and unit number of the Gateway card.
PMTYPE	PM type. The type of peripheral module that the Gateway card is located in. This field is always set to LTC.
PMNO	PM number. The PM number is the host LTC number.

Table 3-1 Table IPINV field descriptions (Sheet 2 of 2)

Field	Description
IPPEC	IP PEC. The product engineering code (PEC) of the Gateway card, which is 7X07AA.
LOAD	Load file name. The name of the Gateway's software load. (Note: The load is always NILLOAD.)
PORT	Port number. The even port number of the DS1 datafilled in table LTCPSINV for this card slot.
IPZONE	IP zone. The primary and secondary IP address for the Gateway card. ***Note:*** IPZONE field is not used in NA012. Datafill as "0 0 0 0 0 0 0 0."
GW_TYPE	GW type. The function of the Gateway card (local loop). Subfields indicate if intraswitching or sparing are enabled. ***Note:*** The GW_TYPE field is always identified as a lines (L) Gateway for Centrex IP.
INTRASW	GW type. The function of the Gateway card (local loop). Subfields indicate if intraswitching or sparing are enabled. ***Note 1:*** If intraswitching is enabled, ensure all routers and firewalls are configured as outlined in the "System engineering" chapter. ***Note 2:*** For more information on intraswitching, refer to the "CO LAN and CO LAN edge device" chapter.
SPARE	Spare Gateway card. ***Note:*** The SPARE field is not used in NA012. Datafill as "N."

Continue to step 11 .

b Or to provision a **primary** NT7X07 card in table IPINV with an **NA013** software load, type

```
>TABLE IPINV
```

```
>ADD <IPNO PMTYPE PMNO IPPEC LOAD PORT IPZONE GW_TYPE
INTRASW SPARE>
```

and press the Enter key.

Example of command

```
>ADD GWIP 0 2 LTC 0 7X07AA NILLOAD 4 47 174 68 31 47
174 68 130 L N N
```

and press the Enter key.

Example of table IPINV (NA013) for a primary Gateway card

```
IPNO
        PMTYPE PMNO     IPPEC                   LOAD
PORT                             IPZONE         GWTYPE
______________________________________________________
GWIP  0 2
          LTC 0       7X07AA                  NILLOAD
 4 47 174 68 31 47 174 68 130 L N N
```

The following table describes the fields in table IPINV.

Table 3-2 Table IPINV field descriptions (Sheet 1 of 2)

Field	Description
IPNO	IP number. The site identifier, frame, and unit number of the Gateway card.
PMTYPE	PM type. The type of peripheral module that the Gateway card is located in. This field is always datafilled as LTC.
PMNO	PM number. The PM number is the host LTC number.
IPPEC	IP PEC. The product engineering code (PEC) of the Gateway card, which is 7X07AA.
LOAD	Load file name. The name of the Gateway's software load. (Note: The load is always NILLOAD.)
PORT	Port number. The even port number of the DS1 datafilled in table LTCPSINV for this card slot.

Table 3-2 Table IPINV field descriptions (Sheet 2 of 2)

Field	Description
IPZONE	IP zone. The primary and secondary IP address for the Gateway card. The first four entries of the IPZONE correspond to the logical IP address of the Gateway card. (These entries must be different from the IP address datafilled in NetID for this card.) The last four entries correspond to the virtual IP address of the Gatekeeper. ***Note:*** For a primary Gateway card, enter datafill in field IPZONE as follows: • Enter the Gateway logical IP address in the first four entries of field IPZONE. This entry must be an available IP address on the same subnet as the physical IP address that the Gateway card receives using the DHCP (that is, 47.174.68.31). • Enter the Gatekeeper IP address in the last four entries of field IPZONE. This entry determines which Gateway cards the same Gatekeeper is to service. They also share the same sparing pool (that is, 47.174.68.130).
GW_TYPE	GW type. The function of the Gateway card (local loop). Subfields indicate if intraswitching or sparing are enabled. ***Note:*** The GW_TYPE field is always identified as a lines (L) Gateway for Centrex IP.
INTRASW	GW type. The function of the Gateway card (local loop). Subfields indicate if intraswitching or sparing are enabled. ***Note 1:*** If intraswitching is enabled, ensure all routers and firewalls are configured as outlined in the “System engineering” chapter. ***Note 2:*** For more information on intraswitching, refer to the “CO LAN and CO LAN edge device” chapter.
SPARE	Spare Gateway card. ***Note:*** Datafill the SPARE field with “N” for a primary card.

Continue to step 11 .

c Or to provision a **spare** NT7X07 card in table IPINV with an **NA013** software load, type

```
>TABLE IPINV
```

```
>ADD <IPNO PMTYPE PMNO IPPEC LOAD PORT IPZONE GW_TYPE
INTRASW SPARE>
```

and press the Enter key.

Example of command

```
>ADD GWIP 0 3 LTC 0 7X07AA NILLOAD 6 0 0 0 0 47 174 68
130 L N Y
```

Example of table IPINV (NA013) for a spare Gateway card

```
IPNO
        PMTYPE PMNO     IPPEC                 LOAD
PORT                             IPZONE       GWTYPE
_______________________________________________________
GWIP  0 3
          LTC 0       7X07AA                NILLOAD
 6 0 0 0 0 47 174 68 130 L N Y
```

The following table describes the fields in table IPINV.

Table 3-3 Table IPINV field descriptions (Sheet 1 of 2)

Field	Description
IPNO	IP number. The site identifier, frame, and unit number of the Gateway card.
PMTYPE	PM type. The type of peripheral module that the Gateway card is located in. This field is always datafilled as LTC.
PMNO	PM number. The PM number is the host LTC number.
IPPEC	IP PEC. The product engineering code (PEC) of the Gateway card, which is 7X07AA.
LOAD	Load file name. The name of the Gateway’s software load. (Note: The load is always NILLOAD.)
PORT	Port number. The even port number of the DS1 datafilled in table LTCPSINV for this card slot.

Table 3-3 Table IPINV field descriptions (Sheet 2 of 2)

Field	Description
IPZONE	IP zone. The primary and secondary IP address for the Gateway card. The first four entries of the IPZONE are not used for a spare Gateway card. The last four entries correspond to the virtual IP address of the Gatekeeper. ***Note:*** For a spare Gateway card, enter datafill in field IPZONE as follows: • Enter the Gateway logical IP address in the first four entries of field IPZONE. For a spare card, set the first four entries to all 0’s. • Enter the Gatekeeper IP address in the last four entries of field IPZONE. This entry must match the datafill of the Gatekeeper IP address for the primary Gateway card (that is, 47.174.68.130).
GW_TYPE	GW type. The function of the Gateway card (local loop). Subfields indicate if intraswitching or sparing are enabled. ***Note:*** The GW_TYPE field is always identified as a lines (L) Gateway for Centrex IP.
INTRASW	GW type. The function of the Gateway card (local loop). Subfields indicate if intraswitching or sparing are enabled. ***Note 1:*** If intraswitching is enabled, ensure all routers and firewalls are configured as outlined in the “System engineering” chapter. ***Note 2:*** For more information on intraswitching, refer to the “CO LAN and CO LAN edge device” chapter.
SPARE	Spare Gateway card. ***Note:*** Set the SPARE field to “Y” for a spare card.

Continue to step 11 .

11 To confirm your selection and quit the table, type

```
>Y
>QUIT
```

and press the Enter key.

At the LTCI frame

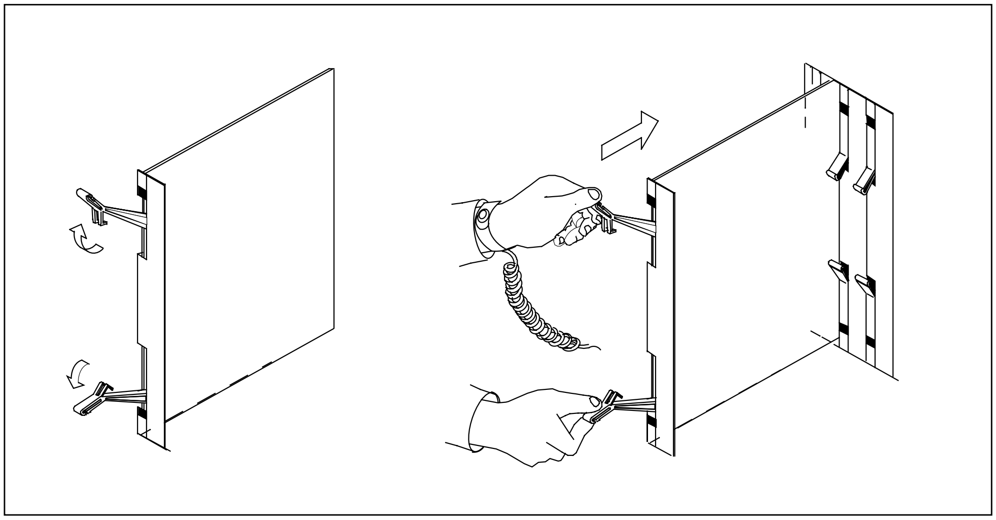
12

> **WARNING**
> **Static electricity damage**
> Before inserting any cards, put on a wrist strap and connect it to the wrist strap grounding point on the left side of the frame supervisory panel of the XPM. This protects the equipment against damage caused by static electricity.

Prepare to install the Gateway card. Put on a wrist strap.

13 Open the locking levers on the Gateway card.

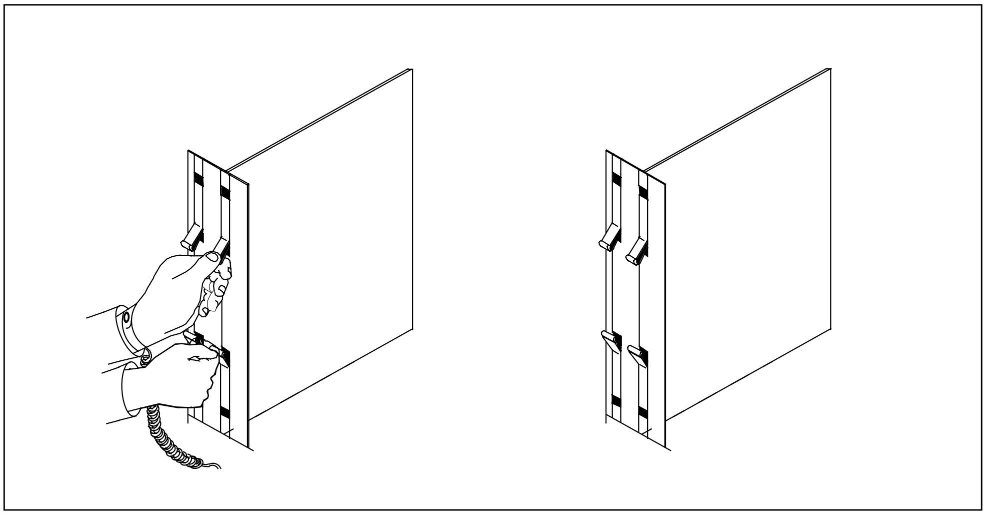
Align the card with the slots in the shelf and gently slide the card into the shelf.



14 Using your fingers or thumbs, push on the upper and lower edges of the faceplate to ensure that the card is fully seated in the shelf.

15 Seat and lock the card.

16 Close the locking levers.



At the MAP terminal

17 Access the PM level of the MAP display and post the LTCI. Type

```
>MAPCI;MTC;PM;POST LTC ltc_no
```

where

ltc_no is the number of the LTCI

and press the Enter key.

Example of a MAP display

```
 CM    MS    IOD    Net   PM   CCS   Lns   Trks    Ext    APPL
  .     .      .      .   1RCC  .     .     .       .      .

 LTC               SysB    ManB   OffL    CBsy   ISTb   InSv
 0 Quit      PM        0       0     1       0     4     22
 2 Post_    LTC        0       0     2       0     2      9
 3 ListSet
 4         LTC  0  ISTb  Links_OOS: CSide 0, PSide 2
 5 Trnsl_  Unit0: Act      InSv
 6 Tst_    Unit1: Inact    InSv
 7 Bsy_
 8 RTS_
 9 OffL
10 LoadPM_
11 Disp_
12 Next
13 SwAct
14 QueryPM
15 DCH
16
17 Perform
18 ISG
```

18 Display the P-side links associated with the Gateway card. Type

>TRNSL P

and press the Enter key.

Example of a MAP response

```
LINK 0    RMM  5           0;CAP   MS:STATUS OK        MSGCOND OPN
LINK 1    LCM REM1  00 0   0;CAP   MS:STATUS OK        MSGCOND OPN
LINK 2    LCM REM1  00 0   1;CAP   MS:STATUS OK        MSGCOND OPN
LINK 3    LCM REM1  00 0   2;CAP    S:STATUS OK
LINK 4    GWIP 0 2 0; CAP MS: STATUS MBSY
LINK 5    GWIP 0 2 1; CAP MS: STATUS MBSY
```

19 The P-side links transition from offline (OFFL) to manual busy (ManB) automatically during the datafill processing for table IPINV.

20 RTS the P-side links. Type

>RTS LINK link_no

and press the Enter key.

where

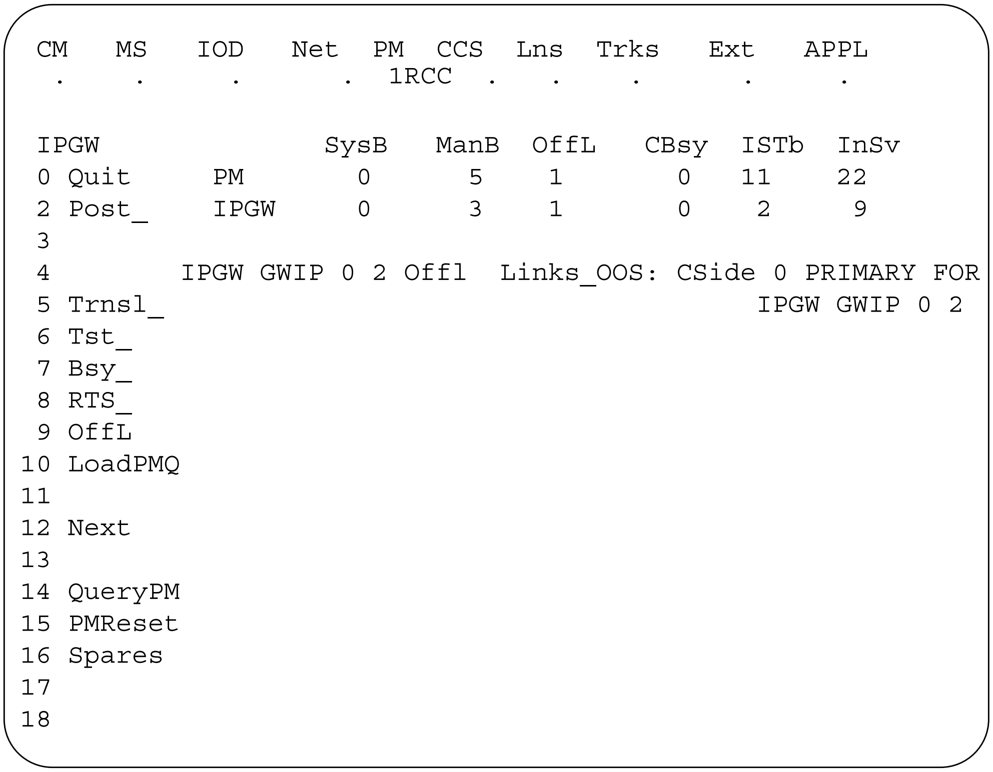
link_no is the number of the links associated with the Gateway card.

21 Access the PM level of the MAP display and post the Gateway card. Type

>MAPCI;MTC;PM;POST IPGW GWIP 0 2

and press the Enter key.

Example of a MAP display



```
 CM   MS   IOD   Net  PM  CCS  Lns  Trks   Ext   APPL
  .    .     .      .  1RCC  .   .    .      .     .

 IPGW              SysB   ManB  OffL   CBsy  ISTb  InSv
 0 Quit     PM       0      5    1       0   11    22
 2 Post_    IPGW     0      3    1       0    2     9
 3
 4        IPGW GWIP 0 2 Offl  Links_OOS: CSide 0 PRIMARY FOR
 5 Trnsl_                                     IPGW GWIP 0 2
 6 Tst_
 7 Bsy_
 8 RTS_
 9 OffL
10 LoadPMQ
11
12 Next
13
14 QueryPM
15 PMReset
16 Spares
17
18
```

22 Busy the Gateway card. Type

>BSY

and press the Enter key.

23 Load the Gateway card. Type

>PMRESET

and press the Enter key.

> ***Note 1:*** Check that the NetID and FTP services are running on the Gatekeeper.
>
> ***Note 2:*** This command may take a few minutes to execute. The command will timeout after 10 minutes. A shorter timeout indicates that system resources are unavailable. In this case, re-enter the command.
>
> ***Note 3:*** After the Gateway receives its load, the Processor LED on the Gateway faceplate is lit.

24 Bring the Gateway card into service. Type

>RTS

and press the Enter key.

Note: The RTS command registers the Gateway with the Gatekeeper. Check that Gatekeeper services are running.

For information about provisioning a terminal, refer to the “DMS Maintenance” chapter.

Physical description

The Gateway card contains six main functional components:

- Control processor complex (CPC)
- Signal processing complex (SPC)
- Telephony and WAN interface (TWI)
- High-speed datacom interface (HSDI)
- Backplane interface and processor support (BIPS)
- Power conversion system (PCS)

Figure 3-3 shows the main functional components of the Gateway card and the primary signal connectivity.

Figure 3-3 Gateway high-level block diagram

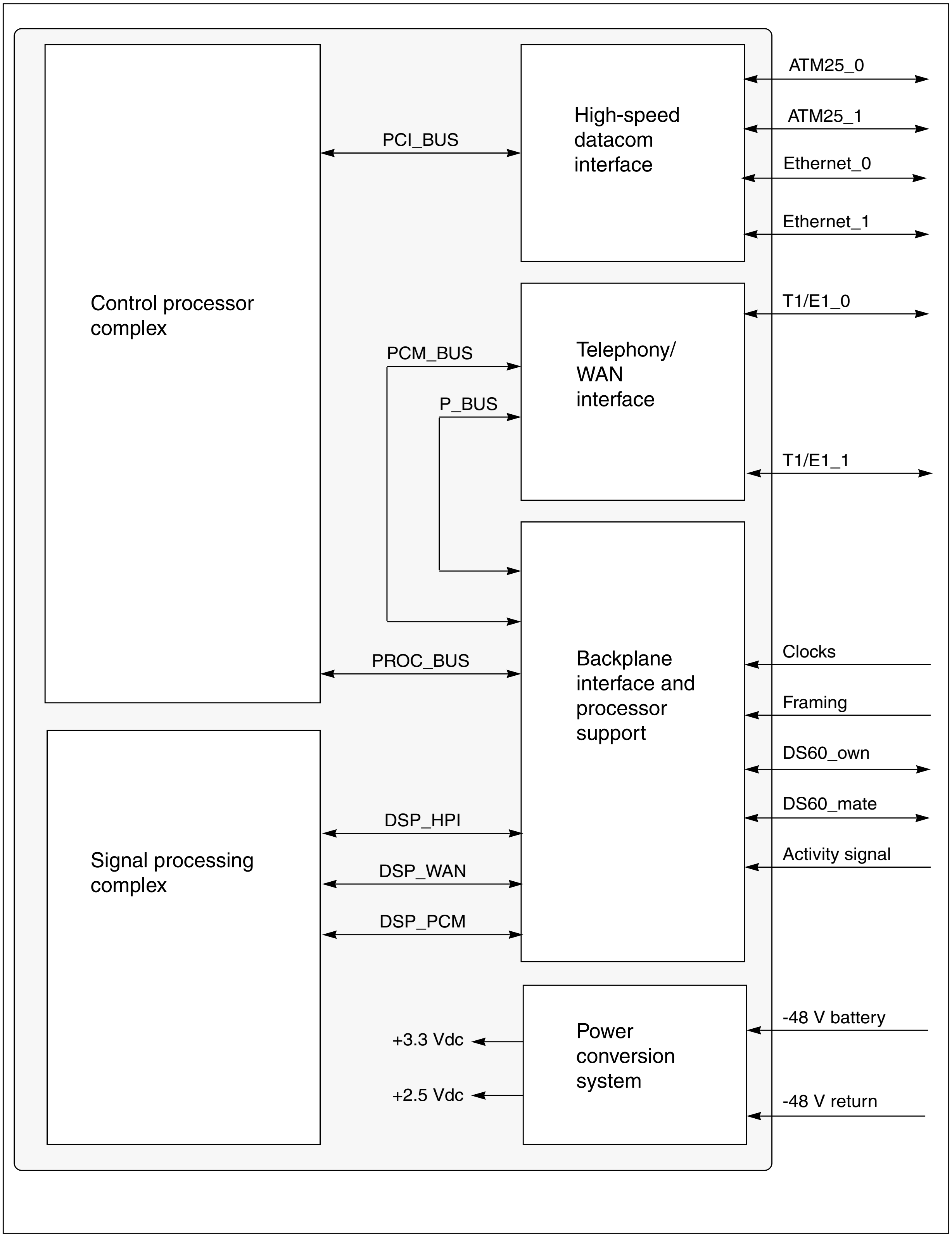
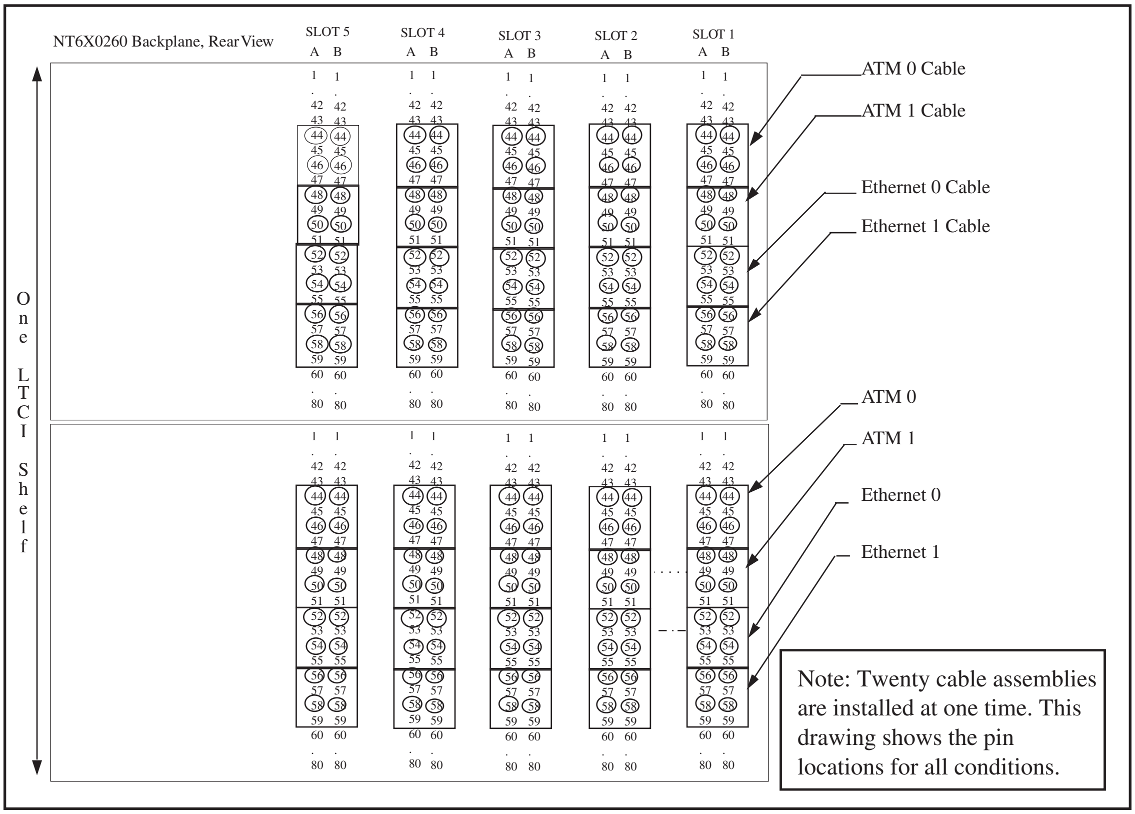


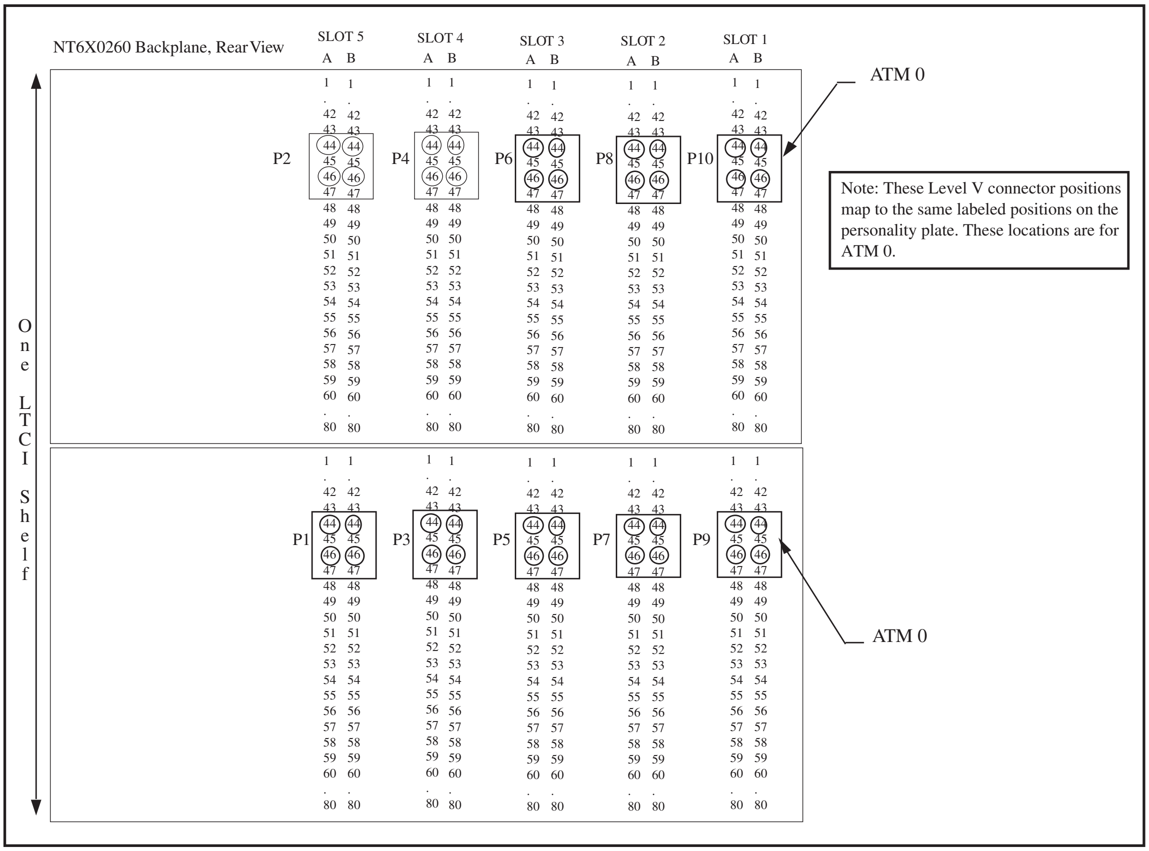
Figure 3-4 and figure 3-5 show rear views of the LTCI backplane, NT6X0260, with pin outs.

Figure 3-4 LTCI backplane rear view 1



Note: Twenty cable assemblies are installed at one time. This drawing shows the pin locations for all conditions.

Figure 3-5 LTCI backplane rear view 2



Note: These Level V connector positions map to the same labeled positions on the personality plate. These locations are for ATM 0.

Functional components

The following sections describe the functional components of the Gateway card.

Control processor complex

The CPC is driven by a single high-performance microprocessor. In addition to providing central intelligence and card-based maintenance functions, the control processor performs message operations with the XPM shelf processor and the H.323 clients. The CPC contains the following hardware components:

- one 266 MHz embedded PowerPC-based processor for local control and protocol processing
- 64 Mbyte of dynamic random access memory (DRAM) memory for control processor operations
- 2 Mbyte flash electrically erasable programmable read-only memory (EEPROM) as non-volatile memory
- 512 kbyte static RAM for log storage and scratchpad memory

Signal processing complex

The SPC performs the signal processing operations for the Gateway card. To support the 60-channel density required by the Gateway card, 12 digital signal processors (DSP) are built into the SPC. Each DSP supports 5 channels. The DSPs perform the following operations:

- transcoding functions between the toll-quality G.729 pulse code modulation (PCM) of the PSTN and the packetized PCM required by the H.323 clients
- dual-tone multifrequency (DTMF) detection and generation
- voice activity detection
- echo cancellation
- comfort noise generation
- packet loss management

Telephony and WAN interface

The TWI provides the Gateway card with two T1/E1 interfaces for transmission facilities. The T1 interface is the equivalent of a DS-1 link interface with 24 channels at 1.544 Mbit/s. The E1 interface carries data at 2.048 Mbit/s on 32 channels for European facilities only. The selection between the T1 and E1 link formats is managed by software. These interfaces can serve the facilities that follow:

- channelized PCM transmission facilities at 24 or 32 channels
- unchannelized links that support ISDN PRI or asynchronous transfer mode (ATM) communications

The TWI permits the Gateway card to exist in remote locations without external LAN-to-WAN routing equipment for the T1/E1 WAN facility.

High-speed datacom interface

The HSDI provides the interface between the Gateway card and the H.323 client. The CPC uses the HSDI to pass packetized PCM, control messaging, and signaling to the H.323 clients. The HSDI supports the interfaces that follow:

- two redundant unshielded twisted pair (UTP) ATM25 (25.6 Mbit/s) interfaces as alternate datacom interface to the T1/E1 or Ethernet links
- two redundant UTP Ethernet (10/100 Mbit/s) interfaces for connectivity to external LAN routing equipment

The Simple Link Redundancy (SLR) feature allows the active Ethernet link to switch traffic over to a standby link in the event of a hardware failure.

Backplane interface and processor support

The BIPS block is the electrical interface between the Gateway card and the XPM backplane. The main components of this block are the DS60 interface, the field programmable gate array (FPGA) device, and the high-level data link control (HDLC) interface.

The DS60 physical interface contains two multiplexed DS30 links. There are five types of channels on the DS60 link. Each provisioned Gateway card requires these channels, which are described as follows:

- messaging channel for all messaging traffic (call processing and maintenance). This is the primary messaging channel between the XPM and the Gateway card.
- dedicated messaging channel for control and status functions. This connection allows the Node Maintenance subsystem to diagnose card sanity and faults in the absence of an active messaging connection.
- dedicated maintenance loopback channel for XPM diagnostics
- spare messaging channel (not used)
- 60 PCM channels for active voice traffic. The 60 PCM channels can support a maximum of 60 simultaneous calls.

The FPGA device provides the clock generation circuitry for both the control processor and the DSPs. The FPGA also provides a maintenance and diagnostic interface and the HDLC interface to the XPM. The FPGA device provides the following support functions:

- recovers PCM and timing/framing information from the XPM backplane
- distributes PCM and timing/framing information to the DSPs on the Gateway card
- multiplexes the PCM data from the signal processors to redundant DS60 links for transmission to the XPM backplane
- supports the CPC with the processor functions that follow
  - — timers
  - — universal asynchronous receiver transmitter (UART)
  - — interrupt controller
  - — multichannel HDLC interface for the interprocessor communications between the CPC and the XPM shelf processor
- provides a maintenance and diagnostic interface for communication with the XPM shelf processor before and after the Gateway card initializes

The maintenance and diagnostic interface consists of two logical channels on the DS60 link, a loopback channel and a control/status channel. The loopback channel provides link integrity verification over the DS30 PCM links. The control/status channel sends messages about the Gateway card's hardware, such as, reset processor, reset card, or switch HDLC message link. The control/status channel can also receive messages from the Gateway control processor to perform diagnostics. The XPM shelf processor reads the control/status channel to receive information from the Gateway card, including processor state, link status, and diagnostic results.

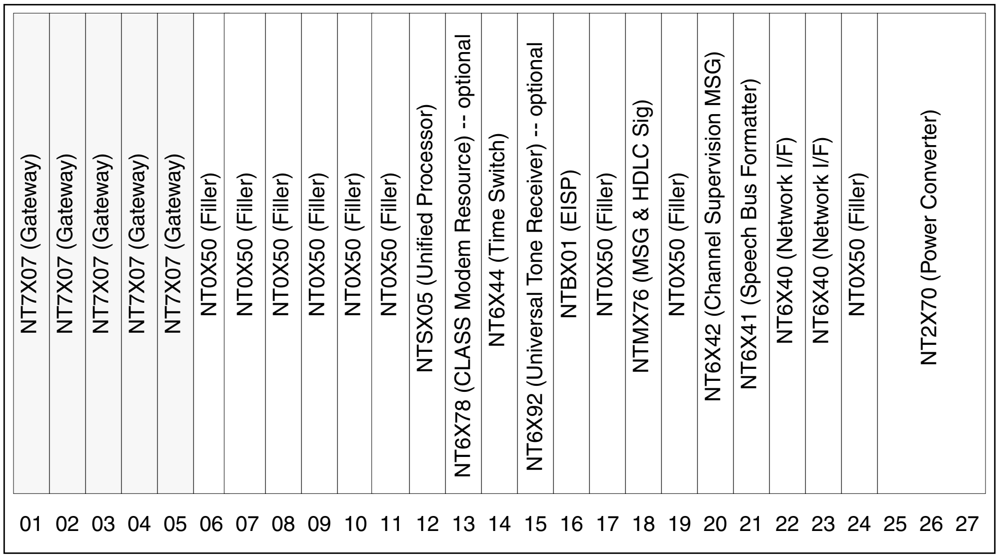
Power conversion system

The only external power required by the Gateway card from the XPM backplane is the -48 V dc battery. The PCS converts the -48 V dc battery power source to the +3.3 V dc and +2.5 V dc on-board point of use power supplies (PUPS) required by the components on the card. The PCS also provides inrush current limiting and overcurrent protection on the -48 V dc power supply.

LTCI shelf structure

The Gateway card is provisioned in DS-1 slots 1 through 5 of the LTCI shelf. These slots provide the optimum combination of processing power and channel capacity. Figure 3-6 illustrates the LTCI shelf packfill provisioned with the Gateway cards.

Figure 3-6 LTCI shelf packfill for Centrex IP



> *Note:* The enhanced ISDN signaling preprocessor (EISP) is included on the LTCI shelf as part of the standard packfill to support ISDN software packaging. It is not used for messaging with the Gateway card.

With five Gateway cards for each shelf, ten Gateway cards can be provisioned on the LTCI. Each Gateway card supports the maximum channel density of a DS-1 slot, which is 60 pulse code modulation (PCM) channels. Because the time switch card limits the number of channels to 480, only 8 Gateway cards can be active at a time.

The Gateway card also supports two DS0 HDLC message channels through the NTMX76 messaging card on the LTCI shelf. These message channels are used for low-level maintenance and call processing control functions. The Gateway card mimics an enhanced D-channel handler (EDCH) card for terminating HDLC messages from the NTMX76 messaging card. The PCM data and messaging paths are shown in the following figures.

Figure 3-7 Gateway voice and data path (non-intraswitched)

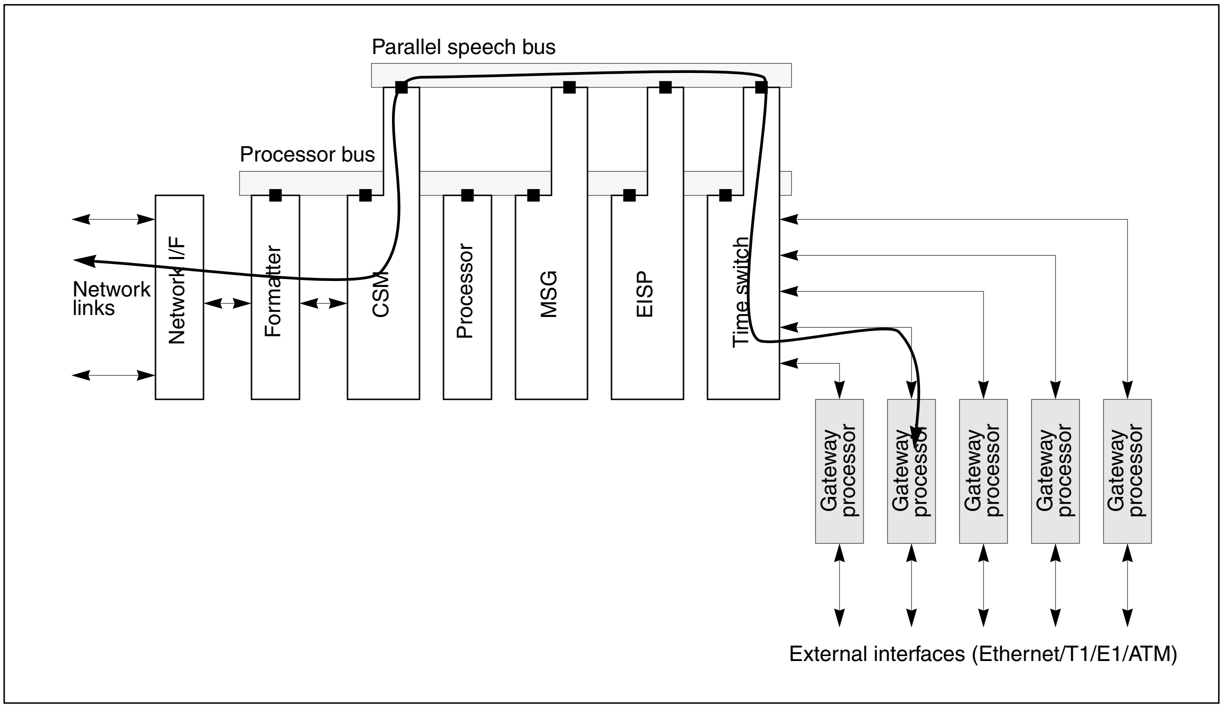
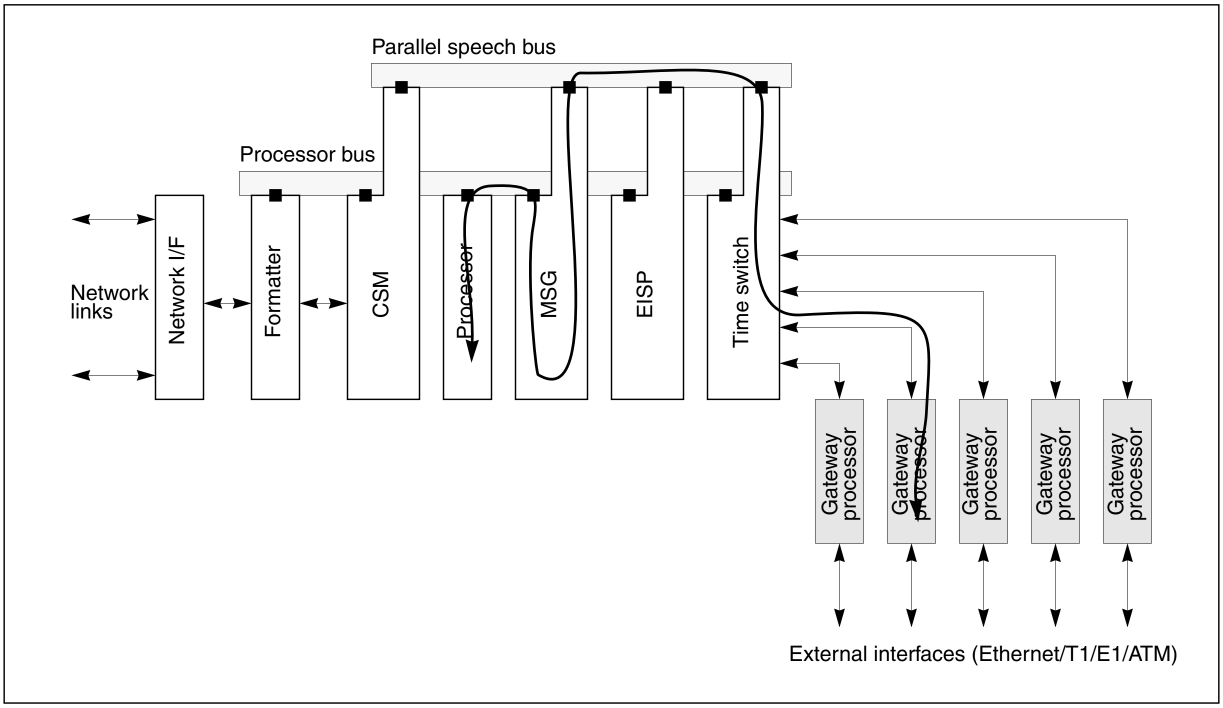


Figure 3-8 Gateway message and control path (intraswitched and non-intraswitched)



Functionality

The following sections describe specific functionality of the Gateway card.

Gateway registration

The Gateway card functions as both an H.323 interface and an H.323 endpoint. All H.323 endpoints must register with the Gatekeeper to process calls in the LAN environment. The H.323 endpoints handle the communication, call control, and call signaling channels that convert H.225 to Q.931 and Q.931 to H.225.

The Gateway receives its IP address and the load server's IP address from the DHCP server. The load server can be located on the Gatekeeper, and therefore, can have the same IP address as the Gatekeeper. After receiving its software load, the Gateway card initiates its boot and load sequence. Upon application of the RTS command at the IPGW MAP level, the Gateway registers with the Gatekeeper. The Gateway first checks the status of the Gatekeeper. If the Gatekeeper is active, the Gateway sends its IP address and node number to the Gatekeeper to complete registration.

The Gatekeeper uses the Gateway registration data to create a mapping table of terminal identifiers (TID) for call processing.

Centrex IP Capacity Enhancement

The Centrex IP Capacity Enhancement feature increases the total number of clients to 4096 that the Centrex IP system supports for each XPM (or LTCI). This feature also expands the number of line equipment numbers (LEN) to 512 for each Gateway card provisioned in the Centrex IP system. (Each LTCI supports up to eight active Gateway cards.)

ATTENTION

This feature requires the NA013 software load. Gateway cards provisioned before NA013 ONP support only 128 TIDs or LTIDs. To expand pre-NA013 Gateway cards to support 512 TIDs or LTIDs, refer to the Centrex IP Release Notes for Release 2 on your software CD.

Before NA013, each Gateway supported a maximum of 128 ISDN loops for Centrex IP. Each Centrex IP ISDN loop supported one logical terminal identifier (LTID). Because each Centrex IP client is provisioned as an ISDN basic rate interface (BRI) LTID, each Gateway node supported only 128 clients.

However, this feature enables Centrex IP to support a total of 4096 clients for each XPM by expanding the number of LTIDs that the XPM supports.

This feature also increase the value of office parameter MAX_BRA_LINES in table OFCOPT (Office Option) to accommodate the number of BRI lines for provisioning. Nortel Networks recommends increasing the value of MAX_BRA_LINES by 50 (or 5000 lines) for each XPM that Centrex IP uses.

Static data download

The LTCI processes and stores the static data required to provision the Gateway card and the client terminals. The static data contains the DNs and the associated TIDs of the client terminals. Static data for the Gateways contain the Gateway's node number and TID. The client terminals have the same node number as the Gateway they are assigned to. The LTCI downloads the static data to the Gateway, which forwards it to the Gatekeeper. The static data is initially downloaded when the Gateway registers with the Gatekeeper. The static data is sent whenever the terminal data on a Gateway is changed. The Gatekeeper requires this information to correctly identify the terminals and transfer their call processing information to the Gateway. The Gatekeeper stores the information on DN assignments to the Gateways and the clients in a DN-to-TID mapping table.

> ***Note:*** The addition of the NA013 feature Centrex IP Capacity Enhancement can increase the time to update static data between the XPM and the Gateway and Gatekeeper. This time increase can affect the recovery time for Centrex IP in relation to the number of datafilled clients.

Component diagnostics

The Gateway processor ROM contains diagnostic utilities that verify the Gateway's hardware components that are required to accept a software load. The ROM-resident diagnostics are run any time the control processor is reset. The Gateway card also has component diagnostics and application diagnostics that are downloaded as part of the application software of the Gateway card.

The XPM shelf processor also uses the ROM-resident diagnostic utilities on the Gateway card for the XPM-based diagnostics. The XPM processor sends messaging requests to the Gateway card during runtime. The current node state of the Gateway card and the XPM determines what subtests the XPM executes.

The following diagnostic utilities are part of the Gateway operating system and not part of the XPM software:

- register test—verifies read/write ability of each register bit
- address bus test—verifies entire address range can be accessed
- data bus test—verifies all values on the data bus
- ROM test—computes checksum over entire ROM and compares to stored value
- RAM test—verifies read/write patterns and bits
- interrupt device test—verifies card interrupts and register states
- interrupt controller test—runs control, status, and mask register tests
- timer test—verifies watchdog timer and real-time clocks
- PCM interface test—verifies XPM backplane interface paths
- communications port test—runs register and loopback tests

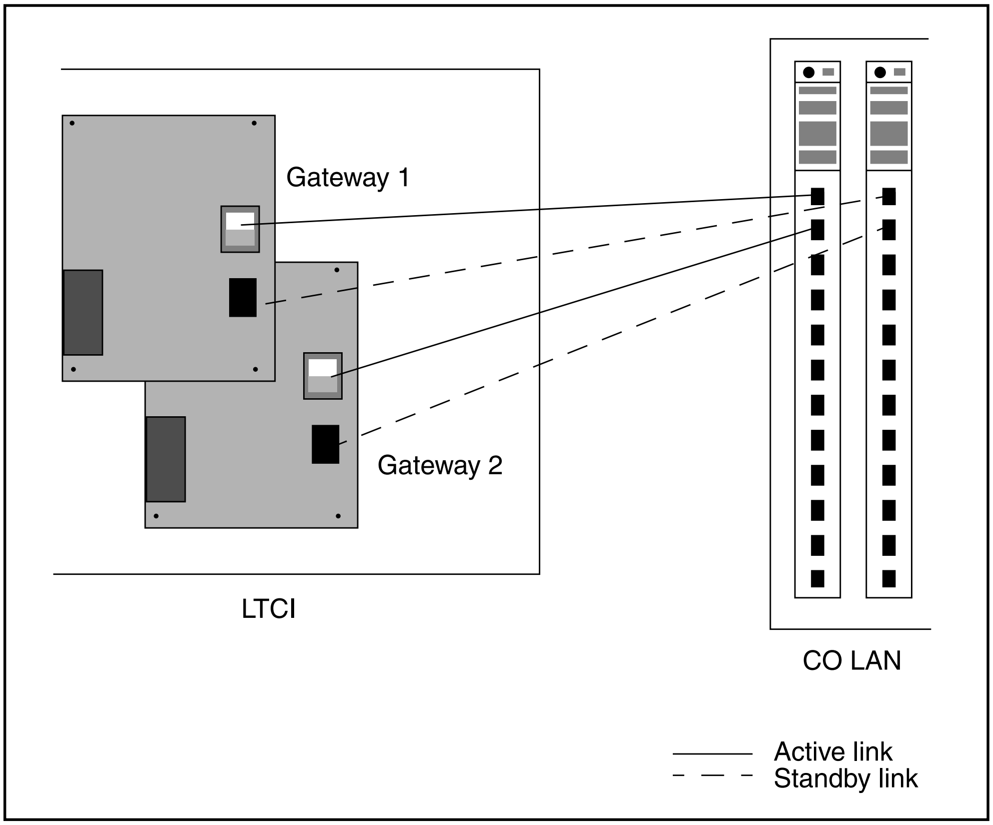
Link redundancy

The Gateway software can detect a fault condition on the redundant Ethernet links. The SLR feature allows the active Ethernet link to switch traffic over to a standby link in the event of a hardware failure. The possible types of hardware failures are a cable, hub, or card failure. These failures are known as layer 1 faults because they occur at the hardware level. The SLR feature does not address layer 2 or protocol-related faults. Each link has an LED indicator on the Gateway faceplate that is lit when the link is active. Gateway diagnostics check that both Ethernet ports are connected.

> ***Note:*** Each Ethernet interface on the Gateway card has the same MAC and IP address. However, the inactive link does not send out a MAC or IP address. Identical MAC addresses on multiple hub ports can cause errors in legacy networking equipment.

Figure 3-9 shows the physical connection of the redundant Ethernet links from the Gateway card to the switch modules in the CO LAN to support the SLR feature.

Figure 3-9 Redundancy from Gateway to switch modules



The Gateway cards connect to the switch modules in the CO LAN in a redundant pattern to eliminate a single point of failure. Table 3-4 lists possible port connections to achieve redundancy.

Table 3-4 Redundant port connections between Gateway and switch modules (Sheet 1 of 2)

Gateway	Switch modules
Gw1P1	Sw1P1
Gw1P2	Sw2P2
Gw2P1	Sw2P1
Gw2P2	Sw1P2
Gw3P1	Sw1P3

Table 3-4 Redundant port connections between Gateway and switch modules (Sheet 2 of 2)

Gateway	Switch modules
Gw3P2	Sw2P4
Gw4P1	Sw2P3
Gw4P2	Sw1P4
...	...

In table 3-4 , each Gateway card connects to two switch modules in the CO LAN to eliminate the single point of failure. An example follows:

- Gateway 1 Port 1 is the active link and Gateway 1 Port 2 is the inactive link.
- A fault occurs in switch module 1.
- Gateway 1 Port 2 becomes the active link and switch module 2 assumes the activities of switch module 1. Traffic flow resumes immediately.

LED indicators

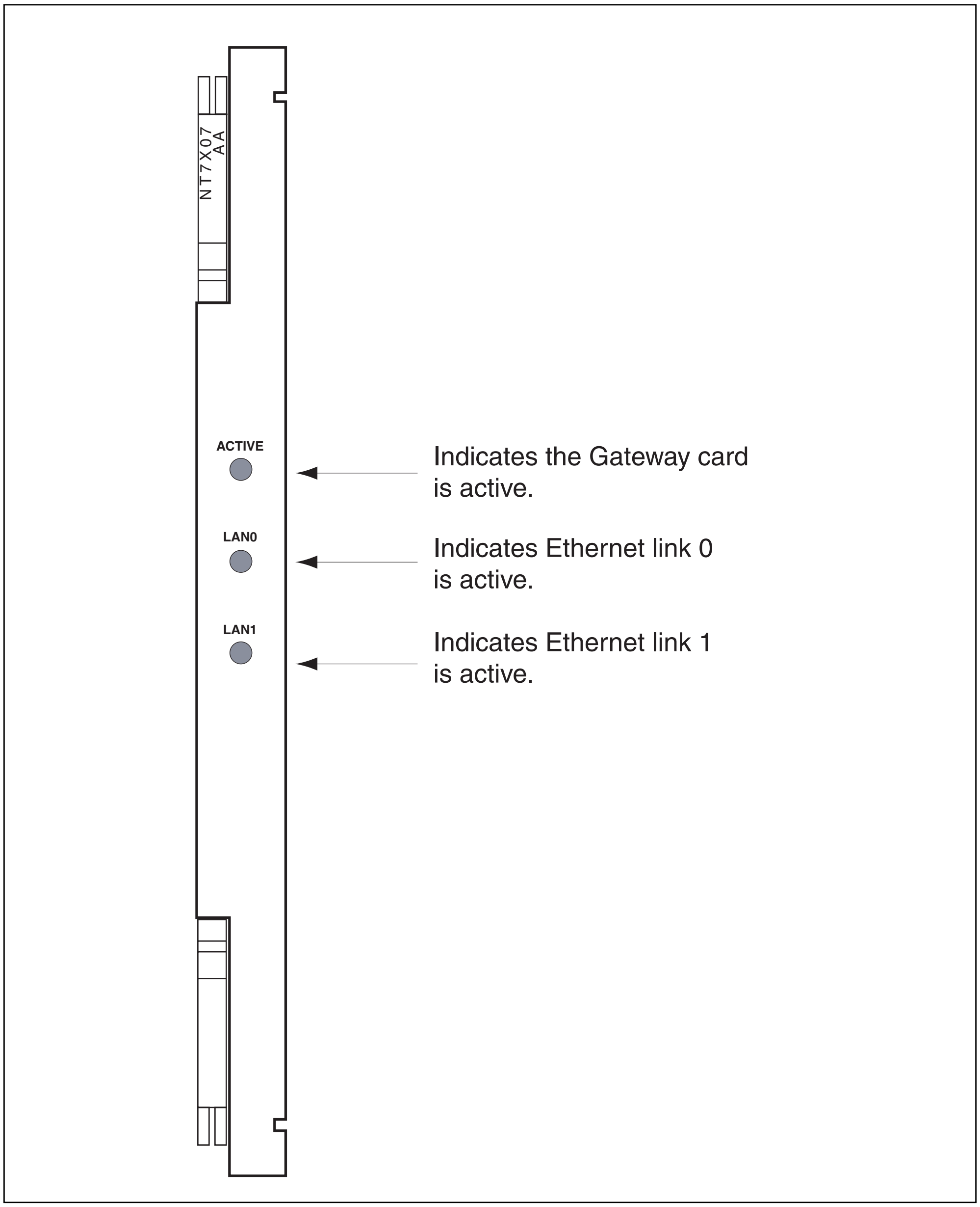
The Gateway faceplate has three LED indicators, which can be lit or blinking. The following table describes the possible Gateway or link states that correspond to the LED states.

Table 3-5 Gateway LED indications

LED	State	Meaning
Active	on	The Gateway card is in service.
Active	off	The Gateway card did not get its load from the DHCP server.
Active	blinking slowly	The Gateway card has its load but is offline.
Active	blinking fast	The Gateway card is ManB or SysB.
LAN 0	on	Ethernet 0 is getting link beat from the hub.
LAN 0	off	Ethernet 0 is not getting link beat from the hub.
LAN 0	blinking	Indicates a Gateway, cable, or hub hardware failure.
LAN 1	on	Ethernet 1 is getting link beat from the hub.
LAN 1	off	Ethernet 1 is not getting link beat from the hub.
LAN1	blinking	Indicates a Gateway, cable, or hub hardware failure.

For more information about the LED states and their indications, see the "Troubleshooting" chapter. The following figure shows the LED indicators on the Gateway card faceplate.

Figure 3-10 LED indicators on Gateway card faceplate



Indicates the Gateway card is active.

Indicates Ethernet link 0 is active.

Indicates Ethernet link 1 is active.

Network fault notification

The Gateway card monitors all network activities that provide the PSTN with a reliable voice path. Therefore, the Gateway makes the real-time decision on whether the network path is viable. The Gateway card notifies the XPM node maintenance subsystem of any network fault or condition that affects the network voice path. The XPM node maintenance subsystem treats the fault notification as a subtending node P-side link failure.

Gateway Sparing

ATTENTION

The Gateway Sparing feature does not apply to the NA012 load. This feature requires the NA013 load.

An LTCI can be provisioned with a total of 10 Gateway cards in slots 1 through 5 on each unit shelf. Only one to four Gateway cards on each shelf can be active. A spare Gateway card (N + 1) can be provisioned on either shelf for reliability. The Gateway Sparing feature allows the spare Gateway card to assume the call processing load of any active Gateway card on the same XPM if one of those active cards fail. If a primary Gateway card fails and a takeover occurs, the spare card maintains any active calls that were on the primary card. Calls in a transient state, such as ringing or dialing, are dropped and must be re-originated. Gateway Sparing does not support feature invocation on calls that have survived a takeover.

Note: A spare Gateway card does not have provisioning data or call processing TIDs assigned to it.

DMS addressing

Each Gateway card is provisioned as a node in the system, which is addressed by a unique node number. Each Gateway node consists of virtual line cards that are addressed by a terminal identifier (TID). The TID consists of the node number and terminal number of the Gateway. The DMS messaging system uses the TID to determine to which physical card to route a message. There is a fixed mapping between the node number and physical card. To allow the call processing load of a Gateway node to be handled by different physical cards, sparing introduces the concept of moving the call processing TIDs of a Gateway node between cards. From a maintenance perspective, there continues to be a fixed mapping between the node number and physical card.

Packet network addressing

From a packet network perspective, all Gateway cards on an XPM in the same Gatekeeper zone must reside on the same subnet. These cards are addressed by a unique IP address for that subnet. Logical IP addresses allow a Gateway card to map two IP addresses to its network interface.

The two IP address are as follows:

- physical IP
  - — received at boot time from the DHCP
  - — always remains the same for each card
- logical IP
  - — used for communication with other LAN endpoints
  - — exists only for primary Gateways
  - — moves between cards as takeover occurs

Note: For a complete description of the Gateway Sparing feature, refer to the “DMS maintenance” chapter.

Power requirements

Power requirements for the Gateway card are provided in the following table.

Table 3-6 Gateway power requirements

Parameter	Minimum	Typical	Maximum	Units
Input supply voltage	-36	-48	-75	Vdc
Input to output isolation voltage			1500	Vdc
Input isolation capacitance		2500		pF
Input current (V_{in} = 48 Vdc, I_{out} = 1.0 Adc)		0.9	2.5	Adc
Inrush current			1.0	A^2s
Input reflected ripple (5Hz to 20 MHz)		5		mA_{p-p}
Input ripple rejection (120 Hz)		60		dB
Calculated MTBF	2,600,000			hr

4 Packet Telephony Manager

Overview

The Packet Telephony Manager (PTM) is a web-based subnetwork management system. Through the PTM interface, you can remotely monitor and maintain the Centrex IP network components. The PTM system uses standard Simple Network Management Protocol (SNMP) messaging to communicate with the managed nodes in the IP network. The managed nodes for Release 2 are the Gatekeeper, the Gateway, and the Terminal Proxy Server (TPS).

The five key areas of network management defined by the International Organization for Standardization (ISO) are fault, configuration, accounting, performance, and security (FCAPS). The PTM system provides the interface for performance, fault, and security management functions for Centrex IP in Release 2.

The PTM system consists of the following components:

- Java-based graphical user interface (GUI) for management of the IP network
- Java-based web server
- remote method invocation (RMI) server to provide socket permissions to the clients
- SNMP server
- trap handler to store SNMP notifications generated by network elements

Functional capabilities

The following is a list of the PTM system's capabilities for Release 2:

- manages the Gatekeeper, including Gatekeeper's view of the H.323 clients
- provides information on the Gateways registered to the Gatekeeper
- provides information on unregistered Gateways
- provides information on the TPS
- collects and displays trap information

- displays Quality of Service (QoS) metrics
- displays Gatekeeper alarms
- performs element management tests

Security management

The PTM system records the traps generated when a security event happens on the Gatekeeper. A trap occurs when a terminal authentication fails during registration and admission with the Gatekeeper. The PTM receives these security notifications from the Gatekeeper as follows:

- RAS registration reject
- RAS admission reject

Note: See the "Gatekeeper" chapter for more information about the authentication feature.

Requirements

The following sections describe the PTM system software and hardware requirements. The PTM software can reside on the Gatekeeper or on another web server.

Web server

If the PTM software resides on a server other than the Gatekeeper, the minimum software and hardware requirements are as follows:

- 400 MHz Pentium II or above
- 256 Mbyte RAM
- 200 Mbyte of hard disk space
- Windows NT 4.0 (Service Pack 3 or later)
- Java Runtime Environment (JRE) 1.2.2 plug-in for server components
- Display with minimum 1024 x 768 resolution
- Network connection 10/100 Mbit/s

Client workstation

The following list describes the PTM client requirements:

- 300 MHz Pentium II or above
- 128 Mbyte RAM
- 200 Mbyte of hard disk space

- Windows NT 4.0 or Windows 95/98
- Web browser: Netscape 4.6 or Internet Explorer 4.01
- JRE 1.2.2 plug-in
- Display with minimum 1024 x 768 resolution
- Network connection 10/100 Mbit/s

Limitations and restrictions

The following limitations and restrictions apply to the PTM:

- Due to memory requirements, the PTM client application should not run on the same computer that the Gatekeeper application is running on.
- The RMI registry server port number is 8383. If this port number is already allocated, the RMI registry fails to initialize and users cannot log into the PTM. See the PTM release notes for Release 2 on your software CD for instructions on how to resolve the port conflict.
- The PTM does not currently support Release Call on calls through a Network Address Translator (NAT). A NAT is typically used as part of a firewall to separate an internal network from an external network. A NAT translates a terminal's IP address and port number to a different IP address and port number. If a NAT is used on a call that is queried using the DN Search feature, then the terminal's true IP address and port number is unknown to the PTM. Only the NAT's view of the terminal's IP address and port number is visible on the PTM.
- For a MADN call, if the active call leg (the one with the speech path) is released using the Release Call feature, the associated call legs are also released. If an associated call leg is released, the corresponding active call leg is not released.

Installation

The PTM server software comes preinstalled on the Gatekeeper. However, the PTM can run be installed on a server other than the Gatekeeper. PTM installations and upgrades are accomplished using the Centrex IP Install Shield. Refer to the *Centrex IP Upgrade Guide*, 297-5231-590 for more information.

After the PTM installation is complete and the PTM server has rebooted, the PTM software runs automatically in the background as a Windows NT service.

The client PC requires the JRE 1.2.2 plug-in to view the PTM application. The JRE 1.2.2 plug-in is downloaded from the PTM home page. If your browser is

Internet Explorer, the JRE 1.2.2 plug-in is launched automatically after download. If your browser is Netscape, see the following procedure.

> ***Note:*** Only the latest version of the JRE plug-in is available using the following procedure.

Procedure 4-1 Download the JRE 1.2.2 plug-in

At the client PC

1 Go to the PTM home page. (See the system administrator for the correct HTTP address.)

2 From the PTM home page, click on “Element Manager” in the menu column.

If you don’t have the JRE 1.2.2 plug-in, you are prompted to click a link to the java.sun.com web site.

3 From the java.sun.com web page, choose the link

```
Java 2 Runtime Environment Windows 95/98/NT Production
Release
```

4 Download the English version of the Java Runtime Environment.

5 Go to the folder where you saved the JRE executable file and double-click the executable icon to install the JRE plug-in.

The executable file automatically configures your browser for the JRE plug-in.

PTM background

The PTM system communicates with its managed nodes using the network management standard, SNMP. SNMP is an application layer protocol that allows remote management of networked devices. SNMP consists of a master agent and several subagent software processes. The master agent is the central process that receives and routes the SNMP requests. The master agent also performs the authentication, authorization, access control, and privacy functions for the management application, based on a configuration file. The master agent forwards the SNMP requests to the appropriate subagents. The subagents interface with the managed objects to respond to the SNMP requests. An example of an SNMP request is GET, which is a request for information. In addition, the subagents generate event reports in the form of SNMP notifications for the management application.

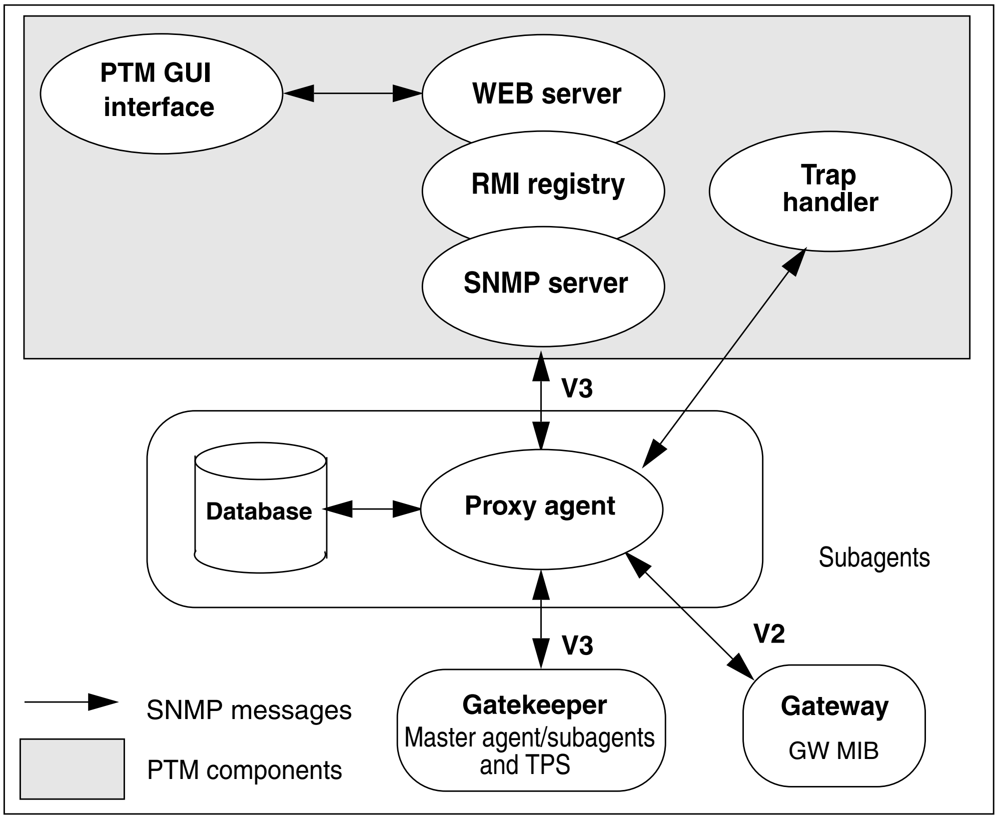
In SNMP, a managed node is referred to as an object. The managed objects have definitions that are stored in a management information base (MIB). A MIB is a specification containing definitions of managed information. The PTM system and the managed nodes use these definitions to monitor and maintain the network elements. Each managed object in the MIB has a unique name called an object identifier (OID). The PTM system contains several MIBs, at least one for each managed node in the network.

The SNMP subagents use the SNMP MIB converter to translate the SNMP messages into maintenance actions. A separate trap event server translates messages from the Gatekeeper into SNMP notifications, which can also be maintenance actions. A maintenance action can include the following:

- retrieve information on an H.323 endpoint (terminal or Gateway)
- force the release of a call
- show status of the Gatekeeper
- generate SNMP notifications

The PTM system components are shown in the figure that follows. The RMI registry server provides transparent access to the remote clients. The Java applets downloaded to the client interface make RMI calls to the SNMP manager to perform SNMP functions.

Figure 4-1 PTM components and messaging interfaces



The PTM system uses a proxy agent that allows the SNMP server to communicate with the SNMP subagents running on the call processing devices. The proxy agent acts as the single point of access between the Gatekeeper and Gateway subagents and the SNMP server. The proxy agent converts the different versions of SNMP (v1, v2, and v3) to the appropriate version used by the managed object.

> ***Note:*** Ensure the SNMP values for the PTM port and the Microsoft port do not match. You must enter 161 for the PTM SNMP port. However, the Microsoft SNMP value for the Gatekeeper can be any unused port number. The recommenced SNMP default value for the Gatekeeper is 8161.

User interface

To access the PTM application, contact your system administrator for the correct HTTP address. You will also need a user name and password. The PTM application is launched from the HTTP address using a web browser. The following sections describe the screens and menus of the PTM user interface.

Login procedure

Use the following procedure to access the PTM user interface.

Procedure 4-2 Log in to the PTM system

At the PTM workstation

1 From the PTM web page, click “Element Manager” in the menu column.

The PTM Login window opens.

2 From the Login window, type your user name and password in the appropriate fields and click Enter.

The Centrex IP Management window opens.

3 From the Navigation tree on the left side of the window, click once on the plus icon to the left of the Gatekeeper folder, or click twice on the Gatekeeper folder.

The list of Gatekeepers displays underneath the folder.

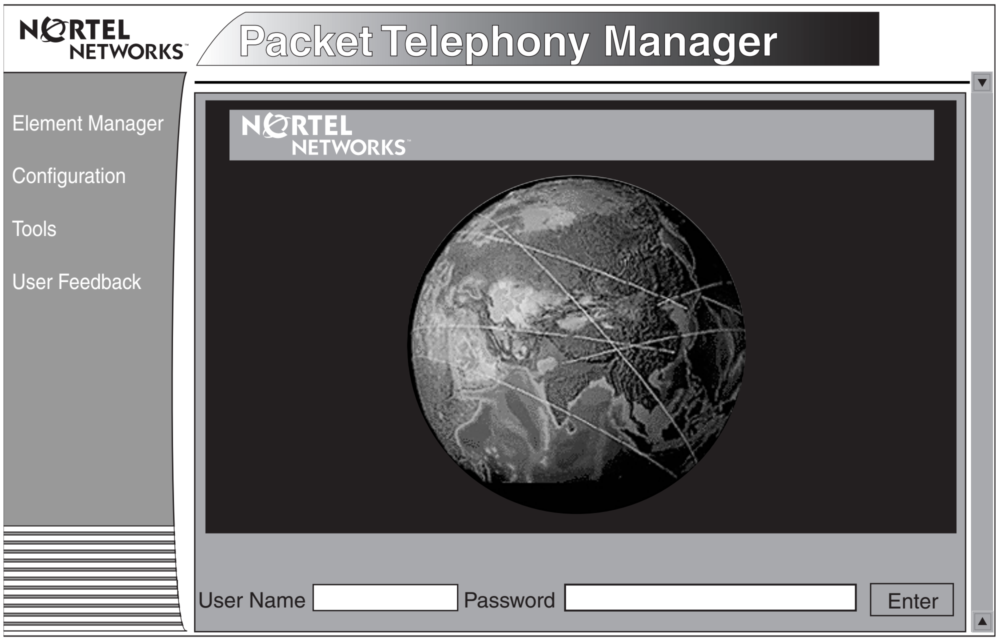
> ***Note:*** The first time the PTM application is launched after installation, there are no elements listed beneath the Network folder. See the section “Configuration menu functions” to add nodes to the network.

4 Click once to select the Gatekeeper that you want to view.

The status bar indicates “Ready.” All fields are updated to show data for that Gatekeeper.

The following figure shows the PTM login window.

Figure 4-2 PTM login window



Menu Bar

After login, the Centrex IP Management window opens. You can navigate to other windows from the Menu Bar at the top of the window, or from the Navigation tree at the left of the window.

The following table describes the functions of the pull-down menus in the Menu Bar.

Table 4-1 Pull-down menus

Menu	Description
File	File-Close closes the active window. File-Exit exits the PTM application.
Fault	Contains four cascading menus: PTM Tests, GK Tests, GW Tests, and Remote Maintenance. These menus are described in the section “Fault menu functions.”
Performance	Allows access to the Element Manager window, the Event History Manager window, and the Quality of Service Browser.
Configuration	Provides the following functions: • Adds additional nodes, such as a Gatekeeper, Gateway, or TPS to the Navigation tree. • Allows device name change and device deletion. • Enables user name security functions (Add user, Delete user, Change password). ***Note:*** You must have administrative privileges to add or delete users.
Help	Contains PTM Help files and the version of the PTM software.

Below the Menu Bar are two buttons. The PTM software displays the Menu Bar and the Button Bar at the top of each screen. The following table lists the buttons and their functions.

Table 4-2 Screen buttons

Button	Description
DN Search	Launches the Find Directory Number window. If one window is already open, a second window will open.
Refresh	Refreshes the data on the current screen. This button is active at all times except when the PTM is in the middle of a refresh activity.

Navigation tree

The PTM Navigation tree shows the elements that are on the network. This panel is displayed to the left of the element windows. An element is a node such as a Gatekeeper, Gateway, or TPS. The hierarchy of the tree shows the user the Gatekeepers that are configured on the network and which Gateways are registered to the Gatekeepers. The registered Gateways are directly underneath the Gatekeeper to which they belong. This allows the user to quickly identify a Gateway's subnet for troubleshooting purposes. Unregistered Gateways are listed under a separate folder. The terminal proxy servers are also listed under a separate folder. See the section "Configuration menu functions" in this chapter for information on how to add a device to the Navigation tree.

Display messages

The PTM GUI provides the user with dialog boxes for the following types of messages:

- information messages, which display descriptive, directional information
- warning messages
- configuration messages, which provide a choice for a given activity
- error messages, which display fault-related activity information
- customized messages, which display more descriptive error information

All of these messages are modal dialog boxes. The user must close each box to proceed with PTM functions.

Fault menu functions

The Fault menu contains maintenance and testing functions. The content of the Fault menu is determined by the network element selected on the Navigation tree. The Fault menu functions are listed as follows:

- View Element Alarms—A Gatekeeper must be selected in the Navigation tree in order for this menu item to appear. Selecting this menu item opens the Alarm Manager window.
- PTM Tests—This submenu contains three network management tools: Ping Test, Traceroute Test, and Continuity Test. These tools allow the user to initiate a Ping, TraceRoute, or Continuity test from the PTM to a node on the network.
- GK Tests—This submenu allows the user to initiate a Ping or Traceroute test from a managed Gatekeeper.

- GW Tests—This submenu allows the user to initiate a Ping test from a managed Gateway and to run diagnostic tests on a Gateway.
- Remote Maintenance—This submenu allows the user to shut down the Gatekeeper, switch activity, or to enable and disable a switch of activity on the Gatekeeper from the PTM.

The following sections describe the windows that perform the Fault menu functions.

Alarm Manager

The Fault menu contains the View Element Alarms selection only when a Gatekeeper is selected in the Navigation tree. Selecting View Alarms opens the Alarm Manager window. There are five alarm types that a Gatekeeper can raise and clear, as follows:

- critical (red)
- major (orange)
- minor (yellow)
- warning (clear)
- clear alarm (not displayed)

> ***Note 1:*** For Release 2, only the Gatekeeper can send alarms to the PTM server.
>
> ***Note 2:*** See the “Troubleshooting” chapter for more information about Gatekeeper alarms.

The Gatekeeper sends an alarm message to the PTM server until the PTM server returns an acknowledgment message that the alarm notification was received. Each alarm has a unique identifier (ID). The Alarm Manager stores the alarm IDs in an alarm table on the PTM server.

Alarms are cleared when the Gatekeeper sends a clear alarm message to the PTM server. The PTM server searches the alarm table for the alarm’s unique ID and deletes it.

The PTM server uses a heartbeat query to determine if the Gatekeeper is in service. If a NULL message is returned, the Gatekeeper is in-service. If the Gatekeeper does not respond to the heartbeat query after two tries, a critical alarm is raised and the Gatekeeper is marked “state unknown.” The PTM server continues to send the query, however, and when it receives a response, the critical alarm is cleared. When the successful query is performed, the Gatekeeper’s alarm table is uploaded to the PTM server.

The Alarm Manager consists of four panels, as follows:

- Alarm Retrieval Criteria
- alarm list
- Element Alarm Counts
- Details of Selected Alarm

The top panel contains the Alarm Retrieval Criteria. This panel allows you to search for a specific alarm based on the date, severity, and category of the alarm. The alarm categories indicate the possible cause of the alarm. The Restore All button restores the default retrieval selections. The second panel contains the alarm list where the active alarms are displayed. The third panel contains the Element Alarm Counts. This panel allows you to view the number of each type of alarm on the selected element. The bottom panel shows the alarm details of an alarm selected in the alarm list.

Procedure 4-3 View alarms with the Alarm Manager

At the PTM workstation

1 Select a Gatekeeper in the Navigation tree.

2 From the Fault menu, select View Alarms.

The Alarm Manager window opens. If there are no alarms, a dialog box opens with the message "Unable to load the Alarm Manager because no alarms exist in the alarm table for this element."

3 Enter the filter criteria, such as the date, the alarm severity, and the category of alarm.

4 Select the maximum number of alarms to be displayed from the pull-down menu. The default is All.

5 Click the Retrieve button.

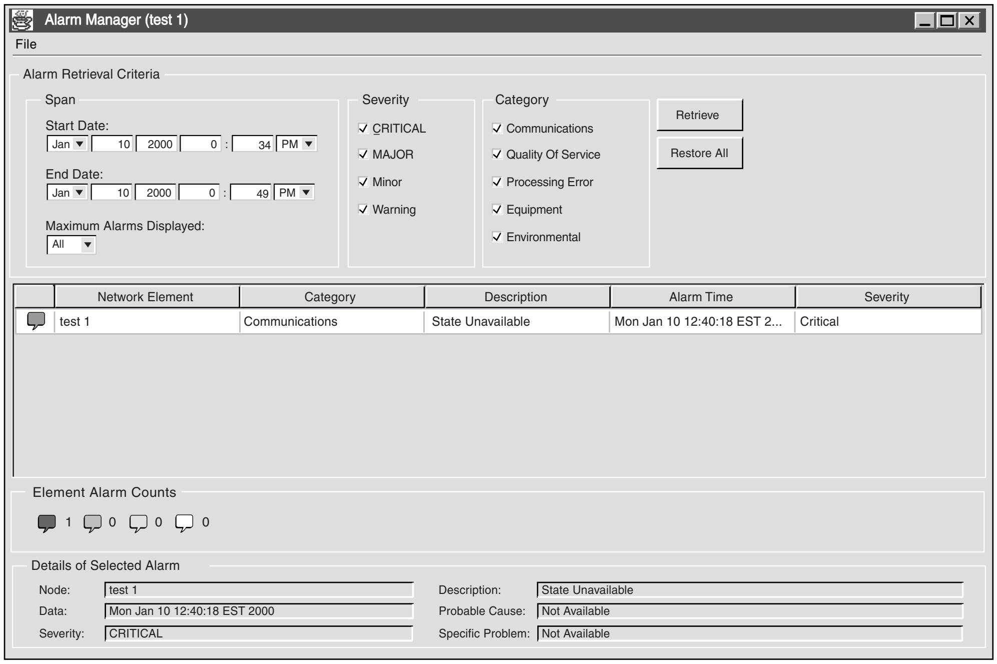
The active alarms for that Gatekeeper are displayed in the alarm list. The alarm list is updated dynamically when new alarms are raised.

6 To view further details for a specific alarm, select the alarm in the alarm list.

The fields in the Details of Selected Alarm panel are populated.

The following figure shows the Alarm Manager window.

Figure 4-3 Alarm Manager



Alarm Manager (test 1)

File

Alarm Retrieval Criteria

Span

Start Date: Jan 10 2000 0 : 34 PM

End Date: Jan 10 2000 0 : 49 PM

Maximum Alarms Displayed: All

Severity

- ☑ CRITICAL
- ☑ MAJOR
- ☑ Minor
- ☑ Warning

Category

- ☑ Communications
- ☑ Quality Of Service
- ☑ Processing Error
- ☑ Equipment
- ☑ Environmental

	Network Element	Category	Description	Alarm Time	Severity
	test 1	Communications	State Unavailable	Mon Jan 10 12:40:18 EST 2...	Critical

Element Alarm Counts

1 0 0 0

Details of Selected Alarm

Node:	test 1	Description:	State Unavailable
Data:	Mon Jan 10 12:40:18 EST 2000	Probable Cause:	Not Available
Severity:	CRITICAL	Specific Problem:	Not Available

PTM Tests

The PTM Tests menu provides the default diagnostic tests that are available from the Fault menu when no element is selected. This menu contains three network diagnostic tools that the user can initiate on a Gatekeeper from the PTM. These are described in the following sections.

PTM Ping Test

The PTM Packet InterNet Groper (Ping) Test window allows the user to determine if a node on the network is active. PTM Ping uses Internet control message protocol (ICMP) messages to determine the round-trip time (RTT) between the node sending the Ping and the target node. The RTT is the time in milliseconds for a Ping packet to travel to and from the PTM and the managed node.

A Ping test can provide the following information:

- the number of packets that have been dropped, duplicated, or reordered
- a checksum to detect if packets are damaged
- a timestamp to determine the RTT
- ICMP messages that may indicate problems on the target end

A Ping test cannot tell you why a packet was delayed, damaged, or duplicated. It cannot provide the reason some packets may go unanswered, or where a problem occurred.

The PTM Ping window contains several components, which are described in the following tables. The PTM Ping selection panel table lists the components in the top panel of the PTM Ping window.

Table 4-3 PTM Ping selection panel

Component	Description
Select Target Nodes	Allows the user to enter the IP address of a destination IP address not configured on the PTM.
Add Address button	Adds the user-defined address of the node to be tested to the list of PTM Ping Target Nodes.
Configured Nodes	Shows the list of nodes that were configured at the time the PTM Ping Test window was launched.
Update Config List	Updates the Configured Nodes list to include all nodes currently configured on the network.
Add Selected button	Adds the selected configured nodes to the list of nodes to be tested.
PTM Ping Target Nodes	Shows the list of nodes that were selected for the PTM Ping Test. The maximum number of nodes that can be selected at a time is 24.
Clear Selected button	Clears the selected nodes from the list of nodes to be tested.
Clear All button	Clears all nodes from the list of nodes to be tested.
Start button	Starts the Ping test on the list of nodes to be tested. Selecting the Start button clears the previous test results and begins the Ping test sequentially through the list of target nodes. After completing a Ping test, the tool pauses the amount of time designated by the Target Node Ping Delay field, and then resumes the diagnostic of the next node in the list of nodes to be tested.
Stop button	Stops the test after the current Ping test is completed.

The following table describes the fields in the PTM Ping Test Attributes panel.

Table 4-4 PTM Ping Test Attributes

Field	Description
Number of Packets	Specifies the number of ICMP echo requests to send to each node that is being tested. The range of values is from 1 to 5 packets. The default value is 2.
Target Node Ping Delay	Specifies the delay between completing a Ping test on a node and starting a Ping test on the next node in the list. Possible values are 1 s, 30 s, 1 min, 5 min, 10 min, and 30 min.
Packet Size	Specifies the size of the ICMP packets to be used during a Ping test. Possible values are 32, 64, 128, 256, and 512 bytes.

The results of the Ping test are displayed in the Test Output panel. To clear output in this panel, click the Clear Output button at the bottom of the window. Use the following procedure to perform a PTM Ping Test.

Procedure 4-4 PTM Ping Test

At the PTM workstation

1 From the Fault menu, select PTM Tests->PTM Ping.

The PTM Ping Test window opens.

2 Select a node from the Configured Nodes list. You can select multiple nodes by pressing the Ctrl key and clicking on each node. You can select a consecutive group of nodes by clicking on the first node, pressing the Shift key and then clicking on the last node. All nodes between the first and last node are selected.

3 Click the Add Selected button.

The selected nodes are added to the PTM Ping Target Nodes list.

4 If a desired node is not in the Configured Nodes list, add the IP address of the node to be tested in the Select Target Nodes input field. Click the Add Address button.

The node’s IP address is added to the PTM Ping Target Nodes list.

5 Select the PTM Ping Test Attributes from the pull-down menus or leave the default values.

6 Make sure the information in the PTM Ping Target Nodes list and the PTM Ping Test Attributes fields is correct.

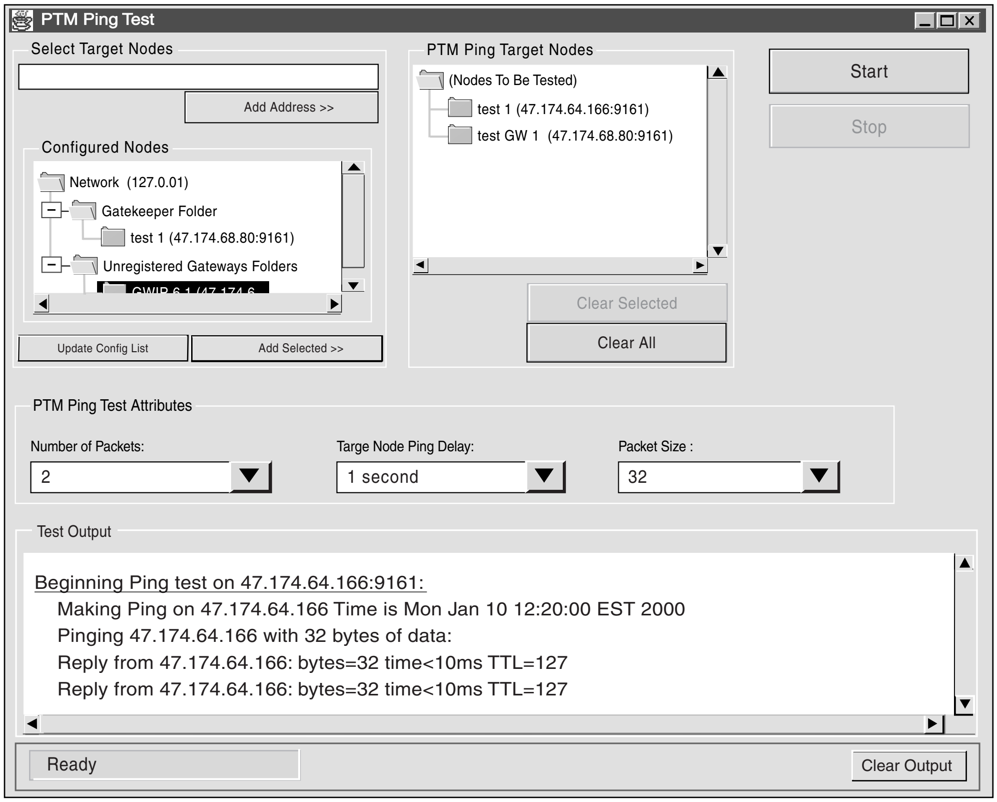
7 Click the Start button to begin the Ping test on the selected target nodes.

The Ping test proceeds sequentially through the PTM Ping Target Nodes list. The progress bar at the bottom of the window shows the percentage of *terminals that have been tested. The PTM Ping test results appear in the Test Output panel.*

8 When the test is complete, the Test Output panel can be cleared by clicking the Clear Output button or by starting a second test.

The following figure shows the PTM Ping Test window.

Figure 4-4 PTM Ping Test window



Number of Packets: 2

Targe Node Ping Delay: 1 second

Packet Size : 32

```
Beginning Ping test on 47.174.64.166:9161:
   Making Ping on 47.174.64.166 Time is Mon Jan 10 12:20:00 EST 2000
   Pinging 47.174.64.166 with 32 bytes of data:
   Reply from 47.174.64.166: bytes=32 time<10ms TTL=127
   Reply from 47.174.64.166: bytes=32 time<10ms TTL=127
```

PTM Traceroute Test

The PTM Traceroute Test window allows the user to trace the route from any managed node to another IP address. The results of the Traceroute test are reported back to the PTM. The PTM Traceroute Test window is identical to the PTM Ping Test window, with the exception that it contains only one test attribute field, Target Node Test Delay. For PTM Traceroute Test, the Target Node Test Delay field has the same values as the PTM Ping Test. Use the following procedure to perform a PTM Traceroute Test.

Procedure 4-5 PTM Traceroute Test

At the PTM workstation

1 From the Fault menu, select PTM Tests->PTM Traceroute.

The PTM Traceroute Test window opens.

2 Select a node from the Configured Nodes list. You can select multiple nodes by pressing the Ctrl key and clicking on each node. You can select a consecutive group of nodes by clicking on the first node, pressing the Shift key and then clicking on the last node. All nodes between the first and last node are selected.

3 Click the Add Selected button.

The selected nodes are added to the Traceroute Target Nodes list.

4 If a desired node is not in the Configured Nodes list, add the IP address of a node to be tested in the Select Target Nodes input field. Click the Add Address button.

The node's IP address is added to the Traceroute Target Nodes list.

5 Select the time interval to pause between tests from the Target Node Test Delay pull-down menu. The possible values are 1 s, 30 s, 1 min, 5 min, 10 min, 30 min.

6 Make sure the information in the Traceroute Target Nodes list and the Target Node Test Delay field is correct.

7 Click the Start button to begin the Traceroute test on the selected target nodes.

The Traceroute test proceeds sequentially through the Traceroute Target Nodes list. The progress bar at the bottom of the window shows the percentage of terminals that have been tested. The test results appear in the Test Output panel.

8 When the test is complete, the Test Output panel can be cleared by clicking the Clear Output button or by starting a second test.

PTM Continuity Test

The PTM Continuity Test window allows the user to validate the continuity between the PTM and a managed node, such as the Gatekeeper, the Gateway, or the terminal proxy server (TPS). This test allows the user to determine where a communication failure is occurring related to a managed node. The PTM Continuity Test window is similar to the other PTM diagnostic windows. The differences are the Continuity Test Attributes and there is no Add Address function, because the Continuity Test can only be performed on configured nodes. The Continuity Test Attributes are described in the following table.

Table 4-5 Continuity Test Attributes

Field	Description
Test Scope	Specifies which tests to perform. The values are • Validate Routing Data—performs a Ping test on the managed node and attempts to validate the integrity of the routing data in the Proxy Agent database. • Continuity to Application—performs a Ping test and attempts to contact the application running on the managed node and get a response from the managed node. This is the default value. • All Tests—performs both of the above tests.
Target Node Test Delay	Specifies the delay between completing a test on a node and starting a test on the next node in the list. Possible values are 10 s, 30 s, 1 min, 5 min, 10 min, and 30 min. The default value is 30 s.
Output Detail	Specifies the level of output to be displayed. The values are Verbose (more detail) or Terse (less detail). The default value is Terse.

When the Test Scope is All Tests, the PTM Continuity Test initiates the following sequence of tests:

- Performs a Ping test from the PTM to a managed node. The Ping test results are displayed in the Test Output panel.
- Sends SNMP messages to the Proxy Agent to validate that the Proxy Agent is in service.
- Sends SNMP messages to the Proxy Agent to check the relationship between the Proxy Agent routing tables for the selected node.
- Sends SNMP messages to the managed node to verify a connection through the Proxy Agent to the application on the managed node (Gatekeeper, Gateway, or TPS).

Use the following procedure to perform a PTM Continuity Test.

Procedure 4-6 PTM Continuity Test

At the PTM workstation

1 From the Fault menu, select PTM Tests->Continuity Test.

The Continuity Test window opens.

2 Select a node from the Configured Nodes list. You can select multiple nodes by pressing the Ctrl key and clicking on each node. You can select a consecutive group of nodes by clicking on the first node, pressing the Shift key and then clicking on the last node. All nodes between the first and last node are selected.

3 Click the Add Selected button.

The selected nodes are added to the Continuity Test Target Nodes list.

4 Select the desired Continuity Test Attributes from the pull-down menus or leave the default values.

5 Make sure the information in the Continuity Test Target Nodes list and the Continuity Test Attributes fields is correct.

6 Click the Start button to begin the Continuity test on the selected target nodes.

The test proceeds sequentially through the Continuity Test Target Nodes list. The progress bar at the bottom of the window shows the percentage of terminals that have been tested. The test results appear in the Test Output panel.

7 When the test is complete, the Test Output panel can be cleared by clicking the Clear Output button or by starting a second test.

GK Tests

The GK Tests menu is active when the user selects a Gatekeeper in the Navigation tree. This menu contains two network tools that initiate a remote Gatekeeper Ping or Traceroute test from a managed Gatekeeper. These are described in the following sections.

GK Remote Ping Test

The Remote Ping Test window is identical to the PTM Ping Test window. The difference is where the Ping originates from. In PTM Ping, the Ping test originates from the PTM Proxy Agent. In Remote Ping, the Ping test originates from a Gatekeeper.

Use the following procedure to perform a remote Ping test from a Gatekeeper.

Procedure 4-7 GK Remote Ping Test

At the PTM workstation

1 Select the Gatekeeper that you want to Ping from in the Navigation tree. From the Fault menu, select GK Tests->GK Remote Ping.

The Remote Ping Test window opens. The remote Ping originator is displayed in the title bar.

2 Select a node from the Configured Nodes list. You can select multiple nodes by pressing the Ctrl key and clicking on each node. You can select a consecutive group of nodes by clicking on the first node, pressing the Shift key and then clicking on the last node. All nodes between the first and last node are selected.

3 Click the Add Selected button.

The selected nodes are added to the Remote Ping Target Nodes list.

4 If a desired node is not in the Configured Nodes list, add the IP address of a node to be tested in the Select Target Nodes input field. Click the Add Address button.

The node's IP address is added to the Remote Ping Target Nodes list.

5 Select the Remote Ping Test Attributes from the pull-down menus or leave the default values.

6 Click the Start button to begin the Remote Ping test on the selected target nodes.

The Remote Ping test proceeds sequentially through the Remote Ping Target Nodes list. The progress bar at the bottom of the window shows the percentage of terminals that have been tested. The Remote Ping test results appear in the Test Output panel.

7 When the test is complete, the Test Output panel can be cleared by clicking the Clear Output button or by starting a second test.

GK Remote Traceroute Test

The Remote Traceroute Test window is identical to the PTM Traceroute Test window. The difference is where the Traceroute originates from. In PTM Traceroute, the Traceroute test originates from the PTM Proxy Agent. In Remote Traceroute, the Traceroute test originates from a Gatekeeper.

Use the following procedure to perform a remote Traceroute test from a Gatekeeper.

Procedure 4-8 Remote Traceroute Test

At the PTM workstation

1 Select the Gatekeeper that you want to Traceroute from the Navigation tree. From the Fault menu, select GK Tests->GK Remote Traceroute.

The Remote Traceroute Test window opens. The remote Traceroute originator is displayed in the title bar.

2 Select a node from the Configured Nodes list. You can select multiple nodes by pressing the Ctrl key and clicking on each node. You can select a consecutive group of nodes by clicking on the first node, pressing the Shift key and then clicking on the last node. All nodes between the first and last node are selected.

3 Click the Add Selected button.

The selected nodes are added to the Remote Traceroute Target Nodes list.

4 If a desired node is not in the Configured Nodes list, add the IP address of a node to be tested in the Select Target Nodes input field. Click the Add Address button.

The node's IP address is added to the Remote Traceroute Target Nodes list.

5 Select the time interval to pause between tests from the Target Node Test Delay pull-down menu. The possible values are 1 s, 30 s, 1 min, 5 min, 10 min, 30 min.

6 Make sure the information in the Remote Traceroute Target Nodes list and the Target Node Test Delay field is correct.

7 Click the Start button to begin the Remote Traceroute test on the selected target nodes.

The Remote Traceroute test proceeds sequentially through the Remote Traceroute Target Nodes list. The progress bar at the bottom of the window shows the percentage of terminals that have been tested. The test results appear in the Test Output panel.

8 When the test is complete, the Test Output panel can be cleared by clicking the Clear Output button or by starting another test.

GW Tests

The GW Tests menu is active when the user selects a Gateway in the Navigation tree. The GW Tests menu supports the following maintenance actions:

- Request a Ping from a selected remote Gateway card to selected nodes on the network.
- Perform internal diagnostic tests on a remote Gateway card.

The GW Test diagnostics are described in the following sections.

GW Remote Ping Test

The GW Remote Ping submenu displays the GW Remote Ping window. This window supports the following maintenance actions:

- Configure a Ping test for a remote Gateway card.
- Run a Ping test from a remote Gateway card.
- View the results of a Ping test from a remote Gateway card.

The GW Remote Ping window is identical to the other Ping Test windows with the exception of one of the Remote Ping Test Attributes. Instead of the Packet

Size attribute, this test has an Automated Force Options test attribute. The following table contains a description of this field.

Table 4-6 Automated Force Options

Field	Description
Automated Force Options	A force can occur when one PTM client session takes over the activities of another PTM client session. A force can be necessary when a PTM client session does not finish a process. For example, a PTM client session can end before a Gateway finishes a Ping. The PTM supports manual force and automated force. This field has the following options. • Request Manual Force—generates a dialog box if a force is needed. This is the default value. • Enable Automated Force—allows one PTM client session to automatically take over the activities of another PTM client session. • Disable Automated Force—disables automated force. One PTM session client *cannot* take over the activities of another PTM client session.

Use the following procedure to perform a Ping from a remote Gateway card to other nodes on the network.

Procedure 4-9 Perform a Ping from a remote Gateway card

From the PTM

1 Select the Gateway card that is the source of the Ping from the Navigation tree.

2 From the Fault menu, select GW Tests->GW Remote Ping.

The GW Remote Ping Test window opens.

3 Select a node from the Configured Nodes list. You can select multiple nodes by pressing the Ctrl key and clicking on each node. You can select a consecutive group of nodes by clicking on the first node, pressing the Shift key and then clicking on the last node. All nodes between the first and last node are selected.

4 Click the Add Selected button.

The Remote Ping Target Nodes list displays the selected nodes.

5 If a desired node is not in the Configured Nodes list, add the IP address of a node to be tested in the Select Target Nodes field, and click the Add Address button.

The Remote Ping Target Nodes list displays the node.

6 Select the Remote Ping Test Attributes from the pull-down menus or leave the default values.

7 Make sure the information in the Remote Ping Target Nodes list and the Remote Ping Test Attributes fields is correct.

8 Click the Start button to begin the Ping test on the selected nodes.

The test proceeds sequentially through the Remote Ping Target Nodes list. The progress bar at the bottom of the window shows the percentage of nodes that have been tested. The test results display in the Test Output panel.

9 When the test is complete, the Test Output panel can be cleared by clicking the Clear Output button or by starting another test.

GW Diagnostics

The GW Diagnostics window supports the following maintenance actions:

- Configure a diagnostic test for a remote Gateway card.
- Run a diagnostic test from a remote Gateway card.
- View the results of a diagnostic test from a remote Gateway card.

The GW Diagnostics window is identical to the GW Remote Ping Test window with the exception that it has only two of the Test Attributes and there is no Add Address function. Only configured nodes can be tested. The two test attributes are Target Node Test Delay and Automated Force Options. These are described in the previous diagnostic sections. Use the following procedure to perform a diagnostic test on a Gateway card.

Procedure 4-10 Perform a diagnostic test on a Gateway card

From the PTM

1 Select a configured Gateway card to test from the Navigation tree.

2 From the Fault menu, select GW Tests->GW Diagnostics.

The GW Diagnostics window opens.

3 Select the desired Gateway cards to test from the Configured Gateway Nodes list. You can select multiple nodes by pressing the Ctrl key and clicking on each node. You can select a consecutive group of nodes by clicking on the first node, pressing the Shift key and then clicking on the last node. All nodes between the first and last node are selected.

4 Click the Add Selected button.

The GW Diagnostic Target Nodes list displays the node.

5 Select the GW Diagnostic Test Attributes from the pull-down menus or leave the default values.

6 Make sure the information in the GW Diagnostic Target Nodes list and the GW Diagnostic Test Attribute fields is correct.

7 Click the Start button to begin the diagnostic test on the selected nodes.

The test proceeds sequentially through the GW Diagnostic Target Nodes list. The progress bar at the bottom of the window shows the percentage of nodes that have been tested. The test results display in the Test Output panel.

8 When the test is complete, the Test Output panel can be cleared by clicking the Clear Output button or by starting another test.

Remote Maintenance

The Remote Maintenance menu supports the following maintenance actions:

- Restart a selected Gatekeeper node.
- Switch activity between Gatekeeper nodes.
- Enable switch of activity on a selected Gatekeeper node.
- Disable switch of activity on a selected Gatekeeper node.

The following table lists the selections in the Remote Maintenance menu.

Table 4-7 Remote Maintenance selection panel

Element	Description
Shut Down Gatekeeper	• Restarts the selected Gatekeeper • Switches activity between Gatekeeper nodes
Enable/Disable Switch Activity and Restart	Enables and disables a switch of activity and restart on the selected Gatekeeper node

Restart a Gatekeeper

Use the following procedure to restart a selected Gatekeeper node from the PTM.

Procedure 4-11 Restart a Gatekeeper

CAUTION
Loss of call information
When a Gatekeeper node restarts, the node loses all information on existing calls. The node sustains existing calls and blocks new calls during the restart.

ATTENTION
The Gatekeeper must be running to perform this procedure. The Gatekeeper cluster software must also be enabled for restart and switch of activity capability from the PTM.

ATTENTION

Options in the Gatekeeper cluster administration software can conflict with changes in restarts and switch of activity. See the section “Restart option for cluster” in the “Gatekeeper” chapter for more information.

From the PTM

1 Select the Gatekeeper node you want to restart.

2 From the General tab, make sure that Switch Activity and Restart Capability is enabled.

3 From the Fault menu, select Remote Maintenance-> Shut Down Gatekeeper.

The Shut Down confirmation window appears The window displays the name of the Gatekeeper node you want to restart.

4 Make sure that the Restart option is selected.

5 Make sure that the Gatekeeper node to be restarted is the Gatekeeper node you want to restart.

6 Click the Yes button.

The Restart Application confirmation window appears.

7 Click the Yes button.

The Gatekeeper node restarts on the same side of the cluster that it currently runs. The restart can take up to 2 minutes.

Switch activity

Use the following procedure to switch activity from the active Gatekeeper node to the inactive Gatekeeper node.

Procedure 4-12 Switch activity on a Gatekeeper node

CAUTION

Loss of call information

When a Gatekeeper node switches activity, the Gatekeeper node loses all information on existing calls. The Gatekeeper node sustains existing calls and blocks new calls during the restart.

ATTENTION

The Gatekeeper node must be in-service to perform this procedure.

From the PTM

1 Select the active Gatekeeper node.

2 From the General tab, make sure that Switch Activity and Restart Capability is enabled.

3 From the General tab, record the Mate IP Address. The Mate IP Address identifies the inactive Gatekeeper node that becomes the active Gatekeeper node.

4 From the Fault menu, select Remote Maintenance-> Shut Down Gatekeeper.

The Shut Down confirmation window appears.

5 Make sure that the Switch Activity from active to inactive GK platform option is selected.

The Switch Activity confirmation window appears.

6 Click the Yes button.

The Gatekeeper switches activity from the active platform to the inactive platform. The switch can take up to 2 minutes.

7 Make sure the switch of activity was successful.

8 Select the newly active Gatekeeper node. Use the Mate IP Address you recorded in step 3 of this procedure. From the General tab, look at the information on the node.

The Gatekeeper screen displays information in all fields.

9 Select the newly inactive Gatekeeper node. From the General tab, look at the information on the node.

The Gatekeeper window displays valid information in the following fields:

- *Name*
- *IP Address*
- *Location*
- *Node System Up Time*
- *Support Contact Information*

The Gatekeeper window displays N/A in all other fields.

Enable switch of activity and restart

Use the following procedure to enable a switch of activity and restart on a Gatekeeper.

Procedure 4-13 Enable switch of activity and restart

From the PTM

1 Select the Gatekeeper node that you want to enable switch of activity and restart.

2 From the General tab, make sure that Switch Activity and Restart Capability is disabled.

3 From the Fault menu, select Remote Maintenance->Enable/Disable Switch Activity and Restart.

The Enable/Disable Switch Activity and Restart window appears.

4 Make sure the Enable option is selected.

5 Click the Yes button.

6 Click the Refresh button.

7 From the General tab, make sure that Switch Activity and Restart Capability is enabled.

Disable switch of activity and restart

Some maintenance activities can need restrictions on shutdowns of the Gatekeeper. For example, an automatic switch of activity during a software upgrade could interrupt service on both nodes of the Gatekeeper. A shutdown includes a restart and switch of activity. A shutdown can be manual.

Use the following procedure to disable a switch of activity and restart on a Gatekeeper.

Procedure 4-14 Disable switch of activity and restart

From the PTM

1 Select the Gatekeeper node that you want to disable switch of activity and restart.

2 From the General tab, make sure that Switch Activity and Restart Capability is enabled.

3 From the Fault menu, select Remote Maintenance->Enable/Disable Switch Activity and Restart.

The Enable/Disable Switch Activity and Restart window appears.

4 Make sure the disable option is selected.

5 Click the Yes button.

6 Click the Refresh button.

7 From the General tab, make sure that Switch Activity and Restart Capability is disabled.

Performance menu functions

The Performance menu allows the user to access the specific element windows and to track the performance of the network. The following windows are available from the Performance menu:

- Element Manager—When the Element Manager window is open, you can select any element in the Navigation tree to go to that element window.
- Event History Manager—This window allows you to view traps that occur on a specific Gatekeeper.
- Quality of Service Browser—This window allows you to view Quality of Service measurements on the voice quality of the network.

The following sections describe the Performance menu windows.

Element Manager functions

The Element Manager is the main PTM window. Using the Navigation tree from within the Element Manager, you can select the following element windows:

- Gatekeeper—This window allows you to view information on the selected Gatekeeper.
- Gateway—This window allows you to view information on the selected Gateway.
- Terminal Proxy Server—This window allows you to view information on the selected terminal proxy server.

The element windows are described in the following sections.

Gatekeeper window

When you select a Gatekeeper in the Navigation tree, the Gatekeeper window opens in the display panel.

In the top section of the Gatekeeper window there are six autopopulated fields. These fields are the Gatekeeper Name, IP Address, Local Date, Status, Cluster IP, and Mate IP. These fields are listed in the following table.

Table 4-8 Autopopulated fields

Field name	Description
Gatekeeper Name	The name of the Gatekeeper.
IP Address	The Gatekeeper’s IP address.
Local Date	Shows the last time the data was refreshed.
Status	Shows the current state of the Gatekeeper.
Cluster IP	Shows the IP address of the Gatekeeper cluster, also known as the virtual IP address. This IP address belongs to the node of the Gatekeeper that is currently active.
Mate IP	Shows the physical IP address of the Gatekeeper’s mate. The Gatekeeper resides in a dual-node cluster. The mate IP address is the standby or inactive node.

The Gatekeeper Status field can show five possible states. These are described in the following table.

Table 4-9 Gatekeeper states

Status	Explanation
Abrupt Shutdown	The Gatekeeper has stopped but did not go through all shutdown procedures.
Graceful Shutdown	The Gatekeeper has stopped and did go through all shutdown procedures.
Receiving Calls Disabled	The Gatekeeper has not connected to the database and, therefore, cannot yet process calls.
Receiving Calls Enabled	The Gatekeeper has connected to its database and can process calls.
N/A	The Gatekeeper is not responding to maintenance messaging requests.

Gatekeeper-General tab

In the bottom section of the Gatekeeper window are three tabs: General, Registered Gateways, and Performance. Table 4-10 describes the fields in the Gatekeeper-General tab.

Table 4-10 Gatekeeper-General field descriptions (Sheet 1 of 2)

Field name	Description
Manufacturer and Model	Defines the maker and model of the Centrex IP Gatekeeper.
Support Contact Information	Provides the name and phone number of the technical support person for the Gatekeeper.
System Software Version	Provides the version of the system software currently installed on the Gatekeeper.
Hardware Version	Provides the version of the Gatekeeper hardware.
Location	Provides the location of the Gatekeeper in the Centrex IP network.
Application System Up Time	Shows the amount of time in days, hours, minutes, and seconds, that the Gatekeeper application has been in service.

Table 4-10 Gatekeeper-General field descriptions (Sheet 2 of 2)

Field name	Description
Node System Up Time	Shows the amount of time in days, hours, minutes, and seconds, that the physical node running the Gatekeeper application has been in service.
Active Connections	Shows the number of active calls on the Gatekeeper.
Available Connections	Shows the number of available call connections on the Gatekeeper.
Maximum Connections	Shows the maximum number of calls that can be handled by the Gatekeeper.
Maximum Response Wait Time	Shows the maximum time in seconds that the Gatekeeper will take to respond to a terminal.
Maximum Message Retries	Shows the maximum number of times the Gatekeeper tries to resend a message to a terminal.
Switch Activity and Restart Capability	Shows whether the Gatekeeper can perform a manual or automatic switch of activity or a restart.

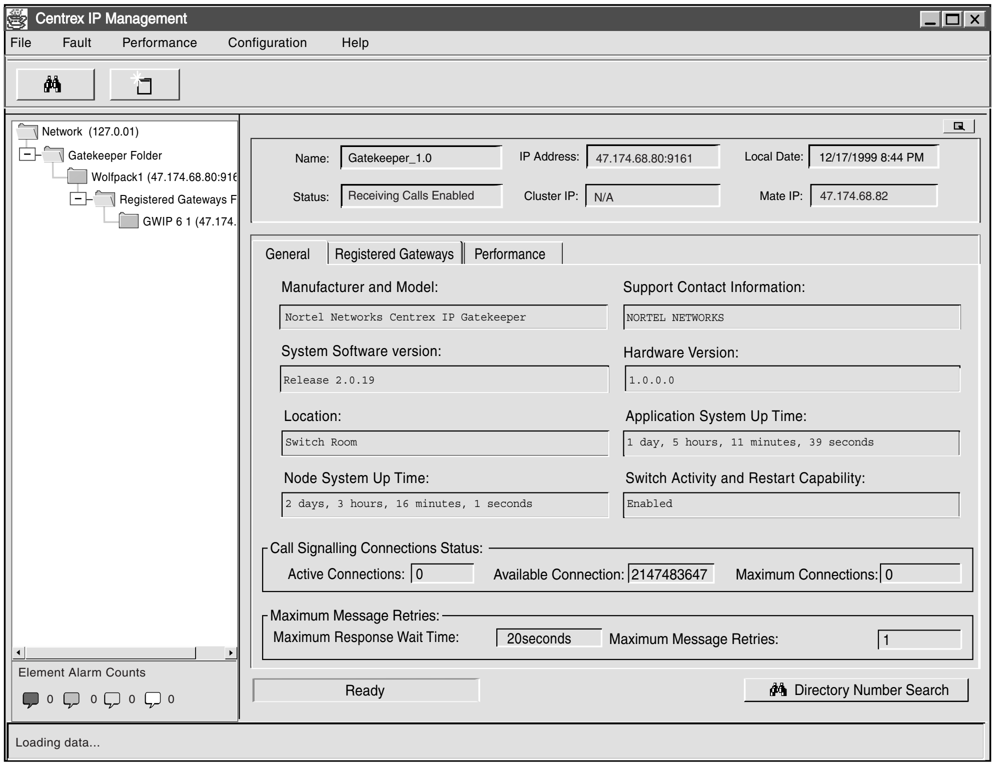
Functions

You can perform the following activities from the Gatekeeper-General window:

- View the Gatekeeper name and IP address.
- Check the Gatekeeper status.
- View the Gatekeeper cluster and mate IP address.
- View the make and model of the Gatekeeper.
- Look up the support contact number.
- View the software and hardware version of the Gatekeeper.
- View the amount of time the node and application have been running since the last restart.
- See if remote switch activity (SWACT) and restart capability is enabled.
- View the number of active, available, and maximum call signalling connections.
- View the maximum message response wait time and message retries.
- View the number and type of active alarms.

The following figure shows the Gatekeeper-General window.

Figure 4-5 Gatekeeper-General tab



Name: Gatekeeper_1.0
IP Address: 47.174.68.80:9161
Local Date: 12/17/1999 8:44 PM
Status: Receiving Calls Enabled
Cluster IP: N/A
Mate IP: 47.174.68.82

Manufacturer and Model: Nortel Networks Centrex IP Gatekeeper
Support Contact Information: NORTEL NETWORKS
System Software version: Release 2.0.19
Hardware Version: 1.0.0.0
Location: Switch Room
Application System Up Time: 1 day, 5 hours, 11 minutes, 39 seconds
Node System Up Time: 2 days, 3 hours, 16 minutes, 1 seconds
Switch Activity and Restart Capability: Enabled

Call Signalling Connections Status:
Active Connections: 0
Available Connection: 2147483647
Maximum Connections: 0

Maximum Message Retries:
Maximum Response Wait Time: 20seconds
Maximum Message Retries: 1

Gatekeeper-Registered Gateways tab

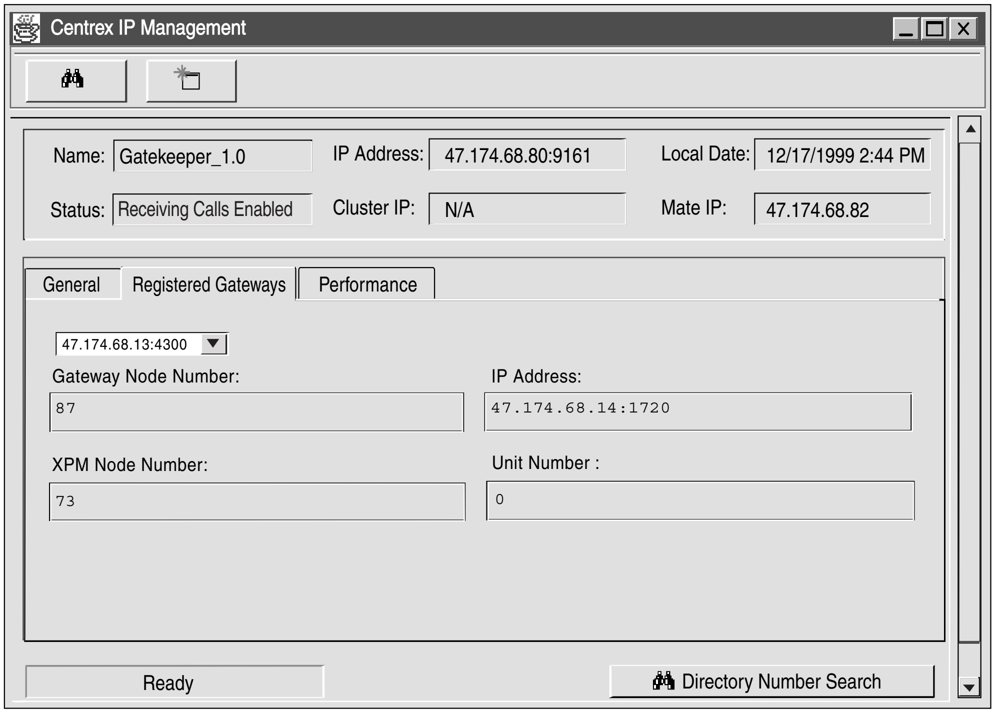
The second tab on the Gatekeeper window shows the information about the Gateways that are registered on the Gatekeeper. A pull-down menu contains the IP addresses of all the Gateways registered with the selected Gatekeeper. The fields in the Gatekeeper-Registered Gateways tab are listed in the following table.

Table 4-11 Gatekeeper-Registered Gateways field descriptions

Field name	Description
Gateway Node Number	Shows the node number of the Gateway card.
XPM Node Number	Shows the node number of the XPM the Gateway card is in.
IP Address	Shows the IP address and port number of the Gateway card.
Unit Number	Shows the unit number of the Gateway card.

The PTM software allows you to detach windows so you can view information screens for multiple Gatekeepers simultaneously. The Detach Window button is in the upper right corner of each screen. Figure 4-6 shows an example of a detached Gatekeeper-Registered Gateways window.

Figure 4-6 Detached Gatekeeper-Registered Gateways tab



Name: Gatekeeper_1.0 IP Address: 47.174.68.80:9161 Local Date: 12/17/1999 2:44 PM

Status: Receiving Calls Enabled Cluster IP: N/A Mate IP: 47.174.68.82

47.174.68.13:4300

Gateway Node Number: 87

IP Address: 47.174.68.14:1720

XPM Node Number: 73

Unit Number : 0

Gatekeeper-Performance tab

From the Gatekeeper element window, the Performance tab allows you to access the Gatekeeper performance metrics. The PTM retrieves the performance metrics in real time. The top section of the Gatekeeper-Performance tab contains the Performance Metrics selection panel for selecting the metrics and retrieval options. The bottom section of the window contains the Performance Results display panel for displaying the retrieved metrics.

The Performance display panel shows each retrieved metric on a separate line that contains the row number, the name of the Gatekeeper (Device Name), the IP address of the Gatekeeper, the metric name, and the metric value. The columns of the display panel can be rearranged by dragging and dropping the column headings to a different position in the display panel.

The following table describes the performance metrics available for the Gatekeeper.

Table 4-12 Gatekeeper performance metrics

Metric	Description
Total Calls	The number of connect messages sent by the node.
Call Process Load	The number of messages in the call processing queue. This gives an indication of the amount of work the Gatekeeper has to perform.
Average Call Duration	The average duration of the call in minutes since system boot time.
Registered Endpoints	The number of registered terminals or Gateways.
Admitted Endpoints	The number of admitted terminals or Gateways.
Gatekeeper Confirms	The number of messages sent by the Gatekeeper granting permission to register.
Gatekeeper Rejects	The number of messages sent by the Gatekeeper declining permission to register.
Registration Confirms	The number of messages sent by the Gatekeeper confirming registration.
Registration Rejects	The number of messages sent by the Gatekeeper rejecting registration.
Unregistration Confirms	The number of unregistration confirmation messages sent by the Gatekeeper.
Unregistration Rejects	The number of unregistration reject messages sent by the Gatekeeper.
Admission Confirms	The number of admission confirmation messages sent by the Gatekeeper.
Admission Rejects	The number of admission reject messages sent by the Gatekeeper.

The Gatekeeper-Performance tab has a Reset button that can globally reset some of the Gatekeeper metrics to a value of zero. The Reset button can only be used by users with write permission. The metrics that can be reset with the Reset button are listed as follows:

- Total Calls
- Average Call Duration

- Gatekeeper Confirms
- Gatekeeper Rejects
- Registration Confirms
- Registration Rejects
- Unregistration Confirms
- Unregistration Rejects
- Admission Confirms
- Admission Rejects

The following procedure describes how to use the Gatekeeper-Performance tab to retrieve performance metrics.

Procedure 4-15 Retrieve Gatekeeper performance metrics

At the PTM workstation

1 From the Element Manager main window, select the Gatekeeper whose performance you wish to view from the Navigation tree.

The Gatekeeper-General window opens.

2 Click the Performance tab.

The Performance tab window moves to the front.

3 Select the desired metrics from the scroll-down list. Any combination of metrics can be selected using the Shift or Ctrl keys in combination with a mouse click.

a The entire list of metrics can be retrieved by a left-click on the top metric, scroll down to the bottom of the list, hold down the Shift key and left-click on the last metric. All of the metrics in the list will be selected.

b Various combinations of metrics can be retrieved by holding down the Ctrl key and left-clicking on the desired metric.

4 After the desired metrics have been selected, click the Retrieve button.

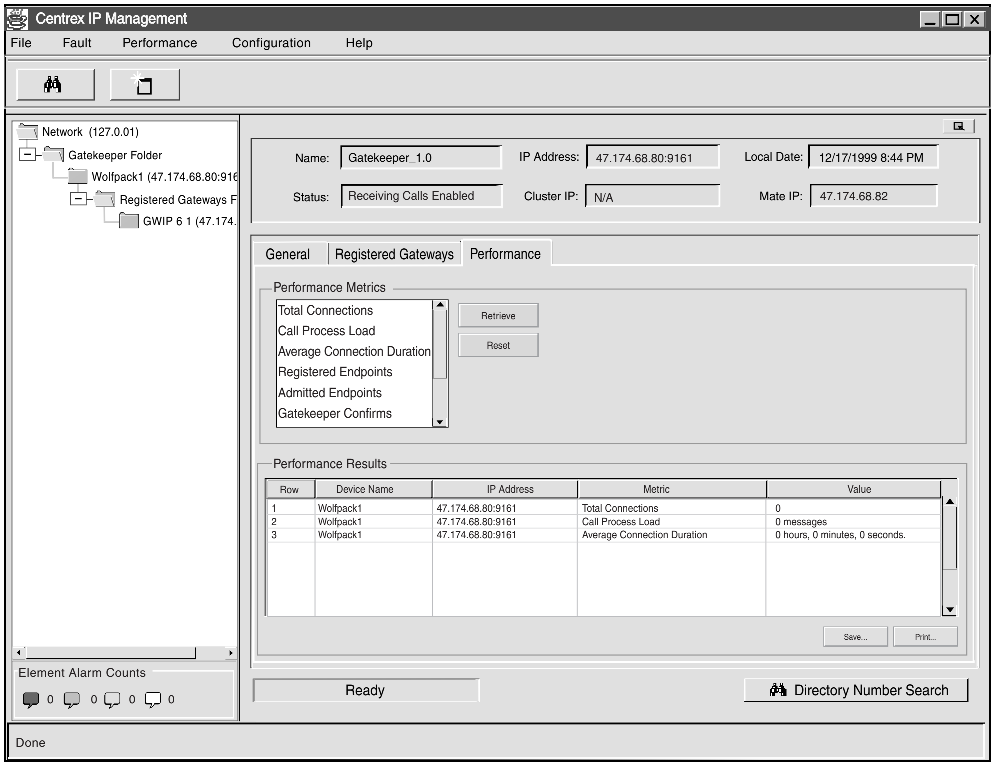
The metrics are output to the display panel. When the metrics are displayed in this panel, the Save and Print buttons are enabled.

5 To save the metrics output in a text file, click the Save button.

6 To print the metrics output in the display panel, click the Print button.

The following figure shows the Gatekeeper-Performance window.

Figure 4-7 Gatekeeper-Performance tab



Name: Gatekeeper_1.0
IP Address: 47.174.68.80:9161
Local Date: 12/17/1999 8:44 PM
Status: Receiving Calls Enabled
Cluster IP: N/A
Mate IP: 47.174.68.82

Performance Metrics

- Total Connections
- Call Process Load
- Average Connection Duration
- Registered Endpoints
- Admitted Endpoints
- Gatekeeper Confirms

Performance Results

Row	Device Name	IP Address	Metric	Value
1	Wolfpack1	47.174.68.80:9161	Total Connections	0
2	Wolfpack1	47.174.68.80:9161	Call Process Load	0 messages
3	Wolfpack1	47.174.68.80:9161	Average Connection Duration	0 hours, 0 minutes, 0 seconds.

Ready

Gateway window

When you select a Gateway in the Navigation tree, the Gateway window opens in the display panel.

The Gateway window shows four fields at the top of the window: Gateway Name, IP Address, Status, and State. The Status field has three possible entries: Primary, Spare, and Unknown. The State field also has three possible entries: In Service, Busy, and Offline.

The Gateway window has two tabs, the General tab and the Performance tab. The fields on the Gateway-General tab are described in the table that follows.

Table 4-13 Gateway-General field descriptions

Field name	Description
Name and Maker	Shows the name and maker of the Gateway card.
Support Contact Information	Provides the name and phone number of the technical support person for the Gateway card.
System Software Version	Provides the version of the system software used with the Gateway card.
Hardware Version	Provides the hardware version of the Gateway card.
XPM Node Number	Shows the node number of the XPM that the Gateway card resides on. (Note 1)
XPM Port Number	Shows the port number of the XPM. (Note 2)
Gateway Logical Node Number	Shows the logical node number of the Gateway card. (Note 3)
Gateway Physical Node Number	Shows the physical node number of the Gateway card. (Note 3)
Gateway Card Uptime	Shows the length of time that the Gateway card has been in service without interruption.
Gateway Application Uptime	Shows the length of time that the Gateway application has been in service without interruption.
Gateway MAC address	Shows the Gateway unique MAC address.

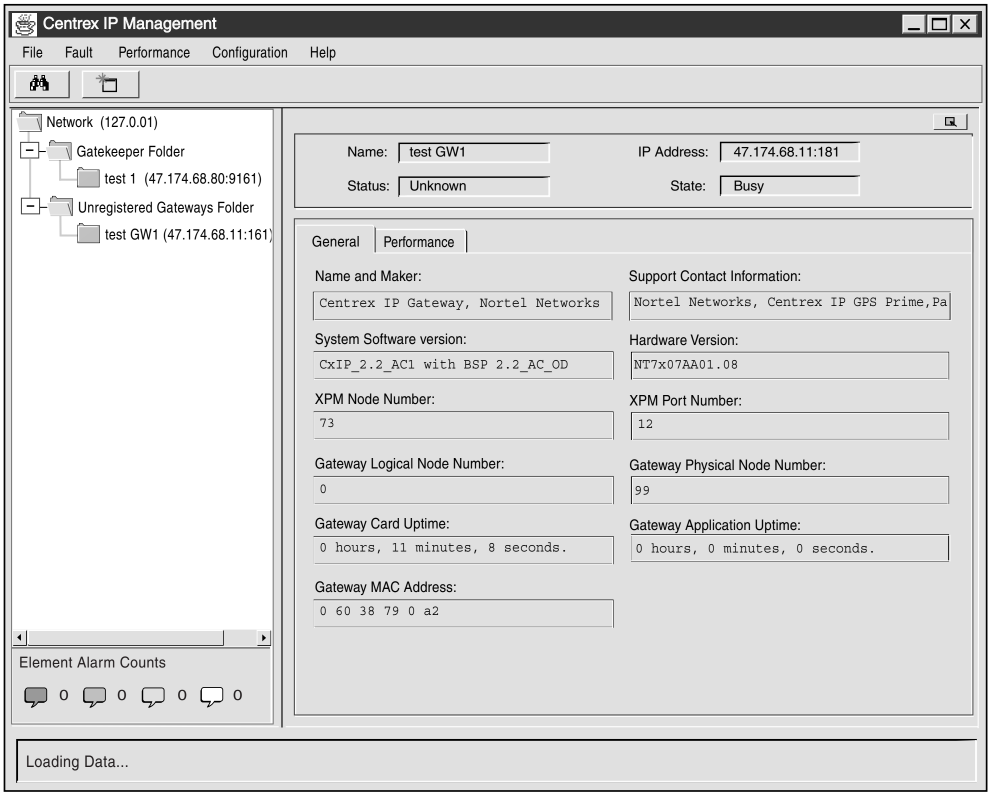
Note 1: To verify the XPM node number, post the XPM at the LTC level of the DMS MAP display. Perform the QUERYPM command and verify the node number matches the number in the Gateway-General window.

Note 2: To verify the XPM port number, go to table IPINV at the DMS MAP display. Verify the XPM port number in the Gateway-General window matches the entry in table IPINV.

Note 3: To verify the Gateway logical and physical node numbers, post the Gateway at the DMS MAP display. Perform the QUERYPM command and verify the node numbers on the DMS switch match the numbers in the Gateway-General window.

The following figure shows the Gateway-General window.

Figure 4-8 Gateway-General tab



Name: test GW1
IP Address: 47.174.68.11:181
Status: Unknown
State: Busy

Name and Maker: Centrex IP Gateway, Nortel Networks
Support Contact Information: Nortel Networks, Centrex IP GPS Prime,Pa
System Software version: CxIP_2.2_AC1 with BSP 2.2_AC_OD
Hardware Version: NT7x07AA01.08
XPM Node Number: 73
XPM Port Number: 12
Gateway Logical Node Number: 0
Gateway Physical Node Number: 99
Gateway Card Uptime: 0 hours, 11 minutes, 8 seconds.
Gateway Application Uptime: 0 hours, 0 minutes, 0 seconds.
Gateway MAC Address: 0 60 38 79 0 a2

Loading Data...

Gateway-Performance tab

From the Gateway element window, the Performance tab allows you to access the Gateway performance metrics. The PTM retrieves the performance metrics in real time. The top section of the Gateway-Performance tab contains the Performance Metrics selection panel for selecting the metrics and retrieval options. The bottom section of the window contains the Performance Results display panel for displaying the retrieved metrics.

The Performance display panel shows each retrieved metric on a separate line that contains the row number, the name of the Gatekeeper, the IP address of the Gatekeeper, the metric name, and the metric value. The columns of the display panel can be rearranged by dragging and dropping the column headings to a different position in the display panel.

The following table describes the performance metrics available for the Gateway.

Table 4-14 Gateway performance metrics (Sheet 1 of 2)

Metric	Description
System Uptime	The time that the Gateway application was started.
Total Calls	The total number of calls conducted by the Gateway since the last startup.
Active Calls	The number of active calls currently conducted by the Gateway.
Average Call Duration	The average duration of a call in minutes since the last restart.
Active Connections	The number of connections currently active on the Gateway.
Origination Attempts	The number of times an IP terminal attempts to initiate a voice, data, or other multimedia call through the Gateway.
Termination Attempts	The number of times a PSTN terminal attempts to terminate a call to an IP terminal.
Non-call Attempts	The number of times an IP terminal invokes a non-call related action through the Gateway.
Average Simultaneous Calls	The average number of simultaneous calls since the last restart.
Estimated Additional Calls	The estimated number of additional simultaneous calls that the Gateway can carry out.
IP Packets Sent	The total number of packets sent by the Gateway to all the H.323 connections since the last startup.
IP Packets Received	The total number of packets received by the Gateway from all H.323 connections since the last startup.
IP Packets Lost	The total number of packets lost since the last startup. This parameter is applicable to the non-guaranteed network.
IP Bytes Sent	The total number of bytes sent by the Gateway to all the H.323 connections since the last startup.
IP Bytes Received	The total number of bytes received by the Gateway from all H.323 connections since the last startup.

Table 4-14 Gateway performance metrics (Sheet 2 of 2)

Metric	Description
IP Active Connections	The total number of H.323 connections currently active on the Gateway.
PSTN Unused Ports	The total number of unused PSTN ports on the Gateway.
PSTN Failed Ports	The number of currently failed or unavailable PSTN ports on the Gateway.
PSTN Active Connections	The number of PSTN connections currently active on the Gateway.

The Gateway-Performance tab has a Reset button that can globally reset some of the Gateway metrics to a value of zero. The Reset button can only be used by users with write permission. The metrics that can be reset with the Reset button are listed as follows:

- Total Calls
- Average Call Duration
- Origination Attempts
- Termination Attempts
- Non-Call Attempts
- Average Simultaneous Calls
- IP Packets Lost
- IP Packets Received
- IP Packets Sent
- IP Bytes Received
- IP Bytes Sent

Procedure 4-16 Retrieve Gateway performance metrics

At the PTM workstation

1 From the Element Manager main window, select the Gateway whose performance you wish to view from the Navigation tree.

The Gateway-General window opens.

2 Click the Performance tab.

The Performance tab window moves to the front.

3 Select the desired metrics from the scroll-down list. Any combination of metrics can be selected using the Shift or Ctrl keys in combination with a mouse click.

- **a** The entire list of metrics can be retrieved by a left-click on the top metric, scroll down to the bottom of the list, hold down the Shift key and left-click on the last metric. All of the metrics in the list will be selected.
- **b** Various combinations of metrics can be retrieved by holding down the Ctrl key and left-clicking on the desired metric.

4 After the desired metrics have been selected, click the Retrieve button.

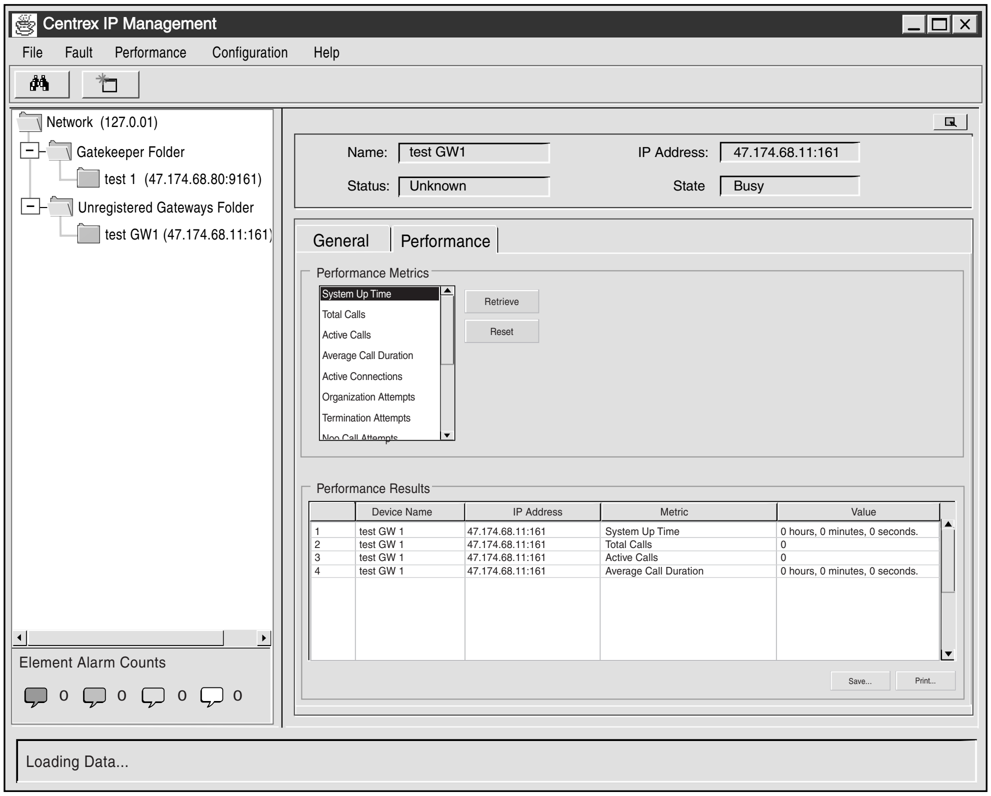
The metrics are output to the display panel. When the metrics are displayed in this panel, the Save and Print buttons are enabled.

5 To save the metrics output in a text file, click the Save button.

6 To print the metrics output in the display panel, click the Print button.

The following figure shows the Gateway window with the Performance tab in front.

Figure 4-9 Gateway-Performance tab



Name: test GW1

IP Address: 47.174.68.11:161

Status: Unknown

State Busy

	Device Name	IP Address	Metric	Value
1	test GW 1	47.174.68.11:161	System Up Time	0 hours, 0 minutes, 0 seconds.
2	test GW 1	47.174.68.11:161	Total Calls	0
3	test GW 1	47.174.68.11:161	Active Calls	0
4	test GW 1	47.174.68.11:161	Average Call Duration	0 hours, 0 minutes, 0 seconds.

Loading Data...

Terminal Proxy Server window

When you select a TPS in the Navigation tree, the TPS window opens in the display panel.

The TPS window shows four fields at the top of the window: Name, IP Address, Local Date, and Status.

The TPS window has one tab, the General tab. The fields in the TPS-General tab are described in the table that follows.

Table 4-15 TPS-General field descriptions

Element	Description
Manufacturer and Model	Shows the manufacturer and model of the TPS.
Support Contact Information	Shows the name and telephone number of the technical support person responsible for the TPS.
System Software Version	Shows the version of the system software used with the TPS.
Location	Shows the physical location of the TPS. Can be a city, building, or location in building.
Up Time	Shows the length of time that the TPS has been in service without interruption.

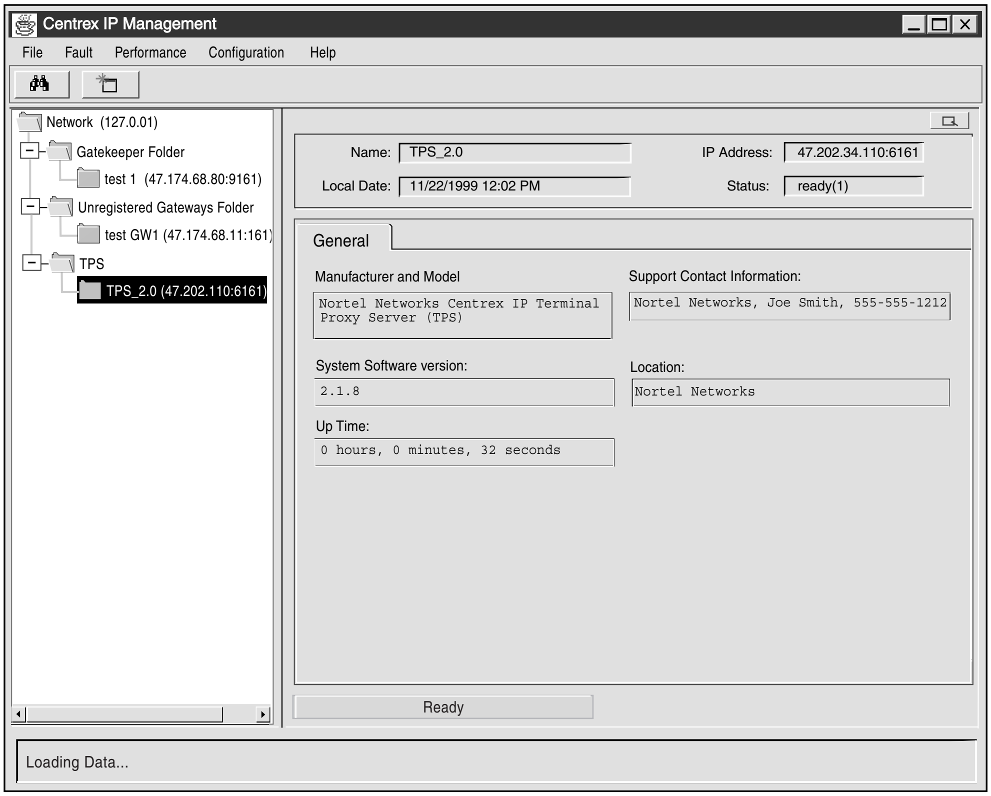
Functions

You can perform the following activities from the TPS-General window.

- View the name and IP address of the TPS.
- View the manufacturer and model of the TPS.
- View the support contact information.
- View the system software version of the TPS.
- View the length of time the TPS has been in service.

The following figure shows the TPS-General window.

Figure 4-10 TPS-General window


Centrex IP Management
File
Fault
Performance
Configuration
Help
Network (127.0.01)
Gatekeeper Folder
test 1 (47.174.68.80:9161)
Unregistered Gateways Folder
test GW1 (47.174.68.11:161)
TPS
TPS_2.0 (47.202.110:6161)
General

Name: TPS_2.0

IP Address: 47.202.34.110:6161

Local Date: 11/22/1999 12:02 PM

Status: ready(1)

Manufacturer and Model: Nortel Networks Centrex IP Terminal Proxy Server (TPS)

Support Contact Information: Nortel Networks, Joe Smith, 555-555-1212

System Software version: 2.1.8

Location: Nortel Networks

Up Time: 0 hours, 0 minutes, 32 seconds

Ready

Loading Data...

Terminal window

From the Terminal window, you can view information with any DN that is registered with a Gatekeeper. To access the Terminal window, click the DN Search button from the Menu Bar of any window. The Find Directory window opens. When you enter a valid DN in the Find Directory window, the Terminal window is displayed.

The following procedure describes how to view calls on the Gatekeeper using the Find Directory window.

> ***Note:*** If you search on a DN that is not registered with a Gatekeeper, a message “Search for Directory Number xxx xxx xxxx Fail” appears at the bottom of the window.

Procedure 4-17 View call details on the Terminal window

At the PTM workstation

1 From the Gatekeeper window, click on either the DN Search button at the top of the window or the Directory Number Search button at the bottom of the window.

The Find Directory Number window opens.

2 Type in the 10-digit DN that you are searching for.

> ***Note:*** Wild cards and partial entries will return a failed search indication in the status bar.

3 Select a Gatekeeper from the pull-down menu and click the Find Now button.

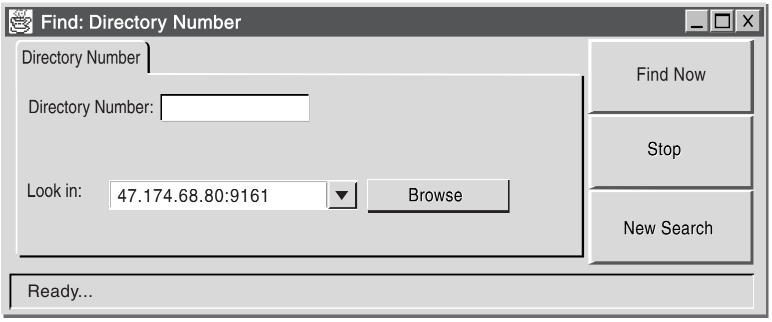
The Terminal window opens with the DN in the banner.

4 Click the Call Details tab.

5 Check the fields in the Call Details tab to view the status of the call.

The figure that follows shows the Find Directory Number window.

Figure 4-11 Find Directory Number window



Directory Number:

Look in: 47.174.68.80:9161

Ready...

The Terminal window displays the following information:

- the DN, multiple-appearance directory number (MADN), and Gatekeepers in the group
- the Active Calls on Associated Terminals panel lists all active calls on the terminal
- a Call Details tab that displays details on a selected call
- a General tab that displays information on the state of the DN and the TPS

The following table lists the fields in the Terminal window.

Table 4-16 Terminal-General field descriptions

Field name	Description
Directory Number	Shows the number of the queried DN.
MADN Count	Shows the number of members of the MADN group.
Gatekeeper Name	Shows the names of the Gatekeepers for the specified MADN group.
Gatekeeper IP Address	Shows the IP addresses of the Gatekeepers for the specified MADN group.
Active Calls on Associated Terminals	See table 4-17 in this chapter.
General tab	See table 4-18 in this chapter.
Call Details tab	See table 4-19 in this chapter.

The following table lists the fields in the Active Calls on Associated Terminals panel.

Table 4-17 Active Calls on Associated Terminals field descriptions

Field name	Description
IP Address	Shows the IP address of a terminal that the DN is provisioned on.
TPS IP Address and Port	Shows the IP address and port of the TPS for the terminal.
Connected To	Shows the DN or the Gateway that the provisioned terminal is connected to.
Gateway IP Address	Shows the IP address of the Gateway that the call is being routed through.
Call Type	Shows the type of call, incoming or outgoing.
State	Shows the state of the call: active (7), callProceeding (6), or callDelivered (2).
Call Start Time	Shows the time that the two endpoints were connected.

Terminal-General tab

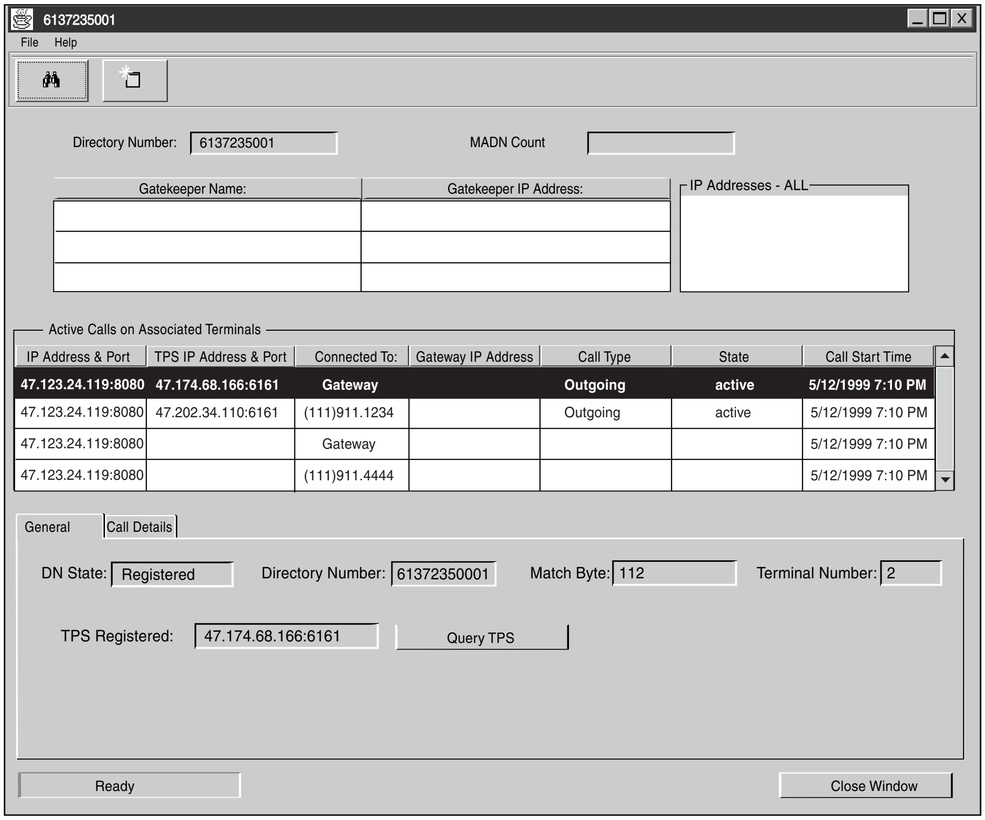
When the Terminal window opens, the General tab is in front. This tab contains general information about the DN. The Terminal-General tab is a read-only window. The following table lists the fields available from the Terminal-General window.

Table 4-18 Terminal-General field descriptions

Field name	Description
DN State	Shows the state of the DN (call processing, registered, or unregistered).
Directory Number	Shows the number of the queried DN.
Match Byte	Identifies the terminal in internal DMS messaging.
Terminal Number	Identifies the loop the terminal resides on.
TPS Registered	Shows the IP address and port of the TPS if the TPS is registered. Shows N/A if the TPS is not registered.

The following figure shows the Terminal-General window. The Query TPS button displays general information on the registered TPS.

Figure 4-12 Terminal-General tab



Directory Number: 6137235001

MADN Count

Gatekeeper Name:	Gatekeeper IP Address:

IP Address & Port	TPS IP Address & Port	Connected To:	Gateway IP Address	Call Type	State	Call Start Time
47.123.24.119:8080	47.174.68.166:6161	Gateway		Outgoing	active	5/12/1999 7:10 PM
47.123.24.119:8080	47.202.34.110:6161	(111)911.1234		Outgoing	active	5/12/1999 7:10 PM
47.123.24.119:8080		Gateway				5/12/1999 7:10 PM
47.123.24.119:8080		(111)911.4444				5/12/1999 7:10 PM

DN State: Registered

Directory Number: 61372350001

Match Byte: 112

Terminal Number: 2

TPS Registered: 47.174.68.166:6161

Terminal-Call Details tab

The second tab in the Terminal window is the Call Details tab. The queried DN shows in the field at the top of the window, along with the Gatekeeper's name and IP address that the queried DN belongs to. The Active Calls on Associated Terminals panel is populated if there is an active call on the queried DN.

DN search interactions

The DN Search feature retrieves and displays all calls that appear on a terminal that contains the queried DN. For example, if a terminal has two DNs, and an incoming call arrives on the first DN, a DN search on the second DN will display the call on the first DN. If an outgoing call is made from the second DN, the DN search will display both calls.

In the case of a MADN, the DN search retrieves and displays the associated call legs of the MADN call. Associated calls means that there is a signaling channel between the terminals that is not involved in the speech path. A DN search on a MADN (where more than one terminal shares a DN) displays all the terminals with that MADN. The terminals are distinguished by their IP addresses in the call list, Active Calls on Associated Terminals.

The following table lists the fields available from the Terminal-Call Details tab.

Table 4-19 Terminal-Call Details field descriptions

Field name	Description
Call State	Shows the state of the call: active (7), callProceeding (6), or callDelivered (2).
Call Type	Indicates an incoming or outgoing call.
Call Start Time	Shows the date and time the call was initiated.
Call Reference Value	Shows the unique ID for that call.
Directory Number	Shows the number the DN is connected to.
Gateway IP Address	Shows the Gatekeeper the DN is connected to.

Functions

You can perform the following tasks from the Terminal-Call Details tab.

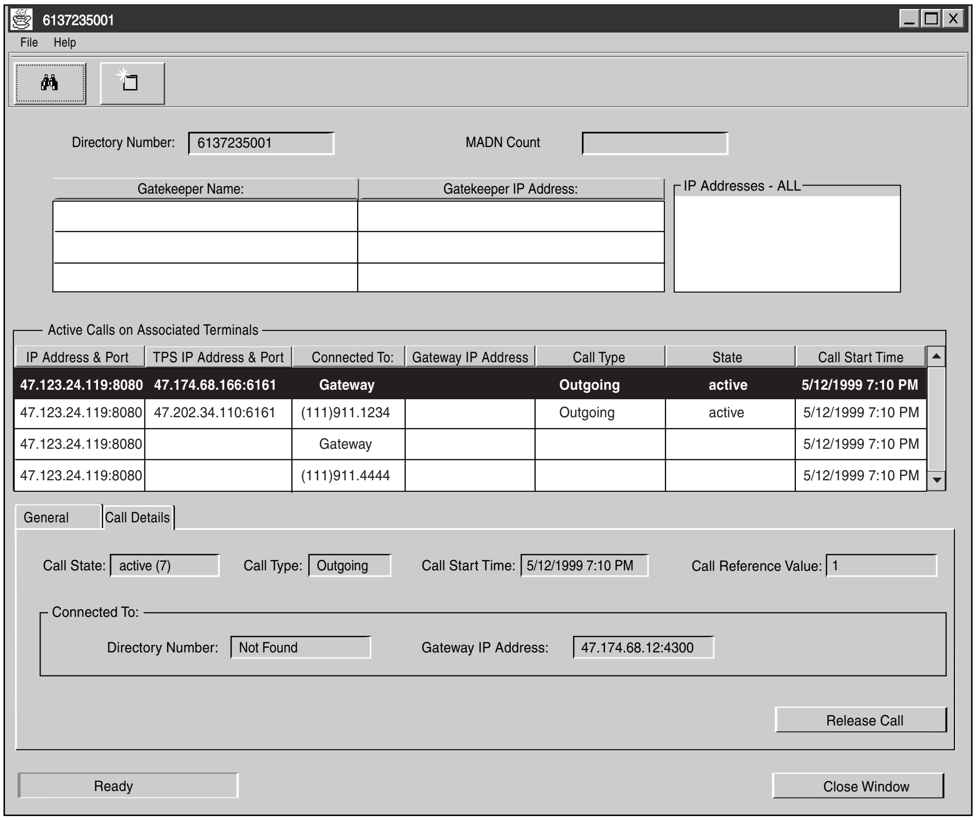
- View the call details of any DN that is registered with the Gatekeeper.
- Force release a call.
- Check the state of a call.
- Check the call type.
- Check the call reference value.

  Note: The call reference value is used for debugging the call from the DMS switch using the xpmist or calltrk tools.

- View what number the DN is connected to.
- View the Gateway Name and IP address that the DN is connected to.

The following figure shows the Terminal-Call Details tab.

Figure 4-13 Terminal-Call Details tab



Directory Number: 6137235001

MADN Count

Gatekeeper Name:	Gatekeeper IP Address:

IP Addresses - ALL

Active Calls on Associated Terminals

IP Address & Port	TPS IP Address & Port	Connected To:	Gateway IP Address	Call Type	State	Call Start Time
47.123.24.119:8080	47.174.68.166:6161	Gateway		Outgoing	active	5/12/1999 7:10 PM
47.123.24.119:8080	47.202.34.110:6161	(111)911.1234		Outgoing	active	5/12/1999 7:10 PM
47.123.24.119:8080		Gateway				5/12/1999 7:10 PM
47.123.24.119:8080		(111)911.4444				5/12/1999 7:10 PM

Call State: active (7)

Call Type: Outgoing

Call Start Time: 5/12/1999 7:10 PM

Call Reference Value: 1

Connected To:

Directory Number: Not Found

Gateway IP Address: 47.174.68.12:4300

If a call needs to be taken down, you can force release the call from the Terminal window using the Release Call button. Use this procedure to force release a call.

> ***Note:*** For a MADN call, if the active call leg (the one with the speech path) is released using the Release Call button, the associated call legs are also released. If an associated call leg is released, the corresponding active call leg is not released.

Procedure 4-18 Force release a call

At the PTM workstation

1 From the Terminal window, select the DN row in the Active Calls on Associated Terminals panel.

2 Click on the Release Call button in the lower right corner of the window.

The Disconnect Call dialog box opens.

3 Click the Yes button to release the call or the No button to cancel.

4 Click the Refresh button and check the Active Calls on Associated Terminals panel to confirm that the call was released.

Event History Manager window

The Event History Manager allows you to search for traps on a Gatekeeper. A trap is a notification of an error or an event. Some traps that can appear in the Event History Manager window are as follows:

- pTMneColdStartInit—indicates the request for the PTM Alarm Manager to start initialization of the alarm table
- h323GatekeeperStart—indicates the Gatekeeper is starting
- h323GatekeeperGoingDown—indicates the Gatekeeper is shutting down
- csAutheneticationFailureRASRegistration—indicates that a RAS registration request message has been rejected because of authentication failure
- csAuthenticationFailureRASAdmission—indicates that a RAS admission request message has been rejected because of authentication failure
- nortelNMIcriticalAlarmNotification—indicates a critical alarm has been raised on the Gatekeeper
- nortelNMImajorAlarmNotification—indicates a major alarm has been raised on the Gatekeeper
- nortelNMIminorAlarmNotification—indicates a minor alarm has been raised on the Gatekeeper
- nortelNMIwarningAlarmNotification—indicates a warning alarm has been raised on the Gatekeeper
- nortelNMIalarmClearNotification—indicates an alarm has been cleared on the Gatekeeper
- scNortelLogNotificationEvent—indicates a software error has occurred

Note: For more information about alarms and traps, see the “Troubleshooting” chapter.

The Event History Manager has a pull-down menu, Filter Type. When you select a filter type, only the traps that correspond to that filter appear in the event table. A selection of No Filter shows all the traps that have been received. See the following table for a description of the search filters.

Table 4-20 Event History search filters (Sheet 1 of 2)

Filter Type	Description
IP Address	Search by the IP address of the node on which the event occurred.
Event Type	Search by a specific event type, such as “coldStart.”
Description of Event	Search by description of event.

Table 4-20 Event History search filters (Sheet 2 of 2)

Filter Type	Description
Entity Name	Search by the name of a specific node.
Entity Type	Search for all traps on a node type. The choices are Gatekeeper or Gateway.
No Filter	Removes previously applied filters and lists all traps.
Note: When the Entity Name or Entity Type says NULL, the trap received was on a device that has not been entered in the PTM.	

After you have selected the filter you want to search on, enter the search criteria in the “Search for” field. The search criteria can be any full or partial string that matches the data in the event table, using one of the five categories that corresponds to the chosen filter. The event table displays the search results for the filter. The following procedure shows a sample search using the Event History Manager.

Procedure 4-19 Search for SNMP events

At the PTM workstation

1 From the Filter Type pull-down menu, select Event Type.

2 In the “Search for” field, enter the search criteria, such as “h323GatekeeperStart.”

> ***Note:*** Any substring of the event text can be entered, such as “start.”

3 Click the Find Now button.

The event table shows a list of the h323GatekeeperStart traps.

> ***Note:*** Only the traps that occurred in the last week are displayed.

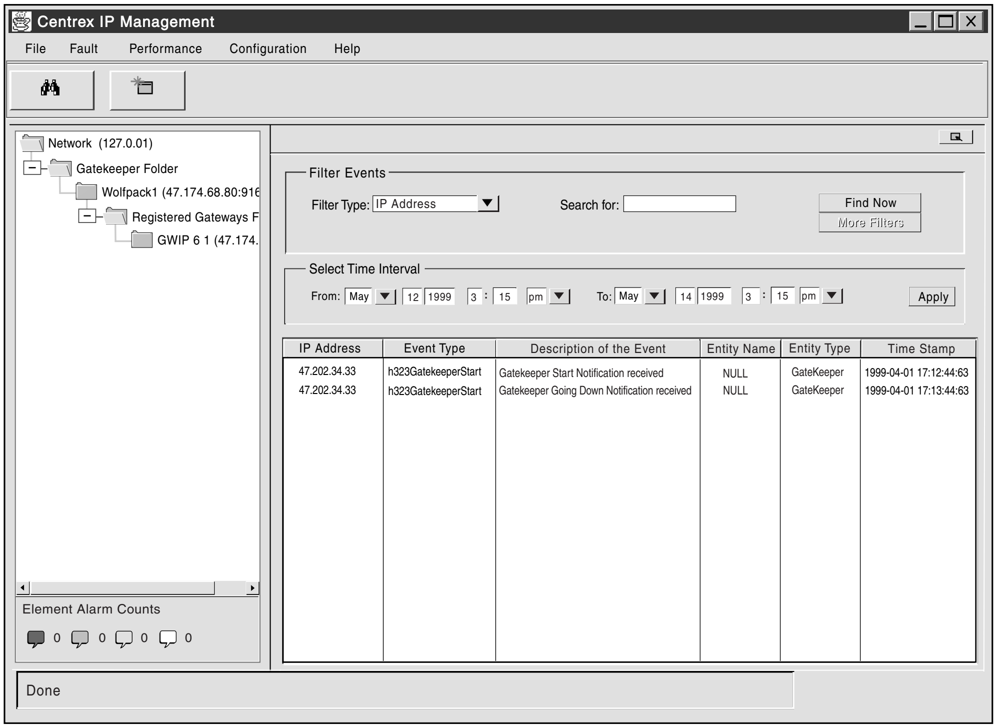
Time interval query

You can also search for traps that occurred during a specific time interval by entering a date and time in the time interval fields. When you click the Apply button, all traps that occurred during the time interval appear in the event table.

> ***Note:*** The Filter Type and Time Interval queries are mutually exclusive and cannot be combined.

The following figure shows the Event History Manager window.

Figure 4-14 Event History Manager window



Filter Type: IP Address

Search for:

From: May 12 1999 3 : 15 pm To: May 14 1999 3 : 15 pm

IP Address	Event Type	Description of the Event	Entity Name	Entity Type	Time Stamp
47.202.34.33	h323GatekeeperStart	Gatekeeper Start Notification received	NULL	GateKeeper	1999-04-01 17:12:44:63
47.202.34.33	h323GatekeeperStart	Gatekeeper Going Down Notification received	NULL	GateKeeper	1999-04-01 17:13:44:63

Quality of Service Browser

The Quality of Service (QoS) Browser allows you to query and display QoS measurements from the PTM to evaluate and monitor the voice quality of the network.

The values associated with QoS are as follows:

- latency—round-trip delay (measured in milliseconds) from sender to receiver and back. Low latency ensures that a conversation has good interactive quality. Latency should not exceed 200 ms.
- packet loss—percentage of voice packets not received at the destination in time for them to be useful. Packet loss can degrade voice quality. The target is a maximum of 4% packet loss.
- jitter—variations in arrival rates of voice packets, some of which can arrive out of order. A jitter buffer can put the data back in the correct order and achieve a smooth playback of voice data. The jitter buffer introduces a delay, which adds to overall latency.

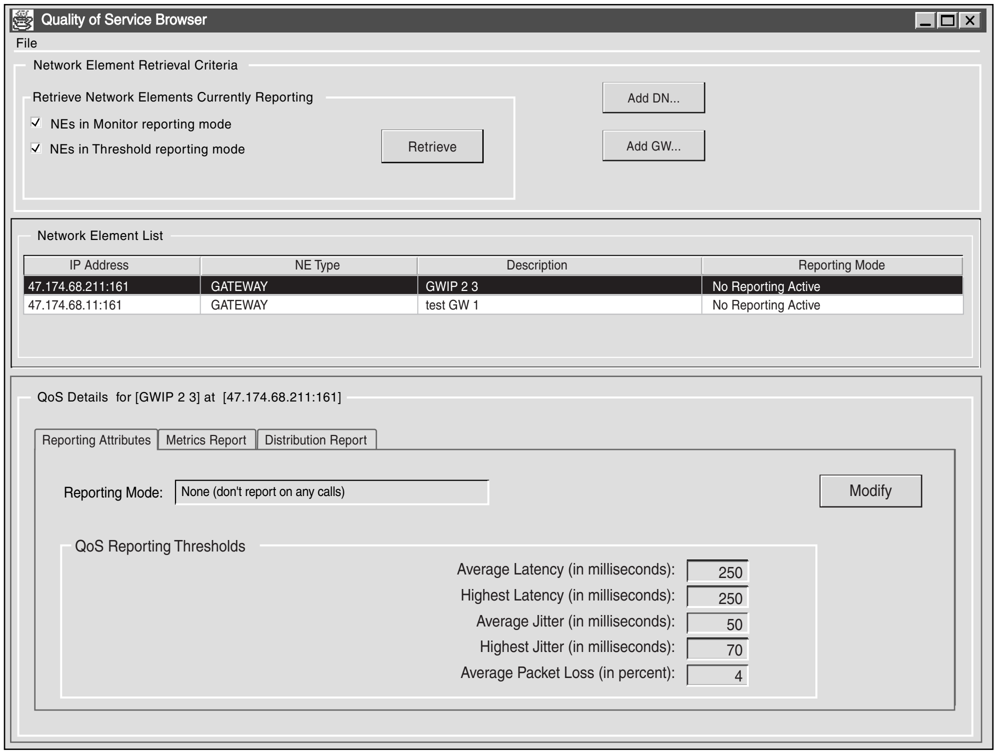
For QoS thresholds and QoS monitor functions, the object window sets and clears thresholds, enables monitoring, and displays results of those functions. To access this object window, select the QoS Browser from the Performance menu.

The QoS Browser consists of the following panels:

- Network Element Retrieval Criteria
- Network Element List
- QoS Details

The following figure shows the Quality of Service Browser.

Figure 4-15 Quality of Service Browser



Quality of Service Browser

File

Network Element Retrieval Criteria

Retrieve Network Elements Currently Reporting

☑ NEs in Monitor reporting mode

☑ NEs in Threshold reporting mode

Network Element List

IP Address	NE Type	Description	Reporting Mode
47.174.68.211:161	GATEWAY	GWIP 2 3	No Reporting Active
47.174.68.11:161	GATEWAY	test GW 1	No Reporting Active

QoS Details for [GWIP 2 3] at [47.174.68.211:161]

Reporting Mode: None (don't report on any calls)

QoS Reporting Thresholds

Average Latency (in milliseconds):	250
Highest Latency (in milliseconds):	250
Average Jitter (in milliseconds):	50
Highest Jitter (in milliseconds):	70
Average Packet Loss (in percent):	4

Network Element Retrieval Criteria

The Network Element Retrieval Criteria panel finds network elements to move into the Network Element List panel below the retrieval criteria panel. The check boxes function to move groups of network elements into the Network Element List panel. For example, if you check the box labeled “NEs in Monitor reporting mode” all network elements with call monitoring enabled will move into the Network Element List. Click the Retrieve button to move the network elements. Add individual network elements to the Network Element list by clicking the Add DN or Add GW buttons. These buttons bring up dialog windows that allow you to add either DNs or Gateways to the Network Element List.

The Add Directory Number(s) dialog window allows you to input individual DNs. Click the Add button to perform a DN search function. If successful, the

DNs are added to a list of DNs. Click the Apply button to add those DNs to the Network Element List.

The Add Gateway(s) dialog window allows you to add individual Gateways or groups of Gateways to the Network Element List. The list Existing Gateways contains all known gateways. Click the Add Selected button to add all selected Gateways to a list of Gateways To Add. Click the Apply button to add those Gateways to the Network Element List.

Network Element List

The Network Element List panel contains the list of all chosen network elements. This list includes the DN or Gateway name associated with each network element. When you select a network element from the list, the details are available in the bottom panel, “QoS Details.”

QoS Details

The QoS Details panel gives the details for the selected IP address.

This panel contains three tabs:

- Reporting Attributes
- Metrics Report
- Distribution Report

Reporting Attributes tab

The Reporting Attributes tab shows what reporting criteria, if any, are currently enabled for the network element selected in the Network Element List. The Current QoS Thresholds will be grayed out. Click the Modify button to display the Modify Reporting Attributes dialog box.

The Modify Reporting Attributes dialog box displays the following thresholds:

- Average Latency (in milliseconds)
- Highest Latency (in milliseconds)
- Average Jitter (in milliseconds)
- Highest Jitter (in milliseconds)
- Average Packet Loss (in percent)

Metrics Report tab

The Metrics Report tab contains the history of QoS events for the selected network element. The Metrics Report shows the history of QoS SNMP traps from the network element selected in the object window. These traps are caused by setting either the threshold or monitoring functions, which were enabled with the Modify Reporting Attributes box.

Distribution Report tab

The Distribution Report tab allows you to query the network element for cumulative QoS information. A bar chart shows the distribution of QoS for the selected metric. The definition of the bar chart can be changed using the Modify button, which displays the Modify Distribution Report dialog box. When you click the Apply button, the collection resets at the selected node. The current counts are all set to zero, and the new base and width values are set in the selected node.

The following procedures describe how to use the QoS browser to manage and monitor QoS thresholds. To add a node or DN for monitoring, see the section “Network Element Retrieval Criteria” in this chapter.

Procedure 4-20 Query cumulative QoS metrics

At the PTM workstation

1 Select the desired node from the Network Element List.

2 Click the Distribution Report tab.

The panel displays the cumulative QoS results for the selected node.

Procedure 4-21 Change QoS thresholds

At the PTM workstation

1 Select the desired node from the Network Element List.

2 Verify that the node is in threshold reporting mode. To change the current values in the QoS Reporting Thresholds panel, click the Modify button.

A dialog box opens with input fields for the reporting thresholds.

3 Enter the new values and click the Apply button.

The specified threshold values are enabled for the selected node. At the end of each call, the selected node examines the QoS metrics and sends an SNMP trap to the PTM if any metric exceeds its threshold.

Procedure 4-22 Enable QoS monitoring

At the PTM workstation

1 Select the desired node from the Network Element List.

2 Check the current reporting mode in the QoS Reporting Thresholds panel. If the selected node is not in Monitoring reporting mode, click the Modify button to change it.

A dialog box opens with a selection field for the reporting mode.

3 Change the reporting mode to Monitoring (report all calls) and click the Apply button.

Monitor reporting mode is enabled for the selected node. At the end of each call, the selected node sends an SNMP trap to the PTM that reports the QoS metrics for that call.

Procedure 4-23 Display QoS results

At the PTM workstation

1 In the Network Element Retrieval Criteria panel, check the NEs in Threshold reporting mode box.

2 Select the desired node from the Network Element List.

3 Click the Metrics Report tab.

The panel displays a list of all threshold traps received for the selected node.

Configuration menu functions

The Configuration menu allows the user to change the configuration of the network as follows:

- add additional nodes, such as Gatekeeper, Gateway, or TPS to the Navigation tree
- change or delete device names
- enable user name security functions

The Configuration menu contains the following windows:

- Add Gatekeeper—allows you to add a Gatekeeper node to the Navigation tree
- Add Gateway—allows you to add a Gateway node to the Navigation tree
- Add TPS—allows you to add a TPS node to the Navigation tree
- Change Device Name—allows you to change the device name
- Delete Device—allows you to delete a device
- Add New User—allows you to add a new user
- Change User Password—allows you to change the user password
- Delete User—allows you to delete a user

Add Gatekeeper

The Add Gatekeeper selection allows you to add a Gatekeeper to the Centrex IP network. The Add Gatekeeper selection displays the Add Gatekeeper dialog box.

Use the following procedure to add a Gatekeeper to the Centrex IP network.

Procedure 4-24 Add a Gatekeeper

At the PTM workstation

1 Select the Gatekeeper you want to add.

2 From the Configuration menu, select Add Gatekeeper.

The Add Gatekeeper dialog box appears.

3 Configure the Gatekeeper.

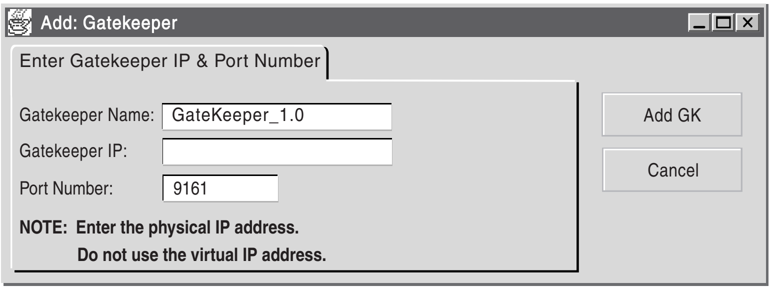
- **a** Enter the name of the Gatekeeper.
- **b** Enter the IP address of the Gatekeeper.
- **c** Enter the port number of the Gatekeeper. The default port is 9161.
- **d** Click the Add GK button.

The system adds the Gatekeeper and updates the Navigation tree.

The following figure shows the Add Gatekeeper dialog box.

> ***Note:*** The Gateway and TPS windows appear in the same format as the Gatekeeper dialog box. Therefore, the figure shows only the Gatekeeper dialog box.

Figure 4-16 Add Gatekeeper dialog box



Gatekeeper Name: GateKeeper_1.0

Gatekeeper IP:

Port Number: 9161

**NOTE: Enter the physical IP address.
Do not use the virtual IP address.**

Add Gateway

The Add Gateway selection allows you to add a Gateway to the Centrex IP network. The Add Gateway selection displays the Add Gateway dialog box.

Use the following procedure to add a Gateway to the Centrex IP network.

Procedure 4-25 Add a Gateway

At the PTM workstation

1 Select the Gateway you want to add.

2 From the Configuration menu, select Add Gateway.

The Add Gateway dialog box appears.

3 Configure the Gateway.

- **a** Enter the name of the Gateway.
- **b** Enter the IP address of the Gateway.
- **c** Enter the port number of the Gateway. The default port is 161.
- **d** Click the Add GW button.

The system adds the Gateway and updates the Navigation tree.

Add TPS

The Add TPS selection allows you to add a terminal proxy server (TPS) to the Centrex IP network. The Add TPS selection displays the Add TPS dialog box.

Use the following procedure to add a TPS to the Centrex IP network.

Procedure 4-26 Add a TPS

At the PTM workstation

1 Select the Gatekeeper with the TPS you want to add.

2 From the Configuration menu, select Add TPS.

The Add TPS dialog box appears.

3 Configure the TPS.

a Enter the name of the TPS.

b Enter the IP address of the TPS.

c Enter the port number of the TPS. The default port is 6161.

d Click the Add TPS button.

The system adds the TPS and updates the Navigation tree.

If the TPS exists and is registered with the Gatekeeper, the TPS appears under the TPS folder in the Navigation tree.

If the TPS exists and is not registered with the Gatekeeper, the TPS appears under the TPS folder in the Navigation tree.

If the TPS does not exist, the TPS does appear in the Navigation tree. The PTM displays an error message.

Change Device Name

The Change Device Name selection allows you to change a device name. The Change Device Name selection displays the Change Device Name dialog box.

The following table displays the fields in the Change Device Name dialog box.

Table 4-21 Change Device Name dialog box

Field	Description
Old Name	Name of the old device (This name displays automatically when you select the device name you want to change.)
New Name	Name of the new device

Use the following procedure to change a device name.

Procedure 4-27 Change Device Name

At the PTM workstation

1 Select the device name you want to change.

2 From the Configuration menu, select Change Device Name.

The Change Device Name dialog box appears. The old device name of the device you selected displays.

3 Change the device name.

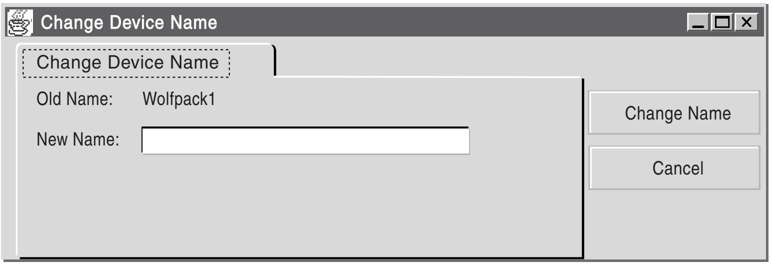
a Enter the new device name.

b Click the Change Name button.

The system changes the device name, and updates the Navigation tree.

The following figure shows the Change Device Name dialog box.

Figure 4-17 Change Device Name dialog box



Old Name: Wolfpack1

New Name:

Delete Device

The Delete Device selection allows you to delete a device. The Delete Device selection displays the Delete Device dialog box.

The Delete Device dialog box displays the name of the device you selected to delete. A prompt asks, “Are you sure you want to delete this device?”

Use the following procedure to delete a device name.

Procedure 4-28 Delete Device

At the PTM workstation

1 From the Navigation tree, select the device you want to delete.

2 From the Configuration menu, select Delete Device.

The Delete Device dialog box appears with the device you selected displayed. A prompt asks, “Are you sure you want to delete this device?”

3 Click the Delete Device button.

The system deletes the device, and updates the Navigation tree.

Add New User

The Add New User selection allows Administrators to add a new user to the Centrex IP network. The Add New User selections displays the Add New User dialog box.

The following table displays the fields in the Add New User dialog box.

Table 4-22 Add New User dialog box

Field	Description
User Name	Name of the user
Password	Password of the user
User Level	Level of access of the user: • Administrator • General Read/Write • General Read Only

An explanation of the three user levels follows:

- Administrator—user has full access to all aspects of the PTM
- General Read/Write—user has access to all maintenance functions of the PTM, but cannot add or delete users
- General Read Only—user can view maintenance information, but cannot release a call, or add or delete users

Use the following procedure to add a new user to the Centrex IP network.

Procedure 4-29 Add New User

At the PTM workstation

1 From the Configuration menu in the menu bar, select Add New User.

The Add New User dialog box appears.

2 Add the new user.

a Enter the name for the new user.

b Enter the password for the new user.

c Select the user level (Administrator, General Read/Write, or General Read only).

d Click the OK button.

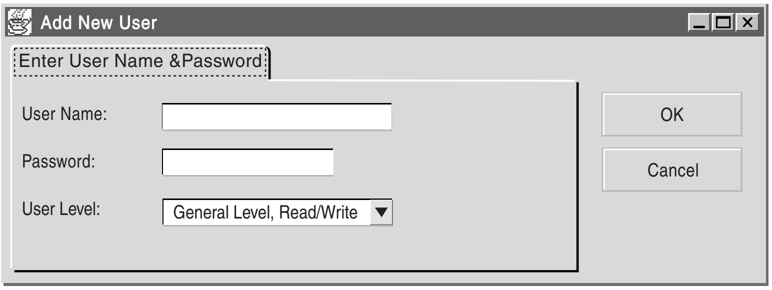
The system adds the new user to the PTM User Name MIB database, and a confirmation message appears

If the add is successful, the user name and password become active immediately.

If the add fails, the user will be informed that the add failed and to try again.

The following figure shows the Add New User dialog box.

Figure 4-18 Add New User dialog box



User Level: General Level, Read/Write

Change User Password

The Change User Password selection allows you to change your password. The Change User Password selection displays the Change Password dialog box.

Use the following procedure to change your password.

Procedure 4-30 Change User Password

At the PTM workstation

1 From the Configuration menu, select Change User Password

The Change Password dialog box appears.

2 Change your password.

- **a** Enter your old password.
- **b** Enter your new password.
- **c** Enter your new password again in “Repeat New Password.”

3 Click the Change Password button.

Delete User

The Delete User selection allows Administrators to delete users from the Centrex IP network. The Delete User selection displays the Delete User dialog box.

Use the following procedure to delete a user.

Procedure 4-31 Delete User

At the PTM workstation

1 From the Configuration menu, select Delete User.

The Delete User dialog box appears.

2 Enter the user name you want to delete.

3 Click the Delete User button.

Help menu

The PTM GUI also provides a help text capability for the following applications:

- user name and password
- Gatekeeper window
- Gateway window
- DN Search window
- individual menu choice
- main screen
- terminal window
- configuration window
- add Gatekeeper, Gateway, user, and change password
- event history window
- TPS
- quality of service (Qos) data

Help text procedures

Use the following procedures to access help text from the PTM GUI.

Procedure 4-32 Accessing PTM help text

At the PTM workstation

1 After you have loaded the PTM GUI, click and hold down the Help pull-down menu.

2 Select Contents...

The PTM Help panel displays to enable the user to access help screens during PTM use.

Three icons in the upper left-corner of the PTM Help panel also display. Use these icons to access customized help text: Table of Contents, Help Index, and Help Search. Also when you move the cursor over the icons on the tabs, the PTM GUI displays tools tips about the contents of the tabs.

For enhanced viewing, use the vertical scroll bar and screen resize capabilities, as needed. Also use the large right and left arrows immediately above the three PTM icons to redisplay previous help screens.

The following procedures describe how to access each of these customized Help capabilities.

Procedure 4-33 Accessing Help Table of Contents

At the PTM workstation

1 Accessing PTM Help automatically loads the default Table of Contents capability.

Information related to Centrex IP operation is available for display in the left side of the PTM panel. Topics includes PTM introductory information. PTM login information includes default user ID, password, available language options, and basic launching instructions.

2 Click any of the of the topics listed in the PTM panel.

The corresponding help text for the selected topic displays in the right-hand side of the PTM Help panel.

3 You can also access Help Table of Contents any time during PTM GUI operation. Just click the first PTM Help icon at the upper-left corner of the PTM Help panel.

Procedure 4-34 Accessing Help Index

At the PTM workstation

1 To display help information on several Centrex IP topics, use the PTM Help Index capability. Click the middle PTM Help icon at the upper-left corner of the PTM Help panel.

An index list of Centrex IP topics display in the left side of the PTM Help panel. (Use the vertical scroll bar to view additional topics.)

2 Click any of the of the topics listed in the PTM panel.

The corresponding help text for the selected topic displays in the right-hand side of the PTM Help panel.

Procedure 4-35 Accessing Help Search

At the PTM workstation

1 To display customized information, use the PTM Help Search capability. Click the third PTM Help icon at the upper-left corner of the PTM Help panel.

The Find field displays below the three PTM Help icons.

2 Enter any word or phrase related to a Centrex IP topic in the Find field. (The Help Search capability is not case sensitive.) Press the Enter key.

The right side of the PTM screen displays help pages containing the entered word.

3 Click on any topic listed in the left side of the PTM panel.

The right side of the PTM panel displays help text corresponding to the selected topic from the previous step. The selected topic is also highlighted.

5 DHCP and load servers

Overview

Centrex IP supports automatic loading and configuration of the Gateway card and the i2004 Internet Telephone through the use of the protocols and servers that follow:

- Dynamic Host Configuration Protocol (DHCP) and a DHCP server
- File Transfer Protocol (FTP) and a load server
- Trivial File Transfer Protocol (TFTP)

Gateway card

The Gateway card uses the DHCP server that runs on the Gatekeeper to retrieve the following information:

- the Internet Protocol (IP) address of the card
- the name of the application loadfile for the card
- the location of the application loadfile for the card
- the IP address of the Gatekeeper
- the IP address for the DHCP server for the card

i2004 Internet Telephone

The i2004 Internet Telephone uses a separate DHCP server that runs on a Windows NT machine to retrieve the following information:

- the IP address of the telephone
- the subnet mask for the i2004 telephones
- the IP address of the default router
- the IP address of the primary Terminal Proxy Server (TPS)
- the IP address of the secondary TPS

DHCP and DHCP server

DHCP allows clients to dynamically retrieve information at start-up from a server. DHCP is an Internet Draft Standard Protocol (RFC 2131) that is based on the Bootstrap Protocol (BOOTP). BOOTP supports the manual configuration of host information in a database. DHCP supports automatic configuration with the dynamic allocation of information to newly attached hosts.

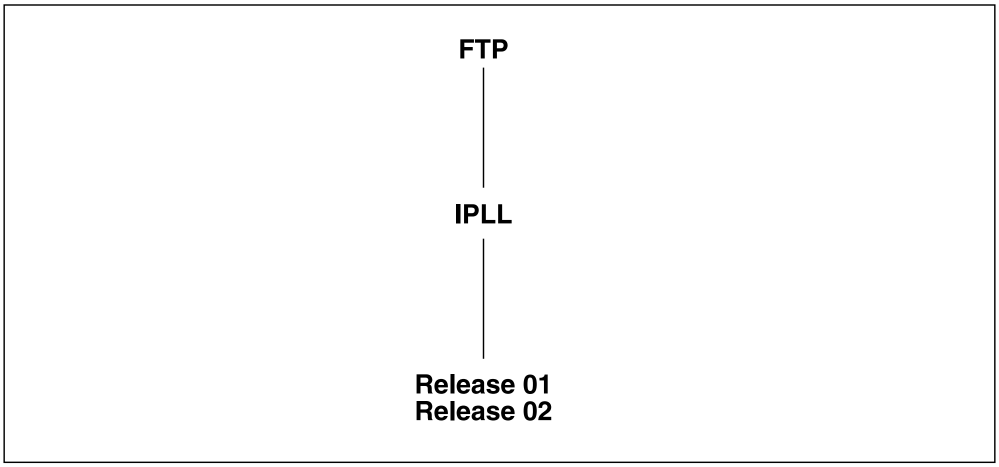
The DHCP server is the software that provides the configuration information to the clients. In Centrex IP, the DHCP server that services the Gateway card is part of the central office (CO) local area network (LAN). For the purposes of this chapter, this DHCP server is referred to as the CO DHCP server. The CO DHCP server runs on the Gatekeeper. The DHCP server that services the IP phones resides on the customer enterprise. For the purposes of this chapter, this DHCP server is referred to the enterprise DHCP server.

FTP load server

The CO DHCP server uses FTP to retrieve the loadfiles from the FTP load server. FTP is a standard high-level protocol for transferring files from one computer to another computer. FTP is an Internet Draft Standard Protocol (RFC 959) that runs on top of the User Datagram Protocol (UDP).

The FTP load server can run on the same machine as the CO DHCP server or a different machine. The loadfiles on the FTP load server reside in the `\ftp` directory. Figure 5-1 shows the directory structure.

Figure 5-1 Example of `\ftp` directory structure

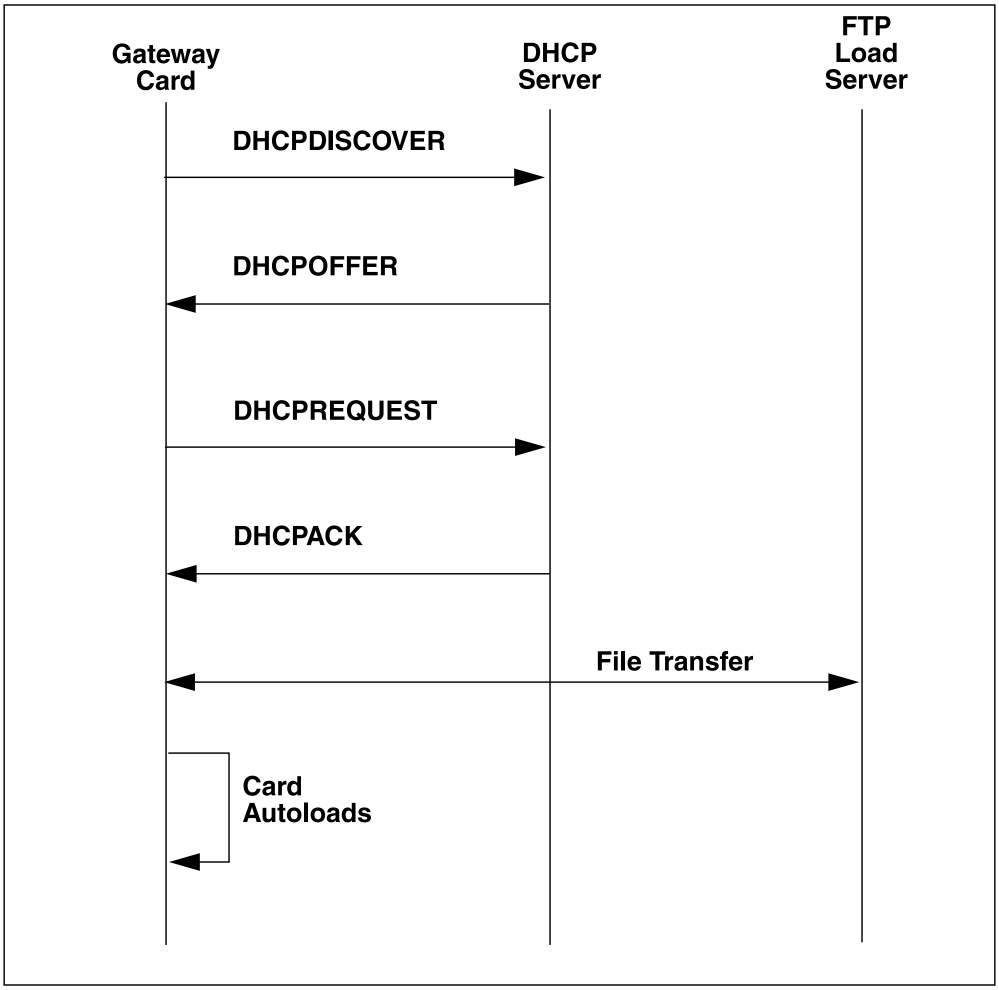


Note: In Figure 5-1, IPLL refers to the IP Local Loop application load.

Message sequence

When the Gateway card boots, the card exchanges messages with the CO DHCP server and FTP load server. Figure 5-2 shows the message sequence.

Figure 5-2 Message sequence when Gateway card boots



Note: If the Gateway card and the CO DHCP server are on separate subnets, a relay agent in the host or router transfers requests from the Gateway card to the CO DHCP server.

Detailed information on the message sequence follows:

1. The Gateway card receives power and boots. The boot activities follow:
   - The Gateway card begins the boot sequence from read-only memory (ROM).
   - The central processing unit (CPU) chip comes up.
   - The Gateway card checks dynamic random access memory (DRAM) availability.
2. The Gateway card broadcasts a DHCPDISCOVER message to locate the CO DHCP server.
3. The CO DHCP server responds with a DHCPOFFER message that includes the information that follows:
   - the IP address of the DHCP server
   - the IP address of the Gatekeeper
4. The Gateway card issues a DHCPREQUEST message for loadfile and configuration information.
5. The CO DHCP server responds with a DHCPACK message that contains the information that follows:
   - the IP address of the Gateway card
   - the name of the application loadfile for the Gateway card
   - the IP address of the FTP load server
6. The Gateway card uses a file transfer protocol to pull the loadfile from the FTP load server.
7. The Gateway card loads the retrieved loadfile and the remainder of the operating system into random access memory (RAM).
8. The Gateway application starts.

Requirements

This section provides the minimum requirements and recommended practices for the CO DHCP server and FTP load server.

CO DHCP server

For Centrex IP, the CO DHCP server must meet the requirements that follow:

- The CO DHCP server must provide full support for RFC 2131 and RFC 2132.
- The CO DHCP server must run on the Gatekeeper.

- The CO DHCP server can run on the same machine as the FTP load server. If the CO DHCP server runs on a different machine, Gateway cards may not be able to boot if the FTP load server is out of service.
- The CO DHCP server is part of the central office LAN.
- The CO DHCP server can run on the same subnet as the Gateway card or a different subnet.

This document describes how to use Nortel Networks NetID as the DHCP server for a Gateway card. Table 5-1 lists the system requirements for NetID.

Table 5-1 NetID system requirements

NetID Product	Platform	Required software	RAM	Disk space
NetID Application Server	Windows NT 4.0	Oracle 7.3 Server and SQL*Net Version 2 *or* Oracle 8 Server and SQL*Net 2	64 Mbyte	10 Mbyte
NetID Management Console	Not applicable	Netscape 4.5 or higher with JDK 1.1 (included with NetID CD)	Not applicable	Not applicable
NetID DHCP Server	Windows NT 4.0	Not applicable	64 Mbyte	10 Mbyte
NetID Server Manager	Windows NT 4.0	Oracle 7.3 Server and SQL*Net Version 2 *or* Oracle 8 Server and SQL*Net 2	64 Mbyte	10 Mbyte

FTP load server

For Centrex IP, the FTP load server must meet the requirements that follow:

- The FTP load server can run on the same machine as the DHCP server and the Gatekeeper.
- The FTP load server can run on the same subnet as the Gateway card or a different subnet.
- The FTP server must provide full support for RFC 959.

This document describes how to use Microsoft's Internet Information Server as the source for FTP service.

Installation and configuration

NetID is preinstalled on the Gatekeeper as the DHCP server for the Gateway card. For NetID installation procedures, refer to Installation Method 26-0332, *3rd Party Integrator Preconfiguration Guide*.

Configure NetID

Use Procedure 5-1 to configure NetID as a DHCP server for Centrex IP. The configuration process consists of the actions that follow:

- Add a network.
- Add a subnet.
- Add a DHCP server host.
- Add a DHCP server.
- Add a Gateway card.

> ***Note:*** NetID identifies a Gateway card as a host.

Procedure 5-1 Configure NetID as a DHCP server for Centrex IP

From the Gatekeeper

1 Open Netscape Communicator.

Enter the physical IP address of the DHCP server.

The NetID Login window opens.

2 Enter the user id and password. The default user id is **admin** and the password is **NETID**. Your office can change the user id and password or create new user ids and passwords.

> ***Note:*** The password is case sensitive.

The NetID Management Console opens.

3

ATTENTION

When you add a DHCP option to a NetID object, NetID erases the existing DHCP option and the NetID managed options for the object.

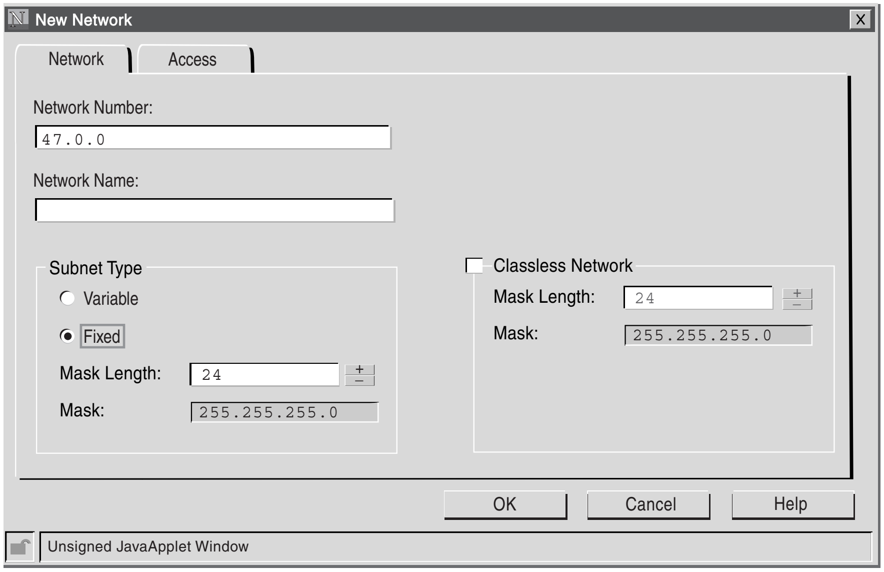
The Norton AntiVirus program can slow the performance of the NetID Management Console. At the first NetID login, the Norton AntiVirus program checks each Java applet as the applet downloads.

Add a new network.

a Click the root object `IP Address`.

b From the pull-down menu, select **Options->New Network**.

The New Network window opens.



New Network

Network Number: 47.0.0

Network Name:

Subnet Type

○ Variable

● Fixed

Mask Length: 24

Mask: 255.255.255.0

□ Classless Network

Mask Length: 24

Mask: 255.255.255.0

Unsigned JavaApplet Window

c Enter the information that follows:

- Network Number
- Network Name
- Subnet Type

> ***Note:*** Contact your network engineering group if you need help with this information.

d Click the OK button.

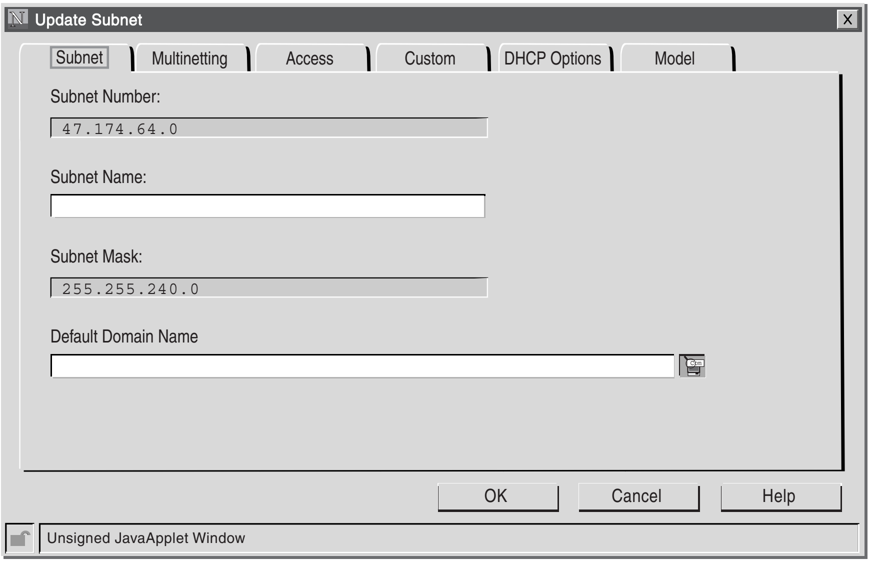
The NetID Management Console opens.

4 Add a new subnet.

a Make sure that the network that you added in step 3 is selected.

b From the pull-down menu, select **Options->New Subnet**.

The Update Subnet window opens.



Subnet Number: 47.174.64.0

Subnet Name:

Subnet Mask: 255.255.240.0

Default Domain Name

c Click the Subnet tab.

d Enter the Subnet Name and Default Domain Name.

> ***Note:*** Contact your network engineering group if you need help with this information.

e Click the DHCP Options tab.

f Click the Add button. Enter the IP address of the virtual Gatekeeper.

g Click the OK button.

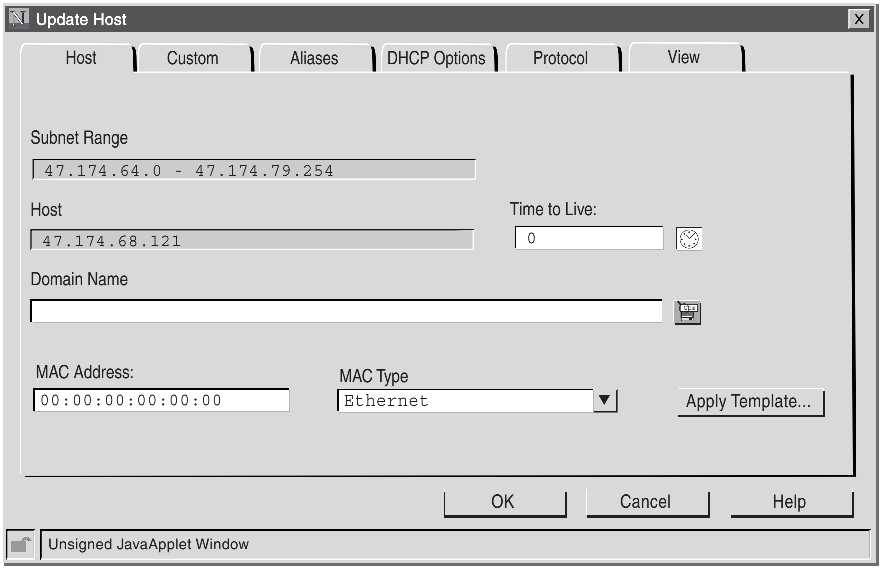
The NetID Management Console opens.

5 Add a new DHCP server host.

a Make sure that the subnet that you added in step 4 is selected.

b From the pull-down menu, select **Options->New Host**.

The Update Host window opens.



Subnet Range: 47.174.64.0 - 47.174.79.254

Host: 47.174.68.121

Time to Live: 0

Domain Name:

MAC Address: 00:00:00:00:00:00

MAC Type: Ethernet

c Click the Host tab.

d Make sure the information is correct.

e Click the OK button.

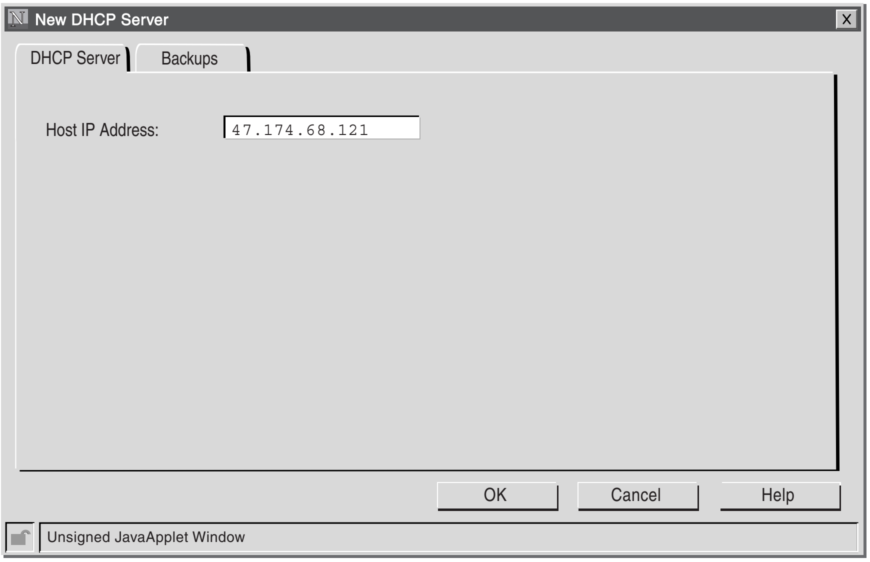
The NetID Management Console opens.

6 Add a new DHCP server.

a Make sure that the DHCP server host that you added in step 5 is selected.

b From the pull-down menu, select **Options->New DHCP server**.

The New DHCP Server window opens.



Host IP Address: 47.174.68.121

c Click the DHCP Server tab.

d Enter the IP Address of the Gatekeeper.

e Click the OK button.

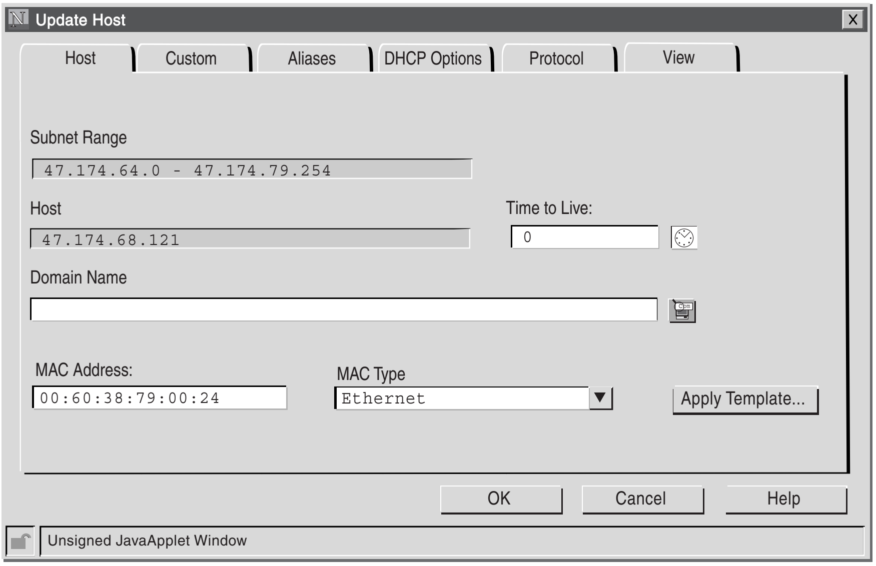
The NetID Management Console opens.

7 Add a new Gateway card.

a Click the subnet that you added in step 4.

b From the pull-down menu select **Options->Update Host**.

The Update Host window opens.



Subnet Range: 47.174.64.0 - 47.174.79.254

Host: 47.174.68.121

Time to Live: 0

Domain Name:

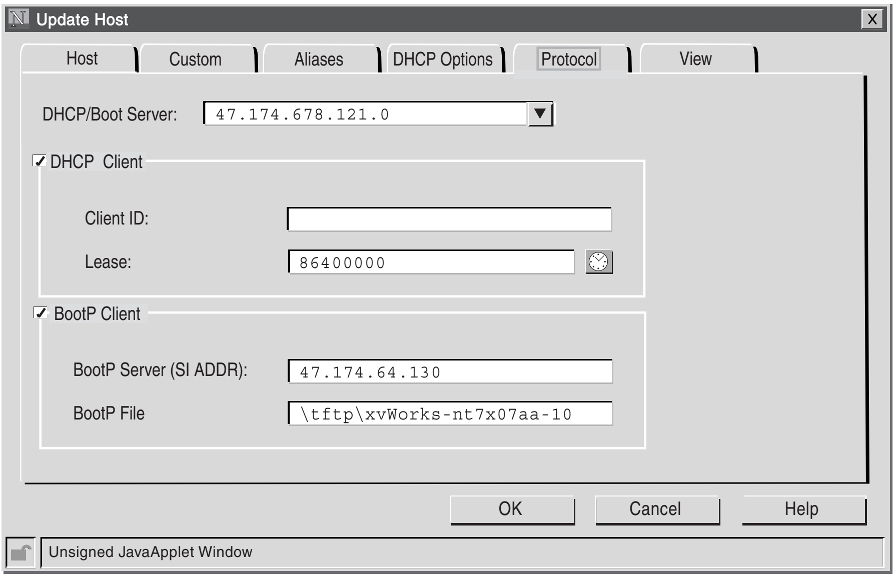
MAC Address: 00:60:38:79:00:24

MAC Type: Ethernet

c Click the Host tab.

- **i** Enter the MAC address of the Gateway card in the MAC Address field. The MAC address is a 12-digit number stamped on the card.
- **ii** Use the pull-down menu to select Ethernet for the MAC Type.

d Select the Protocol tab.



DHCP/Boot Server: 47.174.678.121.0

☑ DHCP Client

Client ID:

Lease: 86400000

☑ BootP Client

BootP Server (SI ADDR): 47.174.64.130

BootP File: \tftp\xvWorks-nt7x07aa-10

e Configure the host with the steps that follow:

- **i** Use the pull-down menu at DHCP/Boot Server to select the DHCP server.

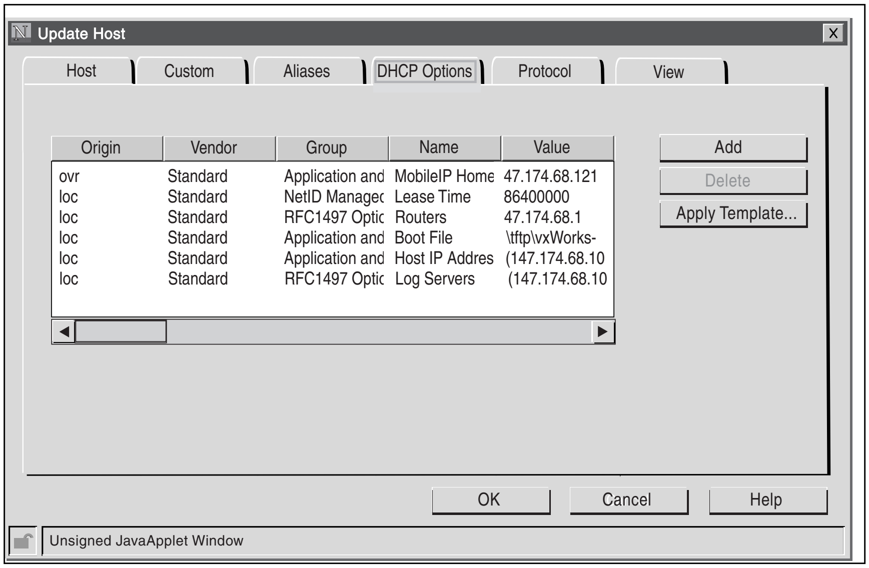
ii Select the DHCP Client and BootP Client boxes.

iii Change the Lease field to **86400000**.

iv Change the BootP Server field to the IP address of the Gatekeeper.

v Change the BootP File field to the location of the application loadfile for the Gateway card. Do not enter the drive letter. The default drive is c. Refer to the section "FTP load server" in this chapter for information on directory structure.

f Select the DHCP Options tab.



Origin	Vendor	Group	Name	Value
ovr	Standard	Application and	MobileIP Home	47.174.68.121
loc	Standard	NetID Managec	Lease Time	86400000
loc	Standard	RFC1497 Optic	Routers	47.174.68.1
loc	Standard	Application and	Boot File	\tftp\vxWorks-
loc	Standard	Application and	Host IP Addres	(147.174.68.10
loc	Standard	RFC1497 Optic	Log Servers	(147.174.68.10

i Click the Add button.

ii Confirm that the options for each host are correct.

iii Click the OK button.

8 Repeat step 7 for each Gateway card.

9 You have completed this procedure.

Configure FTP server

The FTP server comes preinstalled on the Windows NT operating system. To configure the FTP server for Centrex IP, use the following procedure.

Procedure 5-2 Configure the FTP service

From the Gatekeeper PC

1 From the Start menu, select Programs->Microsoft Internet Server (Common) ->Internet Service Manager.

The Microsoft Internet Service Manager window opens.

a Make sure that the state for FTP is Running.

2 Select the FTP service.

3 Use the right mouse button to select Service Properties.

The FTP Service Properties window opens.

4 Under the Service tab, make sure that Allow only anonymous connections is not selected.

5 Select the Logging tab.

6 Review the settings.

- **a** Make sure that Enable Logging is selected.
- **b** Make sure that logs are filed to the directory `c:\Winnt\system32\LogFiles`.
- **c** Make sure that a new log file is opened daily.

7 You have completed this procedure.

Use the following procedure to configure a user for FTP service.

> ***Note:*** Use the OK button to close all windows.

Procedure 5-3 Configure a user for FTP service

From the Windows NT desktop

1 From the Start menu, select Programs->Administrative Tools (Common)->User Manager for Domains.

The User Manager window opens.

2 From the User menu, select New User.

The New User window opens.

3 Enter the information for the new user.

- **a** Enter the Username as `gateway.`
- **b** Enter the Full Name as `IGW Loading`.
- **c** Enter the Description as `Login for IGW card to FTP load`.
- **d** Set the Password to `tasmanian`.
- **e** Make sure that User Cannot Change Password and Password Never Expires are selected.
- **f** Make sure that User Must Change Password at Next Login and Account Disabled are not selected.

4 Click Groups.

The Group Membership window opens.

5 Use the Add button to add the following items from the right side of the window to the left side of the window.

- Domain Users
- Users
- Domain Guest

6 Click OK.

7 Click Profile.

The User Environment Profile window opens.

8 Set the User Profile Path to `c:\ftp`.

9 Make sure that the local path is selected and the path is `c:\ftp`.

10 Click OK.

The New User window opens.

11 Click Add.

12 You have completed this procedure.

Operations

Use the following procedure to verify the DHCP sequence while the Gateway card boots.

Procedure 5-4 Verify DHCP message sequence

From the Windows desktop

1 From Start menu, select Settings->Control Panel.

2 Open the NetID icon.

3 From the pull-down menu, select Selected NetID Service->NetIDDHCP Server.

4 Click the Stop Selected Service button.

5 Enter **-d 9 -l .log** in the Startup Parameters field.

6 Click the Start Selected Service button.

NetID creates a log file in `C:\Program Files\NetID\log`.

7 Open the log file.

8 Look for the DHCP messages to identify the progress of Gateway loading.

9 You have completed this procedure.

Enterprise DHCP server

The enterprise DHCP server is located at the customer premises and runs on a Windows NT machine. It cannot run on the same machine as the CO DCHP server. The DHCP server must have a static IP address, subnet mask, and default router address. The enterprise DHCP server provides the following information to the i2004 telephones:

- the IP address of the telephone
- the subnet mask for the i2004 telephones
- the IP address of the default router
- the IP address of the primary TPS
- the IP address of the secondary TPS

In order for the enterprise DHCP server to automatically configure the i2004 telephones, you must configure the DHCP scope. The DHCP scope provides the DHCP client with the range of IP addresses that the server can supply and a subnet mask to assign to the clients. The subnet mask is the part of the IP address that identifies the subnetwork.

The following procedure is specific to the Microsoft Windows NT DHCP server. However, any DHCP server can be used to configure the i2004 phones as long as it uses the required options. The options required for the Centrex IP phones are as follows:

- router option—defines the default router for the subnetwork
- subnet mask option—defines the subnetwork that the i2004 phones are on
- site specific option (128 or 144)—defines the IP addresses of the primary and secondary TPS, port number, action code for the server, and retry count for the server.

Note: To configure the DHCP scope, you must log on as an administrator.

Procedure 5-5 Configure the enterprise DHCP server

At the Windows NT server

1 From the Start menu, select Settings->Control Panels. Open the Network control panel and select the Services tab.

2 Click the Add button to select the Microsoft DHCP Server from the Select Network Service window. Click OK. The system will prompt you to reboot.

> ***Note:*** You may need the WinNT 4.0 Server Enterprise CD if the DHCP Manager has not been installed.

3 After the system has restarted, go to the Start menu and select Programs->Administrative Tools (Common)->DHCP Manager.

The DHCP Manager window opens.

4 Under DHCP Servers, select the *Local Machine* icon. Local Machine indicates that you are configuring the local DHCP server and not a remote DHCP server.

5 From the Scope menu, select Create.

The Create Scope window opens.

6 Enter the following data to create a scope:

- Set IP Address Pool (Start Address and End Address)
- Subnet Mask
- Exclusion Range (Start Address and End Address)
- Lease Duration (minimum of 1 hour)
- Name (optional)
- Comment (optional)

7 Click the OK button to complete the scope.

A dialog box opens that asks "Activate the new scope now?"

8 Click Yes to activate the scope.

The DHCP Manager window opens with the new scope added. The yellow light bulb next to the IP address indicates an active scope.

The Site Specific option is required for Centrex IP phones. Use the following procedure to add a Site Specific option.

Procedure 5-6 Add a Site Specific option

At the Windows NT server

1 From the DHCP_Options menu, select Defaults.

The DHCP Options: Defaults window opens.

2 Click the New button.

The Add Option Type window opens.

3 Enter the following data in the fields:

- Name: `128 Site Specific Option`
- Data_Type: Select "String" from the pull-down menu
- Identifier: `128`
- Comment: (optional)

4 Click OK to return to the DHCP_Options window.

5 Click OK again to return to the DHCP Manager window.

To apply the DHCP options entered in the previous procedure to a scope, use the following procedure.

Procedure 5-7 Apply DHCP options to a scope

At the Windows NT server

1 From the DHCP Manager window, select Scope from the DHCP_Options menu.

The DHCP Options: Scope window opens.

2 From the Unused Options list, select "003 Router" and click the Add button to add to the Active Options list.

3 Click the Value button.

The DHCP Options window expands.

4 Click the Edit Array button.

The IP Address Array Editor window opens.

5 Enter the IP address for the default router for that subnet. Click the Add button.

The new IP address appears in the IP Address list.

6 Click the OK button to return to the DHCP_Options: Scope window.

7 From the Unused Options list, select “128 Site Specific Option” and click the Add button to add to the Active Options list.

8 In the String field, follow the string format to enter the Site-Specific Option: **Nortel-i2004-A,111.222.333.444:pppp,aaa,rrr;111.222.333.444:pppp,aaa, rrr.**

where

“Nortel-i2004-A” uniquely identifies the Nortel option. The “A” identifies the version of the scope.

“111.222.333.444:pppp” identifies the IP address (pppp identifies the port number)

“aaa” identifies the action code for the server

“rrr” identifies the retry count for the server

Example
Nortel-i2004-A,121.75.98.104:5000,01,05;121.75.98.105:5000,01,05.

Note: The IP address specified should be the IP address of the TPS.

9 Click OK to close the DHCP_Options window and return to the DHCP Manager window.

10 Check the Option Configuration panel in the DHCP Manager window to see the value of the string just entered.

If the DHCP server has not been activated previously, use the following procedure to start the DHCP server.

Procedure 5-8 Start the DHCP Server

At the Windows NT server

1 From the Start menu, select Programs->Administrative Tools (Common)->DHCP Manager.

The DHCP Manager window opens.

2 Select the desired DHCP server under the Local Machine icon. Select Activate from the Scope menu.

The light bulb appears lit by the IP address of the DHCP server.

TFTP/UFTP load server

The TPS uses the TFTP/UFTP load server to update firmware on the i2004 telephones. When the i2004 telephone powers up, the telephone connects to the TPS to verify the firmware. If the i2004 has been loaded with DEV A70 or later, the UFTP server can be used. If not, the TFTP server must be used. If the telephone needs new firmware, the TPS uses TFTP/UFTP and a TFTP/UFTP load server to update the firmware. The TFTP/UFTP load server resides on the same machine as the CO DCHP server (the Gatekeeper) or on a different machine.

Refer to the *i2004 Internet Telephone User Guide* for details on i2004 use.

TFTP and TFTP load server

TFTP is a simple protocol that transfers files without many of the features of FTP. TFTP can read and write files to a remote server, but TFTP cannot provide FTP functions such as directory lists or user authentication.

TFTP is an Internet Draft Standard Protocol (RFC1350) that runs on top of the UDP.

For Centrex IP, the TFTP load server must meet the requirements that follow:

- The TFTP load server can run on the same machine as the Gatekeeper.
- The TFTP load server can run on the same subnet as the Gateway card or a different subnet.
- The FTP server must provide full support for RFC 1350.

Centrex IP uses the Walusoft TFTP Suite Pro package as the TFTP load server. Refer to Installation Method 26-0332, *3rd Party Integrator Preconfiguration Guide*, for instructions on how to install Walusoft TFTP Pro.

Operations

To start the TFTP load server, go to the Start->Programs menu and select the name of the Walusoft TFTP Suite Pro package. The TFTP load server runs as long as the console is open.

The window displays the IP address of the client that receives a file. The text is blue while the file transfers. When the transfer finishes, the text is black. If the transfer times out or does not finish successfully, the text is red.

UFTP and UFTP load server

UFTP is a proprietary protocol that uses the same port as the Unistim messages currently used for the E2 terminal messaging. The UFTP rides on a proprietary Reliable UDP (RUDP) layer to ensure proper message delivery.

Operations

The UFTP server is deployed though the install shield. The install shield places the server program and its supporting files in the proper directories.

The UFTP server consists of the following files:

- UFTPServer.jar - contains the java program files for the server
- ServerParms.ini - resides in a ServerParmDir subdirectory. The ServerParms.dat file contains the configuration variables required for the server.

- UFTPServerAutoStart.bat - starts the server, using the default settings from the ServerParms.ini file. The UFTPServerAutoStart.bat file brings up an MS DOS window, which the user must minimize.
- UFTPServerGUIStart.bat - brings up the user interface to the server. This file allows the following parameters to be altered:
  - server port - port used by the UFTP server to communicate with the i2004
  - max terminals - maximum number of i2004 phones allowed to be loading at one time
  - load path - parameter that tells the server program in which directory the i2004 load file resides.

The UFTP server is installed in the following directory structure:

Program files\Nortel Networks\UFTPServer

User interface

The UFTP server interface is available while the UFTP server is running.

The File menu contains the following options:

- Start - starts the UFTP server. Once started, the server reads the selected parameters and opens the selected port. Only one instance of the server can run at any time.
- Stop - stops the server. Once stopped, the server can be restarted using Start. Stop causes the program to reread the parameters.
- Exit - releases any resources associated with the server and quits the server application

> ***Note:*** Each field in the user interface displays tool tips. Place the mouse cursor over a field to display text identifying the purpose of the field or the valid range of values for that field. An attempt to enter an invalid value results in an error dialog box when performing a SAVE.

Limitations and restrictions

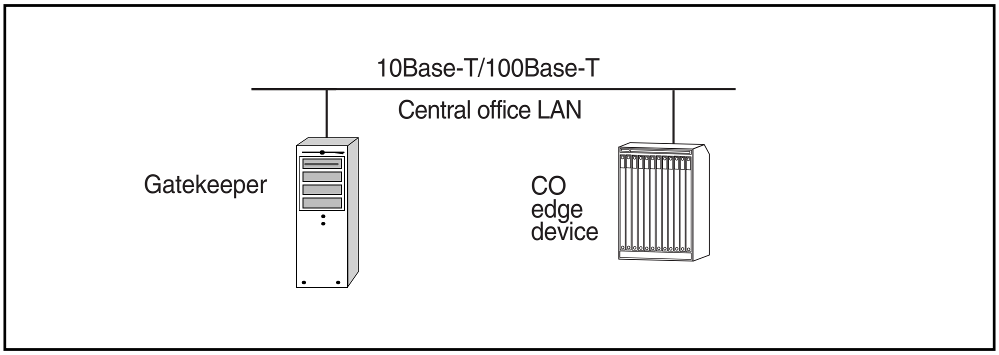
The loads used by the UFTP server must reside on the same device or be mapped to the same device where the UFTP server resides.

6 CO LAN and CO LAN edge device

Overview

The central office (CO) local area network (LAN) and CO LAN edge device connect the CO to the Enterprise network. Figure 6-1 shows an overview of the CO LAN and the CO LAN edge device.

Figure 6-1 Overview of CO LAN



CO LAN

The CO LAN is an Ethernet device that connects the Centrex IP Gateway cards (NT7X07AA) in the ISDN line trunk controller (LTCI) to the CO LAN edge device. The CO LAN can provide connection to the Gatekeeper.

CO LAN edge device

The CO LAN edge device is a router that provides wide area network (WAN) access between the CO, access network, and Enterprise network.

Capabilities of the CO LAN edge device follow:

- examines address information in packets
- sends the packet to the correct destination
- provides traffic control from the CO LAN for transmission on the access network
- can contain firewall functionality

Requirements

Devices that serve as the CO LAN or the CO LAN edge device must meet the requirements that follow:

- The Gateway cards require a 10/100Base-T Ethernet connection to the CO LAN.
- The CO LAN and CO LAN edge device connect with a 100Base-T Ethernet.
- If the Gatekeepers connect to the CO LAN, the Gatekeepers require a 10Base-T Ethernet connection.
- The CO LAN and the CO LAN edge device can reside inside the CO or outside the CO. However, standard restrictions on Ethernet reach apply to all connections.

Redundancy

This section describes configurations and requirements to achieve redundancy for the CO LAN in the Centrex IP network. The primary goal of redundancy is full system redundancy with no single point of failure. However, CO LANs can have different redundancy goals due to the different routing requirements of each configuration.

This section describes possible redundancy in the following configurations:

- CO LAN with routing-enabled edge device
- CO LAN with routing through an external router
- CO LAN without routing

> ***Note:*** This section describes routing and redundancy across the Centrex IP network from the CO LAN to the Enterprise LAN. Refer to the chapter “Overview” for more information on the Centrex IP network.

CO LAN with routing-enabled edge device

An edge device is equipment within the CO LAN that can provide routing over the WAN between the CO LAN and Enterprise LAN. For example, the Nortel Networks 5000S can be used as the CO LAN edge device to provide routing through Model 5381 Ethernet Router modules.

In the Centrex IP network, each LAN has an edge device that provides routing functions. The CO LAN uses the internal router as the CO LAN edge device.

> ***Note:*** This document does not describe the configuration of the Enterprise LAN edge device.

This section discusses redundancy in the following configurations:

- single router and simplex WAN connection
- single router and redundant WAN connections
- redundant routers and redundant WAN connections

Single router and simplex WAN connection

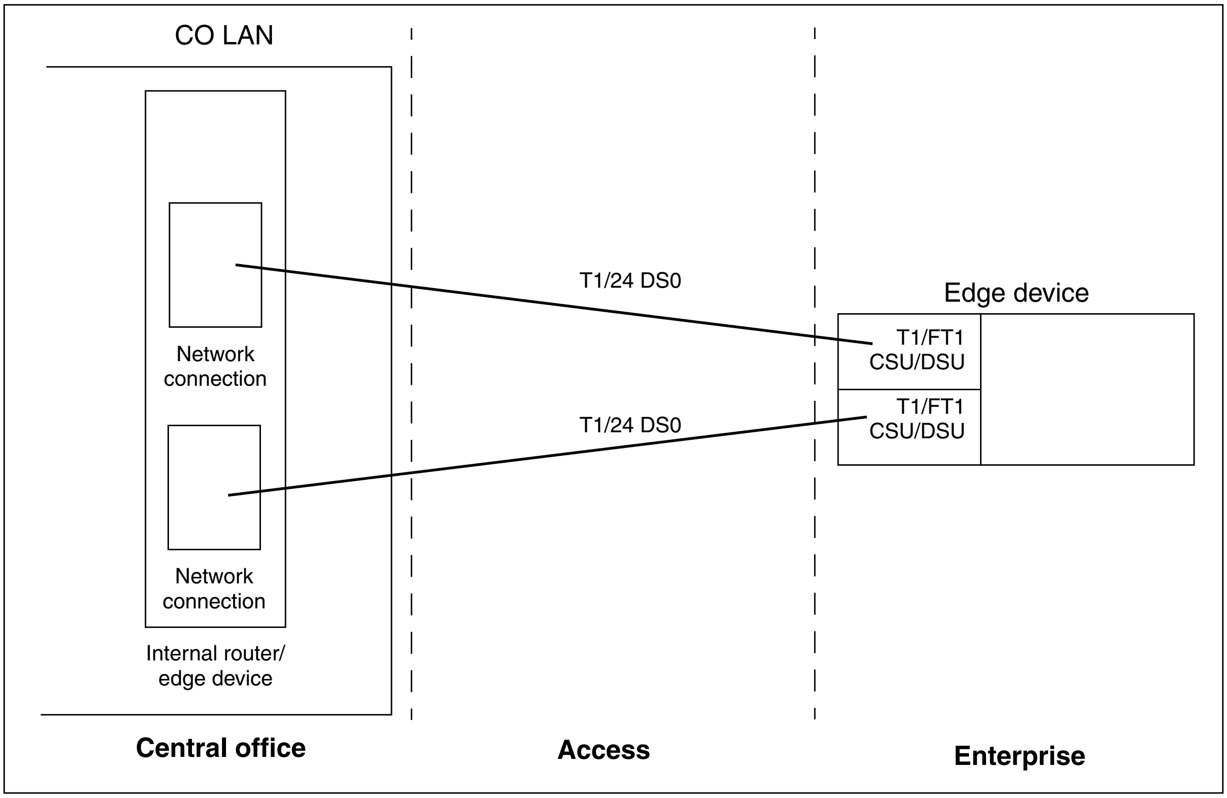
This configuration consists of the following components:

- a single router with two WAN interfaces in the CO LAN edge device
- a simplex WAN connection between the CO LAN and the Enterprise LAN
- a single router as the Enterprise LAN edge device

Figure 6-2 shows the redundancy in this configuration.

> *Note:* In figure 6-2, CSU refers to channel service unit. DSU refers to data service unit.

Figure 6-2 Redundancy with single router and simplex WAN connection



In figure 6-2, each network connection has two T1 interfaces that can operate as redundant interfaces.

This configuration has two single points of failure: the single router in the CO LAN edge device and the Enterprise LAN edge device. If either device fails, the network cannot route traffic.

If the two T1 interfaces in the network connection operate as redundant interfaces, a single T1 interface failure can not stop traffic on the network. The other T1 interface routes traffic.

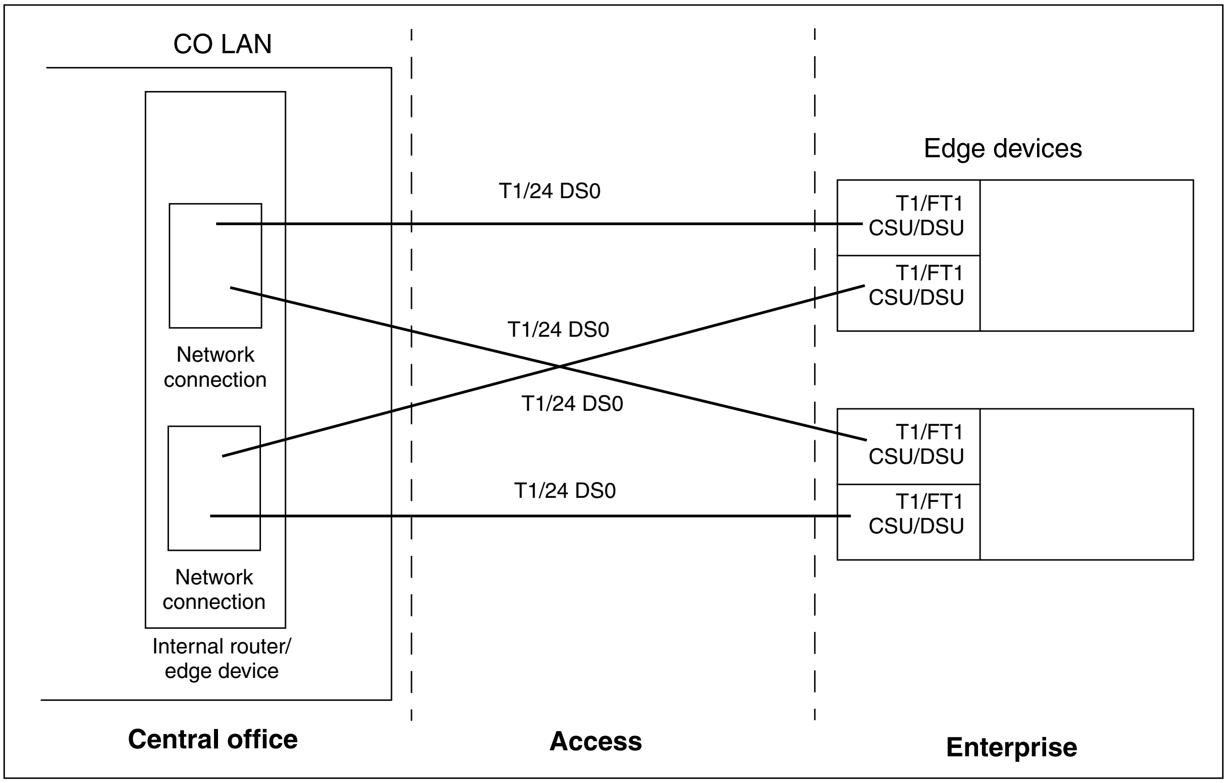
Single router and redundant WAN connections

This configuration consists of the following components:

- a single router with four WAN interfaces in the CO LAN edge device
- redundant WAN connections between the CO LAN and the Enterprise LAN
- two or more routers as Enterprise LAN edge devices

Figure 6-3 shows the redundancy in this configuration.

Figure 6-3 Redundancy with single router and redundant WAN connections



This configuration has one single point of failure: the single router in the CO LAN. If the router fails, the network cannot route traffic.

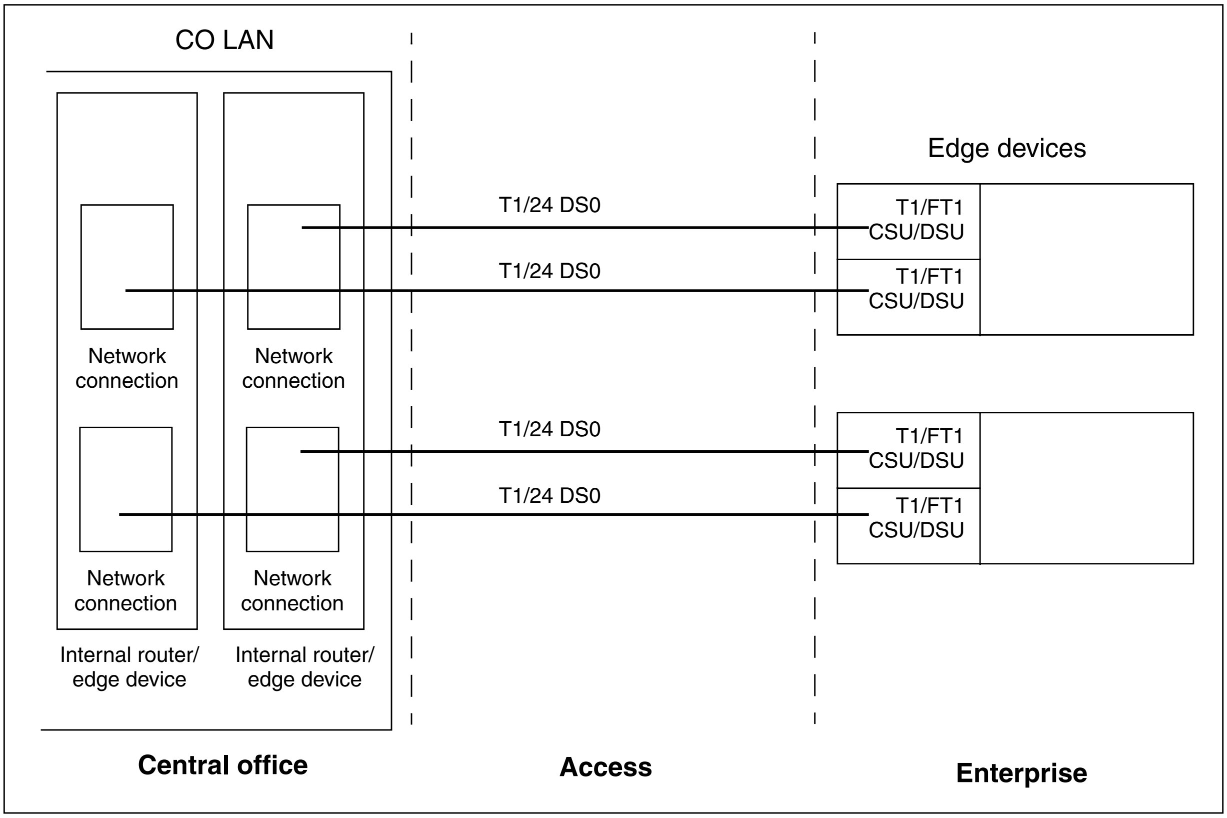
Redundant routers and redundant WAN connections

This configuration consists of the following components:

- two or more routers, each with two or more WAN interfaces in CO LAN edge devices
- redundant WAN connections between the CO LAN and the Enterprise LAN
- two or more routers as Enterprise edge devices

Figure 6-4 shows the redundancy in this configuration.

Figure 6-4 Redundancy with redundant routers and redundant WAN connections



Each network connection has two or more T1 interfaces that can operate as redundant interfaces.

This configuration has no single point of failure. With virtual router redundancy protocol (VRRP) and static routes that provide full backup of the devices and their interfaces, the network can support constant traffic flow. If a virtual router fails, the other virtual routers can assume the traffic flow.

If the two T1 interfaces in the network connection operate as redundant interfaces, a single T1 interface failure cannot stop traffic on the network. The other T1 interface routes traffic.

CO LAN with routing through an external router

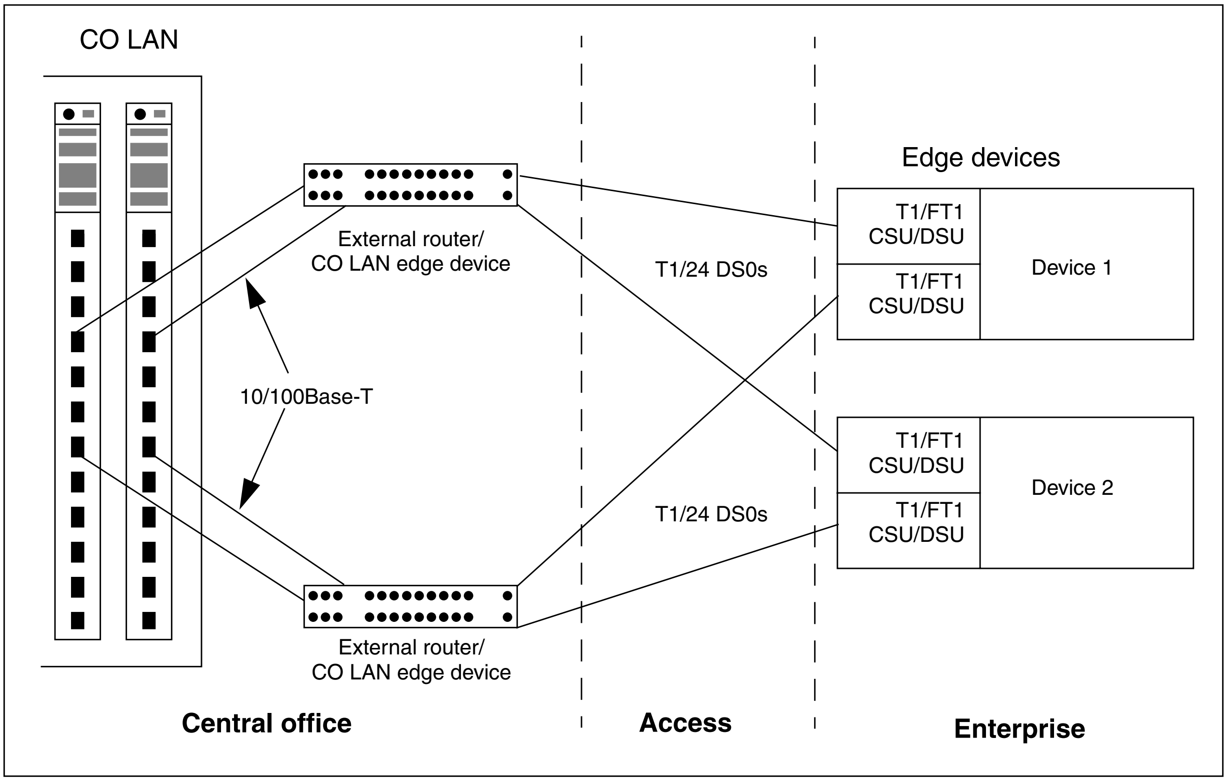
An external router can be used to provide routing over the WAN between the CO LAN and the Enterprise LAN.

In the Centrex IP network, each LAN has an edge device that provides routing functions. In this configuration, the CO LAN uses the external router as the edge device.

> ***Note:*** This document does not describe the configuration of the Enterprise LAN edge device.

Figure 6-5 shows the redundancy in this configuration.

Figure 6-5 Redundancy with 100 Mbyte uplinks



CO LAN without routing

If the CO LAN configuration does not require routing, Centrex IP and the CO LAN uses the redundancy in each Centrex IP component.

Gateway card

The Centrex IP Gateway card (NT7X07AA) provides simple link redundancy (SLR) to switch modules in the CO LAN. Refer to the "Link redundancy" section in the "Gateway" chapter of this document.

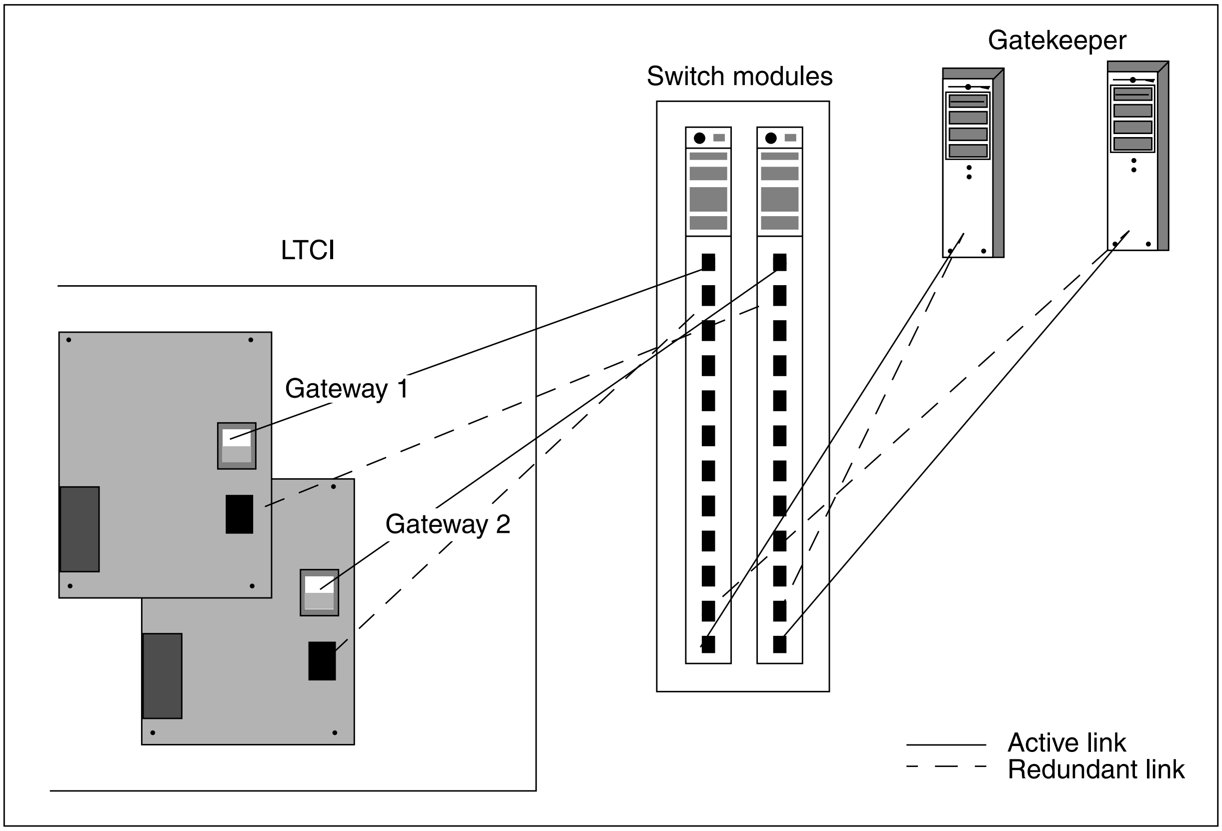
Gatekeeper

The Gatekeeper provides failover capability over two Ethernet connections to switch modules in the CO LAN. Refer to the "Failover" section in the "Gatekeeper" chapter of this document.

CO LAN

The CO LAN can provide redundant switch modules for each Gatekeeper and Gateway card. If one switch module fails, the second switch module assumes the traffic flow. Figure 6-6 shows the physical connection between the CO LAN, the Gatekeeper, and the Gateway card.

Figure 6-6 Redundancy within the CO LAN



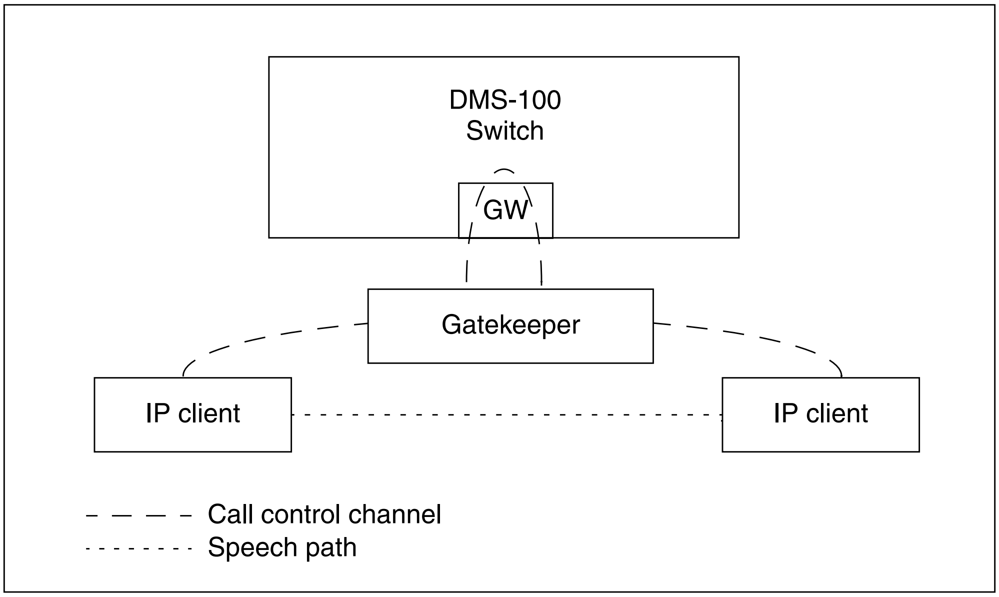
LAN-routed speech

Centrex IP supports LAN-routed speech, which allows two IP clients to establish a direct speech path between each other on a CO LAN. A direct speech path eliminates the need for the IP clients to route speech calls through the DMS switch. A direct speech path has the following benefits:

- decreases latency in a client-to-client IP basic call. Latency can occur due to additional transcoding in the Gateway of each leg of the call, since each call half must pass through a DSP in the Gateway.
- conserves links between remote locations and the host for the speech path, because the speech path does not use the Gateway or the DMS switch

Figure 6-7 illustrates the basic configuration of LAN-routed speech.

Figure 6-7 Basic configuration of LAN-routed speech



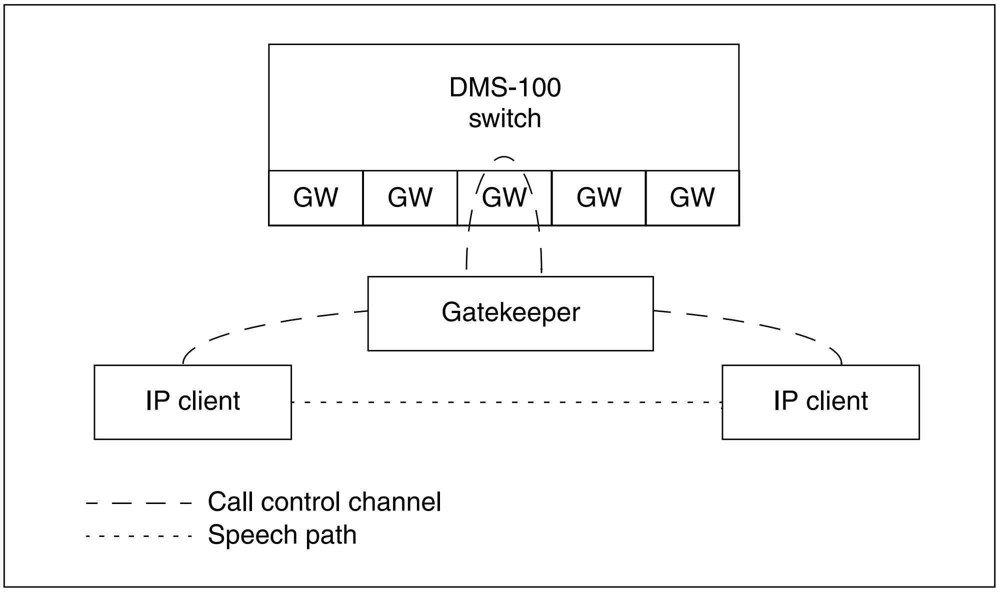
The IP clients use a real-time protocol (RTP) connection set up with FASTSTART messages. The Call Signaling H.225 messages that setup the call contain the FASTSTART messages.

Centrex IP supports LAN routed speech through a common Gateway and a common XMS peripheral module (XPM).

Common Gateway

Two IP clients served by the same Gateway/Gatekeeper pair can establish a direct speech path through an RTP connection set up with FASTSTART messaging. Figure 6-8 shows an example of this configuration.

Figure 6-8 LAN-routed speech through a common Gateway



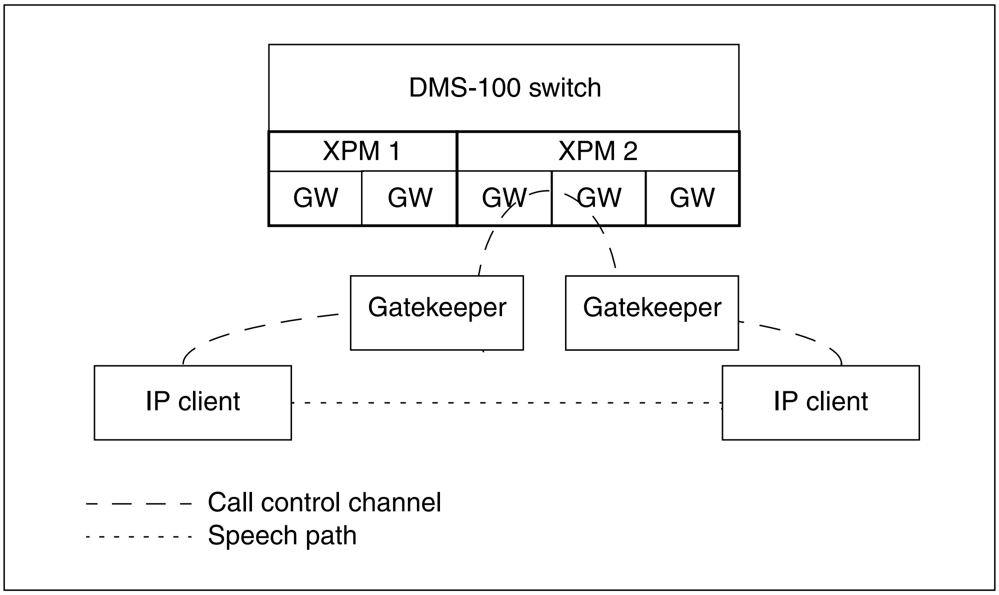
Common XPM

CAUTION
PRSU required for functionality
The LAN Routed Speech feature on a common XPM requires post-release software update (PRSU) HUD78.

Two IP clients served by different Gateways and the same XPM can establish a direct speech path. The clients pass FASTSTART parameters through the Gateways to identify the transmit and receive capabilities and ports. The same Gatekeeper or different Gatekeepers can serve the Gateways.

Figure 6-9 shows an example of this configuration.

Figure 6-9 LAN-routed speech through a common XPM



Provisioning and disabling

Subfield INTRASW in table IPINV (IP Inventory) indicates if the Gateway allows LAN-routed speech. Subfield INTRASW is available when the L selector in field GWTYPE in table IPINV is selected. The valid entries in INTRASW are `Y` or `N`. Enter `Y` to indicate the Gateway allows LAN-routed speech. Enter `N` to indicate the Gateway does not allow LAN-routed speech. The default value is `N`.

> ***Note:*** If an enterprise employs a network address translation (NAT) device for private to public IP address translation, disable intraswitching for the enterprise.

Revert to DMS-routed call

A speech call reverts from a LAN-routed call to a DMS routed call when the call needs supplementary services. Examples of supplementary services follow:

- Call Forward Don’t Answer
- Call Pickup
- Call Transfer
- Conference Calling
- Music On Hold
- Multiple Appearance Directory Number (MADN) bridging

Both configurations allow a speech call to revert from a LAN-routed call to a DMS-routed call. However, a LAN-routed call that reverts to a DMS-routed call cannot go back to a LAN-routed call. The call continues to use DMS network resources for the life of the call.

Part III
Planning and engineering

This part contains the “System engineering” chapter.

7 System engineering

Overview

This chapter provides system planning and engineering information for the following personnel who set up a packet telephony network:

- telephony switch engineers
- data network engineers
- enterprise network engineers

Telephony switch engineers must be familiar with engineering the DMS-100 switch, which includes the XMS peripheral module (XPM). They must be especially familiar with the ISDN line trunk controller (LTCI).

Data network engineers must be familiar with setting up a wide area network (WAN). They must also know how to measure network capacity and performance, and how to engineer central office (CO) data access.

Enterprise network engineers must be familiar with the enterprise data network, including enterprise connectivity. Familiarity with common performance, capacity, and network management tools are also useful in planning the enterprise network of the Centrex IP system.

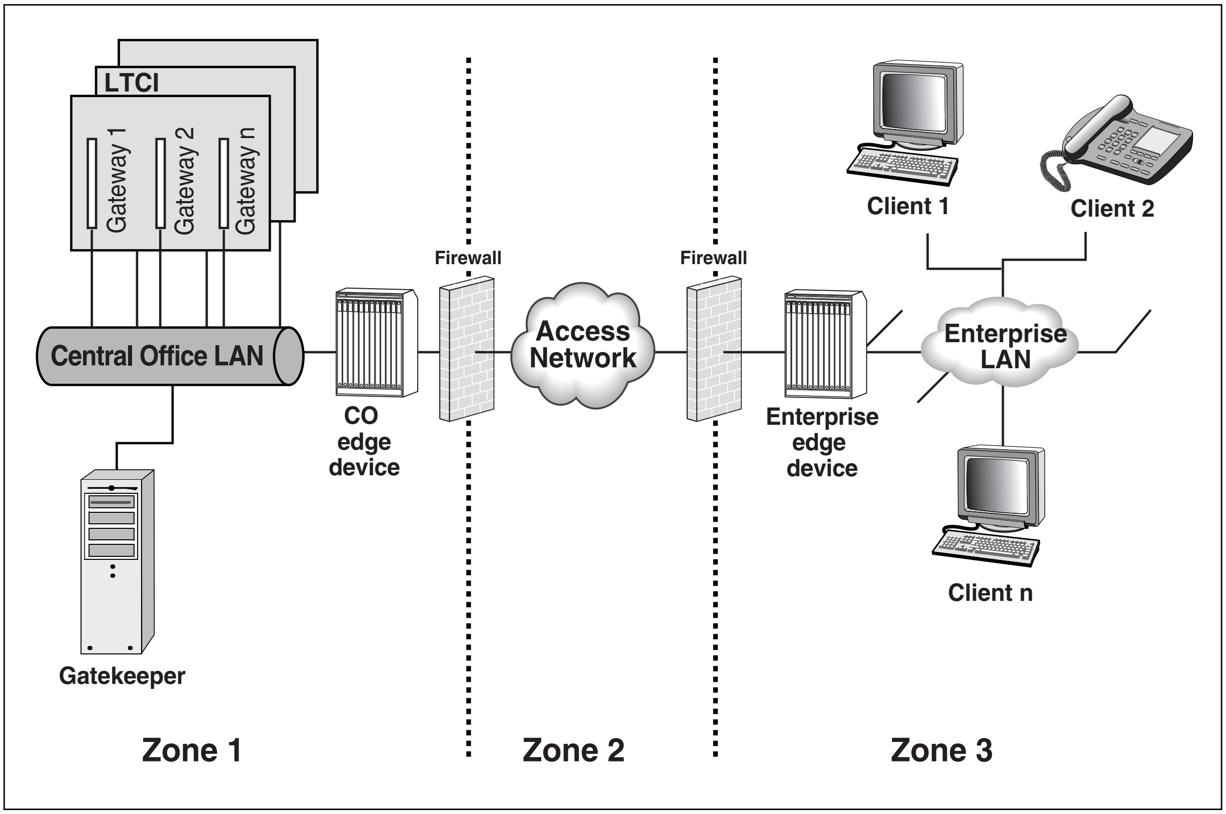
Centrex IP system

The Centrex IP network contains three groups of network components. The three networks are also referred to as zones. This chapter covers the planning and engineering aspects of three zones that comprise the Centrex IP system:

- zone 1: the CO network
- zone 2: the access network
- zone 3: the enterprise network

The following figure shows the division of the three network or zones.

Figure 7-1 Centrex IP network diagram



This chapter includes engineering of the DMS-100 components and the local area network (LAN) for the CO. It does not include the administration of the DMS-100 CO switch for the Centrex IP system.

This chapter includes engineering requirements for bandwidth and latency for the access network. It does not include specific data network topology.

This chapter covers specific capacity and performance parameters for an enterprise network to meet voice quality of service (QoS) requirements. It does not include specific data network topology for enterprise networks.

Central office network

The Centrex IP CO network includes the following components:

- a DMS-100 switch
- an Internet Protocol Gateway (IPGW) card located in an LTCI XPM
- a CO LAN with Ethernet connectivity and routing capability to the access data network

Optionally, telephony switch engineers can install the Gatekeeper in the CO network.

The DMS-100 switch

The computing module (CM) of the DMS-100 switch provides the following functions:

- provisioning support for the H.323-based terminal and the Gateway card
- loop maintenance for the H.323-based terminal
- node maintenance for the Gateway card

The XPM provides the following support functions:

- high-level data link control (HDLC) messaging (class II Q.931 signaling and proprietary messages) between the unified processor (UP) and the Gateway
- logical terminal identification (LTID) association for the H.323-based terminals
- call processing and call failure support
- communication to and from the Gateway card for call processing

An XPM frame or cabinet supports the Centrex IP-ready LTCI.

> *Note:* The LTCI requires an NTMX76BA messaging card.

Gateway card

The Gateway card resides in the LTCI module in the DS-1 P-side card slots. The Gateway card acts as the interface between the LAN infrastructure and the public switched telephone network (PSTN). The Gateway card provides 60 pulse code modulation (PCM) channels for active voice traffic over a packet network. The digital signal processors (DSP) on the Gateway card translate the toll-quality G.711 PCM of the PSTN and the packetized PCM required by the H.323-based clients. The Gateway card can support a maximum of 480 users, or a maximum of 60 simultaneous users.

The Gateway card receives configuration data from a dynamic host configuration protocol (DHCP) server and its software load from a load server (such as a file transfer protocol [FTP] server). Both servers reside on the LAN Gatekeeper, which establishes Internet Protocol (IP) connectivity between the Gateway card and the servers.

> *Note:* The Gateway cards and their associated DHCP server (hosted on the Gatekeeper) must reside on the same IP subnet.

Central office LAN

The CO LAN provides connectivity and routing capabilities from the H.323-based devices in the CO to the access data network. The CO LAN also provides packet forwarding performance that supports the provisioned Centrex IP subscribers.

Gatekeeper

Centrex IP provides IP terminals access to DMS Centrex services through the Gatekeeper. The Centrex IP Gatekeeper consists of a high-availability, dual cluster personal computer (PC), which runs the Windows NT Enterprise Server operating system.

In addition to basic call and supplementary voice services, the Centrex IP Gatekeeper provides the following functions:

- admission control—allows or denies a terminal request to access the packet telephony network
- authentication—blocks calls from unauthorized terminals
- address translation—translates a directory number (DN) to its transport address (IP and transmission control protocol [TCP] port number)
- zone management—provides address translation and admission control for terminals and Gateways that have registered with the Gatekeeper
- call processing—uses provisioned data for call completion and signaling
- call preservation—preserves stable calls and gracefully terminates calls when one of the parties goes on hook

The Gatekeeper PC also hosts the following software functions:

- DHCP server—provides configuration information, including IP address and load server location to the integrated Gateway cards
- FTP server—provides the Gateway software loading function
- Terminal Proxy Server (TPS)—translates proprietary unified network IP stimulus (UNISTIM) protocol from the i2004 terminals into H.323+ messages
- Trivial File Transfer Protocol (TFTP) server—provides the i2004 firmware loading function
- Packet Telephony Manager (PTM) server—the PTM is a client-server architecture network element management system for Centrex IP

The following table shows capacity limits for the Gatekeeper in Release 2.

Table 7-1 Gatekeeper capacity measurements

IP phones supported	High day busy hour (HDBH) call volume	Simultaneous calls (maximum)
2000	3 calls each second	400

Access network

The access network provides connectivity between the Centrex IP CO LAN and an enterprise network. The access network consists of the managed transmission facilities that connect two LANs over a geographical area. Network topologies can include the following:

- point-to-point connections, such as T1 links
- a virtual private network (VPN)
- a public data network (PDN)

Note: The Centrex IP system does not require a particular access network implementation. Data network engineers must ensure that the network meets the performance and bandwidth requirements specified in this chapter for acceptable QoS.

Enterprise network

The enterprise network is the private data network on the customer premises. The components for this network are as follows:

- the enterprise LAN, usually an Ethernet LAN configuration, with routing connectivity to the access network
- i2050 Soft Phone clients and/or i2004 terminals
- an edge device, for connectivity and traffic control between networks
- an optional DHCP server for dynamic configuration of an i2004 terminal

Note: The Centrex IP system does not require a particular enterprise LAN implementation. Enterprise network engineers must ensure that the enterprise network meets performance requirements for acceptable QoS. Refer to sections “Latency allocations” and “Packet loss allocations” in this chapter for the recommended parameters.

Vocoder standards

The complete Centrex IP system supports the G.711, G.729A, and G.723.1 voice-encoding protocols in Release 2.

The following table lists the bandwidth requirements on LANs and WANs to support the encoding schemes.

Table 7-2 Ethernet and WAN bandwidth requirements for various codecs

Codec	Frame duration (payload) in ms (7)	Voice payload in bytes	IP packet in bytes (1)	Ethernet frame (2) bytes	LAN bandwidth usage: kbit/s (3)	WAN (4) bandwidth use on (ATM): kbit/s (5)	WAN (4) bandwidth usage (Frame Relay): kbit/s
G.711 (64 kbit/s)	10 20 30	80 160 240	120 200 280	146 226 306	233.6 (6) 180.8 (6) 163.2 (6)	127.2 106.0 84.7	100.8 82.4 76.3
G.729A G.729 (8 kbit/s)	10 20 30	10 20 30	50 60 70	76 86 96	60.8 34.4 25.6	84.8 42.4 28.3	44.8 26.4 20.3
G.723.1 (6.3 kbit/s)	30	24	64	90	24	28.3	18.7

Note 1: Includes IP header of 20 bytes, User Datagram Protocol (UDP) header of 8 bytes, and Real Time Protocol (RTP) header of 12 bytes.
Note 2: Does not include IEEE 802.1Q virtual LAN (VLAN) tagging.
Note 3: Assumes half duplex transmission with silence suppression, unless otherwise noted.
Note 4: Assumes full duplex transmission.
Note 5: IP over Asynchronous Transfer Mode (ATM Adaption Layer 5)
Note 6: No silence suppression.
Note 7: For Release 2, 20 ms is the default frame duration.

Quality of service

The factors that affect the quality and reliability of the Centrex IP system can reside in any one of the three zones. Because of the network interdependencies, the QoS must be good in each network zone in order to achieve good quality and reliability for the whole system.

QoS parameters

The QoS parameters and targets that affect the Centrex IP system are as follows:

- latency (less than 200 ms, one way)
- packet loss (2% or less)
- jitter (4 ms)
- dial tone delay (1000 ms)
- post dial delay (600 ms)
- blocking (1%)

Latency measures the delay between talking and being heard. Low latency is important in ensuring that a conversation has good interactive quality.

After a call is set up, packet loss measures the percent of voice packets that one party sent but the other party did not receive.

Variations in the arrival rates of voice packets (some of which can arrive out of order) can cause jitter. A jitter buffer can place the data in the correct order and achieve a smooth playback of the voice data. The jitter buffer introduces a delay with magnitude that depends on the amount of jitter that arriving voice packets exhibit.

Dial tone delay measures the interval between going offhook and receiving dial tone from the switch before an end user can enter digits.

Post dial delay measures the time between dialing the last digit and hearing ringing or another tone.

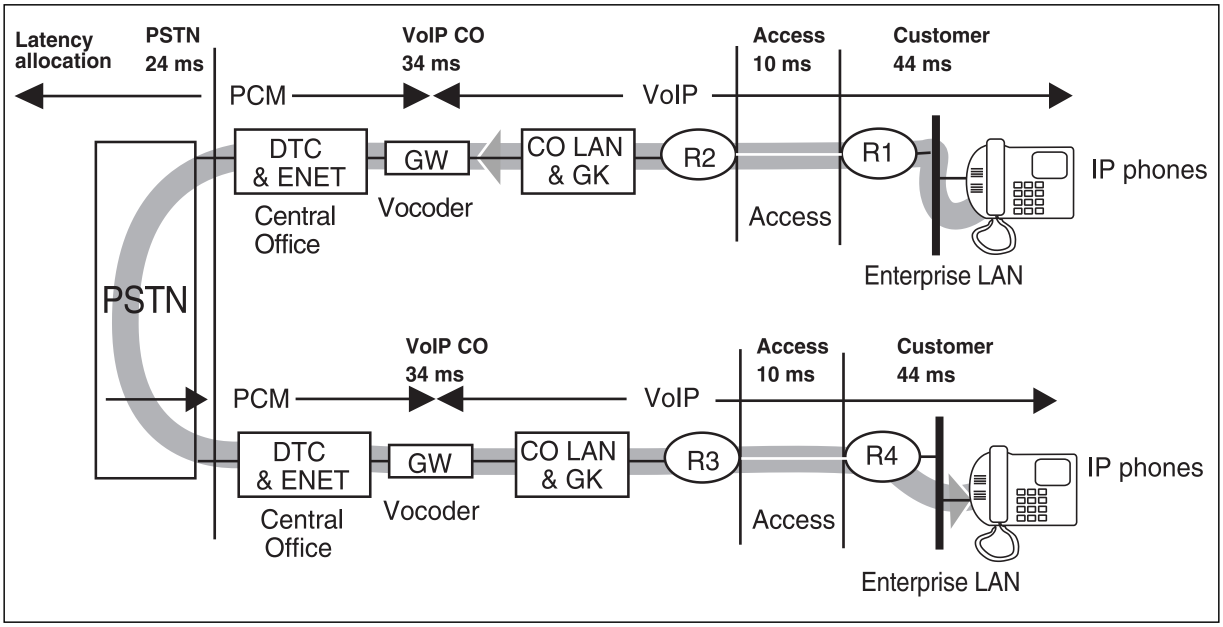
Blocking occurs when a speech path cannot be found to set up the call.

Latency allocations

Latency and packet loss have the largest effect on voice quality ratings. The latency target for Centrex IP Release 2 is 200 ms on an end-to-end, one-way, two-codec system delay basis.

The following figure shows the latency allocation across the three zones to achieve the 200 ms latency target.

Figure 7-2 Latency allocation of inter-LAN call (200 ms)



The speech path for the inter-LAN call is as follows:

1. The IP phone with vocoder encodes speech into the IP packets.
2. The IP packets move along the enterprise LAN to the enterprise edge device R1.
3. The IP packets traverse access facilities to CO edge device R2.
4. Edge device R2 sends IP packets along the CO LAN to the Gateway card.
5. The Gateway card decodes the IP packets to PCM format.
6. The PCM data moves through the switch network (ENET) to a digital trunk controller (DTC) and out to the PSTN.
7. The PCM data transits PSTN switches and trunks to the second Voice over IP (VoIP) CO.
8. In the second VoIP CO, the PCM data moves through the DTC and ENET to the Gateway card.
9. The Gateway card codes the PCM data into IP format and sends the packets over the CO LAN to edge device R3.
10. Edge device R3 sends the IP packets over access facilities to enterprise edge device R4.
11. Edge device R4 directs the IP packets along the enterprise LAN to the receiving IP phone.
12. The receiving IP phone converts the IP packets into speech.

The figure also shows the speech path for a call between two enterprise LANs by way of the PSTN. The enterprise edge device can include the Network Address Translation (NAT) or firewall functionality, or both. The CO LAN edge devices can include firewall functionality.

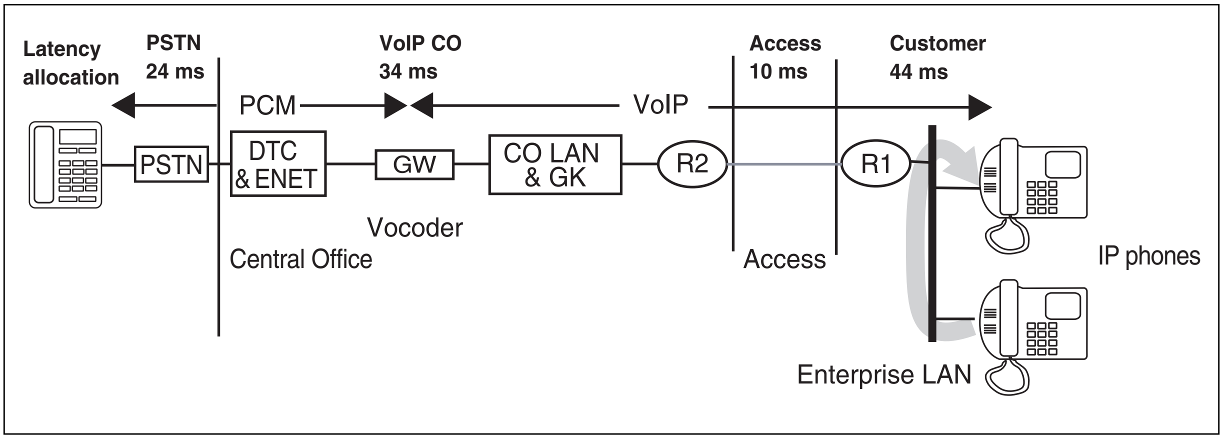
The inter-LAN call produces higher latency than calls involving only one IP terminal. However, when you add all the latency allocations along the speech path, the sum meets the target of 200 ms (44 + 10 + 34 + 24 + 34 + 10 + 44 = 200).

> ***Note:*** The 24-ms allocation for the PSTN is based on about half of the coast-to-coast, round-trip delay on optical fiber, which is 44 ms. This allows a 50/50 allocation of 44 ms for the enterprise, and 44 ms for the operating company (200-24 = 176 / 2 = 88). The 44 ms for the operating company is further partitioned to 34 ms for the CO, and 10 ms for the access network.

The 200-ms latency for the inter-LAN call type is also higher than that for a call between two IP terminals on the same enterprise LAN. This type of call does not involve the PSTN.

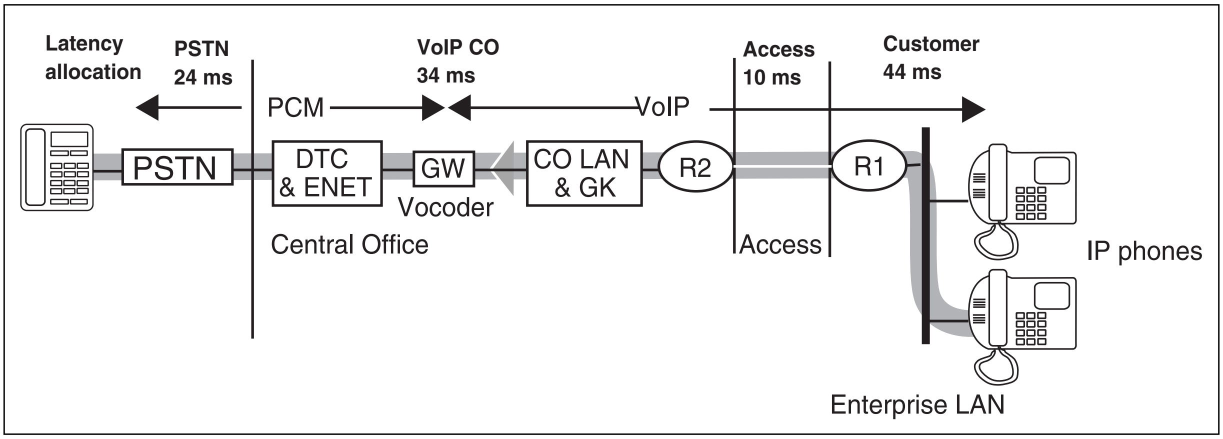
The following figure shows the latency allocation for the intra-LAN call type. The total latency allocations across the speech path equals 88 ms (44 + 44 = 88).

Figure 7-3 Latency allocation of intra-LAN call (88 ms)



The following figure shows the latency allocation for a PSTN-to-IP terminal call. The total latency allocations across the speech path equals 112 ms (24 + 34 + 10 + 44 = 112).

Figure 7-4 Latency allocation of PSTN to LAN call (112 ms)



Engineering to improve latency performance

This section provides some guidelines for improving latency performance and planning improvements as the LAN develops.

Latency increases as the number of hops and the level of congestion in a data network increase. (In general, each additional hop can add 10 ms of latency.) Congestion also plays a significant role in the overall distribution of round-trip times. Based on these conditions, Nortel Networks recommends the following engineering rules:

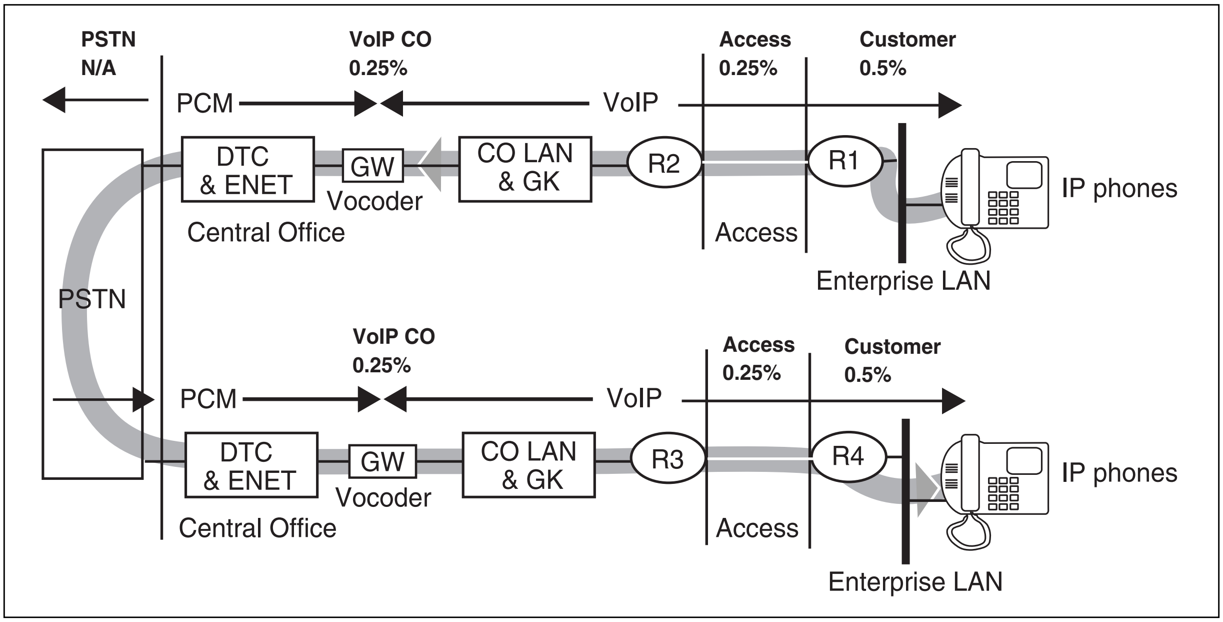
1. Avoid introducing additional hops between clusters of IP terminals and between the operating company boundaries and IP terminal clusters.
2. Provide full duplex capability (switched vs. shared media) on LANs rather than half duplex, which has a higher latency.
3. If available, activate the capability for routers to give priority to VoIP packets.

Packet loss allocations

Packet loss is a feature of a packet-switched network and is not applicable to the PSTN. Packet loss is the percentage of packets that do not arrive at their destination. Packet loss is the gaps in a voice conversation. Studies show that a packet loss greater than 5% has an adverse effect on conversation quality. Centrex IP has a packet loss target of 2% or less.

Transmission equipment problems, high delay, and congestion cause packet loss. The following figure shows the highest packet loss allocation allowable in the inter-LAN call type.

Figure 7-5 Packet loss of inter-LAN call



Reliability engineering

The reliability target for Centrex IP is 99.9%. This translates into approximately 8 hours of total downtime for each system yearly. In comparison, the reliability objective for a DMS switch is 2 minutes of downtime for each system yearly for all causes. Refer to the following recommendations for reliability engineering when designing the CO and enterprise portions of the network.

Routers can be a significant source of downtime. Router downtime arises from both maintenance activities and failures. The amount of maintenance work varies with the amount of change and growth in the data network. In some cases, you must take the router out of service to perform safe maintenance. As a rule, a router can require two or three yearly maintenance activities, with downtime of 2 to 24 hours for each activity. Thus, one router can exceed the Centrex IP system downtime objective of 8 hours for each year.

There are at least two routers in a Centrex IP system: one in the CO and one on the enterprise LAN. Without redundancy, Centrex IP is out of service if either router (or any other critical component) is down. Duplicate routers prevent a single router failure from taking down the Centrex IP system. With duplication, worst-case downtime for a redundant pair of routers is under 16 minutes a year. (This estimate assumes you can perform maintenance on one router at a time.) Use an uninterruptible power source to provide additional protection against downtime due to power failures.

Network security

The following principles help to ensure the security of Centrex IP network components, and the security of voice conversations over the packet telephony network. These principles form the basis for security implementations in Centrex IP network components. To implement security on these network components, refer to the corresponding subsections in this chapter describing the components.

1. The CO LAN and enterprise edge devices require firewall support.

   Centrex IP must support the use of firewalls on the CO LAN edge device, the enterprise edge device, or both. The technology and implementation of these firewalls varies with the specific network topology. Standard firewalls for Internet access do not supply adequate performance for VoIP.

2. The enterprise firewall receives CO LAN IP addresses.

   Each enterprise that Centrex IP serves only receives messages sourced from the Centrex IP CO LAN devices (such as the Gatekeeper and Gateways). Other enterprises hosted off the same CO do not receive messages (directly) from a different enterprise. Inter-enterprise intraswitching requires routing through a Gateway.

3. Enterprise routers receive routes to the CO LAN.

   Similar to the previous principle, the CO edge device only publishes routes to the CO LAN subnetwork. The CO edge device blocks routes to other enterprises.

4. Enterprise LANs require Network Address and Port Translation (NAPT) support.

   The use of private addresses in the enterprise requires that Centrex IP support NAPT devices. Support is expected for generic NA(P)T devices, but requires verification for implementation. The use of NA(P)T in the enterprise applies only to private-to-public address translation. The use NAPT does not apply to securing public addresses from the public domain. Use other methods of address space hiding (proxies, firewalls) when that service is required.

5. The H.323 Gatekeeper must segregate customer information flow.

   A Gatekeeper must support multiple customers (enterprises) and separate address spaces. Data and routing cannot allow inter-enterprise access. The routing capability on the Gatekeeper is disabled. Secure management processes, such as a separate plane or protected access, allow maintenance access (telnet, etc.)

6. Firewall and NA(P)T implementations cannot increase voice latency beyond zone allocations.

   Firewalls and NA(P)T services are a major source of delay in current networks. Although Centrex IP security does support these devices, specific implementations must enable separate service to media streams to provide acceptable QoS. Maintain end-to-end voice latency (“mouth-to-ear”) in the sub-200 ms range.

7. Optionally, encrypt the media stream.

   If required, encrypt the Centrex IP media stream. As in the previous principle, encryption services must provide sufficient performance to maintain voice latency budgets.

Engineering the CO

Engineering the Centrex IP CO involves the DMS-100 components and the CO LAN components. Different organizations within the operating company engineer these areas. The following sections target switch engineering personnel for DMS-100 components and data network engineering personnel for CO LAN components.

DMS-100 components

Engineer the following DMS-100 CO components to provide acceptable QoS:

- the CM for real-time engineering
- the LTCI for real-time performance and channel engineering
- the Gateway card(s) for channel engineering

Also, the CM and Gateway cards provide security measures to control access and changes to component information.

CM real-time engineering

Centrex IP phone calls have a CM real-time cost similar to ISDN basic rate interface (BRI) calls. Calculate the real-time impacts of adding IP terminals or replacing existing non-IP terminals with IP terminals to ensure that sufficient processor capacity is available. The CM REAL::TIME tool calculates the level of call processing utilization (CPUtil) expected for the number of lines and trunks by type and for specified call attempt (CA) and feature activation rates.

When IP terminals are installed without replacing existing phones, add the number of IP terminals to the number of existing BRI lines. Enter this sum to the BRI lines input area of the tool. If IP terminals replace existing lines, such as Centrex, add the number of IP terminals to the BRI lines input area, and subtract from the number of Centrex lines. If the originating CA rate for

Centrex IP terminals is different than existing BRI lines, the adjusted CA rate is a weighted average between the previous BRI CA rate and the IP terminal CA rate.

The following example illustrates the calculations.

1. Provide the following inputs:
   - Number of IP terminals to add to the switch = 500
   - HDBH originating CAs for each IP terminal = 3.0
   - Number of existing BRI lines = 2000
   - HDBH originating CAs for each BRI line = 6.0
2. Compute the adjusted HDBH originating CA rate with IP terminals:

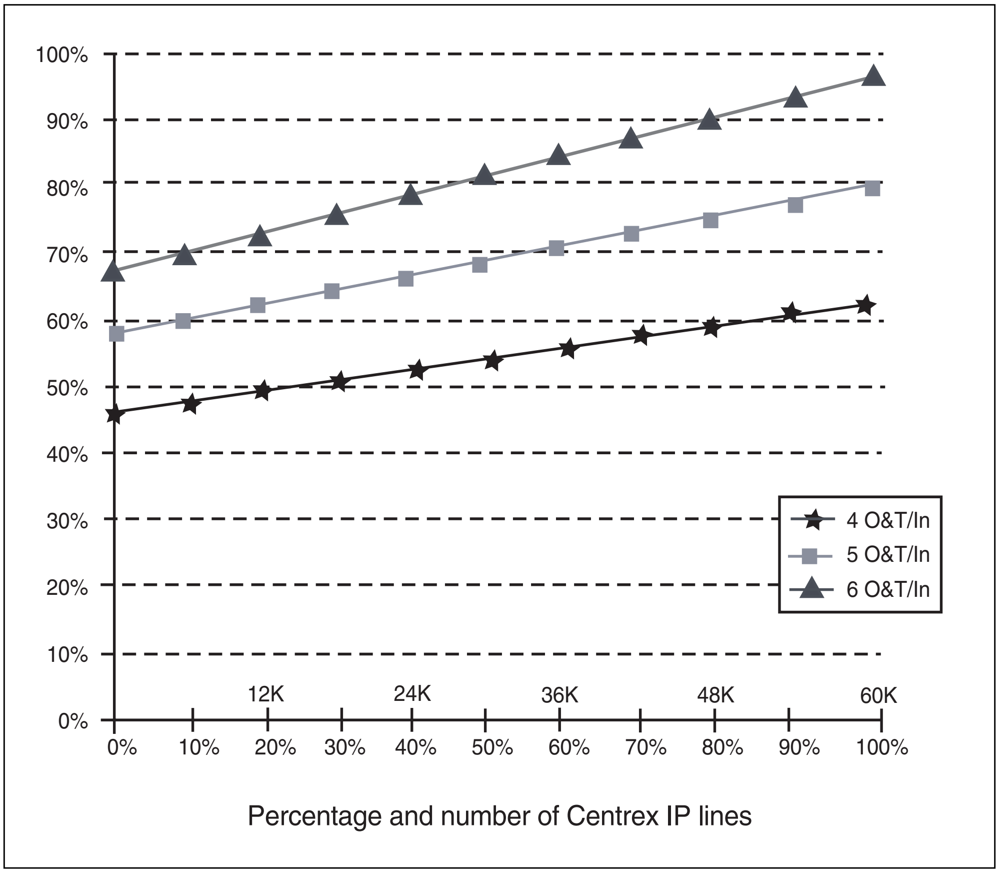
   Adjusted HDBH originating CA rate for each BRI line =
   [(IP Phones X HDBH originating CAs for each IP terminal) +
   (BRI lines X HDBH originating CAs for each existing BRI line)] /
   [IP terminals + existing BRI lines]
3. Substitute the data from step 2 into the formula as follows:

   Adjusted HDBH originating CA rate for each BRI line =
   [500 X 3.0 + 2000 * 6.00] / 2500 =
   [1500 + 12000] / 2500 =
   5.4 originating CAs for each BRI line

Thus, the addition of the 500 Centrex IP lines reduces the BRI originating CA rate from 6.0 to 5.4 CAs for each user hourly.

The REAL::TIME tool calculations show that the increase in CPUtil is small with Centrex IP penetration up to the current maximum of 500 lines. The following chart shows a gradual increase in CPUtil as Centrex IP penetrates the call model of a 60 000-line business switch. The business switch call model was developed from field data on line types and feature use in business offices. The chart assumes a mixture of Centrex IP lines and existing lines types, including residential (RES), Centrex, and non-IP BRI lines, for a total of 60 000 lines. For example, assume four originating and terminating CAs for each line. A mixture of 20% Centrex IP lines and 80% existing line types increases CPUtil from 46% to about 50%.

Figure 7-6 Centrex IP impact on CM real time



The following assumptions apply to the examples that follow:

- Number of Centrex IP terminals = 500
- HDBH hundred call seconds (CCS) for each IP terminal = 6.0

  Note: A hundred call seconds is the measure of a call with a holding time of 100 seconds (that is, 1 CCS of traffic).

- HDBH CAs for each IP terminal = 5.0
- Grade-of-service (blocking level) = 0.01 (1%)
- G.729A encoding at 20-ms frames

CM security

Standard DMS-100 security mechanisms control access to the DMS-100 CM user interface. The same mechanisms also control LTCI debugging interfaces, which are password protected. (Refer to the “Office Security” chapter in *DMS-100 Family Maintenance and Operations Manual*, 297-8991-500, for details of the DMS-100 security mechanisms.)

ISDN LTCI engineering

An LTCI can handle approximately 12 400 CAs hourly. This is a conservative figure based on the largest real time measured for any individual call type that the LTCI supports. To determine the number of CAs that the LTCI can process, add the total CAs from IP terminals, BRI B-channels, and primary rate interface (PRI) trunks. To calculate the total CAs, multiply the number of lines and trunks by the HDBH CA rate for each line or trunk.

The following example shows the calculation for IP phone CAs. If the total exceeds 12 400 CAs an hour, then redistribute lines or trunks, or both, to other LTCI peripherals.

Example

Number of IP phone CAs = 500 IP terminals x 5 CAs hourly = 2500 CAs hourly

One LTCI can carry the IP phone traffic that these 500 users generate (if the addition of the 2500 CAs does not exceed the 12 400 CA hourly limit).

Gateway engineering

The Gateway card is an XPM circuit pack that resides in one of the LTCI DS-1 interface slots. You can provision from one to five cards for each LTCI shelf. With five Gateway cards for each shelf, you can provision up to ten cards for each LTCI. The Gateway can co-reside with any other type of P-side interface cards. There are no additional restrictions on the type or number of interface cards that you can install in the shelf up to the maximum slot capacity.

Each Gateway card supports 60 channels. A channel refers to a communications path that supports a conversation between one subscriber residing on the LAN, and another subscriber residing on the PSTN. The maximum channel capacity of an LTCI is 480 channels (60 channels for each card x 8 active cards for each LTCI). Each Gateway card can support 60 simultaneous calls in any combination of inter- and intra-switched connections.

There are two calculations required in engineering the Gateway card:

1. the physical Gateway requirement
2. the grade-of-service or traffic requirement

Calculate physical Gateway requirement To determine the number of Gateways required, divide the number of IP terminals by 512. (This value refers to the maximum number of TIDs that each Gateway can hold.) If you need a lower number of TIDs to Gateway, then use a number less than the maximum (512) in the calculations.

Example

500 IP terminals / 512 TIDs for each Gateway = 0.98 Gateway card

Calculate grade-of-service For a given grade-of-service, determine the number of required Gateways. Table 7-3, "Generic HDBH traffic capacity," is an excerpt from Table 1, "HDBH Traffic Capacity (0.5% to 6%) (Carried Load)," in Engineering Change Memorandum (ECM) 590, Issue 5, Section 2.7.2.

Table 7-3 Generic HDBH traffic capacity

Carried load							
CHs	P(0.005)	P(0.01)	P(0.02)	P(0.03)	P(0.04)	P(0.05)	P(0.06)
60	1558	1621	1692	1737	1770	1797	1820

Example
500 IP phones x 6.0 CCS / user / 1621 CCS = 1.9 Gateway cards

Calculate number of required Gateway cards To determine the number of Gateway cards required, round up and use the higher of the two numbers from the physical and grade-of-service calculations.

Example
Physical requirement = 0.98 card = > 1 card
Grade-of-service requirement = 1.9 cards = > 2 cards

Therefore, two Gateway cards are required. You can add another card as a spare:

2 cards + 1 spare = 3 Gateway cards required

Note: Centrex IP requires the NA013 load to support dynamic sparing for the Gateway card.

Gateway security

The integrated Gateway has a telnet interface that uses a one-way encryption password. Table 7-4 lists the IP port usage for the Gateway cards.

Table 7-4 Integrated gateway port usage

Port range	Protocol	Usage
5000	UDP	Inter-GW communication
161–162	SNMP	Management via SNMP
2326–2444 (even ports)	UDP/RTP	RTP media streams
2327–2445 (odd ports)	UDP/RTCP	RTCP control streams

CO LAN

The CO LAN consists of an Ethernet segment that provides connectivity between the Centrex IP Gateway cards (NT7X07) residing in an LTCI and an edge device for connecting to the data access network. The CO LAN can also provide connection for the Centrex IP Gatekeeper. There is no requirement to locate the Gatekeeper in the CO, or to connect it directly to the CO LAN. However, the Gateway cards and their associated DHCP server (hosted on the Gatekeeper) must reside on the same IP subnet.

Neither the CO edge device nor the device providing Ethernet connectivity (hub or switch) must reside within the CO. Standard restrictions on Ethernet reach (typically 100 meters) apply for all connections.

Interface requirements

The sections that follow provide interface requirements to a CO LAN for the components of the Centrex IP system. The device that comprises the CO LAN must support at least 100Base-T switched connectivity. The device must also support the aggregate transmission rate calculated from the number of subscribers, calling rate, and codec usage.

Integrated Gateway The integrated Gateway cards require 10/100Base-T Ethernet connectivity to the CO LAN. If possible, set the Gateway interface at 100 Mbit/s to ensure no bandwidth bottlenecks are encountered. Each Gateway card hosts two Ethernet interfaces: one active and one standby interface. If the active interface fails, the standby interface becomes active and carries the Ethernet traffic. To ensure high reliability in the CO LAN, connect each interface from the Gateway card to a separate physical device (such as a blade in an Ethernet switch) on the CO LAN.

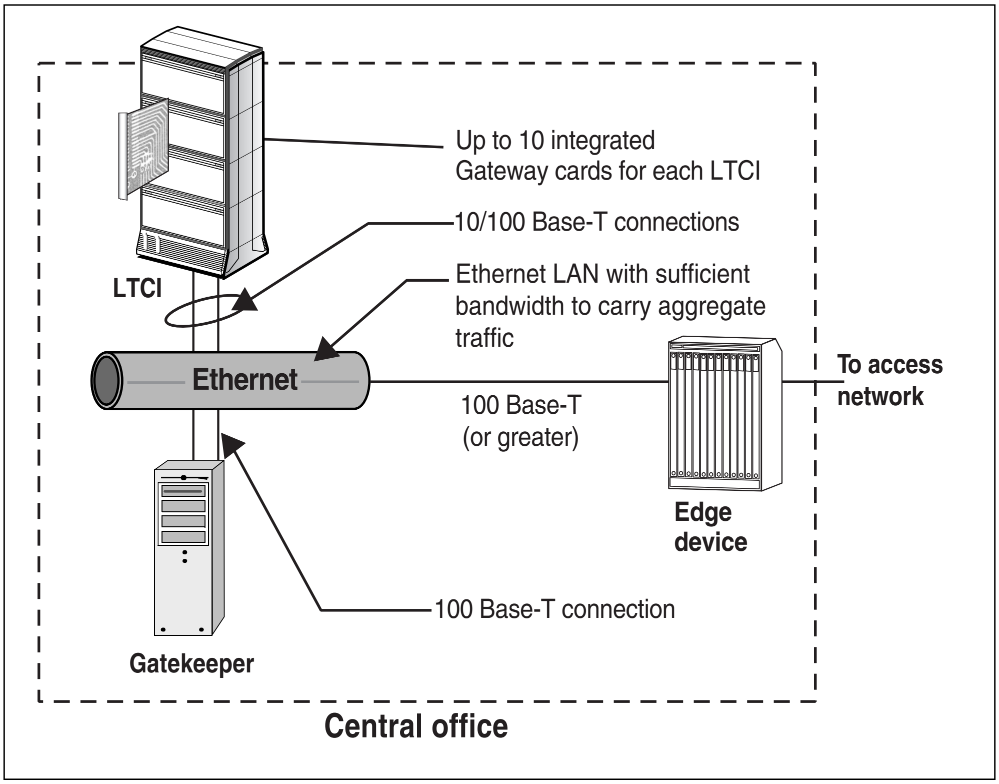
Gatekeeper A Gatekeeper connected to the CO LAN requires four 100Base-T Ethernet connections. Each element of the dual cluster requires two Ethernet connections (for redundancy). To ensure Gatekeeper high availability, attach the connections from each element to separate physical devices (such as a blade in an Ethernet switch) on the CO LAN.

Edge device The CO edge device, connecting the CO LAN to the access network, can be a router or a data switch (depending on the CO LAN configuration and the access network topology).

Because the edge device aggregates traffic from the CO LAN for transmission on the access network, the interface from the LAN must be at least 100Base-T Ethernet. Depending on traffic calculations based on number of subscribers and calling rate, you can increase this interface bandwidth (that is, to 1000Base-T). The edge device interface to the access network must support common WAN technologies such as T1, ATM, Frame Relay, and ISDN. The edge device interface must also support common routing protocols, such as Routing Information Protocol (RIP) and Open Shortest Path First (OSPF).

The following figure shows the CO interfaces to the LAN.

Figure 7-7 CO LAN network topology



Bandwidth requirements

The bandwidth that the CO LAN requires is identical to the amount shown in section “Bandwidth requirements for Centrex IP.” When the CO LAN edge device is duplicated for reliability, the required bandwidth must be available on both edge devices.

The following table lists the IP port use for the Gatekeeper.

Table 7-5 Gatekeeper port usage (Sheet 1 of 2)

Port Range	Protocol	Usage
6000	UDP	Static data download
1718–1720	UDP	RAS messaging
161,162, 9161	UDP	PTM messaging
5000	UDP	UNISTIM signaling
69	UDP	TFTP

Table 7-5 Gatekeeper port usage (Sheet 2 of 2)

Port Range	Protocol	Usage
8282	HTTP	PTM webserver (assuming the PTM server resides on the Gatekeeper)
20–21	TCP	FTP server (internal, Gateway uses)
1099	TCP	RMI protocol for Java applet communication with the PTM server (assuming the PTM server resides on the Gatekeeper)
Dynamic	TCP	Q.931 signaling (one port/active call, internal for i2004)
Provisioned	TCP	i2004 signaling (one port/registered i2004, internal)

Gatekeeper security

The Centrex IP Gatekeeper platform consists of the Compaq High-Availability Windows NT Server, including a Compaq Proliant (dual Pentium III at 550 MHz). The use of Windows NT Server requires adhering to the following recommendations for Windows NT security.

Passwords

Account security on the Gatekeeper requires special attention to ensure that unauthorized access is denied to the Windows NT server. The following recommendations deal with securing the accounts on the Gatekeeper.

1. Set passwords to expire after a certain period of time. (This rule does not apply to the Administrator and ClusterAdmin accounts, as their passwords do not expire.)

   If passwords do not expire, an unauthorized user has an endless length of time to decrypt the passwords.

   To set a password to expire:

   a. Open **User Manager.**

   b. Select user from list.

   c. Under **User** menu, select **Properties.**

   d . Uncheck “Password Never Expires.”

2. Set minimum password length to ***n*** characters (***n***=10 recommended).

   To set the minimum password length to 10:

   a. Open **User Manager.**

   b. Under **Policies** menu, select **Account.**

   c. Click **At Least.**

   d. Enter the minimum password length as “10.”

3. Set password history length to *z* (*z*=4 recommended).

   Decrease the reuse of passwords to increase security.

   To set the password history length to four:

   a. Open **User Manager.**

   b. Under **Policies** menu, select **Account.**

   c. Click **Remember Passwords.**

   d. Enter “4.”

4. Enable and encourage users to change passwords frequently. (This rule does not apply to the Administrator and ClusterAdmin accounts, as their passwords do not expire.)

   To allow users to change passwords:

   a. Open **User Manager.**

   b. Select user from list.

   c. Under **User** menu, select **Properties.**

   d. Uncheck “User Cannot Change Password.”

File system

To protect files and directories, use the Access Control Lists (ACL) Editor in Windows NT Explorer. The ACL Editor allows you to change access on the system drive (by default “C:\”) to grant full control permissions to Administrator and System accounts, and to grant read-only permission to all other users.

The Windows NT file system holds many critical security files, most of which are in the system root directory (usually named “WINNT”). Many files and directories are protected by default; however, sometimes permissions are relaxed for compatibility reasons. This is not advised for more secure sites.

The following list shows the directories and files that should have full access for administrators and read-only access for public:

- C:\ directory
  - Io.sys
  - Msdos.sys
  - Boot.ini
  - Ntdetect.com
  - Autoexec.bat
  - Config.sys
- C:\TEMP directory
- C:\WINNT directory
  - Win.ini
  - Control.ini
  - Netlogon.chg

User accounts and groups

The following list describes the guidelines for setting up user accounts and groups.

1. Disable guest accounts.

   By default, the Guest account is disabled at startup. If the Guest account is enabled, disable it. Disabling accounts is described under "Disabling and Enabling User Accounts" in the User Manager for Domains Help and User Manager Help.

   Disable the Guest account (select "Account Disabled" on the main account window). For extra assurance, add the following restrictions:

   - give it a long, random password that you do not retain
   - set its logon hours to none
   - allow it to log on no workstations
   - set its expiration date to a date past

2. Disable blank password.

   To prohibit blank passwords, use the User Manager or User Manager for Domains window. Under the "Policies...Account..." menu, ensure that "Permit Blank Password" is not checked.

3. Allow network-only lockout for the Administrator account.

   The Administrator account is locked out if an attacker attempts a brute force or dictionary attack, but the administrator can still log on locally at the server. Under the “Policies...Account...” menu, select the following restrictions:

- Account Lockout is checked
- Lockout after “5” bad logon attempts
- Lockout Duration is “forever (until admin unlocks)”

User rights

The User Manager for Domains window allows you to modify user rights. The trusted users are the Administrator and the Cluster Administrator. See the following table for the recommendations on setting user rights.

Table 7-6 User rights membership (Sheet 1 of 2)

User right	Gatekeeper server
Access this computer from network	Anyone
Act as part of the operating system	None (do not assign to any user)
Add workstation to domain	None
Back up files and directories	Trusted users
Bypass traverse checking	Anyone
Change the system time	Trusted users
Create a page file	Trusted users
Create a token object	None (do not assign to any user)
Create permanent shared objects	None
Debug programs	None (this right is not auditable and should not be assigned to any user, including system administrators)
Force shutdown from a remote system	Trusted users
Generate security audits	None (do not assign to any user)
Increase quotas	Trusted users
Increase scheduling priority	Trusted users
Load and unload device drivers	Trusted users
Lock pages in memory	None
Log on as a batch job	Trusted users (as needed)

Table 7-6 User rights membership (Sheet 2 of 2)

User right	Gatekeeper server
Log on as a service	Trusted users (as needed)
Log on locally	Trusted users
Manage auditing and security log	Trusted users
Modify firmware environment values	Trusted users
Profile single process	Trusted users
Profile system performance	Trusted users
Replace a process level token	None (do not assign to any user)
Restore files and directories	Trusted users
Shut down the system	Trusted users
Take ownership of files or other objects	Trusted users

Network sharing

To control access to a computer and shared information from a network interface, allow only administrators to create new shares. To prevent non-administrators from creating shares, do the following:

1. Use the Registry Editor to find the following registry subkey:

   Path: HKEY_LOCAL_MACHINE\SYSTEM

   Subkey: CurrentControlSet\Services\LanmanServer\Shares

2. Select Shares and all its subkeys, click the Security menu, and then click Permissions.

3. For Shares and each of its subkeys, set the permissions for Everyone and all untrusted users to a maximum of Read, and then click OK.

Network and workgroups

The following list describes the network and workgroup security settings.

1. Restrict null session access over named pipes.

   Restricting null session access over named pipes helps prevent unauthorized access over the network. To add these restrictions, make the following changes to the Registry:

   Hive: HKEY_LOCAL_MACHINE

   Key: System\CurrentControlSet\Services\LanmanServer\Parameters

   Value Name: NullSessionPipes and NullSessionShares

Type: REG_MULTI_SZ

Value: remove all values

2. Restrict anonymous network access.

   Windows NT has a feature that allows non-authenticated users to enumerate users on a Windows NT domain. If you do not want this functionality, make the following changes in the Registry:

   Hive: HKEY_LOCAL_MACHINE

   Key: System\CurrentControlSet\Control\LSA

   Value Name: RestrictAnonymous

   Type: REG_DWORD

   Value: 1

3. Unbind NetBIOS from TCP/IP.

   Unbinding NetBIOS from TCP/IP prevents a user from accessing machine information using tools like NBTSTAT. This can protect you against unauthorized information-gathering techniques and some denial of service attacks.

4. Disable IP routing.

   If routing is enabled, you can risk passing data between the intranet and the Internet. To disable routing, open the Network Control Panel and select Protocols->TCP/IP Protocol->Properties->Routing and clear the Enable IP Forwarding check box.

5. Enable the filtering of fragmented IP packets.

   Some denial of service attacks are based on fragmented IP packets.

   To enable filtering of fragmented IP packets in the Gatekeeper, make the following changes to the Registry:

   Hive: HKEY_LOCAL_MACHINE

   Key: System\CurrentControlSet\IPFilterDriver\Parameters

   Value Name: EnableFragmentChecking

   Type: REG_DWORD

   Value: 1

6. Turn off the forwarding of fragmented IP packets.

   Along with the previous recommendation, do not forward fragmented IP packets.

To disable forwarding of fragmented IP packets in the Gatekeeper machine, make the following changes to the Registry:

Hive: HKEY_LOCAL_MACHINE

Key: System\CurrentControlSet\IPFilterDriver\Parameters

Value Name: DefaultForwardFragments

Type: REG_DWORD

Value: 0

7. Hide servers from the browser list.

   If you have a secure server or workstation you wish to hide from the general browser list, add this registry setting.

   To hide a server from the browser, edit:

   Hive: HKEY_LOCAL_MACHINE

   Key: \SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

   Value Name: Hidden

   Type: REG_DWORD

   Value: 1

8. Disable automatic hidden shares.

   This key controls whether the administration shares are created. Set AutoShareServer to “0” to disable admin shares for a server.

   Hive: HKEY_LOCAL_MACHINE

   Key: \SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

   Value Name: AutoShareServer

   Type: REG_DWORD

   Value: 0

9. Disable file and printer sharing.

   When “File and printer sharing...” is installed, it allows users to make services available to other users on a network. To disable this functionality, change this setting as follows:

   a. Use Regedit to find the key below. If it doesn't already exist, create it.

   b. Create two new DWORD values of “NoFileSharing” and “NoPrintSharing.”

   c. Modify the values of “NoFileSharing” and “NoPrintSharing” to “1” sharing disabled.

Registry settings

The Windows NT registry contains entries that are important to the security of the machine. The following list provides recommendations on registry settings that improve Gatekeeper security.

1. Deny remote anonymous access to the server's registry.

   Anonymous access to the server's registry can enable a remote, unauthorized user to compromise the Gatekeeper server.

   To deny remote access to the server's registry, set the following key so that only administrators have access:

   Hive: HKEY_LOCAL_MACHINE

   Path: System\CurrentControlSet\Control\SecurePipeServers

   Key: Winreg

2. Deny guest access to the Application Log.

   The Application Log contains sensitive information that can compromise the security of the system.

   To restrict viewing to administrators only, make the following changes to the Registry:

   Hive: HKEY_LOCAL_MACHINE

   Key: System\CurrentControlSet\Services\EventLog\Application

   Value Name: RestrictGuestAccess

   Type: REG_DWORD

   Value: 1

3. Deny guest access to the Security Log.

   The Security Log contains sensitive information that can compromise the security of the system.

   To restrict viewing to administrators only, make the following changes to the Registry:

   Hive: HKEY_LOCAL_MACHINE

   Key: System\CurrentControlSet\Services\EventLog\Security

   Value Name: RestrictGuestAccess

   Type: REG_DWORD

   Value: 1

4. Deny guest access to the System Log.

   The System Log contains sensitive information that can compromise the security of the system.

To restrict viewing to administrators only, make the following changes to the Registry:

Hive: HKEY_LOCAL_MACHINE

Key: System\CurrentControlSet\Services\EventLog\System

Value Name: RestrictGuestAccess

Type: REG_DWORD

Value: 1

5. Restrict the installation of printer drivers to the administrator user.

   Unrestricted access to printer driver installation enables the installation of infected printer drivers on the Gatekeeper.

   To restrict installation for printer drivers to administrators, make the following changes to the Registry:

   Hive: HKEY_LOCAL_MACHINE

   Key: System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers

   Value Name: AddPrintDrivers

   Type: REG_DWORD

   Value: 1

6. Secure base objects.

   This step increases security of the base objects and prevents users from gaining local administrator privileges using a dynamic-link library (DLL). Refer to Microsoft Security Bulletin 99-006 for more detail. To implement this security, make the following changes to the Registry:

   Hive: HKEY_LOCAL_MACHINE

   Key: System\CurrentControlSet\Control\Session Manager

   Value Name: ProtectionMode

   Type: REG_DWORD

   Value: 1

7. Secure additional base-named objects.

   This step increases security of additional base-named objects such as RotHintTable or ScmCreatedEvent, which the previous ProtectionMode key entry does not address. To implement this security, make the following changes to the Registry:

   Hive: HKEY_LOCAL_MACHINE

   Key: System\CurrentControlSet\Control\Session Manager

Value Name: AdditionalBaseNamedObjectsProtectionMode

Type: REG_DWORD

Value: 1

8. Protect kernel object attributes.

   This step ensures that the object manager does not change attributes of a kernel object in the object table for the current process, unless the previous mode of the caller is kernel mode.

   Hive: HKEY_LOCAL_MACHINE

   Key: System\CurrentControlSet\Control\Session Manager

   Value Name: Add new REG_DWORD value named EnhancedSecurityLevel

   Type: REG_DWORD

   Value: 1

9. Clear the page file at system shutdown.

   Windows normally does not clear or recreate the page file. On a heavily used system this can be both a security threat and performance drop. Enabling this setting will cause Windows to clear the page file whenever the system is shut down.

   Hive: HKEY_LOCAL_MACHINE

   Key: System\CurrentControlSet\Control\Session Manager\Memory Management

   Value Name: ClearPageFileAtShutdown

   Type: REG_DWORD

   Value: 1

10. Restrict untrusted users' ability to plant Trojan horse programs.

    Trojan Horse programs can take advantage of the Run utility if it is unguarded. Some Trojan horse programs are written to execute during an uninstall operation. To restrict the ability of users to plant Trojan horse programs, do the following:

    a. Use the Registry Editor to find the following keys:

       Hive: HKEY_LOCAL_MACHINE\SOFTWARE

       Key: Microsoft\Windows\CurrentVersion

       Value Name: Run, RunOnce, Uninstall (if present), AEDebug and all their subkeys

    b. Select each subkey, click the Security menu, and then click Permissions.

c. For each subkey, set the permissions for Everyone and all untrusted users to a maximum of Read, and then click OK.

11. Remove the Shutdown button from the logon dialog.

    Set the following value in the Registry to remove the Shutdown button at logon:

    Hive: HKEY_LOCAL_MACHINE

    Key: \Microsoft\Windows NT\CurrentVersion\Winlogon

    Value Name: ShutdownWithoutLogon

    Type: REG_SZ

    Value: 0

    if the Registry key:

    HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon

    has a value named "ShutdownWithoutLogon" with a REG_SZ value of "1," then a "Shutdown" button appears on the logon window that allows anyone to shut the system down without logging on. These guidelines do not treat shutting the system down (a "denial of service") as a security issue, although it may be an important operational issue. There are no known examples of using system shutdown to compromise system security apart from denial of service.

12. Remove the OS2 subsystem.

    The OS2 subsystem can provide local vulnerabilities on a Windows NT machine.

    To remove the OS2 subsystem, remove the following key in the Registry:

    Hive: HKEY_LOCAL_MACHINE

    Key: System\CurrentControlSet\Control\Session Manager\Subsystems

    Value Name: Os2

13. Remove the Posix subsystem.

    The Posix subsystem can provide local vulnerabilities on a Windows NT machine.

    To remove the Posix subsystem, remove the following key in the Registry:

    Hive: HKEY_LOCAL_MACHINE

    key: System\CurrentControlSet\Control\Session Manager\Subsystems

    Value Name: Posix

14. Disable support for 16-bit applications.

    Although new technology file system (NTFS) can support older applications, many 16-bit applications open security holes. Nortel Networks does not support these applications on the Gatekeeper.

    To disable support for 16-bit applications on the Gatekeeper, make the following changes to the Registry:

    Hive: HKEY_LOCAL_MACHINE

    Path: System\CurrentControlSet\Control\FileSystem

    Key: NtfsDisable8dot3NameCreation

    Type: REG_DWORD

    Value: 1

15. Restrict the allocation of CD ROMs and diskettes to only the currently logged-in user. Without this restriction, unauthorized users could potentially insert diskettes and CD ROMs in the Gatekeeper to execute malicious programs.

    To restrict allocation of CD ROMs and diskettes to the current user, make the following changes to the Registry:

    Hive: HKEY_LOCAL_MACHINE

    Key: Software\Microsoft\WindowsNT\CurrentVersion\Winlogon

    Value Name: AllocateCDRoms (for CD), AllocateFloppies (for floppy disks)

    Type: REG_SZ

    Value: 1

16. Disable CDROM autorun.

    Along with the previous recommendation, this restriction prevents an unauthorized user from compromising Gatekeeper security with a malicious program that runs automatically when inserting a CD ROM.

    To disable CD AutoRun, make the following changes to the Registry:

    Hive: HKEY_LOCAL_MACHINE

    Key: System\CurrentControlSet\Services\CDRom

Value Name: Autorun

Value: 0

17. Disable the display of the last user name on the login screen.

    By concealing the user name of the last user logged into the system, it is more difficult for an unauthorized user to log into the Gatekeeper.

    To hide the user name of the last user logged into the Gatekeeper, make the following changes to the Registry:

    Hive: HKEY_LOCAL_MACHINE

    Key: Software\Microsoft\WindowsNT\CurrentVersion\Winlogon

    Value Name: DontDisplayLastUserName

    Type: REG_SZ

    Value: 1

CO edge device security

Security for the CO edge device consists of configuring the routing capabilities and establishing policies for firewall instances. Also, apply security management access to the device.

Routing

Configure the CO edge device to restrict routes only between the address space of the CO LAN and the various enterprises. A route from one enterprise must not be published to another enterprise. The process for restricting these routes depends on the edge device used.

Management access

Restrict access to the edge device for element management through the use of password security or another appropriate challenge system.

Firewalls

Firewalls protect the CO or the enterprise network (or both) from potential intrusions and attacks from untrusted networks. Set up the firewall implementation on a router or a separate server. This section discusses both implementations and provides sample rules for use in any Centrex IP network implementation.

Security strategy

The CO LAN firewall strategy defines a set of rules to provide seamless functionality for Centrex IP. At the same time, the CO LAN firewall protects the key systems from intrusions, attacks, and denials of service. All signaling between the i2004 terminals and the TPS must route through the firewall without dropping any packets. This same rule applies to all communications between the Gateways and the i2004 terminals. These flows include both the bearer stream and the signaling messages.

The other key type of traffic that needs a policy rule is TFTP traffic. Since the i2004 terminals occasionally need to download a new software load from the TFTP server to perform an upgrade, TFTP packets are also accepted. (The TFTP server resides on the CO LAN.)

Network functionality requires policing of the routing protocols. The wide number of protocols requires that the network administrator add, enable, or disable desired and undesired protocols.

The second part of the strategy applies to blocking as many attacks as possible. The remaining rules allow the optional use of telnet, FTP and Internet control message protocol (ICMP), which are blocked by default.

CO LAN firewall implementation

This section describes the security rules and policies for the CO LAN firewall. The following rules describe an implementation of Checkpoint Firewall-1 version 3.0b running on a CO LAN edge device (router).

Table 7-7 lists network objects that the administrator can define to implement CO LAN firewall rules. The object names are arbitrary. The administrator must add other local information (such as IP addresses) to define these objects in Checkpoint Firewall-1.

Table 7-7 Objects used to set up CO LAN firewall rules

Name	Object type	Location	Comments
ARN	Router	Internal	CO edge device
CO-LAN	Network	Internal	
Gateway10	Workstation (Host)	Internal	Gateway in LTCI
TPS-121	Workstation (Host)	Internal	Software object (in Gatekeeper)
TFTP-Server	Workstation (Host)	Internal	Software object (on Gatekeeper)
Enterprise-LAN	Network	External	

Table 7-8 lists defined services allowable on the CO LAN firewall. The services “VoiceStreamIn” and “VoiceStreamOut” represent the data streams traveling between the i2004 terminals and the H.323 Gateway. The current port range of the voice origination on the Gateway is from 2325 to 2446.

“SignalingE2Set” shows the signaling stream between the i2004 and the TPS, while “tftp-return” represents the TFTP traffic leaving the TFTP server. “NAT-Enabler-In” and “NA-Enabler-Out” are used for signaling between the i2004 phone and the TPS, which enables NAT mapping at the enterprise.

Table 7-8 Defined services on CO LAN

Name	Source port range	Destination port range	Protocol
VoiceStreamOut	2325–2446	6000–6011 (Note)	UDP/RTP
VoiceStreamIn	6000–6011 (Note)	2325–2446	UDP/RTP
SignalingE2Set	5000	5000 (Note)	UDP/UNISTIM
NAT-Enabler-In	6000-6011 (Note)	6066	UDP/UNISTIM
NAT-Enabler-Out	6066	6000-6011 (Note)	UDP/UNISTIM
Note: These ports are valid only when NAT is disabled. For a NAT configuration, substitute the NAT external ports, which the Enterprise LAN uses. When NAT is enabled on the enterprise LAN, firewall functionality is upstream from the NAT functionality.			

The network administrator can implement a secure combination of rules for Centrex IP by defining the previous objects and services, and predefined services of most firewall implementations (including Firewall-1).

Table 7-9 shows a typical set of rules that secures the CO LAN and guarantees functionality for Centrex IP.

Table 7-9 CO LAN firewall rules (Sheet 1 of 2)

No.	Source	Destination	Service	Action	Comment
1	Enterprise-LAN	CO-LAN	OSPF RIP RIP-response BGP-UDP BGP-TCP	Drop	Routing protocols. Some/all to be removed (depending on CO LAN choice).
2	Enterprise-LAN	CO-LAN	Telnet	Drop	Change action to Accept to Telnet.
3	Enterprise-LAN	CO-LAN	FTP	Drop	Change action to Accept to FTP.
4	CO-LAN	Enterprise-LAN	ICMP-Proto	Drop	Change action to Accept to Ping and Traceroute.

Table 7-9 CO LAN firewall rules (Sheet 2 of 2)

No.	Source	Destination	Service	Action	Comment
5	Enterprise-LAN	CO-LAN	ICMP-Proto	Drop	Change action to Accept to Ping and Traceroute.
6	Enterprise-LAN	Gateway10	VoiceStreamIn	Accept	Voice stream to gateways. Source port range: 6000–6011. Dest. port range: 2325–2446. Additional gateways can be added in this rule.
7	Gateway10	Enterprise-LAN	VoiceStreamOut	Accept	Voice stream from gateways. Source port range: 2325–2446. Dest. port range: 6000–6011. Additional gateways can be added in this rule.
8	Enterprise-LAN	TFTP-server	TFTP	Accept	TFTP requests from i2004 terminals.
9	TFTP-server	Enterprise-LAN	TFTP	Accept	TFTP load to i2004 terminals.
10	Enterprise-LAN	TPS-121	SignalingE2Set	Accept	Signaling from TPS. Source port: 5000. Destination port: 5000.
11	TPS-121	Enterprise-LAN	SignalingE2Set	Accept	Signaling to TPS. Source port: 5000. Destination port: 5000.
12	Any	CO-LAN	Any	Drop	Drop everything else.
13	CO-LAN	Any	Any	Drop	Drop everything else.
14	Enterprise-LAN	TPS-121	NAT-Enabler-In	Accept	To allow messaging for NAT configuration
15	TPS-121	Enterprise-LAN	NAT-Enabler-Out	Accept	To allow messaging for NAT configuration

Explanations for the rules in the previous table follow.

- Rule 1 examines common routing protocols. The CO LAN administrator can remove the unused protocols. The CO LAN administrator also can change the rule so that the firewall drops all of the protocols if static routing is used.

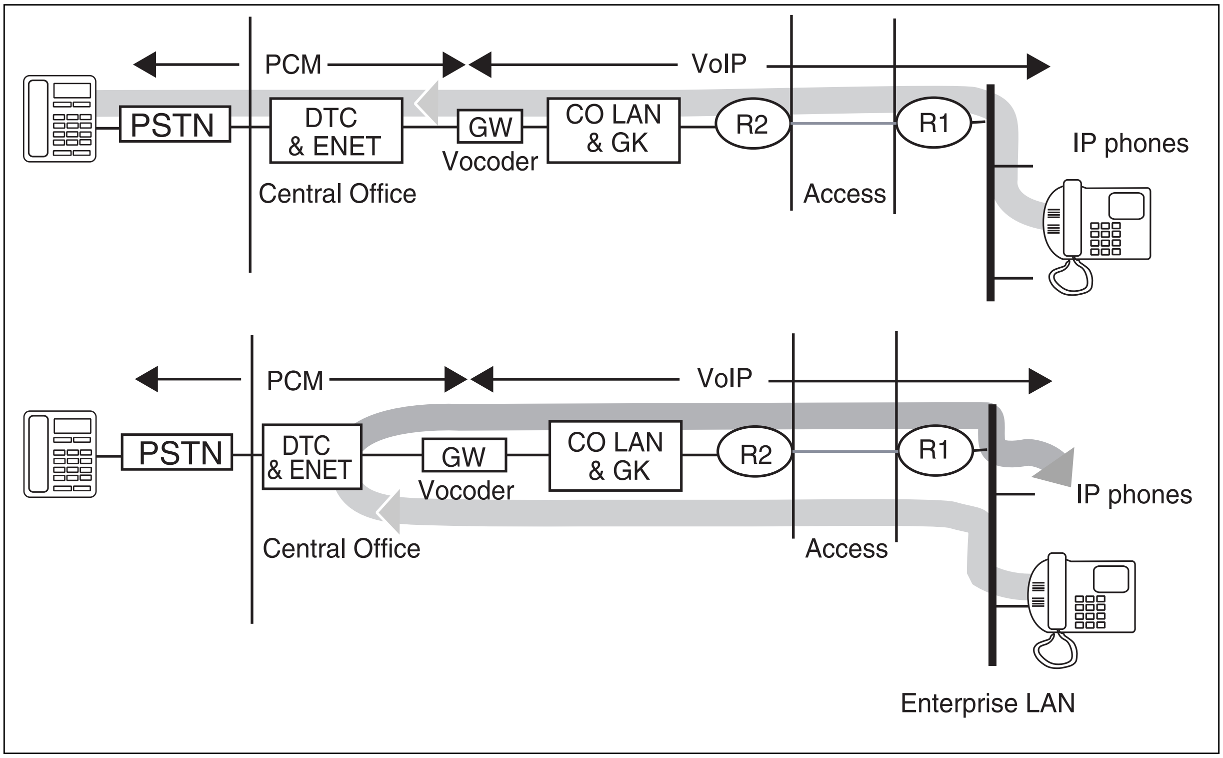
- Rules 2, 3, 4, and 5 examine common network protocols, including Telnet, FTP, and ICMP. Nortel Networks suggests dropping these protocols and enabling them only when their brief use is necessary.
- Rules 6 and 7 accept the packets exchanged between a fixed port range on the H.323 Gateways and a fixed range of ports inside the CO LAN. An administrator can add other Gateways to this rule by defining a new network object.
- Rules 8 and 9 accept the TFTP packets going to and from the TFTP server on the CO LAN. This rule allows the i2004 terminals to retrieve new loads.
- Rules 10 and 11 accept the signaling messages going from a pre-determined port on the TPS to a pre-determined port on the i2004 terminals. (Table 7-13 lists the port usage for the i2004 terminal.)
- Rule 12 drops all the packets with the CO LAN as a destination address that rules 1 to 11 do not describe.
- Rule 13 drops all the packets with the CO LAN as a source address that rules 1 to 11 do not describe.
- Rules 14 and 15 accept signaling between the i2004 phone and the TPS to enable NAT mapping at the enterprise.

Engineering the access network

Also, engineer access facilities joining the enterprise LAN to the VoIP CO LAN to carry the VoIP packets. Calculate the level of traffic using the number of IP terminals and the traffic that each terminal generates. The total traffic expected is expressed in terms of bandwidth, which is translated into facilities required.

The top part of the following figure shows the speech paths for an IP phone to an PSTN call. The bottom part of the figure shows the speech path for an intra-LAN IP phone to IP phone call. Within the speech paths are the facilities and equipment that must be engineered for traffic.

Figure 7-8 Call paths illustrating traffic-sensitive components



Traffic engineering calculations

To engineer the access network for Centrex IP service, perform the following calculations:

1. Calculate the bandwidth requirements for Centrex IP services between the enterprise and the CO LAN.
2. Calculate the latency in the access network.
3. Calculate the packet loss in the access network.

Access bandwidth requirements

The access facilities connect edge devices R1 and R2, as Figure 7-8 shows. (Refer to section “Bandwidth requirements for Centrex IP.” This section contains the steps for calculating the channel requirements for the example assumptions listed on page 7-15.) Assuming G.729A encoding, 20-ms frames, and an ATM-based WAN (see Table 7-2, “Ethernet and WAN bandwidth requirements for various codecs” on page 7-6), the following equation shows the total WAN bandwidth requirement.

103 x 42.4 kbit/s = 4367 kbit/s

The bandwidth requirement translates into the number of T1 transmission circuits needed. A T1 circuit has a capacity of 1.544 Mbit/s.

Use the following equation to compute the number of T1 circuits required.

Bandwidth required / 1.544 Mbit/s = 4.367 / 1.544 = 2.8 or 3 T1s

If fractional T1s are available, it is not necessary to round up to a whole number of T1s.

Access network latency

Use a network management performance tool, such as Packet InterNet Groper (Ping), to determine the latency between the CO LAN edge device and the enterprise edge device. For the access network, do not use voice encoding latency components. For higher than expected latency measurements, also use Traceroute to determine the number of router hops in the access network. You can use standard network management tools, such as HP OpenView or Bay Networks Optivity, to gather this performance information.

One-way latency in the access network should be less than 10 ms to ensure quality voice transmission. Longer haul transmission or complex access network topologies can require greater than 10 ms latency. Therefore, reduce the latency allocations for zones 1 and 3 so the end-to-end latency is less than 200 ms.

Access network packet loss

Use standard network management and performance tools to measure the packet loss in the access network. The transmission packet loss for the access network should not exceed 0.25%.

Engineering the enterprise network

The enterprise network consists of the customer LAN, and the edge device to connect to the access data network. The protocols, topologies, and configurations within enterprise networks vary greatly. Therefore, this section concentrates on measuring and engineering parameters in the enterprise network that have the greatest effect on voice quality, without regard to enterprise network topology.

To engineer the enterprise network for Centrex IP services, perform the following calculations:

1. Calculate network latency from IP terminals to the enterprise edge device connected to the Centrex IP data access network.
2. Calculate network packet loss from IP terminals to the enterprise edge device connected to the Centrex IP data access network.
3. Calculate network bandwidth requirements based on the projected number of IP terminals and user calling rates.
4. Calculate the bandwidth availability in the network for Centrex IP services.

Enterprise network latency

Use network performance tools, such as Ping and Traceroute, to determine latency and packet loss in the enterprise network. (These tools are not part of the Centrex IP product offering.) Use other network analysis or management tools in the enterprise to collect this performance information.

The Ping tool sends an ICMP echo request message to a host and waits for an ICMP echo reply. This enables measurement of round-trip time to a particular host. You can also measure the percent of packets lost for a route by sending repeated ICMP echo request messages.

To determine the latency in the enterprise network, collect performance data over an extended period of time (for example, 24 hours). Collect this data for messages between candidate IP terminals and the enterprise edge device connected to the Centrex IP access network.

If you use Ping to collect performance data, divide the average round-trip time for the Ping statistics in half to determine the average, one-way latency in the enterprise. For the Ping results example in Figure 7-9, the network-induced latency from an IP terminal to an edge device is 33.5 ms. The Ping results do not include enterprise latency, due to voice encoding at the IP terminal.

Figure 7-9 Ping example statistics for IP terminal to enterprise edge device

```
% ping brtph323 314 -n 10
PING brtph323: 314 byte packets
314 bytes from 47.127.127.55: icmp_seq=0. time=67. ms
314 bytes from 47.127.127.55: icmp_seq=1. time=72. ms
314 bytes from 47.127.127.55: icmp_seq=2. time=66. ms
314 bytes from 47.127.127.55: icmp_seq=3. time=72. ms
314 bytes from 47.127.127.55: icmp_seq=4. time=69. ms
314 bytes from 47.127.127.55: icmp_seq=5. time=69. ms
314 bytes from 47.127.127.55: icmp_seq=6. time=64. ms
314 bytes from 47.127.127.55: icmp_seq=7. time=67. ms
314 bytes from 47.127.127.55: icmp_seq=8. time=62. ms
314 bytes from 47.127.127.55: icmp_seq=9. time=68. ms
----47.127.127.55 PING Statistics----
10 packets transmitted, 10 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 62/67/72
```

Voice encoding latency is the sum of the voice sample size (or payload) and encoding delay. In Release 2 of Centrex IP, the voice payload duration is 20 ms.

For acceptable voice QoS, the total one-way enterprise latency cannot exceed 44 ms. The following equation shows the total one-way latency, L_T.

Equation 7-1 Number of available channels

$$L_T = L_N + L_E$$

where
L_N = one-way latency attributed to the enterprise network
L_E = one-way latency attributed to voice encoding/decoding at the IP terminal

Assuming a best-case encoding delay, L_E, of 30 ms for G.711, the enterprise latency, L_T, for the example network in Figure 7-9 is

Example
$L_T = 67 / 2 + 30 = 33.5 + 30 = 63.5$ ms

which exceeds the desired latency limit for the enterprise network.

To gather additional performance information, use Traceroute to determine the latency contributors. Traceroute uses the IP time-to-live (TTL) field to determine router hops to a specific IP address. Figure 7-10 shows an example of the Traceroute results from the IP terminal to the enterprise edge device, indicating that five router hops are required. The third hop in this figure introduces the majority of the latency in the path. One method to reduce latency in this enterprise is to reduce the number of router hops in the path from IP terminal to edge device.

Figure 7-10 Traceroute example for IP terminal to enterprise edge device

```
% traceroute brtph323 314
traceroute to brtph323 (47.127.127.55), 30 hops max, 314 byte packet
 1 brtph225 (47.192.192.29)  7 ms    2 ms    3 ms
 2 47.7.7.10 (47.7.7.10)     2 ms    2 ms    2 ms
 3 47.24.24.1 (47.24.24.1)  63 ms   64 ms  121 ms
 4 tcarh245 (47.50.50.14)   71 ms   62 ms   61 ms
 5 brtph323 (47.127.127.55) 64 ms   65 ms   67 ms
```

Enterprise network packet loss

Also use Ping to determine the packet loss in the path between the IP phone host and the enterprise edge device. Collect Ping statistics over an extended period of time to calculate the average packet loss. Also examine the network performance information to ensure that there are no extended periods of packet loss “bursts,” which can adversely affect voice quality. As with latency, you can use other network analysis or management tools currently in the enterprise network to collect this performance information.

The enterprise network for acceptable QoS requires an average packet loss of less than 0.5%.

Bandwidth requirements for Centrex IP

For the traffic generated by the IP phones to receive service equivalent to that of ordinary phones, provide enough bandwidth on the enterprise LAN. This bandwidth for VoIP packets is in addition to the bandwidth that all other data traffic on the LAN requires. The following example shows the steps for calculating the bandwidth using 500 IP phones.

1. Provide inputs from assumptions on page 7-15.

   Note: Estimate the HDBH CCS from Subscriber Line Usage studies for the lines that are being converted to IP terminals. Use a factor of 1.3 to convert Busy Hour (BH) usage into HDBH usage.

2. Compute the total HDBH traffic in CCS for all IP terminals.

   Number of IP terminals x HDBH CCS for each IP terminal =
   500 x 6.0 = 3000 CCS

3. Refer to the traffic capacity tables (ECM 590, Issue 05), to find the required number of channels for the total traffic at the specified grade-of-service. If the calculated total traffic does not appear in the table, use the lowest number of channels with traffic exceeding the calculated total traffic.

   Number of channels = 103 channels at 3014 CCS

4. Convert the number of channels into Ethernet LAN bandwidth required. The G.729A codec with a frame duration of 20 ms requires 34.4 kbit/s for each channel. (Refer to Table 7-2, "Ethernet and WAN bandwidth requirements for various codecs" on page 7-6.)

   Number of channels x 34.4 kbit/s channel =
   103 x 34.4 kbit/s = 3543 kbit/s

   Note 1: The enterprise LAN bandwidth required, from step 4, is understood as effective available bandwidth after accommodating bandwidth requirements for all other non-VoIP packets. However, the calculated LAN bandwidth requirement can overstate the requirements, depending on LAN configuration and segmentation. These engineering guidelines cannot include all of the possibilities for how clusters of VoIP users are located on different segments of the LAN.

   Note 2: Step 4 shows the incremental bandwidth that the enterprise LAN edge device requires. When R1 is duplicated for reliability, the required incremental bandwidth must be available on both R1 and the spare edge device.

Bandwidth availability

To calculate the bandwidth available in the enterprise network for Centrex IP voice services, subtract the “busy hour” LAN bandwidth utilization for non-Centrex IP services from the engineered utilization limit for the LAN. In this case, the busy hour refers to the hour of the day with the highest average utilization for a LAN segment in the path from an IP terminal to the enterprise edge device. Use standard network management tools, such as HP OpenView or Bay Networks Optivity, to gather this utilization information. These tools rely on Simple Network Management Protocol (SNMP) messaging to query network element management information base (MIB) data.

For example, assume the following conditions:

- Busy hour LAN segment utilization = 10%
- Engineered utilization limit = 35%

Then the utilization available for Centrex IP services:

35% - 10% = 25%

The available bandwidth would then be 25% of the transmission speed of the LAN segment(s) that carry Centrex IP traffic.

Use the procedure from section “Bandwidth requirements for Centrex IP.” to compare the Centrex IP bandwidth requirements to the available bandwidth on the enterprise LAN.

> ***Note:*** This comparison is a conservative view of the bandwidth usage. It assumes coincident “busy hours” for Centrex IP services and other LAN traffic.

Recommendations for bandwidth constraints

If the available LAN bandwidth is less than that required for Centrex IP service, refer to the following recommendations:

- Rearrange the deployment of IP phones to off-load the overloaded LAN segment(s).
- Choose a less bandwidth-intensive encoding scheme for the IP phones. (That is, use G.729A instead of G.711 encoding.)
- Upgrade LAN segments to higher bandwidth media or upgrade LAN segments from shared to switched access.
- Rearrange existing network devices to reduce the network traffic on LAN segments that carry Centrex IP services.
- If appropriate, and necessary network equipment is available, give priority service to voice traffic in the network.

Enterprise network security

Security considerations in the enterprise network include firewall policies and NAT configuration.

Denial of service attacks

To reduce network vulnerability to denial of service (DoS) attacks, a firewall is recommended. There are several DoS programs that can attack a network system. The goal of these programs is to either crash the object being attacked (such as the Gateway or Gatekeeper) or to slow it down severely. The CO LAN components have been designed to survive certain attacks. For example, the Gateway card can survive a Ping Storm attack and still sustain 60 calls. A Ping Storm is when a person sends repeated Ping requests to a system several times a second.

A UDP attack is when a person sends thousands of UDP packets per second to a system in an attempt to crash or overload the system. These packets can be any size. Large UDP packets can tie up system resources or crash the system. The Gateway card can survive this type of attack for smaller packet sizes (1,000 byte packets). Larger packet sizes can cause the Gateway card to go system busy (SysB).

Firewall strategy and implementation

A recommended enterprise firewall policy reflects the firewall rules that the CO LAN implements. Enterprises employ various policies to protect their network. These rules only address the required functionality for Centrex IP. The enterprise firewall administrator can use additional rules to protect the enterprise network from unauthorized intrusions.

Table 7-10 lists network objects that the administrator can define to implement enterprise firewall rules. The object names are arbitrary. The administrator must add other local information (such as IP addresses) to define these objects in Checkpoint Firewall-1.

Table 7-10 Objects used to set up enterprise LAN firewall rules (Sheet 1 of 2)

Name	Object type	Location	Comments
ARN	Router	Internal	Enterprise edge device
CO-LAN	Network	External	
Gateway10	Workstation (Host)	External	Gateway in LTCI
TPS-121	Workstation (Host)	External	Software object (in Gatekeeper)

Table 7-10 Objects used to set up enterprise LAN firewall rules (Sheet 2 of 2)

Name	Object type	Location	Comments
TFTP-Server	Workstation (Host)	External	Software object (on Gatekeeper)
Enterprise-LAN-Local	Network	Internal	
Enterprise-LAN-Remote	Network	External	For intraswitching purposes

Table 7-8 lists defined services allowable on the CO LAN firewall. The enterprise LAN firewall also allows these same services.

The network administrator can implement a secure combination of rules for Centrex IP by defining these objects and services, and predefined services of most firewall implementations (including Firewall-1).

Table 7-11 lists defined services allowable on the enterprise LAN firewall

Table 7-11 Defined services on the enterprise LAN

Name	Source port range	Destination port range	Protocol
VoiceStreamIn	2325–2446	6000–6011 (Note)	UDP/RTP
VoiceStreamOut	6000–6011 (Note)	2325–2446	UDP/RTP
VoiceStream Intraswitched	6000–6011 (Note)	6000-6011 (Note)	UDP/UNISTIM
SignalingE2Set	5000 (Note)	5000	UDP/UNISTIM
NAT-Enabler-Out	6000-6011 (Note)	6066	UDP/UNISTIM
NAT-Enabler-In	6066	6000-6011 (Note)	UDP/UNISTIM

Note: These ports are valid only when NAT is disabled. For a NAT configuration, substitute the NAT external ports, which the Enterprise LAN uses. When NAT is enabled on the enterprise LAN, firewall functionality is upstream from the NAT functionality.

Table 7-12 shows a typical set of rules that secures the enterprise LAN and guarantees functionality for Centrex IP.

Table 7-12 Enterprise LAN firewall rules (Sheet 1 of 2)

No.	Source	Destination	Service	Action	Comment
1	CO-LAN	Enterprise-LAN-Local	OSPF RIP RIP-response BGP-UDP BGP-TCP	Drop	Routing protocols. Some or all to be removed (depending on enterprise LAN choice).
2	CO-LAN	Enterprise-LAN-Local	Telnet	Drop	Change action to Accept to Telnet.
3	CO-LAN	Enterprise-LAN-Local	FTP	Drop	Change action to Accept to FTP.
4	Enterprise-LAN-Local	CO-LAN	ICMP-Proto	Drop	Change action to Accept to Ping and Traceroute.
5	CO-LAN	Enterprise-LAN-Local	ICMP-Proto	Drop	Change action to Accept to Ping and Traceroute.
6	Enterprise-LAN-Local	Gateway10	VoiceStreamOut	Accept	Voice stream to gateways. Source port range: 6000–6011. Dest. port range: 2325–2446. Additional gateways can be added in this rule.
7	Gateway10	Enterprise-LAN-Local	VoiceStreamIn	Accept	Voice stream from gateways. Source port range: 2325–2446. Dest. port range: 6000–6011. Additional gateways can be added in this rule.
8	Enterprise-LAN-Local	TFTP-server	TFTP	Accept	TFTP requests from i2004 terminals.
9	TFTP-server	Enterprise-LAN-Local	TFTP	Accept	TFTP load to i2004 terminals.
10	Enterprise-LAN-Local	TPS-121	SignalingE2Set	Accept	Signaling from TPS. Source port: 5000. Destination port: 5000.

Table 7-12 Enterprise LAN firewall rules (Sheet 2 of 2)

No.	Source	Destination	Service	Action	Comment
11	TPS-121	Enterprise-LAN-Local	SignalingE2Set	Accept	Signaling to TPS. Source port: 5000. Destination port: 5000.
12	Any	Enterprise-LAN-Local	Any	Drop	Drop everything else.
13	Enterprise-LAN-Local	Any	Any	Drop	Drop everything else.
14	Enterprise-LAN-Local	TPS-121	NAT-Service-Out	Accept	To allow messaging for NAT support
15	TPS-121	Enterprise-LAN-Local	NAT-Service-In	Accept	To allow messaging for NAT support
16	Enterprise-LAN-Local	Enterprise-LAN-Remote	Voice Stream Intraswitching	Accept	For intraswitching
17	Enterprise-LAN-Remote	Enterprise-LAN-Local	Voice Stream Intraswitching	Accept	For intraswitching

Explanations for the rules in the previous table follow.

- Rule 1 examines common routing protocols. The enterprise LAN administrator can remove the unused protocols. The administrator can also change the rule so that the firewall drops all of the protocols if static routing is used.
- Rules 2, 3, 4, and 5 examine common network protocols, including Telnet, FTP, and ICMP. Nortel Networks suggests dropping these protocols and enabling them only when their brief use is necessary.
- Rules 6 and 7 accept the packets exchanged between a fixed port range on the H.323 Gateways and a fixed range of ports inside the enterprise LAN. An administrator can add other Gateways to this rule by defining a new network object.
- Rules 8 and 9 accept the TFTP packets going to and from the TFTP server on the enterprise LAN. This rule allows the i2004 terminals to retrieve new loads.
- Rules 10 and 11 accept the signaling messages going from a pre-determined port on the TPS to a pre-determined port on the i2004 terminals. (Table 7-13 lists the port usage for the i2004 terminal.)
- Rule 12 drops all the packets with the enterprise LAN as a destination address that rules 1 to 11 do not describe.
- Rule 13 drops all the packets with the enterprise LAN as a source address that rules 1 to 11 do not describe.
- Rules 14 and 15 accept signaling between the i2004 phone and the TPS to enable NAT mapping at the enterprise.
- Rules 16 and 17 allow intraswitching to another i2004 outside the firewall.

The following tables lists the port use for the i2004 telephone.

Table 7-13 i2004 port usage

Port range	Protocol	Usage
5000	UDP/UNISTIM	UNISTIM signaling
Dynamic (starts at 6000–6010, even ports)	UDP/RTP	RTP media stream (Gatekeeper assigned)
Dynamic (starts at 6001–6011, odd ports)	UDP/RTCP	RTCP control stream (Gatekeeper assigned)
1024-65536	TFTP	E2 firmware download

NAT configuration

Centrex IP supports static or dynamic NAT. Static NAT is a one-to-one, private-to-public address mapping. Dynamic NAT is a many-to-one, private-to-public address mapping. Dynamic NAT uses ports on a public address to map multiple private addresses to a single public address. Performance is a primary concern for NAT devices. If the NAT device at the enterprise edge introduces unacceptable additional latency to the media streams, upgrade or replace the device.

> *Note:* Centrex IP does not support intraswitching between two i2004 phones behind the same NAT. Two i2004 phones can intraswitch behind the same firewall.

To prevent the expiration of NAT mapping, the keep-alive audit interval of the i2004 telephones by the TPS must be less than the NAT map expiration time.

NAT and firewall considerations

In the presence of dynamic NAT, the i2004 RTP media stream can be mapped to dynamic port ranges, depending on the NAT implementation. Adjust the CO LAN firewall rules accordingly to accommodate these port changes. Alternatively, the NAT dynamic port mapping should be confined to a chosen range, provided the NAT has such control. When a NAT is used at the Enterprise LAN in conjunction with a firewall, the firewall function is upstream from the NAT function.

Part IV Operations and maintenance

This part contains the following chapters:

- DMS maintenance
- Card replacement
- Logs
- Terminal proxy server
- Troubleshooting

8 DMS maintenance

Overview

The DMS-100 switch contains a node maintenance and a line maintenance system that provide maintenance functions for the Gateway card (NT7X07AA) and the lines associated with the Gateway card. Both the computing module (CM) and the XMS peripheral module (XPM) node maintenance subsystems provide maintenance for the Gateway card. The Gateway software load also contains maintenance diagnostic utilities.

The CM supports the following maintenance functions:

- node maintenance for the Gateway card
- loop maintenance for the H.323 terminals
- provisioning for the H.323 terminals and the Gateway card
- state transitions for the Gateway card

The XPM supports the following maintenance functions:

- local node maintenance for the Gateway card
- maintenance messaging between the CM and the Gateway card
- HDLC messaging between the XPM processor and the Gateway card
- dynamic maintenance data updates to the inactive unit
- Gateway loading request from the CM to the Gateway card
- mapping of the call processing node number to physical card
- diagnostic failure reports to the CM
- fault notifications from the Gateway card to the CM

The ISDN line trunk controller (LTCI) does not provide maintenance support for the local area network (LAN) side of the Gateway card. All events on the LAN side are managed by the Gateway card, independent of the LTCI. The Gateway card notifies the XPM node maintenance subsystem of conditions that compromise the voice path on the LAN.

CM node maintenance

The CM node maintenance subsystem forwards static provisioning data to the Gateway card. The data is limited to a set of operating parameters passed in the status message as indicated in the list that follows:

- CM and XPM BCS number
- XPM external node number
- Gateway external node number
- Gateway type or variant

  Note: For Centrex IP, the Gateway type is local loop.

- DMS system timestamp
- even port number of the Gateway card

CM to XPM messaging

All IPGW maintenance requests originate in the CM as requests using the normal DS-30 messaging path.

Provisioning the Gateway card

The CM handles provisioning for the Gateway card and the Centrex IP terminals. Centrex IP software features are provisioned using the standard basic rate interface (BRI) Service Order System (SERVORD). Hardware provisioning is accomplished through table control.

Provisioning of the Gateway card requires datafill of the following tables. The tables are listed in the order in which they are to be datafilled.

- Table CARRMTC
- Table LTCPSINV
- Table SITE
- Table IPINV

Note: For a procedure for installing and provisioning the Gateway card, refer to the “Gateway” chapter.

The sections that follow provide examples of datafill and field descriptions for tables CARRMTC, LTCPSINV, and IPINV.

Note: Table SITE is not documented here. This document assumes the user is familiar with table SITE.

Table CARRMTC

Table CARRMTC defines a set of carrier attributes you can use when you define a carrier (p-side) link in table LTCPSINV. Table CARRMTC allows you to enter maintenance control information in peripheral modules (PM), out of service limits for alarms, and system return to service occurrences.

The following example shows sample datafill for table CARRMTC.

Figure 8-1 Example of table CARRMTC

```
CSPMTYPE    TMPLTNM  RTSML  RTSOL                 ATTR
________________________________________________________________
LTC        GWIP 255 255 DS1 NT7X07AA MU_LAW SF ZCS
           BPV NILDL  N 250 1000 50 50 150 1000 3 6 864 100
            17 511 4 255
```

The following table describes the fields in table CARRMTC.

Table 8-1 Table CARRMTC field descriptions

Field	Description
CSPMTYPE	C-side node peripheral module type.
TMPLTNM	Template name. The template name for the PM. The default value is DEFAULT. For gateways, the value is GWIP.
RTSML	Return to service maintenance limit. The number of times within the audit interval that a carrier can be returned to service by the system before a warning is issued. The value 255 disables this feature. Gateways use the value 255.
RTSOL	Return to service out of service limit. The number of times within the audit interval that a carrier can be returned to service by the system before it is put permanently out of service. The value 255 disables this feature. Gateways use the value 255.
ATTR	Attribute. Contains subfields to characterize the carrier encoding, framing, cardtype, and so on. Enter the datafill for the gateway ATTR field as shown in the example of table CARRMTC.

Table LTCPSINV

Table LTCPSINV contains the assignment of the P-side links for peripheral modules.

The following example shows sample datafill for table LTCPSINV.

Figure 8-2 Example of table LTCPSINV

```
LTCNAME                                        PSLNKTAB
________________________________________________________________

LTC   0
  N (0 DS1 GWIP N) (1 DS1 GWIP N)
   (2 DS1 GWIP N) (3 DS1 GWIP N)  (4 NILTYPE)
   (5 NILTYPE) (6 DS30A) (7 DS30A) (8 DS30A) (9 DS30A)
   (10 DS30A ) (11 DS30A) (12 DS30A) (13 DS1 DEFAULT N)
   (14 NILTYPE)  (15 DCH)  (16 NILTYPE)  (17 DCH)
   (18 NILTYPE )  (19 DCH) $
```

The following table describes the fields in table LTCPSINV.

Table 8-2 Table LTCPSINV field descriptions

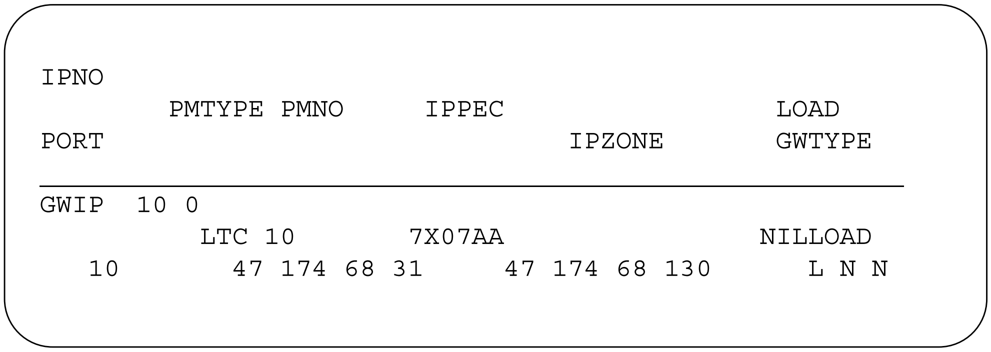
Field	Description
LTCNAME	Link trunk controller name. This field contains subfields XPMTYPE and XPMNO. The XPMTYPE is the alphanumeric peripheral module type of PM (for example, LTC). The XPMNO is the numeric peripheral module number. The range is from 0 to 255 to specify the PM number.
PSLNKTAB	P-side link table. The field is a vector of up to 20 entries for P-side links. Each link has the subfields PSLINK and PSDATA. PSLINK is the P-side port number. PSDATA is the carrier type from table CARRMTC. For gateways, the PSDATA is DS1 GWIP.

Table IPINV

The status of a Gateway card in table IPINV is static as opposed to the MAP display, where the status is dynamic.

The following example shows sample datafill for table IPINV.

Figure 8-3 Example of table IPINV



```
IPNO
        PMTYPE PMNO     IPPEC                LOAD
PORT                             IPZONE      GWTYPE
______________________________________________________
GWIP  10 0
          LTC 10       7X07AA               NILLOAD
   10       47 174 68 31     47 174 68 130      L N N
```

Note: In NA013, for a spare Gateway card to take over for a primary Gateway card, both cards must reside in the same Gatekeeper zone. Gatekeeper IP addresses in table IPINV must match.

The following table describes the fields in table IPINV.

Table 8-3 Table IPINV field descriptions (Sheet 1 of 2)

Field	Description
IPNO	IP number. The site identifier, frame, and unit number of the Gateway card.
PMTYPE	PM type. The type of peripheral module that the Gateway card is located in.
PMNO	PM number. The number of the PM that the Gateway card is located in.
IPPEC	IP PEC. The product engineering code (PEC) of the Gateway card.
LOAD	Load file name. The name of the Gateway's software load. (Note: The load is always NILLOAD.)
PORT	Port number. The number of the host XPM's P-side port. The card uses two ports. Specify the even port number.

Table 8-3 Table IPINV field descriptions (Sheet 2 of 2)

Field	Description
IPZONE	IP zone. The primary and secondary IP address for the Gateway card. ***Note 1:*** In NA013, for a primary Gateway card, the IPZONE field must be datafilled with two IP addresses. One IP address is the logical IP address (for example, 47.174.68.31), which must be unique. The other IP address is the Gatekeeper address (for example, 47.174.68.130). The logical IP is entered in the first four fields of IPZONE. The Gatekeeper IP is entered in the last four fields of IPZONE. ***Note 2:*** In NA013, for a spare Gateway card, the IPZONE field must be datafilled with a Gatekeeper IP address only (for example, 47.174.68.130). The logical IP address must be set to 0s.
GWTYPE	GW type. The function of the Gateway card (local loop). Subfields indicate if intraswitching or sparing are enabled. ***Note:*** In NA013, the spare bool under the GWTYPE field identifies the Gateway as a spare (Y) or primary (N) Gateway card. This field is applicable only if the Gateway is datafilled as a lines (L) Gateway.

Provisioning a terminal

Terminals are provisioned using BRI SERVORD. The LTID of the terminal is attached to a virtual line equipment number (LEN) on the Gateway.

> *Note:* A Gateway card provisioned as a spare cannot have terminals provisioned on it. A Gateway card with no terminals provisioned on it allows the card to take over the call processing for another Gateway card when sparing occurs.

Procedure 8-1 Create an LTID for a terminal

At the MAP display

1 Add a LEN to table LNINV (Line Circuit Inventory).

```
>TABLE LNINV
>ADD GWIP 10 0 0 1 BX27AA NPDGP WORKING N NL Y NIL
>QUIT
```

2 Add a tuple to table LTGRP (Logical Terminal Group).

```
>TABLE LTGRP
>ADD CIP 0 $ Y
```

```
>QUIT
```

Note: Adhere to the following recommendations for entering datafill in table LTGRP:

- The name of the logical terminal group cannot be the same name entered in table SITE.
- The number of the logical terminal group must be unique.

3 Create an NI2 LTID using SERVORD.

```
>SERVORD
>SLT $ CIP 1 ADD BRAFS NI2 N 64 N DTEI 001 N $ YY
```

4 Create a directory number (DN) for the NI2 LTID that was created in step 2.

```
>NEW $ 7235001 ISDNKSET BNR 0 0 613 1 Y NILLATA 0 CIP
1 1 CRBL 2 0 $ YY
```

Note: Circuit node data is not supported.

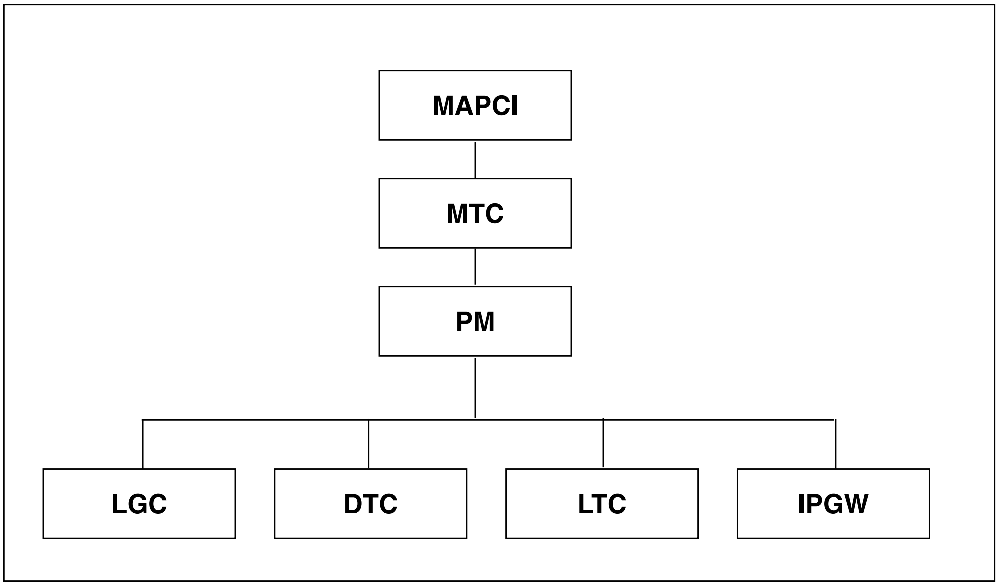
5 Attach the NI2 LTID to the LEN that was created in step 1.

```
>SLT $ CIP 1 ATT GWIP 10 0 0 1 $ YY
>QUIT
```

IPGW MAP level

CM node maintenance introduces a new sublevel at the PM level of the MAP display. This new sublevel, IPGW, allows the user to post a provisioned Gateway or group of Gateways. The following figure shows the MAP menu hierarchy.

Figure 8-4 IPGW menu hierarchy



IPGW MAP commands

The commands for the IPGW MAP level are described as follows in the order in which they appear.

QUIT

The QUIT command returns the user to the previous MAP level or, if used with the parameter ALL, returns the user to the command interpreter (CI) level of the MAP display.

POST

The POST command allows the user to display a specific Gateway or group of Gateways for maintenance purposes.

TRNSL

The TRNSL command allows the user to display the C-side links to the Gateway card.

TST

The TST (test) command allows the user to invoke diagnostics that test the Gateway card in in-service (InSv) and out-of-service (OOS) states. These two sets of tests are available based on the Gateway node state (for example, InSv, ManB [manual busy], or SysB [SysB]).

BSY

The BSY (busy) command allows the user to change the state of the Gateway node and the associated IP lines datafilled against the Gateway node to a ManB state.

> ***Note:*** In NA013, the NOSPARE option was added to the BSY command. The NOSPARE option allows a BSY to be performed without triggering a takeover.

RTS

The RTS (return to service) command allows the user to return the Gateway card to an in-service call processing ready state, including Gatekeeper registration. The RTS command invokes the OOS set of diagnostic tests to determine the general capability of the Gateway.

OFFL

The OFFL (offline) command allows the user to change the state of the Gateway from a ManB state to an offline state. All messaging to and from the Gateway is disabled. Unsolicited messages are blocked.

> ***Note:*** In NA013, checks are made to ensure a Gateway can be offlined safely.

LoadPMQ

The LoadPMQ (load peripheral module query) command allows the user to query the Gateway regarding its current load status. The Gateway returns the current default load type in response to this query, which results in an indication to the user if the Gateway contains a valid load. The user can use the PMRESET command to determine if the Gateway successfully loaded or not.

NEXT

The NEXT command allows the user to post the next PM or place the first PM of the next PM-type post set in the MAP post position.

QUERYPM

The QUERYPM (query peripheral module) command allows the user to obtain standard information about the Gateway. This information includes node status and configuration of the Gateway.

PMRESET

The PMRESET (peripheral module reset) command allows the user to reset and reload or restart the Gateway card.

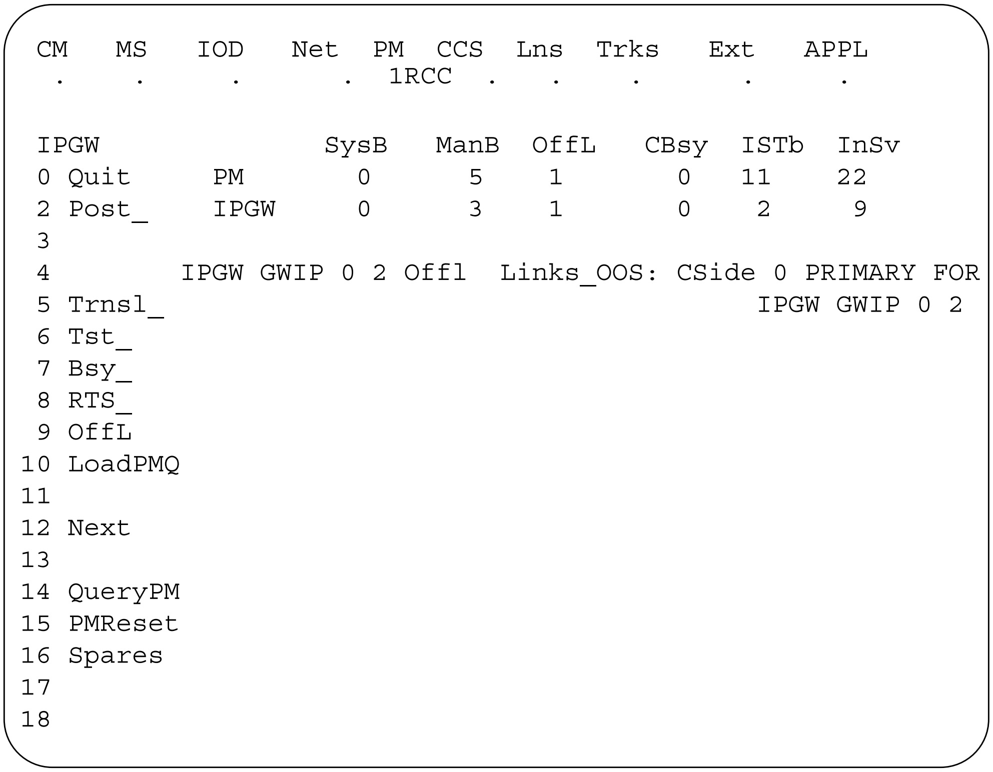
SPARES

The SPARES command allows the user to obtain information on the spare status of InSv Gateway cards on the same LTCI. The SPARES command used with the parameter ALL provides the spare status of all local Gateways datafilled in table IPINV.

> ***Note:*** In NA013, the ALL option in the SPARES command was enhanced to provide call processing node mappings.

The following figure shows an example of the IPGW MAP display.

Figure 8-5 IPGW MAP example



```
 CM   MS    IOD    Net   PM  CCS   Lns   Trks    Ext    APPL
  .    .     .       .   1RCC  .    .     .       .      .

 IPGW              SysB   ManB  OffL   CBsy  ISTb  InSv
 0 Quit      PM       0      5    1       0   11    22
 2 Post_     IPGW     0      3    1       0    2     9
 3
 4         IPGW GWIP 0 2 Offl  Links_OOS: CSide 0 PRIMARY FOR
 5 Trnsl_                                      IPGW GWIP 0 2
 6 Tst_
 7 Bsy_
 8 RTS_
 9 OffL
10 LoadPMQ
11
12 Next
13
14 QueryPM
15 PMReset
16 Spares
17
18
```

Limitations and restrictions

For RTS, TST, and BSY commands, options NOWAIT and ALL are not available with IPGWs.

Parameter downloading

The Centrex IP system supports DMS parameter downloading to i2004 phones on the IP network. Parameter downloading is the capability for the terminal proxy server (TPS) to receive provisioned features directly from a DMS switch.

To support BRI parameter downloading, the TPS acts as a BRI agent through the Gatekeeper and Gateway to the XPM. The Q.931 protocol messaging between the XPM and the Gateway and Gatekeeper passes the Q.931 messages to the TPS.

QPIN command

The CI command QPIN (query personal identification) displays a DN Key number of a Centrex IP i2004 phone. Use this command to retrieve the DN Key number when setting up the TPS. (This number is used also during initialization of an i2004 phone.)

To display the DN Key of an i2004 phone, enter a 10-digit primary directory number (PDN).

The QPIN output for a DN Key number consists of a 20-digit format, as follows.

```
aabbbbbbbbbbccccdddd
```

where:

aa	=	the two-digit terminal type (00 refers to a Centrex IP i2004 phone)
bbbbbbbbbb	=	the ten-digit PDN
cccc	=	the four-digit PM node number
dddd	=	the four-digit PM terminal number

The following figure shows an example of how to access the QPIN command to display a non-MADN DN.

Example of QPIN command access and output for a non-MADN DN

```
CI:
>QPIN
QPIN - Query PIN/DNKEY for IP-Pphone/IPLL
QPIN:
>DN 9195559990
PIN : 00919555999000840003
```

The following error responses apply to the QPIN command.

Table 8-4 QPIN error responses with associated meanings and actions (Sheet 1 of 2)

MAP response:	`For Centrex IP, use the DN query to get the DN key.`
Meaning:	User has entered a LEN for an i2004 phone without entering the DN first.
Actions:	Re-enter the command, beginning with the DN.
MAP response:	`Invalid Area Code`
Meaning:	User has entered a number for an incorrect area code.
Actions:	Check the area code. Re-enter the correct number.
MAP response:	`Invalid DN: The DN must be 10 digits. Please query again.`
Meaning:	User has entered a DN that is not 10 digits in length.
Actions:	Re-enter with 10 digits.
MAP response:	`Invalid LEN`

Table 8-4 QPIN error responses with associated meanings and actions (Sheet 2 of 2)

Meaning:	User has entered an incorrect value for the LEN.
Actions:	Check the LEN. Re-enter the correct value.
MAP response:	`Invalid Office Code`
Meaning:	User has entered a number for an incorrect office code.
Actions:	Check the office code. Re-enter the correct office code.
MAP response:	`TYPE OF <TEN_DIGIT_REGISTER> IS TEN_DIGIT_REGISTER <TEN_DIGIT_REGISTER>:`
Meaning:	User has entered a non-numeric DN.
Actions:	Re-enter with 10 numerical digits.
MAP response:	`Unassigned DN`
Meaning:	User has entered a DN that has not been assigned to any phone.
Actions:	Check the DN. Re-enter the correct DN.

Enabling parameter downloading

Follow this procedure to enable parameter downloading. If this is an initial TPS installation, proceed to the first step of Procedure 8-2.

If this is not an initial installation for parameter downloading, ensure that following checks are in place:

- The db.ini file only has [TERMINALS] in its first line. The line *cannot* contain an ini file entry.
- No terminal.ini file exists in the db directory.

> ***Note:*** The format for this file name is <hardwareId>.ini (for example, 006038760666.ini).

Procedure 8-2 Enabling parameter downloading

At the MAP display and the Gatekeeper

1 Use the DMS CI command QPIN to identify the DN key number for all terminals. (Refer to section, “QPIN command” for details.)

2 Access the TPS Config Tool. From the Gatekeeper, select Start-->Programs-->Terminal Proxy Server--> Configuration Tool.

The TPS Config Tools window opens. The system administrator can choose the following two TPS Config Tool tabs:

- *System Settings-for updating TPS-related attributes, such as IP addresses, and port settings for the TPS, Gatekeeper, and packet* *telephony manager (PTM). The system administrator can also specify firmware information for the i2004 phone.*

- *DN Key Settings-for entering valid DN keys for Centrex IP parameter downloading.*

3 Select the DN Key Settings tab.

4 Enter the 20-digit DN Key number in the Enter DN Key digits field. (Access the CI command QPIN at the MAP display to identify the specific DN Key number.)

5 If necessary, change the non-Centrex features (such as, Language Selection or Directory).

6 Click the Add button.

A <dnkey>.obj file is created in the dnkeydb directory.

> ***Note:*** *Do not delete this file.*

7 Repeat steps 4 through 6 for all other terminals.

8 Press the Apply button at the bottom of the DN Key Setting menu to apply the changes. Or press the OK button to apply the changes and exit the TPS Config Tool.

9 Plug in the i2004 phone.

For an initial downloading configuration, the system prompts for the DN key.

10 Enter the 20-digit DN Key on the i2004 phone.

The TPS begins parameter downloading and retrieves information on the phone from the DMS switch.

Changing a DN on an i2004 phone

Follow this procedure to change a DN that is associated with a DN Key on an i2004 phone.

Procedure 8-3 Changing a DN on an i2004 phone

At the desk, MAP display, and the Gatekeeper

1 Unplug the existing i2004 phone.

2 Access the TPS Config Tool. (See step 2 of Procedure 8-2.)

The TPS Config Tools window opens.

3 Select the DN Key Settings tab.

4 Delete the existing DN key entry.

Select the corresponding DN Key number in the DN Keys list. Click the Delete button.

5 Change the PDN using the SERVORD command CDN (Change DN).

```
>SERVORD
>CDN 9195559990 9195559900 CANN
```

6 At the MAP display, use the CI command QPIN to obtain the new DN Key number.

7 From the DN Key Settings menu in the TPS Config Tool, enter the new DN Key number in the Enter DN Key digits field. Click the Add button.

8 Press the Apply button at the bottom of the DN Key Setting menu to apply the changes. Or press the OK button to apply the changes and exit the TPS Config Tool.

9 Plug in the i2004 phone.

10 When prompted, enter the new DN Key number on the i2004 phone.

Note: Follow all the steps in Procedure 8-3 for PDNs to ensure that all components in a Centrex IP system have proper DN Key information.

Detaching and reattaching an LTID from one LEN to another LEN

Follow this procedure to detach an LTID from one LEN and reattach the LTID to another LEN.

Procedure 8-4 Detaching and reattaching an LTID from one LEN to another LEN

At the desk, Map display, and the Gatekeeper

1 Unplug the existing i2004 phone.

2 Access the TPS Config Tool. (See step 2 of Procedure 8-2.)

The TPS Config Tools window opens.

3 Select the DN Key Settings tab.

4 Delete the existing DN key entry.

Select the corresponding DN Key number in the DN Keys list. Click the Delete button.

5 At the MAP display, detach the LTID from the existing LEN using the SERVORD command SLT DET (Set Up Logical Terminal Detach).

6 Attach the LTID to the new LEN using the SERVORD command SLT ATT (Set Up Logical Terminal Attach).

7 Use the CI command QPIN to obtain the new DN Key number.

8 From the DN Key Settings menu in the TPS Config Tool, enter the new DN Key number in the Enter DN Key digits field. Click the Add button.

9 Press the Apply button at the bottom of the DN Key Setting menu to apply the changes. Or press the OK button to apply the changes and exit the TPS Config Tool.

10 Plug in the i2004 phone at the new location.

11 When prompted, enter the new DN Key number on the i2004 phone.

Swapping LTIDs using the SERVORD SWLT command

To ensure that all components in the Centrex IP system operate properly, follow these steps with the SERVORD command SWLT (swap logical terminals).

Procedure 8-5 Swapping LTIDs using the SERVORD SWLT command

At the desk, MAP display, and the Gatekeeper

1 Power off (cycle off) any i2004 phones associated with the LTIDs to be changed.

2 Access the TPS Config Tool. (See step 2 of Procedure 8-2.)

The TPS Config Tools window opens.

3 Select the DN Key Settings tab.

4 Delete the existing DN key entry.

Select the corresponding DN Key number in the DN Keys list. Click the Delete button.

5 At the MAP display, move the LTIDs using the SERVORD command SWLT.

6 Use the CI command QPIN to obtain the new DN Key numbers.

7 From the DN Key Settings menu in the TPS Config Tool, enter the new DN Key number in the Enter DN Key digits field. Click the Add button.

8 Press the Apply button at the bottom of the DN Key Setting menu to apply the changes. Or press the OK button to apply the changes and exit the TPS Config Tool.

9 Plug in the i2004 phone.

10 When prompted, enter the new DN Key number on the i2004 phone.

Limitations and restrictions

The following restrictions apply to parameter downloading.

- Only use the QPIN command with a DN assigned to key 1 of the phone. If you try to use the QPIN command with a secondary DN, the DN Key is not valid.
- A terminal remains in the unregistered state if it has not completed parameter downloading. When the Gatekeeper does not recognize a terminal as registered, it does not forward parameter downloading notifications to the TPS.
- If a user tries to program another i2004 phone with his or her DN Key, the user is denied service.
- Ensure that the PDN of an i2004 phone is unique to the DMS switch. MADN cannot be datafilled on the PDN (key 1) of an i2004 phone.
- Do not use QPIN by LEN for Gateway nodes.
- If a member of a MADN group originates a call, a user of an i2004 phone cannot bridge into the call until the remote party has answered.

Note: Refer to *The i2004 Internet Telephone User Guide* for details on i2004 phone use.

XPM node maintenance

The XPM node maintenance subsystem treats the Gateway card as a subtending node of the XPM. The Gateway node name is Internet Protocol Gateway (IPGW). XPM node maintenance uses the existing peripheral-side (P-side) node maintenance path to handle Gateway maintenance requests.

XPM node maintenance receives node state information on each provisioned Gateway card from the CM. The Gateway card receives maintenance messages from the CM over a high-level data link control (HDLC) messaging channel. The Gateway card also uses the HDLC messaging channel to notify XPM node maintenance of conditions on the LAN side that affect call processing and the service state of the node. The XPM notifies the CM of any problem conditions and changes the node state as directed by the CM.

Node states

The XPM node maintenance subsystem supports the following IPGW node states:

- OFFL—standard PM offline
- MANB—standard PM manual busy
- SYSB—critical software or hardware condition
- ISTB—non-critical software condition, non-critical hardware condition, or non-critical IP network condition
- INSV—normal call processing condition, with no software, hardware, or network faults

> ***Note:*** A non-critical condition is a fault condition that does not adversely affect call processing capability or quality of service (QoS). A critical condition is a fault condition that adversely affects call processing capability or QoS.

XPM to Gateway card messaging

Based on the P-side slot physical connections to the shelf backplane, the communications interface between the XPM and all installed Gateway cards is the DS60 serial interface. Four of the 64 DS60 channels for each Gateway card are available for messaging. The remaining 60 channels carry pulse code modulation (PCM) voice traffic or an idle PCM bit pattern. The following sections describe the messaging channels.

Messaging channel

The messaging channel uses the HDLC protocol to carry all types of messaging traffic between the XPM and the Gateway card. The XPM node maintenance subsystem uses this path for maintenance-related messaging to the card.

Dedicated maintenance channel

The dedicated maintenance channel is used by XPM diagnostics. All access to the Gateway card's maintenance control and status registers are through this channel. It also allows the XPM node maintenance subsystem to diagnose card sanity or faults in the absence of an active messaging connection.

Dedicated maintenance loopback channel

The dedicated maintenance loopback connection is used by XPM diagnostics. This is a permanent loopback available from both the active and inactive units of the XPM. The loopback can be disabled through a bit in the control byte in the maintenance control/status channel.

> *Note:* Currently only three of the four available messaging channels are used. The fourth messaging channel remains available for future development.

Gateway sparing

ATTENTION

The Gateway sparing feature does not apply to the NA012 load. This feature requires the NA013 load.

In any LTCI, a maximum of eight Gateway cards can be provisioned as primary cards. Gateway sparing allows any number of Gateway cards to be provisioned as spares, provided each LTCI has at least one primary Gateway card. A spare Gateway card can serve primary cards on either shelf of the LTCI.

> *Note:* A spare Gateway card can takeover only for the primary Gateway cards that are in the same IPZONE. For example, the Gatekeeper IP address is identical in table IPINV.

Gateway N+1 sparing allows a spare Gateway card to assume the call processing load of an active Gateway card on the same XPM if one of the active cards fails. If a primary Gateway card fails and a takeover occurs, all calls in a talking state will be maintained. Calls in a non-talking state, including held calls will be dropped. Dropped calls must be re-originated.

Gateway N+1 sparing requires that at any one time, a physical node must be capable of handling the work load of any of the logical nodes.

DMS addressing

Each Gateway card is provisioned as a node in the system, which is addressed by a unique node number. Each Gateway node consists of virtual line cards that are addressed by a terminal identifier (TID). The TID consists of the node number and terminal number of the Gateway. The DMS messaging system uses the TID to determine to which physical card to route a message. There is a fixed mapping between the node number and physical card. To allow the call processing load of a Gateway node to be handled by different physical cards, sparing introduces the concept of moving the call processing TIDs of a Gateway node between cards. From a maintenance perspective, there continues to be a fixed mapping between the node number and physical card.

Packet network addressing

From a packet network perspective, all Gateway cards on an XPM in the same Gatekeeper zone must reside on the same subnet. These cards are addressed by a unique IP address for that subnet. Logical IP addresses allow a Gateway card to map two IP addresses to its network interface.

The two IP address are as follows:

- physical IP
  - received at boot time from the DHCP
  - always remains the same for each card
- logical IP
  - used for communication with other LAN endpoints
  - exists only for primary Gateways
  - moves between cards as takeover occurs

Data sync

To maintain calls in a talking state, call data must transfer from primary to spare cards so the call topology can be recreated in the spare card if it becomes active.

Data sync of Gateways between primary and spare cards is performed over the packet network with IP multicasting as follows:

- A multicast IP address is assigned for synching Gateway call data.
- When a primary card comes in service, it joins the multicast group. From then on, as calls are made and released, it sends this data to the multicast IP.
- When a spare card comes in service, it joins the multicast group, and sends a bulk call request to the multicast IP. All in-service primary cards in the group respond with call data messages for all the currently active calls. From then on, the spare card receives data from the multicast group.

Sparing triggers

The following actions will trigger a takeover:

- The user performs a BSY of a primary Gateway card when a spare Gateway card is in service.
- The user performs an RTS of a spare Gateway card when a primary Gateway card in out of service.
- A primary Gateway card reports a critical internal fault to the XPM.
- The XPM detects the HDLC communication link to a primary Gateway card is down.
- A primary Gateway card fails the in service tests that are routinely run by XPM maintenance.

The following actions will *not* trigger a takeover:

- The user performs a BSY of a primary Gateway card when no spare Gateway cards are currently in service.
- The user performs a BSY NOSPARE of a primary Gateway card.
- A primary Gateway card reports a critical p-side fault indicating that the Gatekeeper is not responding.

Spares command

Procedure 8-6 Accessing the Spares command

At the MAP display

1 Go to the PM level of the MAP display and post the Gateway card. Type

>MAPCI;MTC;PM;POST IPGW GWIP 02

and press the Enter key.

2 Determine the SPARE status of the Gateway card. Type

>spares

and press the Enter key.

Example of a MAP response

```
Spares
Sparing status of InSv spares off same host:
Spare IPGW GWIP 02 0 Is In-Service
```

3 Determine the status of all local IPGWs. Type

>spares all

and press the Enter key.

Example of a MAP response

```
Spares all
Sparing status of all local IPGWs:
Spare IPGW GWIP 06 0 Is In-Service
Spare IPGW GWIP 08 0 is Man Busy
Primary IPGW GWIP 10 0 Is In-Service Servicing GWIP 10 0
Spare IPGW GWIP 12 0 is Off-Line
```

Limitations and restrictions

The following limitations and restrictions apply to Gateway sparing:

- Feature invocation on a call that has survived a takeover is not supported, including hold. If the user attempts to hold a spared call, that call will be released. Calls that are on auto hold by the terminal are also released. For example, if the user receives an incoming call while currently on a call that survived a takeover, the takeover call will be released if the user answers the incoming call.
- Active calls placed on hold by a LAN agent will not survive a takeover.
- In a worst case scenario, detection of Gateway failure can take over four minutes, based on the type of failure.
- QoS data collected for an active call prior to a takeover will not survive the takeover.
- Prior to taking a primary Gateway OFFL, ensure the lines datafilled on the Gateway are not being serviced by another gateway. If the lines are being serviced by another gateway, use the BSY NOSPARE command to take the lines out of service.

Note: Refer to the release notes for Release 2 on your software CD for the necessary procedures to invoke sparing on a Gateway when NA013 is applied in an office.

Gateway diagnostics

Gateway diagnostics consist of test utilities that reside in the Gateway firmware and are requested by the XPM. The diagnostics are controlled and invoked by the XPM. XPM maintenance uses the diagnostics in a manner consistent with existing CM and XPM maintenance interfaces.

Gateway card diagnostics provide the XPM maintenance system with the following:

- ability to detect and isolate faults at the card level
- ability to establish card sanity during in-service and out-of-service state transitions of the node
- ability to run audits at specific time intervals

The following diagnostics are available:

- Activity test—checks the activity of the unit in which the diagnostic is running
- Port range test—checks the port of the Gateway card against datafill to ensure correct provisioning of the card and the validity of the port number
- Hardware presence test
    - verifies the Gateway card is present in the shelf
    - verifies the messaging and time switch cards are present and functional
- Out-of-service tests
    - check the integrity of the DS60 channels to the XPM interface of the Gateway card
    - verifies messaging paths to the DSPs of the Gateway card on all 60 channels
    - executes the diagnostic set on-board the Gateway card by a maintenance request message (for example, RAM test, ROM test, address test, communication test, and so on)
- In-service tests
    - tests all accessible communication paths without impact to call processing
    - runs a sub-set of the on-board diagnostics

Diagnostic enhancements include the following:

- The Gateway card is a resource for P-side loop allocation subroutines, used by other XPM diagnostics and fault isolation.
- Fault isolation diagnostics include the Gateway card in the card fault list.
- Diagnostic tests take the module and card state into account before requesting testing. The diagnostic tests rely on the state of the Gateway card as reported by the Gateway.
- Error reporting includes new message type definitions for errors reported by the Gateway to the XPM and then forwarded to the CM.

- The response to the QUERYPM command is modified to indicate if the posted Gateway card is handling the call processing load for a node.
- The MAP display is modified to show if the posted Gateway card is currently handling the call processing for the node.
- The node state audit is modified so real time sparing status queries are initiated through Gateway node maintenance requests.
- New warning messages are generated to indicate the sparing capability for group of provisioned Gateways due to maintenance activities.
- The SPARES command is added to the IPGW MAP level. The SPARES command displays the spare status only. The SPARES command is a query command only that has no effect on the maintenance system.
- The messaging definitions for XPM Gateway maintenance is altered to always return the current sparing status of the Gateway being reported.
- The interface between Gateway node maintenance and Gateway line maintenance is modified so that only transitions of the Gateway node to the OFFL state and to the initial INSV state are reflected by the Gateway lines datafilled for that node.
- Maintenance response messages are displayed on the MAP display (for example, TST failure reason: “Card Insane, HDLC Link Down”).

Alarms

A Gateway card that goes SysB generates a major alarm. To clear the alarm, follow this procedure.

Procedure 8-7 Clearing a major alarm

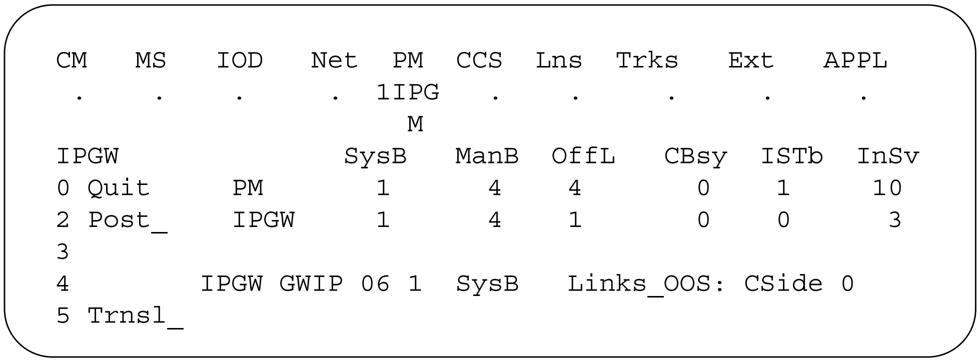
At the MAP display

1 Go to the PM level of the MAP display and check for SysB Gateway cards. Type

>MAPCI;MTC;PM;POST IPGW SYSB

and press the Enter key.

Example of a MAP response



```
CM   MS   IOD   Net  PM  CCS  Lns  Trks   Ext   APPL
 .    .    .     .  1IPG  .    .     .     .     .
                      M
IPGW              SysB   ManB  OffL   CBsy  ISTb  InSv
0 Quit     PM       1      4    4       0    1     10
2 Post_    IPGW     1      4    1       0    0      3
3
4        IPGW GWIP 06 1  SysB   Links_OOS: CSide 0
5 Trnsl_
```

2 Determine your next step.

If	**Do**
the system recovery controller automatically clears the alarm	step 6
the system recovery controller does not automatically clear the alarm	step 3

3 Manually busy the Gateway card. Type

>BSY

and press the Enter key.

> ***Note:*** If the maintenance flag is up, type **ABTK;BSY** to clear.

4 Bring the Gateway card into service. Type

>RTS

and press the Enter key.

5 Determine your next step.

If	**Do**
the Gateway card returns to service	step 6

If	Do
the Gateway card does not return to service	refer to the “Troubleshooting” chapter in this document

6 The procedure is complete.

Line maintenance

The user can use the line test position (LTP) MAP level to post commands on an Internet Protocol Local Loop (IPLL) directory number (DN) or virtual LEN. The IP terminal is an H.323-based terminal that is connected to the Centrex IP LAN.

Posting an IPLL line

The following sections describe how IPLL lines are posted at the LTP level.

LEN

Post the virtual LEN or range of LENs within a “drawer.” Because the Gateway is a circuit board, it has virtual, rather than physical, drawers. The post command can be used to post a group of lines from one LEN to another LEN.

Card

The IPLL virtual line has a BX27AA card code as part of its datafill in table LNINV. To post by BX27AA cards displays real ISDN BX27AA cards, as well as IPLL cards. The IPLL lines are distinguished by the “site” portion of their LEN, which is “GWIP” (or any four characters) rather than “HOST.”

DN

The IPLL DNs can be included in the Post by DN command with up to five DNs listed.

LTID

The IPLL logical terminal identifier (LTID) can be included in the Post by LTID command.

State

The IPLL DNs can be included in the Post by State command for appropriate states with command options to select only ISDN lines or a range of LENs.

Hunt group

The IPLL lines that are part of hunt groups can be posted by the hunt group.

MADN group

An IPLL line that is part of a multiple appearance directory number (MADN) group can be posted by the MADN group.

All

The Post All command can be used to post IPLL lines, with optional modifiers of ISDN or a range of LENs.

DN key

The Post by DN Key command can be used to post an IPLL DN key.

IPLL line states

The IPLL line states are virtual lines that represent the DMS view of the IP terminals. The IPLL line states appear the same to the DMS switch as Basic Rate Interface (BRI) and Plain Ordinary Telephone Service (POTS) lines. They are at the LTP level of the MAP terminal for a posted LEN or DN.

The Gatekeeper has its own states for each DN and is managed by the element manager on the LAN. A line can be in an IDL state in the DMS switch, but the Gatekeeper can see this as a BUSY state. The line state on the DMS side defines the ability of the IP terminal to make calls through the DMS switch.

> ***Note:*** The Line Module Busy (LMB) state means the Gateway card is down for a particular posted LEN or DN.

The table that follows lists the states and their descriptions.

Table 8-5 IPLL line states

State	Description
NEQ	not equipped
INB	installation busy
IDL	idle
CPB	call processing busy
CPD	call processing deload
MB	manual busy
LMB	line module busy - the Gateway card is not in service

Existing commands supported

Some MAP commands do not apply to IPLL lines. These commands are disabled. The disabled commands, when invoked, display only a message explaining the command is “inappropriate” with the posted IPLL line. The tables that follow show which commands are allowed and which are disabled.

LTP commands

The table that follows lists the LTP commands and their descriptions.

Table 8-6 LTP commands

Command	IPLL	Description
QUIT	Yes	Exit LTP level
POST	Yes	Move a new set to the control position
BSY	Yes	Change the state of the posted line
RTS	Yes	Return the posted line to service
DIAG	No	Perform diagnostics on the posted line
ALMSTAT	Yes	Query or set the lines (LNS) alarm thresholds
CKTLOC	Yes	Display circuit location information for posted line
HOLD	Yes	Move posted line to hold position
NEXT	Yes	Move a line to the control position
FULLDN	Yes	Display full national number
PREFIX	Yes	Set prefix digits for posting by DN
LCO	No	Operate or release the line cutoff relay
LEVEL	Yes	Access LTP sub-level
FRLS	Yes	Force release posted line
LTPRSRC	Yes	Display status of LTP level resources
HAZSUSP	No	Suspend line card monitor test

The LTP command CKTLOC delivers the following information about the Gateway card assigned to the IP terminal:

- XPM status (as is currently done for BRI and POTS)
- physical location of the Gateway card and its status (similar to what is currently done with the DCH card)

LTPISDN commands

The tables that follow list the LTPISDN commands and their descriptions.

Table 8-7 LTPISDN commands (Sheet 1 of 2)

Command	IPLL	Description
QUIT	Yes	Exit LTPISDN level
POST	Yes	Move a new set to the control position
TERMCHK	No	Query protocol status of posted line
SUSTATE	No	Display state of line card and subscriber equipment
BCHCON	No	Perform Bb channel continuity test
LTLOOPBK	No	Set, release, or query loopbacks
DCHCON	No	Perform D channel continuity test
TEST	No	Perform selected layer 1 test
HOLD	Yes	Move posted line to hold position
NEXT	Yes	Move a line to the control position
TSTSGNL	No	Activate a test signal from the line card
TEI	No	Check status of TEIs or restore removed TEI
QLOOP	Yes	Query all LTIDs, DNs, TEIs, RM states on posted line
QLAYER	No	Query performance or protocol monitoring data
RLAYER	No	Reset performance or protocol monitoring data
L2LOGCTL	No	Turn on or off layer 2 log control
L3LOGCTL	No	Turn on or off layer 3 log control
L1THRSH	No	Set or query layer 1 performance thresholds
L1BLMALM	No	Set or query automatic alarm reporting for the posted line

Table 8-7 LTPISDN commands (Sheet 2 of 2)

Command	IPLL	Description
QPHINFO	No	Display terminating DNs for X.25 packet calls
DCSIG	No	Perform DC signature test
COLDST	No	Perform a cold start test
SCUR	No	Perform sealing current test
DET	No	Perform BLM detection test
THR	No	Perform BLM threshold test
ALM	No	Perform an alarm test for loss of signal
IMP	No	Perform impulse noise measurements
NSE	No	Perform wideband noise measurements
ILOSS	No	Perform insertion loss measurements
CRLIM	No	Perform current limiter test

LTPDATA commands

The table that follows lists the LTPDATA commands and their descriptions.

Table 8-8 LTPDATA commands (Sheet 1 of 2)

Command	IPLL	Description
QUIT	Yes	Exit LTPDATA level
POST	Yes	Move a new set to the control position
EQUIP	No	Define DTA monitor equipment
CONNECT	No	Apply a DTA monitor to posted loop or channel
SUSTATE	No	Display the state of the line card and subscriber equipment
LOOPBK	No	Activate a specified loop back point on an ISDN loop
BERT	No	Start, stop, or query ISDN B-channel bit error rate test
BPVO	No	Control bipolar violation overflow reporting on data lines
HOLD	Yes	Move posted line to hold position

Table 8-8 LTPDATA commands (Sheet 2 of 2)

Command	IPLL	Description
NEXT	Yes	Move a line to the control position
BERTTIME	No	Set duration of ISDN bit error rate tests (BERT)

9 Card replacement

This chapter contains a card replacement procedure for the Centrex IP Gateway card (NT7X07AA).

NT7X07AA in an LTCI

Application

Use this procedure to replace an NT7X07AA in a line trunk controller with ISDN (LTCI).

Common procedures

This procedure does not refer to any common procedures.

Next level of maintenance

Repeat this procedure if it is not successful when you first perform the procedure.

A problem can occur that requires the help of the local maintenance personnel. Gather all important logs, reports, and system information (that is, product type and current software load) for analysis. The related logs, maintenance notes, and system information help make sure that the next level of maintenance and support can find the problem. More detail about logs appears in the *Log Report Reference Manual*.

Card settings

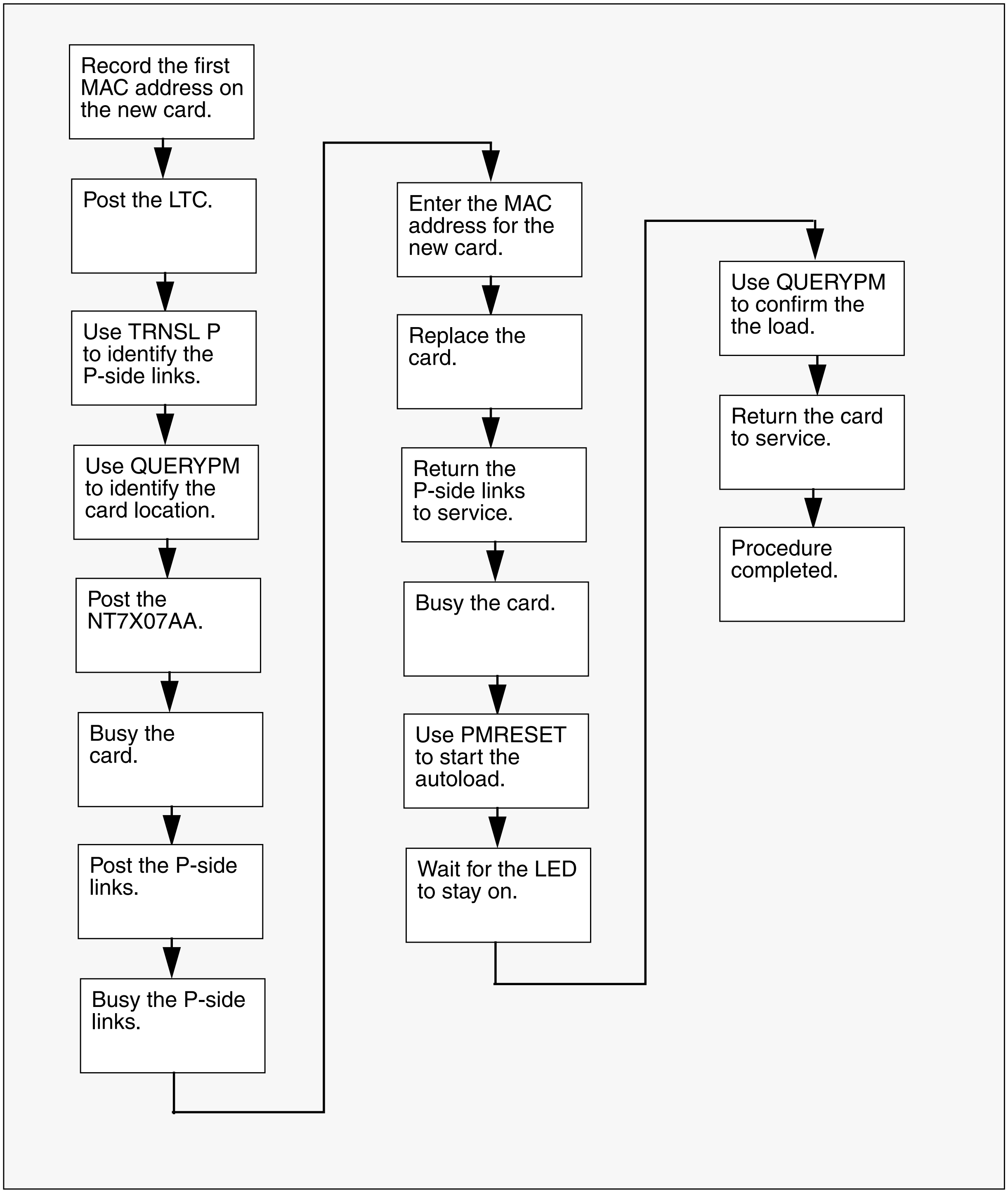
Not applicable

Action

The flowchart that follows provides a summary of this procedure. Use the instructions in the step action procedure that follows the flowchart to replace the card.

NT7X07AA in an LTCI (continued)

Summary of replacing an NT7X07AA in an LTCI



Record the first MAC address on the new card.

Post the LTC.

Use TRNSL P to identify the P-side links.

Use QUERYPM to identify the card location.

Post the NT7X07AA.

Busy the card.

Post the P-side links.

Busy the P-side links.

Enter the MAC address for the new card.

Replace the card.

Return the P-side links to service.

Busy the card.

Use PMRESET to start the autoload.

Wait for the LED to stay on.

Use QUERYPM to confirm the the load.

Return the card to service.

Procedure completed.

NT7X07AA in an LTCI (continued)

Replacing an NT7X07AA in an LTCI

At your current location

1 Get a new card. Make sure that the new card and the card you will replace have the same PEC and PEC suffix.

2 Find the two media access control (MAC) addresses on the faceplate of the new card. Record the first address.

At the MAP terminal

3 Go to the PM level of the MAP display and post the LTCI with the card you will replace. Type

```
>MAPCI;MTC;PM;POST LTC ltc_no
```

and press the Enter key.

where

ltc_no is the number of the LTCI.

Example of command

```
>MAPCI;MTC;PM;POST LTC 0
```

4 Display the P-side links for the LTCI. Type

```
>TRNSL P
```

and press the Enter key.

Example of a MAP response

```
LINK 10: IPGW GWIP 10 0     0:Cap MS;Status:O      , P;MsgCond:MTC
LINK 11: IPGW GWIP 10 0     1:Cap  S;Status:O      , P
LINK 12: IPGW GWIP 12 0     0:Cap MS;Status:O      , P;MsgCond:MTC
LINK 13: IPGW GWIP 12 0     1:Cap  S;Status:O      , P
```

5 Record the numbers of the P-side links for the NT7X07AA card that you will replace.

6 Query the PM to determine the location of the card. Type

>QUERYPM

and press the Enter key.

Example of a MAP response

```
PM Type: LTC  PM No.: 0  PM Int. No.: 1  Node_No.: 71
PMs Equipped: 25  Loadname: ELI11BD  EEPRom Load: UPFWQG04
 Warning! Unit 0 is missing patches
 Warning! Unit 1 is missing patches
WARM SWACT is supported but not possible: node redundancy lost.
 LTC 0 is included in the REX schedule.
REX on LTC 0 has not been performed.
Node Status: {OK, FALSE}
Unit 0   Act, Status: {OK, FALSE}
Unit 1 Inact, Status: {MAN_BUSY, FALSE}
Site Flr RPos  Bay_id   Shf  Description    Slot     EqPEC
   TEAM02      HOST  01 AA18  LTEI 001  18  LTC : 000       6X02NA
```

7 Go to the PM level and post the NT7X07AA. Type

>POST IPGW site_name frame_no unit_no

and press the Enter key.

where

site_name is the name of the site of the LTCI.

frame_no is the number of the LTCI.

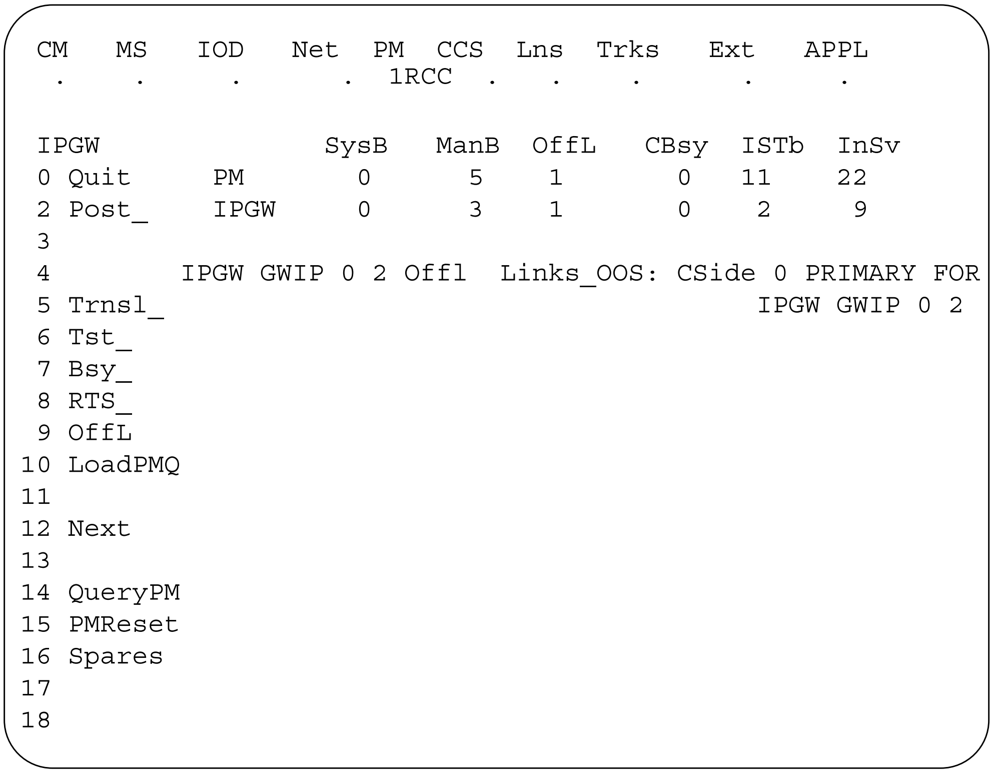
unit_no is the even port number assigned to the NT7X07 divided by 2.

Example of command

>POST IPGW GWIP 10 0

NT7X07AA in an LTCI (continued)

IPGW MAP display



```
 CM   MS   IOD   Net  PM  CCS  Lns  Trks   Ext   APPL
  .    .     .      .  1RCC  .    .    .      .     .

 IPGW              SysB   ManB  OffL   CBsy  ISTb  InSv
 0 Quit     PM       0      5    1       0    11    22
 2 Post_    IPGW     0      3    1       0     2     9
 3
 4        IPGW GWIP 0 2 Offl  Links_OOS: CSide 0 PRIMARY FOR
 5 Trnsl_                                     IPGW GWIP 0 2
 6 Tst_
 7 Bsy_
 8 RTS_
 9 OffL
10 LoadPMQ
11
12 Next
13
14 QueryPM
15 PMReset
16 Spares
17
18
```

Note: The command **LoadPMQ** is available in offices at NA012 or higher. If the office is at NA011, the command **Ld_PMQ** provides this functionality.

8 Busy the NT7X07AA. Type

>BSY

and press the Enter key.

9 Quit the IPGW level. Type

>QUIT

and press the Enter key.

10 Post the LTCI.

>POST LTC ltc_no

and press the Enter key.

where

ltc_no is the number of the LTCI.

Example of command

>POST LTC 0

11 Busy one P-side link for the card you will replace. Type

```
>BSY LINK link_no
```

and press the Enter key.

where

link_no is the number of the P-side link.

Example of command

```
>BSY LINK 4
```

12 Confirm the action. Type

```
>Y
```

and press the Enter key.

13 Repeat steps 11 and 12 for each P-side link of the card you will replace.

At NetID

14 Record the MAC address for the new card.

a Expand the IP Address object three levels.

b Expand the network object of the subnet with the NT7X07 card.

c In the tree area, click on the NT7X07 card that you want to update. NetID identifies the NT7X07 card as a host.

d Select **Options->Update Host**.

e Enter the MAC address that you recorded in step 2 in the Mac Address field.

f Click OK. Then click Yes when the warning messages display.

g After the host information updates, click OK again to exit.

At the LTC frame

15

> **DANGER**
> **Static electricity damage**
> Before you remove any cards, put on a wrist strap and connect it to the wrist strap grounding point on the left side of the frame supervisory panel of the XPM. This strap protects the equipment from damage caused by static electricity.

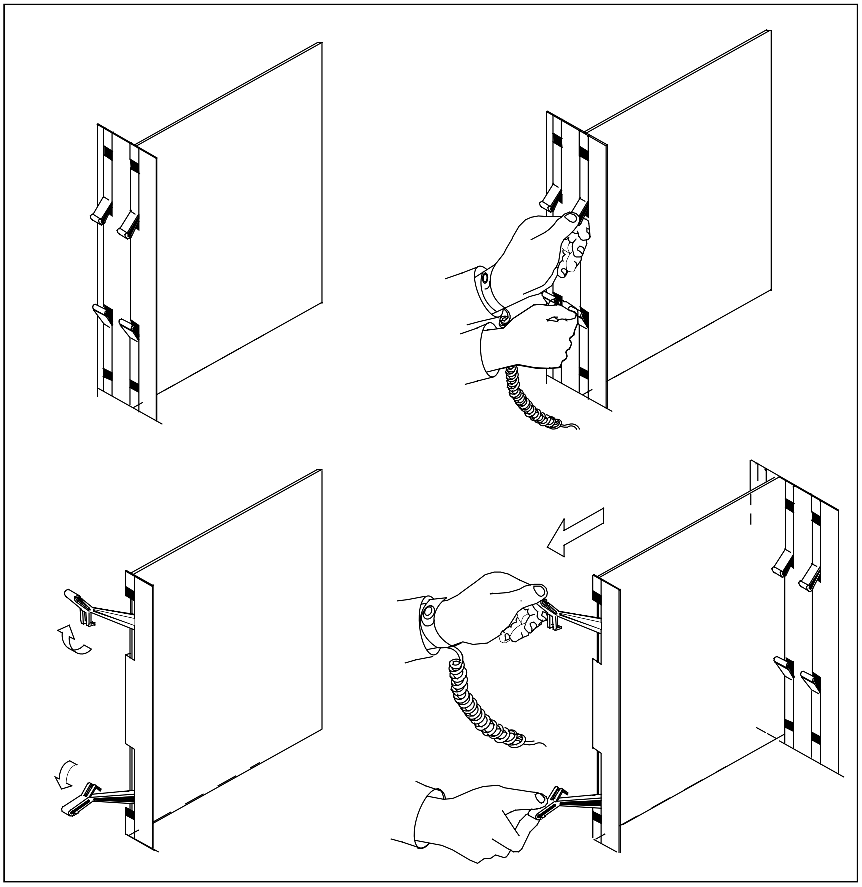
Put on a wrist strap.

NT7X07AA in an LTCI (continued)

16 Replace the NT7X07 card.

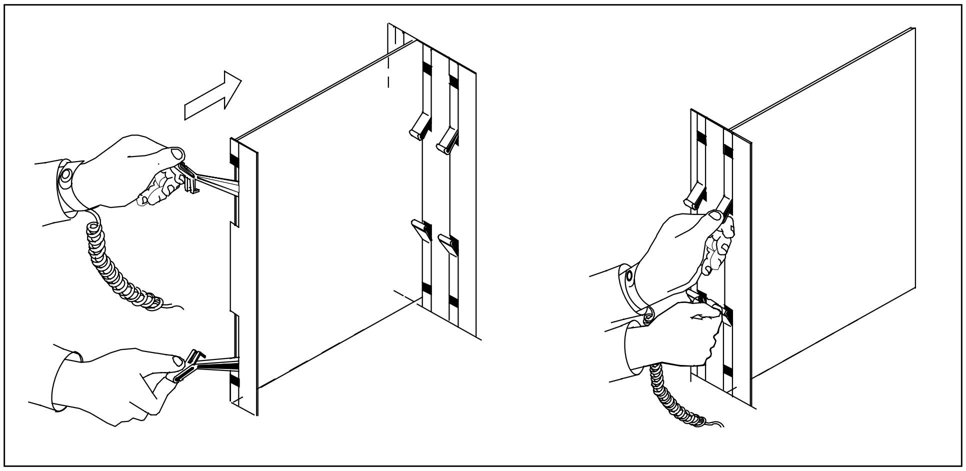
a Locate the NT7X07 card to be removed.

b Open the locking levers on the card and gently pull the card towards you until the card clears the shelf.



c Remove the card from the slot and shelf.

d Push the new card into the slot and close the locking levers.



At the MAP terminal

17

ATTENTION
If you have not changed the MAP display since step 11, the MAP display is at the PM level and the LTCI with the NT7X07 card is posted. If you have changed the MAP display, return to the PM level and post the LTCI with the NT7X07 card.

Return one P-side link to service. Type

```
>RTS LINK link_no
```

and press the Enter key.

where

link_no is the number of the P-side link.

Example of command

```
>RTS LINK 4
```

18 Repeat step 17 for each P-side link.

19 Go to the PM level and post the NT7X07AA. Type

```
>POST IPGW GWIP 10 0
```

and press the Enter key.

20 Load the card.

a Start the autoload of the NT7X07 card. Type

```
>PMRESET
```

NT7X07AA in an LTCI (end)

and press the Enter key.

b Watch the processor LED on the card. Wait for the LED to stay on.

c Confirm the new card has the correct load. Type

>QUERYPM

and press the Enter key.

Example of MAP response

```
QueryPM
PM Type: IPGW  PM Int. No.: 6  Node_No: 84
IPGW Card Location Information:
   Site Flr RPos  Bay_id   Shf  Description  Slot  EqPEC
   HOST  01 AA18  LTEI 001  32  LTC : 100     05   7X07

   LOAD STATUS:
   IPGW CONTAINS A VALID LOAD.
```

If the Map display confirms the card has a valid load, proceed to step 21.

d If you cannot PMRESET the Gateway card, Nortel Networks recommends stopping and restarting all NetID services.

i From the Gatekeeper, select **Start->Settings->Control Panel**.

ii Select NetID Services from the drop-down window.

iii At the top of the NetID Services menu, select All NetID services from the list.

iv Click the Stop Selected Services button for each listed NetID service.

v Then restart each NetID service from the same window to reset the cache.

vi Click OK. The NetID Services window closes.

vii Repeat step 20, a through c.

21 Return the NT7X07AA to service. Type

>RTS

and press the Enter key.

22 You have completed this procedure.

10 Logs

Overview

This chapter describes the logs for Centrex IP. Error messages can be solicited or unsolicited. The Gateway sends error messages to the XMS peripheral module (XPM). The type of error will be mapped into an appropriate message in the XPM and sent to the computing module (CM). The log utility system (LOGUTIL) will generate the appropriate log.

ATTENTION

The information about log PM189 contained in this chapter is specific to Centrex IP. For a complete description of log PM189, refer to *Log Report Reference Manual*.

The table that follows briefly describes each log that affects Centrex IP. A detailed description of each log follows this table.

Table 10-1 Centrex IP logs (Sheet 1 of 2)

Log number	Type	Log name	Description
IPGW300	TBL	IPGW Trap	Reports a trap to the XPM
IPGW500	INFO	IPGW State Change	Reports a change in the state of an IP Gateway
IPGW600	INFO	IPGW SWERR	Reports a software error (SWERR) to the XPM
IPGW601	INFO	IPGW HW Exception	Reports problems associated with a hardware fault
IPGW602	INFO	IPGW SW Exception	Reports problems associated with a software fault

Table 10-1 Centrex IP logs (Sheet 2 of 2)

Log number	Type	Log name	Description
IPGW603	INFO	IPGW	Reports the current state of the IP Gateway. If the state of the IP Gateway is CBsy or SysB, a major alarm generates.
IPGW604	INFO	IPGW Takeover	Reports the takeover of an IP Gateway due to sparing. Identifies the IP Gateway that was spared and the spare IP Gateway that has taken over the call processing of the spared IPGW.
PM189	INFO	PM SW Information Report	Reports hardware and software events in the peripheral module (PM)

Log IPGW300

Explanation

The Internet Protocol Gateway (IPGW) subsystem generates log IPGW300 to report a trap to the XPM. The XPM forwards this message to the CM for display. The trap is seen by the IP Gateway as an exception report. This report does not result in maintenance actions on the IP Gateway.

Format

The format for log report IPGW300 follows.

```
IPGW300 <mmmdd> < hh:mm:ss> <ssdd> TBL IPGW Trap
IPGW <site> <nn> <n> <host xpm> TASK <taskid>,TIME:<hh:mm:ss:ms>
IPGW TRAP/EXCEPTION TYPE: <except. type>,ADDRESS:<2bytes> <2bytes>
FUNCTION NAME and OFFSET: <function name> + <1 byte>
```

Example

An example of log report IPGW300 follows.

```
IPGW300 JUN16 17:01:10 4500 TBL IPGW Trap
   IPGW GWIP 10 1 on LTC 4,TASK:media_,TIME:05:04:10.02
   IPGW TRAP/EXCEPTION TYPE: External Interrupt,
   ADDRESS: 190B 0706 FUNCTION NAME and OFFSET:
   sendWAI_8XpmProxy +17
```

Field descriptions

The following table explains each of the fields in the log report.

Table 10-2 Log IPGW300 field values and descriptions (Sheet 1 of 2)

Field	Value	Description
IPGW	IPGW name	Identifies the IP Gateway reporting the trap
Host XPM	Host XPM name	Identifies the host XPM where the IP Gateway resides
TASK	Task name	Identifies the IP Gateway task that was running when the trap occurred
TIME	Time of day	Indicates the time of day in hours, minutes, seconds, and hundreths of seconds when the trap occurred

Table 10-2 Log IPGW300 field values and descriptions (Sheet 2 of 2)

Field	Value	Description
IPGW TRAP/EXCEPTION TYPE	Names of exceptions as identified by the IP Gateway include: System Reset, Machine Check, Data Memory Access, Instruction Fetch, External Interrupt, Memory Access, Program, Floating Point Unavailable, Decrementor, System Call, Trace, Floating Point Assist	Lists the name of the exception type as identified by the IP Gateway. This is the type of trap.
ADDRESS	Four hex bytes	Identifies the address in the memory of the IP Gateway where the exception occurred
FUNCTION NAME and OFFSET	Name of the function. A hex byte representing the offset.	Lists the name of the function that was running when the exception occurred. The offset is a measurement into the function indicating how much code had executed before the exception/trap occurred.

Action

This log report is for information only. No action is required.

Related OM registers

None

Additional information

None

Log IPGW500

Explanation

The IPGW subsystem generates log IPGW500 to report a change in the state of an IP Gateway. Log report IPGW500 information includes the “from” and “to” states of the IP Gateway. For example, the following IPGW500 log report example shows the state of IP Gateway 10 1 on LTC 4 changes from the OffL state to the ManB state. If the “to” state of the IP Gateway is SysB or CBsy, a major alarm generates.

Format

The format for log report IPGW500 follows.

```
alm IPGW500 <mmmdd> <hh:mm:ss> < ssdd> INFO IPGW State Change
      IPGW <site> <nn> <n> on <host XPM> <to_state> from <from state>
```

Example

Examples of log report IPGW500 follow.

Example 1

Example of log report IPGW500 with no alarm generated follows.

```
IPGW500 JUN15 17:15:28 3000 INFO IPGW State Change
   IPGW GWIP 10 1 on LTC 4: ManB from OffL.
```

Example 2

Example of log report IPGW500 with major alarm generated follows.

```
**IPGW500 JUN15 17:15:28 3000 INFO IPGW State Change
   IPGW GWIP 10 0 on LTC 14: SysB from InSv.
```

Field descriptions

The following table explains each of the fields in the log report.

Table 10-3 Log IPGW500 field values and descriptions (Sheet 1 of 2)

Field	Value	Description
alm	(blank)	Indicates no alarm
	**	Indicates a major alarm
IPGW	IPGW name	Identifies the IP Gateway that changed state
Host XPM	Host XPM name	Identifies the host XPM where the IP Gateway resides

Table 10-3 Log IPGW500 field values and descriptions (Sheet 2 of 2)

Field	Value	Description
To state	OffL, ManB, CBsy, InSv, ISTb, SysB	Indicates the state of the IP Gateway after the log report
From state	OffL, ManB, CBsy, InSv, ISTb, SysB	Indicates the state of the IP Gateway before the log report

Action

This log report is for information only. No action is required.

Related OM registers

None

Additional information

None

Log IPGW600

Explanation

The IPGW subsystem generates log IPGW600 to report a software error (SWERR) to the XPM. The XPM forwards the SWERR report to the CM. The CM generates log IPGW600 to describe the SWERR as reported by the IP Gateway.

Format

The format for log report IPGW600 follows.

```
IPGW600 <mmmdd> <hh:mm:ss> <ssdd> INFO IPGW SWERR
     IPGW <site> <nn> <n> on <host XPM> TASK: <task_name>
     IPGW SWERR TYPE: <swerr_type>, TIME: <nn: nn:nn.nn>
     TEXT: <text_supplied_by_Gateway>
```

Example

An example of log report IPGW600 follows.

```
IPGW600 JUN16: 06:00:45 4400 INFO IPGW SWERR
   IPGW GWIP 10 1 on LTC 4, TASK: tSwExcTask
   IPGW SWERR TYPE: Swerr, TIME: 04:03:10.05
   TEXT: Value out of range for type.
```

Field descriptions

The following table explains each of the fields in the log report.

Table 10-4 Log IPGW600 field values and descriptions (Sheet 1 of 2)

Field	Value	Description
IPGW	IPGW name	Identifies the IP Gateway reporting the SWERR
Host XPM	Host XPM name	Identifies the host XPM where the IP Gateway reporting the SWERR resides
TASK	Task name	Identifies the task that was running in the IP Gateway when the SWERR occurred
IPGW SWERR TYPE	SWERR or INFO	Indicates the type of SWERR as classified by the IP Gateway. The IP Gateway classifies a software error SWERR as more severe than an information (INFO) SWERR.

Table 10-4 Log IPGW600 field values and descriptions (Sheet 2 of 2)

Field	Value	Description
TIME	Time of day	Indicates the time of day in hours, minutes, seconds, and hundreths of seconds when the SWERR occurred
TEXT	30 characters	The IP Gateway supplies up to 30 characters of text related to the SWERR to provide additional information.

Action

This log report is for information purposes only. No action is required.

Related OM registers

None

Additional information

None

Log IPGW601

Explanation

The IPGW subsystem generates log IPGW601 to report a problem associated with a hardware fault.

Format

The format for log report IPGW601 follows.

```
IPGW601 <mmmdd> < hh:mm:ss> <ssdd> INFO IPGW HW Exception
     IPGW <site> <nn> <n> on <host XPM>, REASON:  <text_reason>
```

Example

An example of log report IPGW601 follows.

```
IPGW601 JUN16 05:55:53 3800 INFO IPGW HW Exception
   IPGW GWIP 10 1 on LTC 4, Reason: 7X07 Self Test failed
```

Field descriptions

The following table explains each of the fields in the log report:

Table 10-5 Log IPGW601 field values and descriptions

Field	Value	Description
IPGW	IPGW name	Identifies the IP Gateway reporting the hardware problem
Host XPM	Host XPM name	Identifies the host XPM where the IP Gateway reporting the hardware problem resides
REASON	IPGW P-side Alarm, IPGW Card Audit Failure, P-side Overload MAJOR ALARM, P-side Overload MINOR ALARM, XPM Interface Alarm, Exception Report, 7X07 Self Test Failed, 7X07 Diagnostics failed, IPGW Link Audit failed	Describes the hardware related fault being reported by the IP Gateway

Action

This log report is for information only. No action is required.

Related OM registers

None

Additional information

None

Log IPGW602

Explanation

The IPGW subsystem generates log IPGW602 to report a problem associated with a software fault.

Format

The format for log report IPGW602 follows.

```
IPGW602 < mmmdd> < hh:mm:ss> <ssdd> IPGW SW EXCEPTION
    IPGW <site> <nn> <n> on <host XPM>, REASON: <text_reason>
```

Example

An example of log report IPGW602 follows.

```
IPGW602 JUN16 05:35:63 3800 INFO IPGW SW EXCEPTION
  IPGW GWIP 10 1 ON LTC 4,REASON:P-side Overload MINOR ALARM
```

Field descriptions

The following table explains each of the fields in the log report:

Table 10-6 Log IPGW602 field values and descriptions

Field	Value	Description
IPGW	IPGW name	Identifies the IP Gateway reporting the software related fault
Host XPM	Host XPM name	Identifies the host XPM where the IP Gateway reporting the software related fault resides
REASON	IPGW P-side Alarm, IPGW Card Audit Failure, P-side Overload MAJOR ALARM, P-side Overload MINOR ALARM, XPM Interface Alarm, Exception Report, 7x07 Self Test failed, 7x07 Diagnostics failed, IPGW Link Audit failed	Describes the software related fault being reported by the IP Gateway

Action

This log report is for information only. No action is required.

Related OM registers

None

Additional information

None

Log IPGW603

Explanation

The IPGW subsystem generates log IPGW603 to report information not included in the other IPGW log reports. The log report includes both the current state of the IP Gateway and a line of descriptive text, for example, no response from XPM. If the state of the IP Gateway is CBsy or SysB, a major alarm generates.

Format

The format for log report IPGW603 follows.

```
alm IPGW603 <mmmdd> <hh:mm:ss> <ssdd> INFO IPGW
      IPGW <site> <nn> <n> on <host XPM>, IPGW State: <state>
     <text_description>
```

Example

Examples of log report IPGW603 follow.

Example 1

An example of log report IPGW603 with no alarm generated follows.

```
IPGW603 JUN16 09:49:05 5500 INFO IPGW
   IPGW GWIP 10 0 on LTC 0,IPGW State: ISTb
   SST320 No response from XPM
```

Example 2

An example of log report IPGW603 with major alarm generated follows.

```
**IPGW603 JUN16 09:49:05 5500 INFO IPGW
   IPGW GWIP 10 0 on LTC 0,IPGW State: SysB
   Diag Failed: Check for possible logs
```

Field descriptions

The following table explains each of the fields in the log report.

Table 10-7 Log IPGW603 field values and descriptions (Sheet 1 of 2)

Field	Value	Description
alm	(blank)	Indicates no alarm
	**	Indicates major alarm
IPGW	IPGW name	Identifies the IP Gateway being reported
Host XPM	Host XPM name	Identifies the host XPM where the IP Gateway resides

Table 10-7 Log IPGW603 field values and descriptions (Sheet 2 of 2)

Field	Value	Description
IPGW State	OffL, ManB, CBsy, SysB, InSv, IStb	Indicates the state of the IR Gateway when this log report generates
Text description	line of text	Information about the IP Gateway being reported

Action

This log report is for information only. No action is required.

Related OM registers

None

Additional information

None

Log IPGW604

Explanation

The IPGW subsystem generates log IPGW604 to report the takeover of an IP Gateway due to sparing. Log report IPGW604 identifies the IP Gateway that was spared as well as the spare IP Gateway that has taken over the call processing of the spared IPGW.

If there are no spares available or datafilled when an out-of-service IP Gateway returns to service (RTS), a log report IGW604 generates that lists the IP Gateway as primary for itself. See log report format 2 for an example.

Format

Log report IPGW604 has two possible formats.

Format 1

Format 1 for log report IPGW604 follows.

```
IPGW604 <mmmdd> < hh:mm:ss> <ssdd> INFO IPGW Takeover
    IPGW <site> <nn> <n> Spared by IPGW <site> <nn> <n>
```

Format 2

Format 2 for log report IPGW604 follows.

```
IPGW604 <mmmdd> < hh:mm:ss> <ssdd> INFO IPGW Takeover
    IPGW <site> <nn> <n> Primary for IPGW <site> <nn> <n>
```

Example

Examples of log report IPGW604 follow.

Example for format 1

Example of log report IPGW604 for format 1 follows.

```
IPGW604 JUN16 05:55:53 3500 INFO IPGW Takeover
    IPGW GWIP 10 1 SPARED BY IPGW GWIP 4 4
```

Example for format 2

Example of log report IPGW604 for format 2 follows.

```
IPGW604 JUN16 02:23:39 3900 INFO IPGW Takeover
    IPGW GWIP 1 1 Primary for IPGW GWIP 2 3
```

Field descriptions

The following table explains each of the fields in the log report.

Table 10-8 Log IPGW604 field values and descriptions

Field	Value	Description
IPGW	IPGW name	Identifies the IP Gateway that either has gone out of service and was spared by another IP Gateway or became a primary IP Gateway for another IP Gateway that has gone out of service. See the additional information that follows.

Action

This log report is for information only. No action is required.

Related OM registers

None

Additional information

Format 1 identifies an IP Gateway that goes out of service and has its call processing taken over by a spare IP Gateway. The first IP Gateway listed is the IP Gateway that has gone out of service. The second IP Gateway listed is the IP Gateway that becomes a primary IP Gateway taking over the call processing for the out of service IP Gateway.

Format 2 identifies an IP Gateway that becomes the primary IP Gateway for another IP Gateway that has gone out of service. The system software assigns an IP Gateway that is not processing calls as a spare. When a spare IP Gateway begins call processing for an out of service IP Gateway, it becomes a primary IP Gateway.

Log PM189

Explanation

The PM subsystem generates log PM189 to report hardware and software events. The XPM node maintenance subsystem adds 17 new log events to the PM189 log for Gateway maintenance. The text field of the log report identifies a specific log event.

> ***Note:*** The information about log PM189 contained in this chapter is specific to Centrex IP. For a complete description of log PM189, refer to *Log Reports Reference Manual*.

Format

The log report format follows.

PM189 mmmdd hh:mm:ss ssdd INFO PM SW Information Report

pmid n Unit n : acttxt

TASKID:taskid, TIME: hh:mm:ss.cc, COMID: comid

TEXT : swerrtxt logdata

Example

A PM189 log report example follows.

```
PM189 MAR01 12:31:03 8100 INFO PM SW Information Report

 LTC 2 Unit 0: Act

 TASKID: 00690069 MTCSLAV, TIME: 12:31:03.16

 TEXT : ipgw_range_err 00 03
```

Log events

The IPGW log events for log PM189 are described in the sections that follow. The pointer is the additional numeric data that follows the SWERR text in the text field. Not all log events have pointer data.

upd_inact_err

Description: failure of the get_mate_msg function

Result: no update of the inactive unit for this specific IPGW operation

Pointer: no data

ipgw_range_err

Description: “gw_index” value is out of the valid range of 0 through 9

Result: the current maintenance operation associated with this invalid index will not be performed

Pointer: gw_index value

ipgw_ack_err
Description: failure to build a CC ACKnowledgement message

Result: no ACK sent to CC

Pointer: IPC index of CC request being processed

inv_7x07_rts
Description: attempt to RTS an IPGW node that is already in an “ls_running” node state

Result: RTS request is ignored and an invalid request response is sent to the CC

Pointer: IPC index of CC request being processed

gw_stat_err
Description: failure of the get_gw_stat function

Result: STATUS will not be sent to the IPGW node

Pointer: internal node number of the IPGW node

ipgw_inv_req
Description: CC request could not be interpreted

Result: CC request is discarded and an invalid request response is sent to the CC

Pointer: no data

ipgw_inv_req_buf
Description: failure to obtain an IPC buffer for an invalid request response

Result: CC is not notified of the invalid request condition

Pointer: no data

get_gw_msg_error
Description: failure of get_gw_msg function

Result: current CC originated request is not forwarded to the Gateway card

Pointer: no data

ipgwaudt_ipc_err

Description: failure to obtain an IPC buffer to notify CC of a diagnostic audit failure

Result: CC is not notified of diagnostic audit failure

Pointer: no data

IPGW: No Proc

Description: failure to bind the IPGW drop procedure, “ipgw_tbl_copy”

Result: drop procedure “ipgw_tbl_copy” is not executed when SwAct bit is set and a bulk “ipgw_tbl” update is not performed prior to SwAct

Pointer: no data

bd_pt

Description: port number derived from port table and node table is out of range

Result: no port value is returned to caller

Pointer: port table record

IPGW: inv ack

Description: response is received from the Gateway card prior to receipt of ACKnowledgement

Result: response is discarded

Pointer: IPC index of response message

IPGW:no-ipc-buf

Description: failure to obtain IPC buffer to send test request to the Gateway card

Result: test request is not sent to the Gateway card

Pointer: no data

IPGW: inv typ

Description: invalid IPGW subtest in message reply

Result: reply is discarded

Pointer: subtest name

Elem_Not_In_Diag

Description: diagnostic is invoked with an invalid element

Result: diagnostic will not run

Pointer: no data

GW_AUD:NoMtcResp

Description: no indication from IPGWMTCE of receipt of audit request

Result: audit subsystem continues normal operation

Pointer: no data

GW_AUD:NoIpcBuf

Description: audit subsystem could not acquire an IPC buffer

Result: audit subsystem continues normal operation

Pointer: no data

Field descriptions

The table that follows describes the fields in the log report.

Table 10-9 Log PM189 field values and descriptions (Sheet 1 of 2)

Field	Value	Description
INFO PM SW Information Report	Constant	Indicates a report of PM software information
pmid	Symbolic text	Identifies the affected PM
Unit	0 or 1	Identifies the PM unit that generates report
acttxt	Act	Identifies activity state of PM unit as active (Act)
	Inact	Identifies activity state of PM unit as inactive (Inact)
IPE	node	Identifies the IPE node that generates the report
	shelf	Identifies the shelf in the IPE node that generates the report
TASKID	Symbolic text	Provides identification for task

Table 10-9 Log PM189 field values and descriptions (Sheet 2 of 2)

Field	Value	Description
TIME	00:00:00.00 through 23:59:59.59	Indicates the time the PM issued the log
COMID	00-FF, character string	Provides communication port identification. Not provided for digital line module (DLM).
TEXT	Character string and hexadecimal numbers	Represents the swerrtxt log data. There is a total of 16 bytes, composed of character string and hex bytes.

Action

This log report is for information only. No action is required.

Related OM registers

None

Additional information

None

11 Terminal proxy server

Overview

The terminal proxy server (TPS) is a software application that allows Ethernet-based terminals to communicate with the public switching telephone network (PSTN). The TPS acts as a proxy agent for the i2004 Internet Telephone by converting the Unified Network IP Stimulus (UNISTIM) protocol to the H.225 protocol for call control services from the Gatekeeper.

The TPS is a mandatory component in the network whenever the i2004 telephone is present. When the i2004 user presses a hard key or selects a softkey from the display, the TPS translates the stimulus messages and transmits them to the Gatekeeper and the Gateway for call processing. The TPS processes some of the stimulus messages locally to provide a set of specific i2004 services, such as the softkey options. In Release 2, the TPS resides on the Gatekeeper.

The TPS database stores the configuration data of the i2004 phones, such as the DNs assigned to the phones, the key assignments for voice features, and the IP address of the Gatekeeper. The TPS performs the following functions for the i2004 phone:

- makes call setup requests to the Gatekeeper
- processes and transmits Gatekeeper messages to the i2004 phone
- performs admission signaling for the i2004 phone
- performs call control signaling for the i2004 phone
- maintains the call state and the user interface

Installation

To install the TPS, refer to the *Centrex IP Upgrade Guide*, 297-5231-590. After installing the TPS, start the TPS Config Tool to provide information necessary to run the TPS.

To start the TPS Config Tool, select the following item from the PC Start menu:

Programs ->Nortel Networks ->Terminal Proxy Server ->Configuration Tool

TPS Config Tool

The TPS Config Tool allows the user to customize settings of the TPS. The TPS Config Tool window contains the following tabs:

- System Settings - This tab allows the user to update attributes related to the TPS system, such as IP address and port settings for the TPS, Gatekeeper, and PTM.
- DN Keys- This tab allows the user to enter valid DN keys when using Centrex IP parameter downloading.
- Codec Settings- This tab defines the codec list for i2004 calls.

  Note: Refer to Appendix B, "Changing the vocoder," in this document for information about the Codec Settings tab.

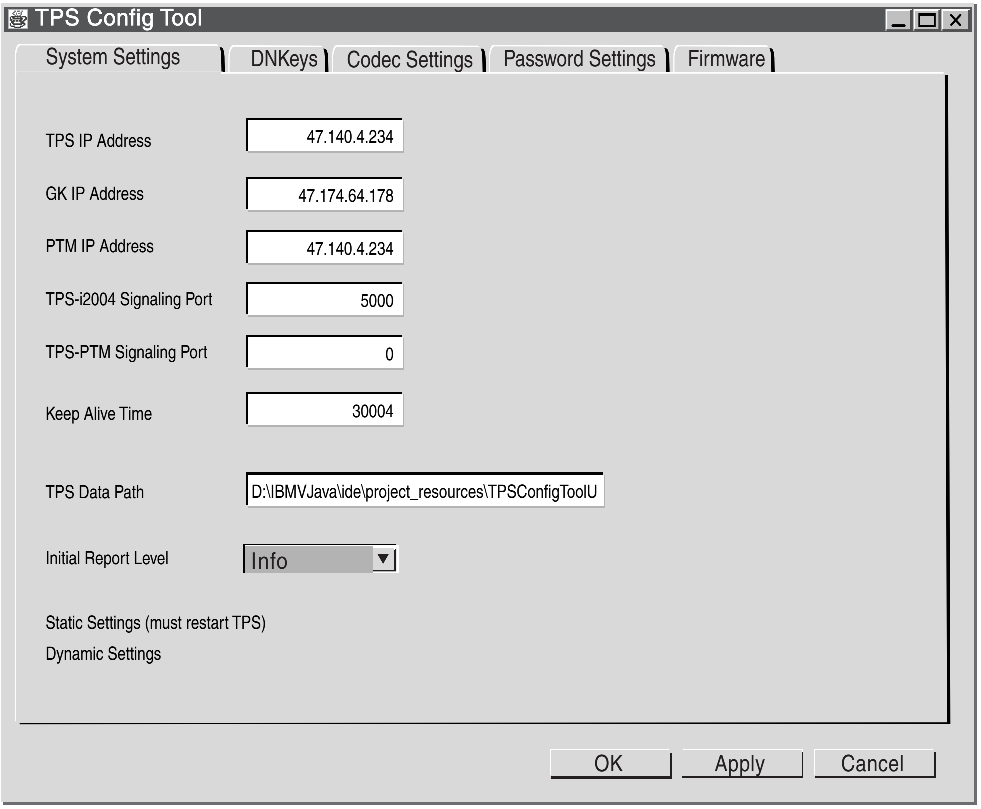
- Password Settings - This tab allows the user to change the ID and password for the TPS Debug Tool.
- Firmware - This tab defines information about i2004 firmware.

The System Settings, DN Keys, Password Settings, and Firmware tabs are described in the sections that follow.

System Settings tab

The figure that follows shows the TPS Config Tool System Settings tab.

Figure 11-1 TPS Config Tool System Settings tab



TPS IP Address 47.140.4.234

GK IP Address 47.174.64.178

PTM IP Address 47.140.4.234

TPS-i2004 Signaling Port 5000

TPS-PTM Signaling Port 0

Keep Alive Time 30004

TPS Data Path D:\IBMVJava\ide\project_resources\TPSConfigToolU

Initial Report Level Info

Static Settings (must restart TPS)

Dynamic Settings

The fields in the System Settings tab are described in the following table.

Table 11-1 System Settings tab field descriptions (Sheet 1 of 2)

Field	Description
TPS-IP Address	Virtual IP address of the TPS. Because the TPS and Gatekeeper reside on the same PC, the IP addresses for the TPS and Gatekeeper are the same.
GK IP Address	Virtual IP address of the Gatekeeper
PTM IP Address	IP address of the PTM
TPS-i2004 Signaling Port	Port from which the TPS listens for the UNISTIM messages sent by the i2004 phones. The recommended setting is 5000.

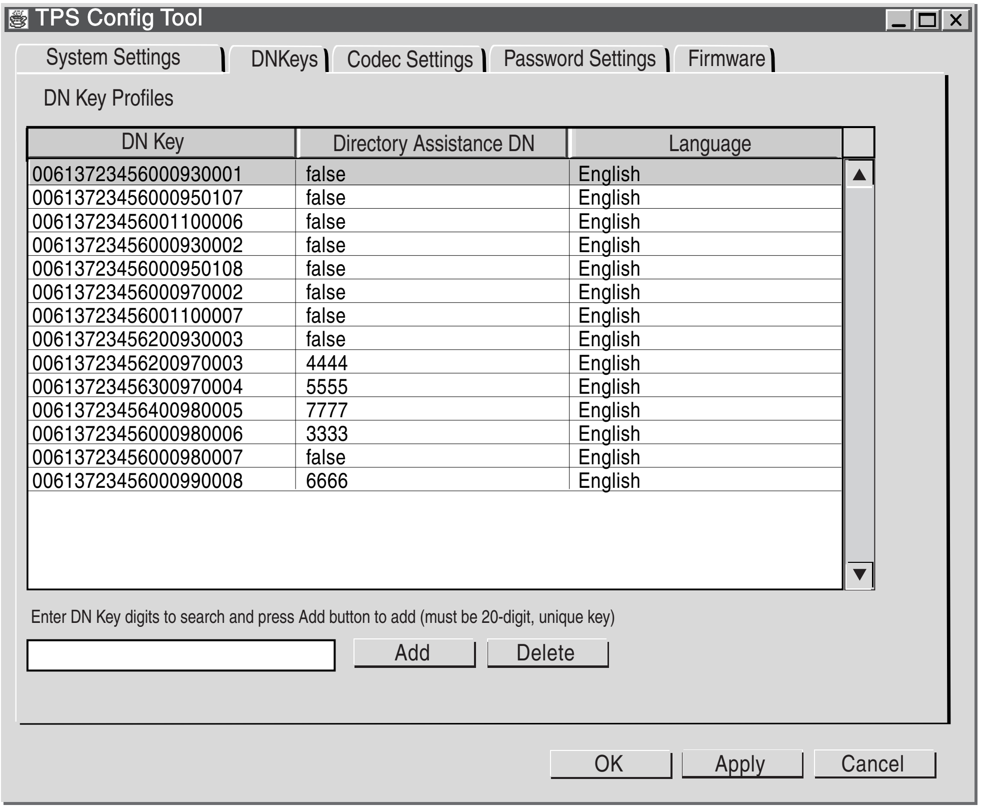
Table 11-1 System Settings tab field descriptions (Sheet 2 of 2)

Field	Description
TPS-PTM Signaling Port	Port from which the TPS listens for messages from the PTM
Keep Alive Time	The time in seconds before the TPS verifies an i2004 phone is still connected to the network. The default value is 30,000 seconds (approximately eight hours). ***Note:*** To enable interworking with Enterprise LANs that use Network Address Translators (NATs), the value of the Keep Alive Time should be less than any NAT mapping expiration time.
TPS Data Path	Specifies the drive and directory where the TPS persistent data files are stored.
Initial Report Level	Determines the amount of information provided in the TPS log files. The initial report level can be set to one of the following levels: • Fatal • Serious • Warning • Info • Debug1 • Debug 2 • Debug 3 • Debug 4 The recommended level is Info. ***Note:*** Setting the Initial Report Level to a debug level significantly degrades the performance of the TPS. Use these levels only to capture detailed information about a particular problem. Use these levels during off-hours when no users are using their i2004 phones. If multiple users attempt calls while the Initial Report Level is set to a debug level, the TPS drops calls.

DN Keys tab

The figure that follows shows the TPS Config Tool DN Keys tab.

Figure 11-2 TPS Config Tool DN Keys tab



DN Key Profiles

DN Key	Directory Assistance DN	Language
00613723456000930001	false	English
00613723456000950107	false	English
00613723456001100006	false	English
00613723456000930002	false	English
00613723456000950108	false	English
00613723456000970002	false	English
00613723456001100007	false	English
00613723456200930003	false	English
00613723456200970003	4444	English
00613723456300970004	5555	English
00613723456400980005	7777	English
00613723456000980006	3333	English
00613723456000980007	false	English
00613723456000990008	6666	English

Enter DN Key digits to search and press Add button to add (must be 20-digit, unique key)

The fields in the DN Keys tab are described in the following table.

Table 11-2 DN Keys tab field descriptions

Field	Description
DN Key	20-digit number that uniquely identifies the profile of the user
Directory Assistance DN	The number dialed when the user presses the directory key.
Language	The language preference of the user. Determines whether the text displays in English or French.

Datafilling a new Centrex IP terminal

For information on datafilling a new Centrex IP terminal, refer to the “Parameter downloading” section of the “DMS Maintenance” chapter in this document.

Bringing an i2004 into service

For information on bringing an i2004 into service, refer to the *Centrex IP i2004 Operations and Maintenance Manual,* 297-5231-032.

Changing the language preference

Use the following procedure to change the language preference

Procedure 11-1 Changing the language preference

At the Gatekeeper

1. Start the TPS Config Tool.
2. Select the DN Key Settings tab.
3. On the row that contains the DN key of the user who requested the language change, left-click the Language column for the selected DN key.
4. Left-click the displayed language to select another language for the i2004 display information.

   An asterisk (*) appears next to the DN key entry to show a changed value for that number.

5. Repeat steps 3 and 4 for each DN key entry to be changed.
6. Click the Apply button at the bottom of the DN Key Settings window to apply all changes at once.
7. Or click the OK button at the bottom of the DN Key Settings window to apply all changes and exit the TPS Config Tool.

Changing the directory service number

Use the following procedure to change the directory service number.

Procedure 11-2 Changing the directory service number

At the Gatekeeper

1. Start the TPS Config Tool.
2. Select the DN Key Settings tab.
3. Update the directory service number for the selected DN key.

   a On the row that contains the DN key of the user who requested the directory service number change, left-click the Directory Number column for the selected DN key.

   b Press the backspace key several times to erase the current directory service number.

   c Type the new directory service number for the specified terminal, and press the Enter key.

4. Repeat step 3 for each directory service number to be changed.
5. Click the Apply button at the bottom of the DN Key Settings window to apply all changes at once.
6. Or click the OK button at the bottom of the DN Key Settings window to apply all changes and exit the TPS Config Tool.

Deleting a DN key

Use the following procedure to delete a DN key.

Procedure 11-3 Deleting a DN key

At the Gatekeeper

1 Start the TPS Config Tool.

2 Select the DN Key Settings tab.

3 Left-click the row that contains the DN key of the user.

4 Click the Delete button near the bottom of the window.

A warning box appears, which states, “Are you sure you want to delete <dnkey>?”

5 Click Yes.

If an i2004 phone is currently using that DN key, the TPS deregisters that terminal. The TPS also deletes the DN key from the TPS database and removes the <dnkey>.obj file in the dnkeydb directory.

6 Exit the Config Tool.

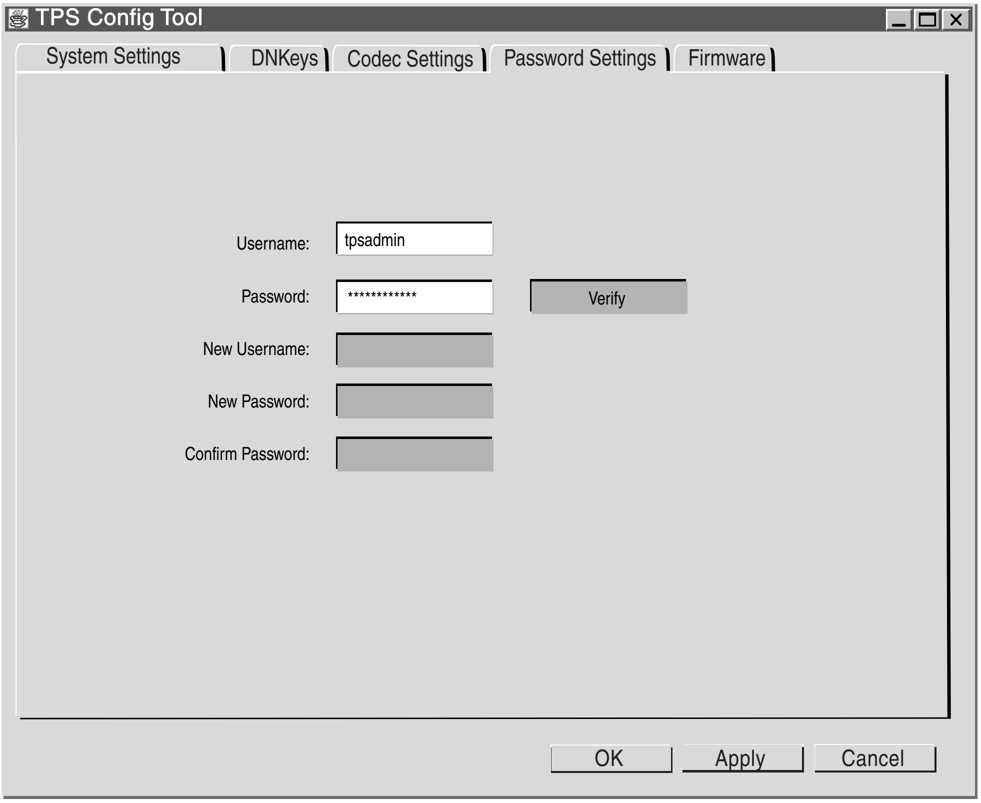
Upgrading the TPS

For information on upgrading the TPS, refer to the *Centrex IP Upgrade Guide*, 297-5231-590.

Password Settings tab

The figure that follows shows the TPS Config Tool Password Settings tab.

Figure 11-3 TPS Config Tool Password Settings tab



Username: tpsadmin

Password: ************

New Username:

New Password:

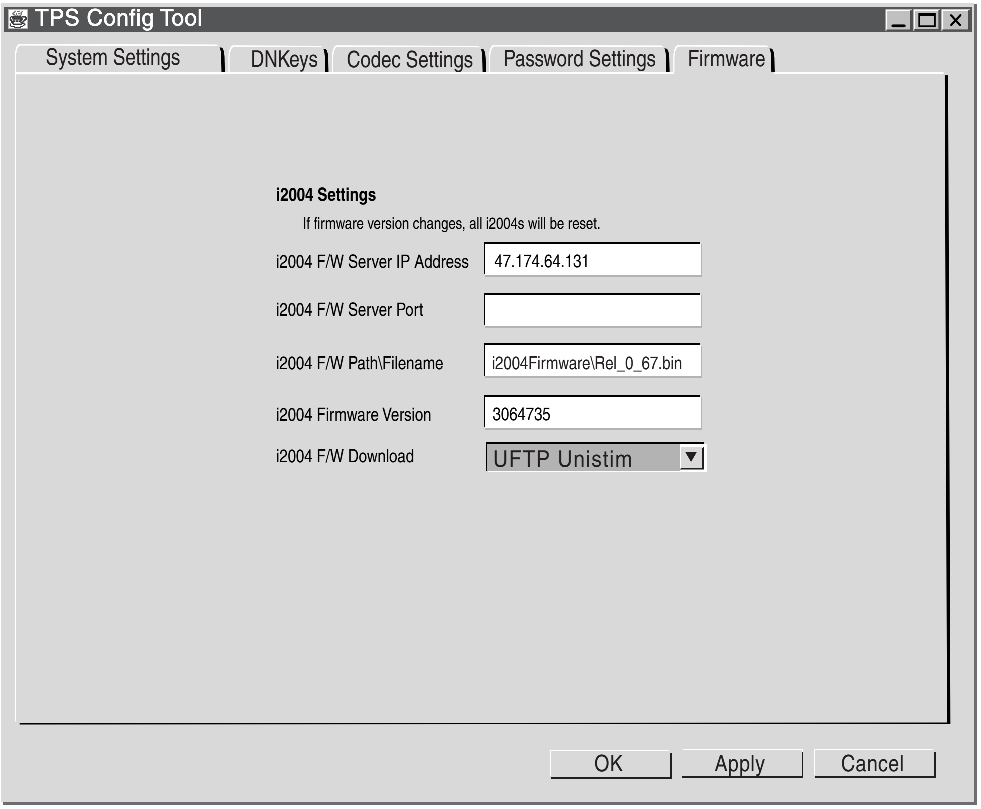
Confirm Password:

The Password Settings window prompts you for the existing TPS Debug Tool user ID and password. After the TPS verifies the user ID and password you entered, you can enter a new user ID and password. The TPS Debug Tool tracks only one user ID and password. When you enter a new user ID and password, the old user ID and password are deleted.

Firmware tab

The figure that follows shows the TPS Config Tool Firmware tab.

Figure 11-4 TPS Config Tool Firmware tab



i2004 Settings

If firmware version changes, all i2004s will be reset.

i2004 F/W Server IP Address: 47.174.64.131

i2004 F/W Server Port:

i2004 F/W Path\Filename: i2004Firmware\Rel_0_67.bin

i2004 Firmware Version: 3064735

i2004 F/W Download: UFTP Unistim ▼

The fields in the Firmware tab are described in the following table.

Table 11-3 Firmware tab field descriptions (Sheet 1 of 2)

Field	Description
i2004 F/W Server IP Address	IP address of the server containing the i2004 firmware. The i2004 phones can contact this IP address to download the latest firmware.
i2004 F/W Server Port	Port on the server containing the i2004 firmware that is listening for firmware download requests from i2004s.
i2004 F/W Path\Filename	Location of the firmware load on the server.

Table 11-3 Firmware tab field descriptions (Sheet 2 of 2)

Field	Description
i2004 Firmware Version	Version of firmware of all i2004 phones on this TPS. When an i2004 phone is powered on, the set first checks if its firmware version matches the one datafilled here. If not, the set contacts the server to download the correct firmware load.
i2004 F/W Download	Protocol used to perform the firmware download. The user can choose either TFTP or UFTP.

TPS failover limitations

When the Gatekeeper has a failover, the TPS restarts on the standby node. The TPS has the following limitations during a failover:

- If the user presses any key during the time it takes for the TPS to come back online (30 to 90 s), the set displays “server unreachable.” A key press initiates communication with the TPS, but during the takeover interval, the TPS is unavailable.
- After the TPS fails over to its standby node, if the user presses any key to invoke a feature (such as “Confer”), the key press will result in the phone producing a beep (indicating the keypress was denied). The call will stay up but the feature will not work for that call.
- A TPS reset means that the TPS application was terminated and then restarted (such as during a failover). If a TPS reset occurs during an active call, the user cannot receive any new calls until the user releases the call.

12 Troubleshooting

Overview

This chapter provides troubleshooting information about Centrex IP components Gateway, Gatekeeper, Terminal Proxy Server (TPS), and i2004 Internet Telephone.

> *Note:* Contact Nortel Networks for support for any action item that remains unresolved.

Gateway troubleshooting

The following sections provide troubleshooting information about the Gateway component.

A Gateway fails to load

The following table lists possible causes if a Gateway fails to load.

Table 12-1 A Gateway fails to load

Cause	Solution
Gateway datafill in the control module (CM)	Verify Gateway datafill in table IPINV is correct.
The dynamic host configuration protocol (DHCP) server is not running.	Verify the NetID application is running.
The DHCP server is not configured correctly.	Verify the NetID is configured for the correct load server. (For example: verify the DHCP server is on the same subnet as the Gateway; verify the MAC address is correct in NetID; check the LAN connectivity.)
The file transfer protocol (FTP) server is not running on the load server.	Verify the FTP server application is running.
The IGW load file is missing from the load server.	Place the correct load file in the load server.

InSv test of a Gateway fails

If the failure reason is in service (InSv) test failure, verify the LAN connectivity is active by checking the Gateway light emitting displays (LEDs).

A Gateway fails to RTS

The following table lists possible causes if a Gateway fails to return to service (RTS).

Table 12-2 A Gateway fails to RTS

Cause	Solution
Gatekeeper registration failure	• Verify the Gatekeeper IP address in NetID. • Verify the Gatekeeper is InSv. • Restart the Gatekeeper application, if necessary.
Static data transfer failed	Reboot the Gatekeeper machine.
No response from PM	• Post the Gateway at the maintenance and administration position (MAP) display. • PMRESET the Gateway card. • Perform an out of service (OOS) test if it fails again.
Diagnostic test fails with “Tst No Resources”	Retry. If it fails again, probable hardware failure

A Gateway goes SysB

Post the Gateway at the MAP display and QUERYPM FLT the Gateway. Refer to the following table for failure causes and solutions.

Table 12-3 A Gateway goes SysB

Cause	Solution
IPGateway P-side alarm	Check the Gatekeeper and restart, if necessary.
7X07 self-test failed	• Post the Gateway at the MAP display. • PMRESET the Gateway card. • Perform OOS tests.
7X07 diagnostics failed	Possible HW fault. PMRESET the Gateway card and perform OOS tests.
A denial of service (DoS) attack	If a PMRESET does not restore the Gateway to service, manually reset the card.

One-way speech

If the Gateway or i2004 phone is not sending or receiving packets, run PMDEBUG to see if packets are being sent and received. Consult the PMDEBUG manual.

Repeated call attempts fail

The following table lists possible causes if repeated call attempts fail.

Table 12-4 Repeated call attempts fail

Cause	Solution
Line is not InSv.	• Verify the line is InSv at the MAP display. • Make sure the line is in an idle (IDL) state before placing a call.
TPS is pointing to a different Gatekeeper.	Verify the i2004 phone and TPS are registered with the same Gatekeeper that the Gateway is using.

Active LED on Gateway off

The following table lists possible causes if the active LED on Gateway is off.

Table 12-5 Active LED on Gateway off

Cause	Solution
Gateway did not get its load from the DHCP server.	Ensure MAC address is datafilled correctly in NetID.
Gateway has no power.	Ensure the -48V fuse is in the frame supervisory panel (FSP) for the slot and shelf where the Gateway is installed.

Active LED on Gateway blinking

The following table lists possible causes if the active LED on Gateway is blinking.

Table 12-6 Active LED on Gateway blinking

Cause	Solution
Gateway loaded or loading, but Gateway is manual busy (ManB), system busy (SysB), or offline (OffL).	Ensure Gateway card is InSv. If not, RTS the Gateway card.
Gatekeeper is offline.	Restart the Gatekeeper. The Gateway will come back InSv when the Gatekeeper is started.

LAN 0 or 1 LED is off or blinking

If there is a lack of connectivity to the LAN switch or a hardware failure, check the Gateway card, cables, or LAN switch for connectivity.

No LEDs are lit

If there is no power to the Gateway card, replace the -48V fuse in the FSP for the slot and shelf where the Gateway is installed.

Gatekeeper troubleshooting

The following sections provide troubleshooting information about the Gatekeeper component.

Gatekeeper does not accept registration of clients or Gateways

The following table lists possible causes if the Gatekeeper does not accept registration of clients or Gateways.

Table 12-7 Gatekeeper does not accept registration of clients or Gateways

Cause	Solution
Installation of Gatekeeper software is incomplete.	Verify the configGatekeeper.val is in the same directory as the GatekeeperCS.EXE file.
Gatekeeper is not running.	• Verify from the cluster administrator that Gatekeeper is not running. • Start Gatekeeper. • BSY and RTS the Gateway. • Re-attempt client registration.
Gateway and clients are not communicating with Gatekeeper.	• Verify the client and Gateway configuration for the Gatekeeper IP address. • Ensure the gatekeeper.ini file in the Gatekeeper IP address is set up correctly. • PING Gatekeeper address specified in client configuration to verify network path to Gatekeeper. • Capture Gatekeeper log file and contact Nortel Networks for support.

Client fails to register with the Gatekeeper

The following table lists possible causes if a client fails to register with the Gatekeeper.

Table 12-8 Client fails to register with the Gatekeeper

Cause	Solution
Client configured with incorrect IP address of Gatekeeper.	• Verify configuration of the IP address of the client Gatekeeper. • PING Gatekeeper address specified in client configuration to verify network path to Gatekeeper.
The client is unable to transmit data over network.	• Verify client has network connectivity. • PING the Gatekeeper IP address.
Directory number (DN) or terminal identifier (TID) information is not present in the Gatekeeper.	• From PTM, check whether the client DN is present in the Gatekeeper. • If the DN is not present, check for DN assignment in DMS. • Capture Gatekeeper log file and contact Nortel Networks for support.

Gateway fails to register with the Gatekeeper

The following table lists possible causes if the Gateway fails to register with the Gatekeeper.

Table 12-9 Gateway fails to register with the Gatekeeper

Cause	Solution
Gateway is configured with the incorrect IP address of the Gatekeeper.	Verify configuration of Gatekeeper IP address of the Gateway.
Gateway is unable to transmit data over the network.	• Verify Gateway has network connectivity. • PING the Gatekeeper IP address. • Capture Gatekeeper log file and contact Nortel Networks for support.

Cluster server fails and restarts the Gatekeeper on the same node

A software bug can cause the cluster server to fail and restart the Gatekeeper on the same node. The following list describes actions to take.

- Verify a failover by looking for the cluster service entries in the NTEventLog.
- From the PTM, check if there is an h323GateKeeperStart trap from this Gatekeeper.
- Capture the Gatekeeper log file and contact Nortel Networks for support.

Cluster server fails and restarts the Gatekeeper on the alternate node

A software bug can cause the cluster server to fail and restart the Gatekeeper on the alternate node. The following list describes actions to take.

- Verify a failover by looking for the cluster service entries in the NTEventLog.
- From the PTM, check if there is an h323GateKeeperStart trap from this Gatekeeper.
- Capture the Gatekeeper log file and contact Nortel Networks for support.

Gatekeeper service goes to a fail state

Gatekeeper service goes to a fail state if the Gatekeeper executable file cannot be accessed. The following list describes the actions to take.

- Uninstall the Gatekeeper software.
- Re-install the Gatekeeper software.

PTM shows a critical alarm on the Gatekeeper

The following table lists possible causes if the PTM shows a critical alarm on the Gatekeeper.

Table 12-10 PTM shows a critical alarm on the Gatekeeper

Cause	Solution
The PTM Alarm Manager shows the Alarm Description as “persistent store failure alarm.” This indicates a database access failure.	• Verify the database directory exists. This directory is specified in the gatekeeper.ini file under DATABASE section named as Shared Database Path. • Verify all files under the database directory exist and are readable and writable. • If the alarm still exists, take the Gatekeeper service off-line. • Delete the database directory and all the files under the directory. • Bring the Gatekeeper service on-line.
A critical alarm can also indicate a hard disk failure, although this is unlikely.	Take the Gatekeeper out of service and replace the hard disk.

PTM shows a major alarm on the Gatekeeper

The following table lists possible causes if the PTM shows a major alarm on the Gatekeeper.

Table 12-11 PTM shows a major alarm on the Gatekeeper

Cause	Solution
The PTM Alarm Manager shows the Alarm Description as “callp overload alarm.” This indicates a state of call processing overload in the Gatekeeper. To prevent call processing quality from degrading, future call attempts are ignored until the alarm is cleared.	No action need be taken. The recovery system automatically clears the alarm. The recovery time depends on the call processing load at that moment.

PTM shows a minor alarm on the Gatekeeper

The following table lists possible causes if the PTM shows a minor alarm on the Gatekeeper.

Table 12-12 PTM shows a minor alarm on the Gatekeeper

Cause	Solution
The PTM Alarm Manager shows the Alarm Description as "endpoint based RAS failures alarm." This indicates that on the individual line RAS request messages are rejected, such as Registration Request (RRQ) messages or Admission Request (ARQ) messages.	• Identify the line according to the IP address provided in the alarm description. • Verify this IP address is associated with a i2004 phone. • Verify that the TPS the i2004 phone is associated with has the correct configuration. • Verify the TID and DN of the i2004 phone are provisioned in the Gateway. • Verify the Gatekeeper has the static data corresponding to the Gateway. • Verify that other TPSs that are also pointing to the Gatekeeper do not contain the TID and the DN of the i2004 phone. • Cycle down the i2004 phone, then cycle up.
The PTM Alarm Manager shows the Alarm Description as "endpoint based Q931 msg failure alarm." This indicates a call signaling processing failure.	• Identify the i2004 phone according to the address provided in the alarm description. • Cycle down the i2004 phone, then cycle up.
The PTM Alarm Manager shows the Alarm Description as "endpoint based TCP disconnection alarm." This indicates a TCP connection failure.	• Identify the line according to the IP address provided in the alarm description. • If the TPS which this line is associated with is running on a separate machine from the machine on which the Gatekeeper is running, verify the network card of the TPS machine is in good condition.

PTM shows a warning alarm on the Gatekeeper

The following table lists possible causes if the PTM shows a warning alarm on the Gatekeeper.

Table 12-13 PTM shows a warning alarm on the Gatekeeper

Cause	Solution
The PTM Alarm Manager shows the Alarm Description as "system-wide authentication failure alarm." This indicates a system-wide authentication failure.	Capture Gatekeeper log file and contact Nortel Networks for support.
The PTM Alarm Manager shows the Alarm Description as "endpoint based authentication failure alarm." This indicates an authentication failure against the individual line.	• Identify the line according to the IP address provided in the alarm description • Verify this IP address is associated with a i2004 phone. • Verify that the TPS the i2004 phone is associated with has the correct configuration. • Verify the TID and DN of the i2004 phone are provisioned in the Gateway. • Verify the Gatekeeper has the static data corresponding to the Gateway. • Verify that other TPSs that are also pointing to the Gatekeeper do not contain the TID and the DN of the i2004 phone. • Cycle down the i2004 phone, then cycle up.

Gatekeeper start trap

When the Gatekeeper start trap (h323GatekeeperStart) appears in the Event History Manager window, it can indicate that a failover has occurred. The following list describes actions to take.

- Verify a failover occurred by looking for the cluster service entries in the NTEventLog.
- Capture the Gatekeeper log file and contact Nortel Networks for support.

Gatekeeper shutdown trap

When the Gatekeeper shutdown trap (h323GatekeeperGoingDown) appears in the Event History Manager window, it can indicate that a failover has occurred. The following list describes actions to take.

- Verify a failover occurred by looking for the cluster service entries in the NTEventLog.
- Capture the Gatekeeper log file and contact Nortel Networks for support.

Cold start trap

When the cold start trap (pTMneColdStartInit) appears in the Event History Manager window, it indicates that the PTM server's Alarm Manager will start initialization of the alarm table. This trap does not require customer action.

RAS registration reject trap

The following table lists actions to take if the RAS registration reject trap (csAuthenticationFailureRASRegistration) appears in the Event History Manager window.

Table 12-14 RAS registration reject trap

Cause	Solution
The RAS registration request message was rejected because of authentication failure.	• Identify the line according to the IP address and the DN provided in the trap table. • Verify this IP address is associated with a i2004 phone. • Verify that the TPS the i2004 phone is associated with has the correct configuration. • Verify the TID and DN of the i2004 phone are provisioned in the Gateway. • Verify the Gatekeeper has the static data corresponding to the Gateway. • Verify that other TPSs that are also pointing to the Gatekeeper do not contain the TID and the DN of the i2004 phone. • Cycle down the i2004 phone, then cycle up.

RAS admission reject trap

The following table lists actions to take if the RAS admission reject trap (csAuthenticationFailureRASAdmission) appears in the Event History Manager window.

Table 12-15 RAS admission reject trap

Cause	Solution
The RAS admission request message was rejected because of authentication failure.	• Identify the line according to the IP address and the DN provided in the trap table. • Verify this IP address is associated with a i2004 phone. • Verify that the TPS the i2004 phone is associated with has the correct configuration. • Verify the TID and DN of the i2004 phone are provisioned in the Gateway. • Verify the Gatekeeper has the static data corresponding to the Gateway. • Verify that other TPSs that are also pointing to the Gatekeeper do not contain the TID and the DN of the i2004 phone. • Cycle down the i2004 phone, then cycle up.

Alarm traps

The alarm traps display in the Event History Manager window as follows. If any of these traps appear, refer to the specific alarm advice for Gatekeeper alarms in this chapter.

- nortelNMIcriticalAlarmNotification
- nortelNMImajorAlarmNotification
- nortelNMIminorAlarmNotification
- nortelNMIwarningAlarmNotification
- nortelNMIalarmClearNotification

SNMP log handling trap

The SNMP log handling trap (scNortelLogNotificationEvent) appears in the Event History Manager window when a software error has occurred. The following table lists the possible types of errors and action to take.

Table 12-16 SNMP software errors

Cause	Solution
• Software error occurred while initializing the subagent. • Software error occurred while setting the logs. • Software error occurred while processing the SNMP event. • Software error occurred while checking the master agent's status.	Capture the Gatekeeper log file and contact Nortel Network's for support.

Log error: Error processing INI file

The following table lists possible causes if the Gatekeeper log has an error message of "Error processing INI file."

Table 12-17 Log error: Error processing INI file

Cause	Solution
The gatekeeper.ini file is missing or out of place.	Get the correct version of the gatekeeper.ini file and put it in the C:/WinNT directory on the Gatekeeper.
There is a syntax error or missing parameter in the gatekeeper.ini file.	Check the copy of the gatekeeper.ini file that is in the WinNT directory for syntax errors. If necessary, replace the file with the original and reset parameters as needed. ***Note:*** It is recommended that a copy of the gatekeeper.ini file be backed up on a regular basis.

Log error: Memory allocation error

The following table lists possible causes if the Gatekeeper log has an error message of “Memory allocation error.”

Table 12-18 Log error: Memory allocation error

Cause	Solution
The Gatekeeper is out of physical or virtual memory.	Increase the size of the virtual memory allocation.
If the problem reoccurs, there is a possible memory leak or software bug.	Capture the Gatekeeper log file and contact Nortel Networks for support.

Log error: Singleton data object not found

The following table lists possible causes if the Gatekeeper log file has an error message of “Singleton data object not found.”

Table 12-19 Log error: Singleton data object not found

Cause	Solution
Memory corruption has occurred.	The Gatekeeper application must be restarted. In some cases, a reboot is necessary.

Error messages in Gatekeeper log file

If error messages other than those listed appear in the Gatekeeper log file, the cause is a software bug. Capture the Gatekeeper log file and contact Nortel Networks for support.

Client cannot originate or terminate calls

The following table lists possible causes if a client cannot originate or terminate calls.

Table 12-20 Client cannot originate or terminate calls (Sheet 1 of 2)

Cause	Solution
The client is not registered.	• Restart the client. • Verify the client registers with the Gatekeeper.

Table 12-20 Client cannot originate or terminate calls (Sheet 2 of 2)

Cause	Solution
The Gateway is not InSv.	• Post the Gateway at the MAP display. • BSY and RTS the Gateway.
The TPS is not InSv	• Start TPS. • Re-attempt client registration. • Capture Gatekeeper log file and contact Nortel Networks for support.

i2004 Internet Telephone and TPS troubleshooting

The following sections provide troubleshooting information about the i2004 Internet Telephone and the TPS.

TPS initialization errors

The following table lists possible causes if the TPS fails to initialize. All i2004 phones are affected in this case.

Table 12-21 TPS initialization errors (Sheet 1 of 2)

Symptom	Cause	Solution
All i2004 phones display the message, “Server Unreachable.”	The TPS failed to initialize.	Check the TPS log file for a Callp Initialized message. If you do not see this log at the beginning of the file, the TPS failed to initialize.
	The TPS IP address is not datafilled correctly.	• Check the TPS log file for a Socket Exception: Can’t Assign Requested Address message. • Use the “System Settings” menu of the TPS Config Tool to correct the TPS IP address.

Table 12-21 TPS initialization errors (Sheet 2 of 2)

Symptom	Cause	Solution
After the TPS is started, all i2004 phones display "Waiting for Connection" indefinitely.	The TPS has not established a connection to the Gatekeeper.	• Check the TPS log file for one of the following logs: — Socket - Successfully established outgoing Q931 connection — Socket - Failed to establish outgoing Q931 • If you see the second log, ensure the Gatekeeper is running. • Ensure the field "GK IP Address" in the "System Settings" menu of the TPS Config Tool is set to the virtual IP address of the Gatekeeper.
	The TPS has restarted. The TPS is allowing only a certain number of terminals to initialize at the same time. A terminal is in the queue to be reinitialized.	Check the TPS log file for a Call Processing message that indicates a login is pending for an available registration slot.

i2004 phone initialization errors

During the i2004 initialization process, the system response "Initializing" displays on an i2004 phone. After an i2004 phone has registered successfully, it displays the DN icons. This display of the DN icons indicates that the end user can begin to make and receive calls with the i2004 phone.

The TPS log file also generates the following logs.

```
Sev 4 Mar 26 21:49:10 Terminal Proxy Server
terminalProxyServer.TerminalManager.DispatchMessage() -
Adding new address:
47.174.64.212

Sev 4 Mar 26 21:49:11 E2 Controller
006038760203
Proper DnKey Received00930001

Sev 4 Mar 26 21:49:12 Call Processing
Login request for new terminal 006038760203/6137234560/93/1

Sev 4 Mar 26 21:49:13 Server
6137234560 1/006038760203/93/1/02/1 registered on port 3624

Sev 4 Mar 26 21:49:14 Server
PDL successful for 6137234560 1/006038760203/93/1/02/1
```

If the TPS did not generate these logs, then the i2004 phone failed to initialize. A corresponding numerical reason code also displays on the i2004 phone.

i2004 reason codes

The i2004 phone can display numerical reason codes. These reason codes correspond to different errors that occur during a component-level failure that the i2004 encounters with the other components with which it interacts. Reason codes range from 1000 to 2999. A value from 1000 to 1999 refers to log-in problems that the i2004 phone encountered with the TPS. A value from 2000 to 2999 refers to registration problems that the i2004 phone encountered with the Gatekeeper.

During an initialization failure, the i2004 phone displays the system response "Initializing," followed by the error messages "Initialization failed" and "Service denied."

Common reason codes that occur during initialization failure on the i2004 phone are 1006, 2000, 2018, 2024, 2031, 2410, 2423, and 2428.

The following table lists possible causes and suggested solutions for commonly occurring reason codes that display during i2004 phone initialization.

Table 12-22 i2004 phone fails to initialize (Sheet 1 of 3)

Symptom	Cause	Solution
Reason code 1006 (DNKEY_ ENTRY_NOT_FOUND) displays.	• The i2004 phone is using an invalid DN Key, or • The i2004 phone is using an DN Key that another i2004 is using	Verify the DN Key number: • Check that the user has entered the correct DN Key. • Check that the TPS has the correct DN Key datafill. • Access the TPS Config Tool. Select the DN Key Settings. Check that the DN Key number exists in the list.
Reason code 1006 (DNKEY_ ENTRY_NOT_FOUND) displays and the TPS generates log “The same DN Key is currently used by other terminal.”	Another i2004 phone is using this DN Key.	To move the DN Key to another i2004 phone: • Log out of (or cycle down) the i2004 phone that is currently using the DN Key. — Press Services button on the i2004 phone. — Press Up/Down arrow keys to select Phone Options in the i2004 display screen. — Press Select Soft Key. — Use Up/Down arrow keys to select Logout. — Press Select Soft Key again. — Press OK Soft Key to end this procedure. (Or press CANCEL to cancel this procedure.) • Cycle power down on the i2004 phone that displayed reason code 1006. Re-cycle power on.

Table 12-22 i2004 phone fails to initialize (Sheet 2 of 3)

Symptom	Cause	Solution
The following reason codes display: • 2000 (RESOURCE_ UNAVAILABLE) • 2018 (UNDEFINED) • 2019 (TERMINAL_ EXCLUDED)	The Gatekeeper does not have all the datafill for the i2004 phone that is trying to register.	Follow any of these procedures: • Check the Gatekeeper logs to determine why the Gatekeeper rejected the registration request. • Ensure the Gatekeeper has static data for the i2004 phone. • Contact Nortel Networks Customer Support for a Centrex IP Gatekeeper failure.
Reason code 2024 (SECURITY_DENIAL) displays.	The Gatekeeper rejected the registration. Authentication failed.	Contact Nortel Networks Customer Support for a Centrex IP Gatekeeper or TPS issue.
Reason code 2031 (TIMEOUT) displays.	The TPS sent a registration request to the Gatekeeper. The TPS did not receive a response back from the Gatekeeper.	Follow one of these procedures: • Access the TPS Config Tool. From the System Settings tab, check that the IP address in the GK IP Address field is correct. • Check that the Gatekeeper is turned on. • Contact Nortel Networks Customer Support for a Centrex IP Gatekeeper issue.
Reason code 2410 (PDL_Q931_ TIMEOUT) displays.	The TPS sent a Q931 register message to the Gatekeeper to initiate parameter downloading. The TPS did not receive a response back from the Gatekeeper.	Contact Nortel Networks Customer Support for a Centrex IP Gatekeeper issue.

Table 12-22 i2004 phone fails to initialize (Sheet 3 of 3)

Symptom	Cause	Solution
Reason code 2423 (PDL_TOO_FREQUENT) displays.	The DMS switch allows two or three requests for parameter downloading from any i2004 phone within a 15-minute interval. This request exceeds the allowable time limit.	Detach and re-attach the LTID to its GWIP on the DMS. Refer to the “DMS Maintenance” chapter. See “Detaching and reattaching an LTIP from one LEN to another LEN” under the “Parameter downloading” section.
Reason code 2428 (PDL_DMS_RESOURCE_ LIMITATION) displays.	The DMS switch rejected the parameter downloading attempt when the following conditions exist: • The i2004 phone belongs to a MADN group when a user attempts parameter downloading. • The member of the MADN group is active on a call with the MADN DN.	The end user can cycle power on the i2004 phone only when the other members of the MADN group are not using the MADN DN.

Individual i2004 phone fails to initialize with error messages

The following table shows error messages that display on an i2004 phone when it has failed to initialize.

Table 12-23 Individual i2004 phone fails to initialize with error messages

Symptom	Cause	Solution
The i2004 phone displays the error message “Server Unreachable.”	The TPS has dropped communication to the i2004 phone.	The i2004 phone was not configured properly. Check that the server address for the i2004 phone matches the IP address of the virtual TPS.
The i2004 phone first displays the error message “Upgrading Firmware...”, followed by “Locating Server...”. The error message “Upgrading Firmware...” redisplays.	The i2004 phone cannot communicate with the TFTP server because the server is down.	• Access the TPS Config Tool. From the System Settings menu, check that the i2004 firmware load is correct. • Also check that the TFTP server is running.

The user cannot make or receive calls

As a rule of thumb for clearing problems with making or receiving calls, end users can first try to cycle down the i2004 phone, and cycle it back up. If cycling down does not clear the problem, end users can try to log out of the i2004 phone.

The following table lists possible causes if the i2004 phone successfully initializes and registers, but the user cannot make or receive calls. These problems affect individual i2004 phones.

Table 12-24 The user cannot make or receive calls (Sheet 1 of 4)

Symptom	Cause	Solution
When the user presses a DN key, the i2004 phone does not respond.	The i2004 phone is locked up.	• Unplug the network cord. • Press the DN key. • If the i2004 phone remains locked up, contact customer support for the i2004 firmware.
	The i2004 phone displays the message “Server Unreachable” if the TPS has dropped communication to the i2004 phone.	• Unplug the network cord. • Press the DN key. • Check the i2004 phone display to read “Server Unreachable.” • Plug the network cord back into the i2004 phone. • Use a packet sniffer to determine what packets are being sent between the TPS and i2004 when you press the DN key.
	NAT resolution	Check the TPS log file for a No Media Resolution message. ***Note:*** If this log is generated each time the i2004 phone attempts to originate a call, then the Echo Server is not datafilled correctly on the TPS. • Use the TPS Config Tool to reset the IP address and port for the Echo Server. • Restart the TPS.

Table 12-24 The user cannot make or receive calls (Sheet 2 of 4)

Symptom	Cause	Solution
	The terminal is not registered.	• Start the TPS debug tool. • Select the "Trace Mask" panel. • Select hardware ID for the terminal that cannot originate a call. If the MAC address for the i2004 phone is not listed, then the i2004 phone is not registered with the TPS.
When the user presses a DN key, the DN key icon shows offhook and then onhook (immediately or 10 seconds later).	No response to outgoing RAS ARQ message	• Check the TPS logs for an Admissions Rejected message. • Contact Nortel Networks Customer Support for a Centrex IP Gatekeeper issue.
	No response to outgoing Q931 Setup message	• Check the TPS logs for a Q931 Timeout message. • Contact Nortel Networks Customer Support for a Centrex IP Gatekeeper issue.
	Incoming Q931 ReleaseComplete	• Check the Gatekeeper logs to determine why it is sending a Release Complete message. • If you cannot locate the cause of the problem, contact Nortel Networks Customer Support for a Centrex IP Gatekeeper issue.
	Incoming Q931 Status	• Check the TPS logs for a Q931 Status Received message. • Contact Nortel Networks Customer Support for a Centrex IP Gateway issue.

Table 12-24 The user cannot make or receive calls (Sheet 3 of 4)

Symptom	Cause	Solution
	Origination rejected because another request is pending	• Check the TPS logs for an Origination Attempt Rejected message. • If the user is not pressing the DN keys too quickly, this log indicates the Gatekeeper or Gateway is not processing messages in a timely manner. Contact Nortel Networks Customer Support for a Centrex IP Gatekeeper issue.
When the user presses a DN key, the DN key shows offhook and then 10 seconds later shows onhook.	No response to outgoing RAS ARQ message	• Check the TPS logs for an Admissions Rejected message. • Contact Nortel Networks Customer Support for a Centrex IP Gatekeeper issue.
	No response to outgoing Q931 Setup message	• Check the TPS logs for a Q931 Timeout message. • Contact Nortel Networks Customer Support for a Centrex IP Gatekeeper issue.
The user cannot receive an incoming call.	NAT resolution	Check the Gatekeeper log file for a New Call Reject message. ***Note:*** This log indicates the i2004 phone did not provide the TPS with the IP and port information needed for the incoming call. If this log is generated each time the i2004 phone receives a call, then the Echo Server is not datafilled correctly on the TPS. • Use the TPS Config Tool to reset the IP address and port for the Echo Server. • Restart the TPS.

Table 12-24 The user cannot make or receive calls (Sheet 4 of 4)

Symptom	Cause	Solution
	Terminal is not registered.	• Start the TPS debug tool. • Select the “Trace Mask” panel. • Select the hardware ID for the terminal that cannot originate a call. • Check to see if the MAC address for the i2004 phone is listed. If not, the i2004 phone is not registered with the TPS.
	Hung MADN call on the TPS	• Check the TPS logs for a message indicating the user already has a call on this MADN appearance. • To determine why the call was not released properly, contact Nortel Networks Customer Support for Centrex IP TPS and Gatekeeper issues.
	Hung (non_MADN) call on the TPS	• Check the TPS logs for a message indicating the terminal does not have an available appearance for incoming call. • To determine why the call was not released properly, contact Nortel Networks Customer Support for Centrex IP TPS and Gatekeeper issues.

The user can make and receive calls

The following table lists possible causes if the user can make and receive calls, but other problems exist.

Table 12-25 The user can make and receive calls (Sheet 1 of 2)

Symptom	Cause	Solution
The i2004 phone is on a call. When the user presses a key (for example, digit key, feature softkey, another DN key, and so on), the call is dropped.	The Gatekeeper dropped the Q931 connection.	• Check the TPS logs for a Q931 Connection Lost message. • Check the Gatekeeper logs for more information. • If you cannot determine the cause of the problem, contact Nortel Networks Customer Support for a Centrex IP Gatekeeper issue.
	The Gateway or Gatekeeper dropped the call.	• Check the TPS logs for a DRQ Received from Gatekeeper message. • Check the Gatekeeper logs for more information. • If you cannot determine the cause of the problem, contact Nortel Networks Customer Support for a Centrex IP Gatekeeper issue.
The user cannot activate or deactivate Call Forwarding or Do Not Disturb.	No response to outgoing Q931 FA message	• Check the TPS logs for a Q931 Timeout message. • Check the Gatekeeper logs for more information. • If you cannot determine the cause of the problem, contact Nortel Networks Customer Support for a Centrex IP Gatekeeper issue.

Table 12-25 The user can make and receive calls (Sheet 2 of 2)

Symptom	Cause	Solution
The i2004 user is on a call to another i2004 user. The caller attempts to hold the call, select a soft key, or select another DN key. The i2004 phone beeps but does not process the request of the user. When the i2004 caller hangs up, the i2004 resets.	The TPS restarted during the call. If the TPS restarts while an i2004 user is talking to a remote party, the TPS preserves the call. After restart, the TPS rejects all key presses by the user. If the user presses a key, the i2004 phone beeps.	• Check the TPS logs for a Received Invalid Key Event during TPS Media Recovery message. • When the user hangs up, the TPS resets the i2004 phone.
The i2004 user cannot retrieve a call.	Another request is pending. The TPS allows a user to have only one outstanding request at a time. This log is generated if the user is pressing DN keys too quickly.	• Check the TPS logs for a Select Attempt Rejected message. • If the user is not pressing the DN keys too quickly, this log indicates the Gatekeeper or Gateway is not processing messages in a timely manner. Contact Nortel Networks Customer Support for a Centrex IP Gatekeeper issue.
When the i2004 user answers a call, the call is dropped.	NAT resolution	Check the TPS logs for a Retrieve request without RTP info message.

Appendix A MSL-100 Internet Protocol

Introduction

This appendix describes the Meridian SuperNode (MSL-100) system with the Internet Protocol (IP) software option. The MSL-100 system with IP is called MSL-100IP. MSL-100IP is based upon the DMS-100 Centrex IP product, which is described in this document.

This appendix is intended for the following audience:

- MSL-100 switch administrators
- enterprise LAN administrators
- Nortel Networks personnel - installation, engineering, and support

This appendix describes the differences between MSL-100IP and Centrex IP. For details on the Centrex IP product, refer to the chapters in this document.

MSL-100 documentation references

In addition to the documentation listed in “About this document,” the following NTPs should be referenced for additional information on the MSL-100 system.

- *MSL-100 Card Replacement Procedures,* 555-4031-547
- *MSL-100 Log Reports Reference Manual,* 555-4031-840
- *MSL-100 Service Orders Reference Manual,* 555-4031-808
- *MSL-100 Customer Data Schema Reference Manual,* 555-4031-851
- *MSL-100 Translations Reference Manual,* 555-4031-350
- *MSL-100 Product Guide,* 555-4031-103
- *MSL-100 Master Index of Publications,* 555-4031-001

These documents can be accessed from the Helmsman documentation CD received with release MSL11.

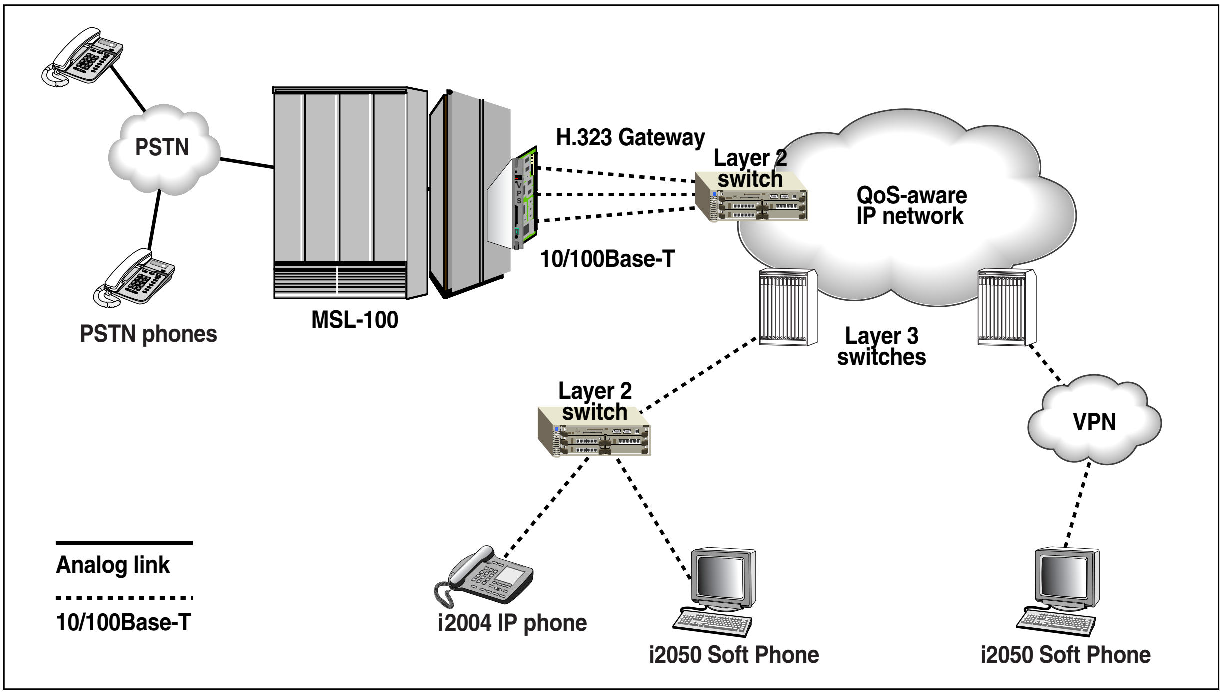
Product overview

MSL-100IP gives users the best of both worlds - permitting the extensive telephony capabilities of the MSL-100 to be extended to both IP-based telephony terminals and existing analog/digital sets. The architecture of the MSL-100IP allows real time, full duplex voice services to easily bridge between the packet-switched and circuit-switched network. The technology of the MSL-100IP offers you an easy-to-implement evolutionary path to voice and data convergence without trading off reliability, scalability, or feature richness.

The MSL-100IP system offers:

- IP line-side services
- complete interoperability between the Internet telephone (i2004) and existing analog and digital telephone sets
- An IP telephony solution based on the International Telecommunications Union (ITU) Recommendation H.323. H.323 is an ITU-T specification that addresses not just IP telephony, but the broader issue of multimedia conferencing. H.323 is currently the standard that is most widely endorsed for the support of telephony services where the underlying transport is a packet-based network.
- current investment protection, with the flexibility to migrate toward a converged network at a pace that aligns with each customer’s business
- all of the OAM&P capabilities that are inherent to the MSL-100 today
- scalability to support large campus environments
  - — 32,000 IP telephony terminals in release MSL11
  - — over 50,000 IP telephony terminals in release MSL12

Figure A-1 MSL-100IP system components



Line-side services

The MSL-100IP line-side services provides telephony capabilities to IP telephony terminals anywhere across the corporate LAN/WAN environment. This technology enables real-time, full duplex voice communication between:

- terminals on an IP network and terminals on the circuit-switched network
- two or more IP telephony terminals

This technology also allows users served by IP telephony terminals to take advantage of a wide variety of line-side applications residing on the switch, including voice mail, conferencing, and PSTN access.

The following core components are required to implement Ethernet-based IP access to line-side features and services on the MSL-100:

- IP ready ISDN line trunk controller (LTCI)
- integrated IP Gateway card (NT7X07AA) in the LTCI
- Gatekeeper
- i2004 Internet Telephone (or i2050 Soft Phone client)
- Terminal Proxy Server (TPS) application
- Packet Telephony Manager (PTM) application

- dynamic host configuration protocol (DHCP) server application
- trivial file transfer protocol (TFTP) load server application

ISDN line trunk controller

The IP-ready LTCI (frame [NT6X01AF] and cabinet [NTNX33CB]) is a peripheral enhanced to integrate the IP gateway card as an IP interface. In addition to a new shelf and backplane, 16 pins are added to the backplane for each slot that accommodates the gateway card. A backplane-to-bulkhead cable assembly and bulkhead personality plate accommodate the additional cables that connect the LTCI to the edge device on the LAN. For more information on the LTCI and its capabilities, refer to chapter 3, “Gateway.”

IP Gateway card

The IP Gateway card is an XPM circuit pack that resides in an IP-ready LTCI and provides the protocol conversion and media transcoding to support real-time, two-way communications between an H.323 IP terminal and a traditional analog or digital telephone. The IP Gateway card allows call processing and traditional telephony capabilities to be extended to IP telephony terminals on the ethernet LAN. The IP Gateway card has the characteristics of an H.323 endpoint on the LAN and interfaces to the IP network with a 10/100Base-T ethernet connection. For more information on the IP Gateway card and its capabilities, refer to chapter 3. “Gateway.”

Gatekeeper

The Gatekeeper facilitates call processing for IP terminals by providing services such as address translation, admissions control, H.225 registration, admission, and status, zone management, and SNMP agent functionality. For more information on the Gatekeeper and its capabilities, refer to chapter 2, “Gatekeeper.”

FTP application

The FTP application runs on the same machine as the DHCP application and supplies the software load to the Gateway card. For more information on the FTP application and its capabilities, refer to chapter 5, “DHCP and load servers.”

TFTP application

When the i2004 Internet telephone powers up, it connects to the TPS to verify its firmware. If the telephone needs new firmware, the TPS uses TFTP (trivial file transfer protocol) and the TFTP application to update the firmware. The TFTP application resides on the same machine as the DHCP application or on a different machine. For more information on the TFTP application and its capabilities, refer to chapter 5, “DHCP and load servers.”

i2004 Internet Telephone

The i2004 Internet Telephone supports native IP and connects directly to an RJ45 ethernet jack. Each i2004 telephone has its own MAC address and its own IP address. The functionality and call features of the i2004 telephone provide the same familiarity and ease-of-use of a basic rate interface (BRI) business telephone. These capabilities are accessible to end users through an intuitive user interface: the familiar dial pad and feature keys. The i2004 telephone requires the terminal proxy server. For more information on the i2004 telephone and its capabilities, refer to the *i2004 User Guide*.

i2050 Soft Phone

The i2050 Soft Phone is a PC telephony application that runs on the Windows 2000 operating system. The Soft Phone provides a graphical user interface (GUI) that allows users to originate and terminate calls to the PSTN from a multimedia PC. The Soft Phone, like the i2004 Internet Telephone, is directed by the TPS. The features implemented in the TPS are downloaded to the i2050 Soft Phone.

Terminal Proxy Server

The i2004 Internet Telephone and the TPS together play the role of an H.323 terminal in the network. To support the i2004 telephones, the TPS is mandatory. For more information on the TPS and its capabilities, refer to chapter 1, “Product overview.”

Packet Telephony Manager

The Packet Telephony Manager (PTM) is a web-based management system that allows you to remotely manage and monitor the MSL-100IP components. The PTM system uses standard simple network management protocol (SNMP) messaging to communicate with the managed nodes in the IP network. The PTM manages the Gatekeeper, including the Gatekeeper’s view of the terminals. The PTM also provides information on the Gateways registered to the Gatekeeper. For more information on the PTM and its capabilities, refer to chapter 4, “Packet Telephony Manager.”

DHCP application

The dynamic host configuration protocol (DHCP) application supports the automatic retrievel of configuration information by newly attached terminals. For example, the DHCP application allows an IP Gateway card to dynamically retrieve information at start-up from the DHCP server such as IP address of the card, name and location of the application loadfile for the card, and IP address of the Gatekeeper. For more information on the DHCP application and its capabilities, refer to chapter 5, “DHCP and load servers.”

Software

System software required to implement IP telephony on the MSL-100IP system consists of software in the Product Computing-module Load (PCL) and a separate non-PCL software load (also referred to as an NCL).

Each MSL-100 software release, or MSL release, consists of PCLs, which contain all generally available software for the MSL-100 market. The PCLs for any MSL-100 system, whether classic circuit-switched or IP-enabled technology, are based on software layering that partitions software code into relatively self-contained modules. Each PCL is comprised of a series of functional groups, which equate to the major system capabilities, such as ISDN or Automatic Call Distribution (ACD). Within these functional groups are individual functionalities that provide the individual feature capability.

IP telephony software in the MSL-100IP PCL (in the MSL11 software release) is contained within the CIP Centrex VoIP functional group, CIP00001. This functional group contains all the software required for the Computing Module (CM) to implement and provide IP telephony services on the MSL-100IP system.

Additional software required for the primary network elements within the managed IP network is provided in an NCL, a separate software load outside of MSL11. This NCL, CIPL0001, must be ordered together with the release MSL11 (or above) PCL.

Dependencies

The CIP00001 functional group within MSL11 requires NI-2 BRI Services, NI00052. (NI-2 BRI Services is part of the optional ISDN BRI functionality, which must be ordered separately along with the MSL11 or above software release.)

The CIPL0001 NCL software requires the CIP00001 PCL software and the NT7X07AA Gateway card.

Limitations and restrictions

The system and component limitations for MSL-100IP are the same as Centrex IP.

System engineering

Refer to the following section for MSL-100IP system engineering requirements.

Engineering to improve latency performance

In addition to the engineering rules Nortel Networks recommends for Centrex IP, the following rule applies:

- Nortel Networks recommends switched ethernet to the desktop for MSL-100IP

> ***Note:*** The recommended engineering rules for Centrex IP are found in the section “Engineering to improve latency performance” in chapter 7.

LAN requirements for Gateway

The integrated Gateway cards require 10/100 Base-T Ethernet connectivity. For MSL-100, set the default for the Gateway interface at 100 Mbps, (refer to the figure A-1, “MSL-100IP system components”).

Appendix B Changing the vocoder

Introduction

A vocoder (or codec) is a type of voice compression protocol. The H.323 standard, which the Centrex IP system components are based on, uses several codecs. The Centrex IP system uses G.729 as its default codec.

This appendix describes how to change the Centrex IP default codec to one of the following values:

- G.711U
- G.711A
- G.723.1
- G.729A

Changing the codec value consists of a two-part procedure to be performed on the following two components of the Centrex IP system:

- changing the codec on the Gateway card (NT7X07AA) using a third-party management information base (MIB) browser
- changing the codec using the terminal proxy server (TPS) software

Note: Ensure that you change the codec values on *both* the Gateway MIB and the TPS. Refer to section "Limitations and restrictions," in this appendix for details.

This information is intended for the following audience:

- TPS system administrators
- Nortel Networks personnel - installation, engineering, and support

Changing the codec on the Gateway MIB

The information in this section identifies the location of the Gateway MIB file and describes the parameters specific to changing the codec values on the Gateway card.

> ***Note:*** Since customers can use several third-party MIB browser applications, such as HP Open View or AdventNet MibBrowser, this section does not provide step-by-step procedures on how to edit the Gateway MIB file. Instead, this section describes the editable parameters for changing the codec for the Gateway MIB.

Overview

The NT7X07AA Vocoder MIB matches the hardware on the NT7X07AA Gateway card and the Centrex IP software application (TPS). This file monitors and control the default parameters that affect the vocoder/digital signal processor (DSP) on the NT7X07AA circuit pack.

The filename for the NT7X07AA Vocoder MIB is "GW-IPCXVOCODER-MIB."

The MIB hierarchy for the GW-IPCXVOCODER-MIB file in the Nortel Networks Voice Over IP (VOIP) MIB tree is as follows:

> NORTEL-VOIP-PTN-PTNGATEWAY-GWIPCENTREX-
> GWIPCXVOCODERMIB

The object identifier (OID) for the GW-IPCXVOCODER-MIB file is 562.28.0.2.1.5.

Accessing the Gateway vocoder MIB file

Perform the following steps to load the Gateway vocoder MIB file.

Procedure B-1 Accessing the Gateway vocoder MIB file

At the Gatekeeper

1 Open the third-party MIB browser application.

2 Load the GW-IPCXVOCODER-MIB file from one of the following locations:

the CD in the GW_Load directory

or, the Primary node in C:\tftp, where the GW load is

3 Refer to the third-party MIB browser instructions to edit the Gateway MIB parameters in the GW-IPCXVOCODER-MIB file. Refer to the tables in the following section, “Gateway MIB OID groups,” for descriptions of the parameters.

Gateway MIB OID groups

The GW-IPCXVOCODER-MIB file consists of the following four OID groups:

- vocoder general group
- vocoder admin group

The following sections describe the OID groups associated with the GW-IPCXVOCODER-MIB file.

Vocoder general group

This group controls the general parameters related to the vocoder. The OID for the vocoder general group is 562.28.0.2.1.5.1. Table B-1 describes the parameters associated with this group.

Table B-1 Vocoder general group parameters

Parameter	Description	Values
Default coder	This parameter sets the default vocoder.	The range is between 0 to 31. The default value is 17, which corresponds to G.729. ***Note:*** Centrex IP only supports values 0 (G.711 Alaw_64), 1 (G.711 Mulaw_64), and 17 (G.729).
Frames per packet	This parameter sets the number of basic vocoder frames that are combined in the outgoing local area network (LAN) packet.	The range depends on the vocoder. For G.711 Alwa_64 and G.711 Mulaw_64, the range is 1 to 6 (or 10-60 ms packet size). For G.729, the values are 2 and 4 (or 20 ms and 40 ms). The default value is 2.

Vocoder admin group

This group controls the MIB on the NT7X07AA circuit pack. The OID for the vocoder admin group is 562.28.0.2.1.5.4. Table B-2 describes the parameters associated with this group.

Table B-2 Vocoder admin group parameters

Parameter	Description	Values
Vocoder values to load on reboot	This parameter instructs the Centrex IP application which vocoder values to load during a reboot.	The values are 0 and 1, as follows: • 0 = load Nortel Networks-set (default) values • 1 = load customer-set values ***Note:*** To retain customer-set values, leave the NT7X07AA circuit pack on the XPM shelf. Software reboots or hardware resets do not affect saved values.
Last custom save	This parameter returns a string with the date and time stamp when the MIB was last saved into static random access memory (RAM).	Not applicable (read-only field)
Save custom values	This parameter instructs the Centrex IP application to save the MIB values to static RAM.	The values are 0 and 1, as follows: • 0 = no action required • 1 = save MIB values and update the Last custom save parameter ***Note:*** This value is always read as 0.
Reset to default	This parameter instructs the Centrex IP application to reset the MIB values to default values (that is, those set by Nortel Networks).	The values are 0 and 1, as follows: • 0 = no action required • 1 = reset MIB values to default ***Note:*** This value is always read as 0.

Changing the codec on the TPS

Perform the following steps to change the value of the codec on the TPS.

Procedure B-2 TPS codec change

At the Gatekeeper

1 Access the TPS Config Tool.

a From the PC Start menu, select Programs-->Nortel Networks-->Terminal Proxy Server-->Configuration Tool.

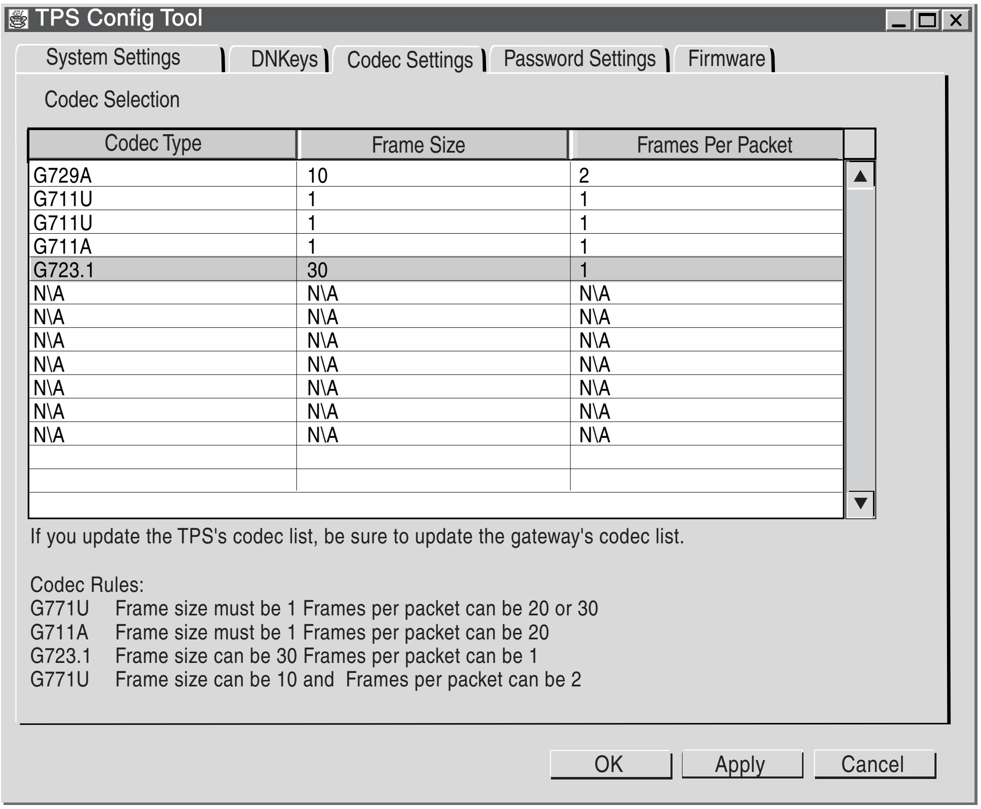
The TPS Config Tool window opens.

> ***Note:*** Refer to the Terminal proxy server chapter for additional information on the TPS Config Tool.

2 Select the Codec Selection Panel tab.

The TPS Codec Selection Panel menu displays, as the following figure shows.

Figure B-1 TPS Codec Selection Panel



Codec Selection

Codec Type	Frame Size	Frames Per Packet
G729A	10	2
G711U	1	1
G711U	1	1
G711A	1	1
G723.1	30	1
N\A	N\A	N\A
N\A	N\A	N\A
N\A	N\A	N\A
N\A	N\A	N\A
N\A	N\A	N\A
N\A	N\A	N\A
N\A	N\A	N\A

If you update the TPS's codec list, be sure to update the gateway's codec list.

Codec Rules:
G771U Frame size must be 1 Frames per packet can be 20 or 30
G711A Frame size must be 1 Frames per packet can be 20
G723.1 Frame size can be 30 Frames per packet can be 1
G771U Frame size can be 10 and Frames per packet can be 2

3 To change a codec value, click over the displayed value of the codec type to be changed.

A list of available codec values displays in a picklist.

> ***Note:*** *Currently, the TPS supports five codecs, with G.729 as the preferred choice.*

4 Position the cursor over the desired value in the codec picklist and release the mouse.

5 The Config Tool automatically selects a Frame Size value and assigns a default Frames Per Packet value to each codec type. The Frame Size value is not customer provisionable. The Frames Per Packet value depends on the selected codec type.

To change the Frames per Packet value, click over the displayed value under the Frames Per Packet column.

A list of available Frames Per Packet values displays in a picklist.

6 Position the cursor over the desired value in the Frames Per Packet picklist and release the mouse.

7 Repeat Steps 3 through 6 to change additional codec values, if necessary.

8 Click the Apply button at the bottom of the Codec Selection Panel menu to apply all changes to this menu. Or click the OK button to apply all changes and exit the TPS Config Tool.

Limitations and restrictions

The following limitations and restrictions apply to changing the MIB vocoder values.

- For TPS codec changes to take effect, restart the TPS after you change the order of the codecs or their values. Codec changes for the Gateway take effect on the next call.
- Ensure that you change the codec values on *both* the Gateway and the TPS. Otherwise, unlike codec values results in i2004-originated calls to PSTN phones passing through the Gateway with one codec, and PSTN-originated calls passing through the Gateway with another codec. Intraswitched calls between two i2004 phones that bypass the Gateway and communicate directly with one another use any codec value. The Gateway does not interfere with the negotiation between the two i2004 phones.
- When changing the preferred codec from G.711, 20 ms, ensure that you change the TPS to the same codec and packet size. Otherwise, calls can fail or use a different codec.
- The i2004 phone does not support G.711 silence compression that the Gateway supports and is proprietary to the third party supplying the DSP software.
- Centrex IP does not support the capability of using one codec for calls through the Gateway and using another codec for intraswitched calls.
- To retain customer set values, leave the NT7X07AA circuit pack on the XPM shelf. Software reboots or hardware resets do not affect saved values.

List of terms

asynchronous transfer mode (ATM)

A type of fast packet switching that uses a fixed size packet called a cell. This technique makes it possible to transmit data at great speed, and can make voice, multimedia, full-motion video, and video conferencing available to users. It also makes dynamic allocation of bandwidth possible; telephone and cable companies can charge individual customers based on the amount of bandwidth they use.

ATM

See asynchronous transfer mode (ATM).

backup domain controller (BDC)

In a Windows NT server, a copy of the primary domain controller (PDC). The BDC is periodically synchronized with the PDC. See also primary domain controller (PDC).

basic input/output system (BIOS)

A set of instructions stored on a read-only memory (ROM) chip inside personal computers (PC), which handles all input-output functions.

basic rate interface (BRI)

A type of access to ISDN service provided by a set of time-division multiplexed digital channels of information, including two B-channels, one D-channel, and one or more maintenance channels, often described as 2B (channels) + D (channel). A BRI is typically used on lines between customer premises and a central office (CO) switch. (Formerly known as basic rate access.)

BDC

See backup domain controller (BDC).

BERT

See bit error rate test (BERT).

BH

See busy hour (BH).

BIOS

See basic input/output system (BIOS).

bit error rate test (BERT)

A test that measures the transmission quality of a loop. A BERT transmits a known bit pattern over a line and compares the reflected signal against the initial pattern.

Bootstrap Protocol (BOOTP)

Protocol used by nodes, when booted, to learn about its own IP address and/or the IP address of the server it must contact to download the load it should boot.

BOOTP

See Bootstrap Protocol (BOOTP).

BRI

See basic rate interface (BRI).

busy hour (BH)

The uninterrupted period of 60 min, not necessarily a clock hour, for which the average intensity of traffic is at the maximum.

CA

See call attempt (CA).

call attempt (CA)

A dialing attempt that the switch processes and bids for service.

CCS

See centum (hundred) call second (CCS).

CD

See compact disk (CD).

central office (CO)

A switching office arranged for terminating subscriber lines and provided with switching equipment and trunks for establishing connections to and from other switching offices. Also known as local office.

central processing unit (CPU)

The hardware unit of a computing system that contains the circuits that control and perform the execution of instructions.

central side (C-side)

The side of a node that faces away from the peripheral module (PM) and toward the central control (CC). Also known as control side. *See also* peripheral side (P-side).

centum call second (CCS)

The use in 1 hour that is expressed in units of hundred-call seconds. (Also called 100 call seconds.)

CM

See computing module (CM).

CO

See central office (CO).

CODEC

See coder/decoder (CODEC).

coder/decoder (CODEC)

A device that converts analog signals to digital to be read by a computer or transmitted over a network, and converts the digital signals back to analog. (Sound cards and video cards use this kind of CODEC).

compact disk (CD)

A format for storing audio data in digital form, which can be played on a CD player or with a CD-ROM drive.

computing module (CM)

The processor and memory of the dual-plane combined core used by the DMS SuperNode. Each CM consists of a pair of central processor units (CPU) with memory that operate in a synchronous-matched mode on two separate planes. Only one plane is active. It maintains overall control of the system while the other plane is on standby.

CPE

See customer premise equipment (CPE).

CPU

See central processing unit (CPU).

C-side

See central side (C-side).

customer premises equipment (CPE)

Equipment, such as ISDN terminals and 1-Meg Modem, located on the subscriber's premises

DCH

See D-channel handler (DCH).

D-channel handler (DCH)

A card in an ISDN line group controller (LGCI) or in an ISDN trunk controller (LTCI) that provides the primary interface to all D-channels. The CDH also performs Q.921 link access procedure on the D-channel (LAPD) layer 2 processing. The DCH is connected permanently to an ISDN loop and receives or sends messages on the signaling/packet data channel.

DHCP

See Dynamic Host Configuration Protocol (DHCP).

digital signal level 1 (DS-1)

The 8-bit, 24-channel, 1.544-Mbit/s digital signaling format used in the DMS-100 Family switches. The DS-1 signal is the North American standard for digital trunks. It is a closely specified bipolar pulse stream. The DS-1 is the standard signal to interconnect Nortel Networks' digital systems. The DS-1 carries 24 information channels of 64 kbit/s each (DS-0s).

digital signal processor (DSP)

A special-purpose CPU that provides ultra-fast instruction sequences (such as shift and add, and multiply and add) which are commonly used in math-intensive signal processing applications. DSP chips are used in sound cards, fax machines, modems, cellular telephones, high-capacity hard disks, and digital televisions.

digital trunk controller (DTC)

A peripheral module (PM) that connects DS30 links from the network with digital trunk circuits.

directory number (DN)

The full complement of digits required to designate a subscriber's station within one numbering plan area (NPA)--usually a three-digit central office (CO) code followed by a four-digit station number.

DLM

See digital line module (DLM).

DN

See directory number (DN).

DRAM

See dynamic random access memory (DRAM).

DS-1

See digital signal level 1.

DSP

See digital signaling processor (DSP).

DTC

See digital trunk controller (DTC).

DTMF

See dual-tone multifrequency (DTMF).

dual-tone multifrequency (DTMF)

The tones on a push-button telephone.

Dynamic Host Configuration Protocol (DHCP)

Protocol used to dynamically assign and unassign an IP address to a host. This is an extension to BOOTP. The DHCP servers will also accept and respond to BOOTP requests.

dynamic random access memory (DRAM)

A random access memory system that employs transistor capacitor storage cells. The logic state is stored in the capacitor and buffered by the transistor. The capacitive charge must be refreshed at a periodic rate to maintain its programmed state.

EISP

See enhanced ISDN signaling preprocessor (EISP).

EKTS

See electronic key telephone set (EKTS).

electronic key telephone set (EKTS)

A set of services for ISDN voice terminals on a basic rate interface (BRI). EKTS provides shared DNs, multiple DNs for each service profile, and conference and intercom calling.

ENET

See enhanced network (ENET).

enhanced ISDN signaling preprocessor (EISP)

A card in the ISDN remote cluster controller (RCCI) that provides interfaces to the signaling processor (SP) and to the speech bus (SB). The EISP terminates a single message link for each D-channel handler (DCH) and processes layer 3 information. Signaling information extracted by the DCH routes to the master processor through the EISP. The EISP replaces the ISDN signaling preprocessor in the XPM-Plus modules.

enhanced network (ENET)

A channel-matrixed time switch that provides pulse code modulated voice and data connections between PMs. ENET also provides message paths to the DMS-bus components.

File Transfer Protocol (FTP)

A software protocol that operates over the Internet or other wide area networks. When called, it connects to a specified server or site that is set up to utilize FTP protocol. Files and information are retrieved by the connecting server.

FTP

See File Transfer Protocol (FTP).

graphical user interface (GUI)

A display format that allows the user to choose commands, start programs, and see lists of files. A GUI is a visual metaphor which uses icons representing actual desktop objects for the user to access and manipulate with a pointing device

GUI

See graphical user interface (GUI).

HDBH

See high day busy hour (HDBH).

HDLC

See high-level data link control (HDLC).

high day busy hour (HDBH)

The hour with the highest business day traffic throughout the busy season.

high-level data link control (HDLC)

The channel by which high-level control messages from the central control are carried between the digital carrier module (DCM) and remote line modules (RLM).

integrated services digital network (ISDN)

A set of standards proposed by the CCITT to establish compatibility between the telephone network and various data terminals and devices.

Internet Protocol (IP)

The Internet Protocol is part of TCP/IP and is a connectionless OSI layer 3 routing commonly used to interconnect LANs (an internet). Each packet of data is routed independently through the network. The IP packets commonly can travel over LANs, X.25, frame relay virtual circuits, ATM or leased lines from the source to the destination. The IP routing function uses a protocol to determine the best route through the network to the destination.

IP

See Internet Protocol (IP).

IPLL

IP Local Loop (IPLL).

ISDN

See Integrated Services Digital Network.

ISDN line trunk controller (LTCI)

A peripheral module (PM) that combines the line group controller (LGC) and the digital trunk controller (DTC) and provides all the services offered by both. It also supports ISDN channeling.

International Telecommunications Union (ITU)

One of the organizations working on forming international standards for communication. ITU-T is the arm of ITU responsible for telecommunications standards.

ITU

See International Telecommunications Union (ITU).

LAN

See local area network (LAN).

LCM

See line concentrating module (LCM).

LEN

See line equipment number (LEN).

line concentrating module (LCM)

A peripheral module that connects the line trunk controller or line group controller and up to 640 subscriber lines using two to six DS30A links.

line test position (LTP)

A maintenance and administration position (MAP) terminal specially equipped for performing line tests.

line equipment number (LEN)

A seven-digit functional reference that identifies line circuits. The LEN provides physical location information on equipment such as site, frame number, unit number, line subgroup (shelf) and circuit pack.

local area network (LAN)

A network that permits the interconnection and intercommunication of multiple computers, primarily for sharing resources such as data storage devices and printers.

logical terminal identifier (LTID)

The unique identifier assigned to a logical terminal when datafilled in the ISDN access termination.

LTCI

See ISDN line trunk controller (LTCI).

LTID

See logical terminal identifier (LTID).

LTP

See line test position (LTP).

MAC

See medium access control (MAC).

MAP

See maintenance and administration position (MAP).

maintenance and administration position (MAP)

A group of terminals that are connected to one or more central office switches to monitor their status.

management information base (MIB)

A collection of objects that can be accessed using a network management protocol. In an SNMP-managed network, an MIB is a database of objects representing the characteristics and status of the managed devices.

MCU

See multipoint control unit (MCU).

MDC

See Meridian Digital Centrex (MDC).

medium access control (MAC)

In LANs, the sublayer of the data link control layer that supports medium-dependent functions and uses the services of the physical layer to provide services to the logical link control (LLC) sublayer. The MAC sublayer includes the method of determining when a device has access to the transmission medium.

Meridian Digital Centrex (MDC)

A special DMS business services package that uses the data handling capabilities of DMS-100 Family offices to provide a centralized telephone exchange service. (Formerly known as Integrated Business Network [IBN].)

MIB

See management information base (MIB).

multipoint control unit (MCU)

A device that enables more than two teleconference terminals to be connected. It can be located in a network or it can be considered as a part of terminal giving the possibility of multiple connections to the network.

network interface card (NIC)

A network adapter.

NIC

See network interface card (NIC).

OAM

See operations, administration, and maintenance

object identifier (OID)

A text or numeric string that identifies an object within a MIB tree.

OID

See object identifier (OID).

operations, administration, and maintenance

All the tasks necessary for providing, maintaining, or modifying the services provided by a switching system. These tasks include provisioning of hardware, creation of service, verification of new service, and trouble recognition and clearance.

PCI

See peripheral component interconnect (PCI).

PCM

See pulse code modulation (PCM).

PDC

See primary domain controller (PDC).

PDN

See public data network (PDN).

PEC

See product engineering code (PEC).

peripheral component interconnect (PCI)

A PC local bus, which runs at 33 MHz, and provides a high-speed connection of seven peripheral devices.

peripheral module (PM)

Any hardware module in the DMS-100 Family switches that provides an interface between external line, trunk, or service facilities. A PM contains peripheral processors, which perform local routines, thus relieving the load on the central processing unit (CPU).

peripheral side (P-side)

The side of a node facing away from the central control (CC) and toward the PM. *See also* central side (C-side.)

Ping

A protocol function in TCP/IP that tests the ability of a computer to communicate with a remote computer by sending a query and receiving a confirmation response.

PM

See peripheral module (PM).

primary domain controller (PDC)

A Windows NT service that manages security for its local domain. Every domain has one PDC, which contains a database of user names, passwords, and permissions. *See also* backup domain controller (BDC).

product engineering code (PEC)

An eight-character unique identifier for each marketable hardware item that Nortel Networks manufactures.

P-side

See peripheral side (P-side).

PSTN

See public switched telephone network (PSTN).

pulse code modulation (PCM)

A pulse code modulation can consist of one of the following:

- The process to convert an analog (voice waveform) to a digital code.
- A form of modulation in which the modulating signal is sampled, and the sample is quantified, coded, and sent as a bit stream.
- The representation of an analog waveform by coding and quantifying periodic samples of the signal, such that each element of information consists of a binary number representing the value of the sample.

public data network (PDN)

A communications common carrier network providing data communications services over switched or non-switched lines.

public switched telephone network (PSTN)

PSTN, the ordinary dial-up telephone system, refers to data or other non-telephone services carried over a path initially established using normal telephone signaling and ordinary switched long distance telephone circuits.

QoS

See quality of service (QoS).

quality of service (QoS)

The quality specification of a communications channel or system quantitatively indicated by channel or system performance parameters, such as signal-to-noise (S/N) ratio, bit error ratio, message throughput rate, and call blocking probability.

RAID

See redundant array of inexpensive disks (RAID).

RAM

See random access memory (RAM).

random access memory (RAM)

Memory where data can be written and read. A solid state memory device used for transient memory stores. Information can be entered and retrieved from any storage position.

RAS

See registration, admission, and status (RAS).

read-only memory (ROM)

Memory that can be read but not changed. Read-only memory is non-volatile storage; it holds its contents even after the power is off. Data is placed in ROM only once, and stays there permanently. ROM chips are used for storage of the essential software of the computer, called firmware.

Realtime Control Protocol (RTCP)

A companion protocol to RTP that maintains quality of service (QoS). RTP nodes analyze network conditions and periodically send each other RTCP packets that report on network congestion. *See also* RTP and User Datagram Protocol.

Realtime Transport Protocol (RTP)

An IP protocol that supports realtime transmission of voice and video. An RTP packet rides on top of UDP and includes timestamping and synchronization information in its header for proper reassembly at the receiving end. *See also* Realtime Control Protocol.

redundant array of inexpensive (or independent) disks (RAID)

The use of two or more disk drives instead of one disk, which provides better disk performance, error recovery, and fault tolerance. RAID also includes interleaved storage techniques and mirroring of important data.

remote method invocation (RMI)

A standard from Sun for distributed objects written in Java. RMI is a remote procedure call (RPC), which allows Java objects (software components) stored in the network to be run remotely.

registration, admission, and status (RAS)

A type of signaling defined by ITU-T Recommendation H.323. RAS signaling uses H.225 messages to perform registration, admission, status, bandwidth changes, and disengage procedures between endpoints and Gatekeepers.

request for comment (RFC)

A series of numbered international documents (RFC 822, RFC 1123, etc.) that sets standards which numerous software manufacturers in the Internet community follow.

RFC

See request for comment (RFC).

RMI

See remote method invocation (RMI).

ROM

See read-only memory (ROM).

RTCP

See Realtime Control Protocol (RTCP).

RTP

See Real Time Protocol (RTP).

SCSI

See small computer system interface (SCSI).

SCU

Service control unit (SCU).

Service Order System (SERVORD)

A user interface consisting of commands used to change, add, or delete subscriber lines. The format used for commands in the SERVORD complies with the standard telephone industry format; for example, 3WC is three-way calling; ADO is add option; DEL is delete, and CWT is call waiting.

SERVORD

See Service Order System (SERVORD).

Simple Network Management Protocol (SNMP)

The most popular and widely implemented management protocol. Typically, Simple Network Management Protocol (SNMP) is a request/reply protocol where a network management application polls server agents with data inquiries and the server agent replies. There are exceptions to polling when the server agent informs the network management system asynchronously of a change of state called a trap.

The SNMP defines the format of the requests and replies exchanged between the network management application and the server agent. The SNMP manages objects that are collected in a database called the Management Information Base or MIB. In the xEMS context, this is the protocol is used to communicate with the DBIC in order to manage it.

small computer system interface (SCSI)

A high-speed interface that can connect to computer devices, such as hard drives, CD-ROM drives, floppy drives, tape drives, scanners, and printers. A SCSI can connect up to seven devices; each one is given an identification number from 0 to 7, which is set with a manual switch. Newer versions of SCSI can connect up to 15 devices.

SNMP

See Simple Network Management Protocol (SNMP).

TCP

See Transmission Control Protocol (TCP).

TCP/IP

See Transmission Control Protocol/Internet Protocol (TCP/IP).

TDM

See time division multiplexing (TDM).

terminal identifier (TID)

An identifier internal to the Digital Multiplex System (DMS) family of switches that identifies specific terminal equipment involved in a call.

terminal processing task (TPT)

Call processing software located in the subscriber carrier module-100S remote (SMSR) master processor. The TPT receives and decodes central control (CC) call processing messages and then sends its own messages to other call processing software to have CC requests performed.

terminal proxy server (TPS)

A component of the Centrex IP product. Its software performs call control services for the i2004 Internet Telephone and resides on the Gatekeeper component.

TFTP

See Trivial File Transfer Protocol (TFTP).

TID

See terminal identifier (TID).

time division multiplexing (TDM)

A multiplexing technique (that is, the transmission of two or more signals at the same time over the same communications channel) in which the individual signals are combined by interleaving bits. Wide area networks use T-1 carriers for this technique.

TPS

See terminal proxy server (TPS).

TPT

See terminal processing task (TPT).

Transmission Control Protocol (TCP)

A data transport protocol that provides reliable, connection-oriented data delivery in the TCP/IP stack.

Transmission Control Protocol/Internet Protocol (TCP/IP)

A protocol stack, designed to connect different networks, on which the Internet is based.

Trivial File Transfer Protocol (TFTP)

A protocol used to download BOOTP files, similar to FTP, but without the security. TFTP uses User Datagram Protocol (UDP) instead of TCP.

UDP

See User Datagram Protocol (UDP).

User Datagram Protocol (UDP)

The UDP is the transport protocol used for packet delivery service. It is a lightweight protocol because it does not have the overhead of creating connections and verifying delivery.

virtual private network (VPN)

A network which has the appearance and functionality of a dedicated line. A VPN is really like a private network within a public network because the telephone company controls it, and all customers use its backbone trunks.

Voice over Internet Protocol (VoIP)

The technology that delivers voice information in digital form in discrete packets using IP rather than the traditional circuit-committed protocols of the PSTN. VoIP involves the conversion of voice from telephone format (analog) into a packet format (digital) that can be transported over an internet.

VoIP

See Voice over Internet Protocol (VoIP).

VPN

See virtual private network (VPN).

XMS peripheral module (XPM)

The generic name for PMs that use the Motorola 68000 microprocessor. An XPM has two processors in a hot-standby configuration: a master processor (MP) and a signaling processor (SP).

XPM

See XMS peripheral module (XPM).

DMS-100 Family

Centrex IP

Service Implementation Guide

Product Documentation-Dept. 3423
Nortel Networks
P.O. Box 13010
RTP, NC 27709-3010

electronic mail: cits@nortelnetworks.com

NORTEL NETWORKS CONFIDENTIAL: The information contained herein is the property of Nortel Networks and is strictly confidential. Except as expressly authorized in writing by Nortel Networks, the holder shall keep all information contained herein confidential, shall disclose the information only to its employees with a need to know, and shall protect the information, in whole or in part, from disclosure and dissemination to third parties with the same degree of care it uses to protect its own confidential information, but with no less than reasonable care. Except as expressly authorized in writing by Nortel Networks, the holder is granted no rights to use the information contained herein.

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

Publication number: 297-5231-021
Product release: CIPL0001
Document release: Standard 02.07
Date: October 2000
United States of America

NORTEL
NETWORKS™