



PRIMENET™
Planning and
Configuration Guide

Revision 22.0

DOC7532-4LA

Update Package
UPD7532-41A
July 1989

PRIMENET Planning and Configuration Guide

DOC7532-4LA

This Update Package, UPD7532-41A, is Update 1 for the Fourth Edition of the PRIMENET Planning and Configuration Guide, DOC7532-4LA. This package updates the book to Master Disk Revision 22.1. Pages that have been changed are listed on the next page.



UPD7532-41A

Prime Computer, Inc., Prime Park, Natick, MA 01760

Update Package, UPD7532-41A

Pages to change:

Replace Pages

i to xii
1-1 to 1-6
1-9 to 1-10
1-13
2-3 to 2-6
6-15 to 6-16
8-3 to 8-4
9-1 to 9-2
A-7 to A-8
GL-17 to GL-18
Index-1 to Index-7

With Pages

i to xii
1-1 to 1-6
1-9 to 1-10
1-13
2-3 to 2-6
6-15 to 6-16
8-3 to 8-4
9-1 to 9-2
A-7 to A-8
GL-17 to GL-18
Index-1 to Index-7

Add Pages

11-1 to 11-3



PRIMENET™ Planning and Configuration Guide




Fourth Edition

Andrew Shores

Updated by



Betsey Ruben



*This guide documents the software operation
of the Prime Computer and its supporting
systems and utilities as implemented at
Master Disk Revision 22.1 (Rev. 22.1).*

Copyright Information

The information in this document is subject to change without notice and should not be construed as a commitment by Prime Computer, Inc. Prime Computer, Inc. assumes no responsibility for any errors that may appear in this document.

The software described in this document is furnished under a license and may be used or copied only in accordance with the terms of such license.

Copyright © 1989 by Prime Computer, Inc., Prime Park, Natick, Massachusetts 01760

PRIME, PR1ME, PRIMOS, and the PRIME logo are registered trademarks of Prime Computer, Inc. 50 Series, 400, 750, 850, 2250, 2350, 2450, 2455, 2550, 2655, 2755, 2850, 4050, 4150, 4450, 6150, 6350, 6550, 9650, 9655, 9750, 9755, 9950, 9955, and 9955II, DISCOVER, PRIME/SNA, PRIME EXL, FM+, Prime INFORMATION EXL, PRIME MEDUSA, INFO/BASIC, EDMS, MIDAS, MIDASPLUS, PERFORM, PERFORMER, Prime INFORMATION, INFORM, PRISAM, PRIMAN, PRIMELINK, PRIMIX, Prime INFORMATION CONNECTION, PRIMENET, MDL, PRIMEWAY, PRODUCER, Prime INFORMATION/pc, PRIME TIMER, PRIMEWORD, RINGNET, SIMPLE, PT25, PT45, PT65, PT200, PT250, PST 100, PW153, PW200, and PW250, are trademarks of Prime Computer, Inc.

Printing History

First Edition (DOC7532-1LA) April 1984 for Revision 19.3

Second Edition (DOC7532-2LA) April 1985 for Revision 19.4

Third Edition (DOC7532-3LA) July 1987 for Revision 21.0

Fourth Edition (DOC7532-4LA) September 1988 for Revision 22.0

Update 1(UPD7532-41A) July 1989 for Revision 22.1

Credits

Editorial: Mike McNulty, Barbara Fowlkes, Mary Skousgaard

Design: Carol Smith

Project Support: Scott Sminkey, Clarise Patton, Jacki Forbes, Kathe Rhoades, Anita Horn

Illustration: Robert Alba

Document Preparation: Mary Mixon, Kathy Normington

Composition: Julie Cyphers, Anne Marie Fantasia

Production: Judy Gordon

How To Order Technical Documents

Follow the instructions below to obtain a catalog, a price list, and information on placing orders.

United States Only: Call Prime Telemarketing, toll free, at 800-343-2533, Monday through Friday, 8:30 a.m. to 5:00 p.m. (EST).

International: Contact your local Prime subsidiary or distributor.

Customer Support Center

Prime provides the following toll-free numbers for customers in the United States needing service:

1-800-343-2320

For other locations, contact your Prime representative.

Surveys and Correspondence

Please comment on this manual using the Reader Response Form provided in the back of this book. Address any additional comments on this or other Prime documents to:

Technical Publications Department
Prime Computer, Inc.
500 Old Connecticut Path
Framingham, MA 01701

About This Book	ix
1 PRIMENET Overview	1-1
PRIMENET Services	1-1
Types of PRIMENET Communications Lines	1-4
2 Installing PRIMENET Software	2-1
Installing Prime Network Products	2-1
Setting ACLs for PRIMENET, FTS, ISC, and NETLINK	2-2
Configuring DSM for LAN300 Network Management	2-5
3 PRIMENET Security	3-1
General Security Considerations	3-2
Node-to-node Access Rights	3-2
Non-Prime Node Access Rights Guidelines	3-6
Symmetry Requirements	3-6
Remote Naming	3-7
Node-to-node Passwords	3-8
Forced User Validation	3-9
Controlling Remote File Access	3-10
Controlling Remote Logins	3-12
Security Considerations With NETLINK	3-13
Half-duplex Passwords	3-13
Security Considerations Over a Gateway Link	3-14
Controlling Access From PSDNs and Dialup Terminal Lines	3-14
Security on Pre-Rev. 19.3 Nodes	3-16
4 PRIMENET Network Configuration	4-1
The Network Configuration File	4-1
Global Configuration	4-2

Using Different Configuration Files in the Same Network	4-3
CONFIG_NET Versus the NETCFG Utility	4-5
Specifying Addresses to CONFIG_NET	4-6
5 Preparing to Configure Your PRIMENET Network	5-1
Preparing for Configuration: Example One	5-1
Preparing for Configuration: Example Two	5-5
Configuration Checklist	5-9
6 Configuring Your PRIMENET Network	6-1
Invoking CONFIG_NET	6-2
Displaying Help Text	6-2
Using CONFIG_NET	6-3
Verification	6-4
Creating a Configuration	6-5
Defining the Network Topology	6-6
Providing Per-node Information	6-11
Editing a Configuration	6-27
Strategy for Adding Objects to a Configuration	6-43
Strategy for Modifying Objects in a Configuration	6-45
Strategy for Deleting Objects From a Configuration	6-49
Strategy for Changing Gateway Access	6-51
Special Editing Features	6-52
Displaying a Configuration	6-54
Saving and Validating a Configuration	6-55
Quickly Saving a Configuration	6-55
Terminating CONFIG_NET	6-56

7	Sample PRIMENET Configurations	7-1
	Create Mode Examples	7-2
	Edit Mode Examples	7-70
	List Mode Examples	7-108
8	Setting PRIMENET-related CONFIG Directives	8-1
	Summary of the PRIMENET-related CONFIG Directives	8-1
	Using the PRIMENET-related CONFIG Directives	8-2
	LHC	8-2
	NPUSR	8-2
	NRUSR	8-3
	NSLUSR	8-4
	REMBUF	8-4
	SYNC CNTRLR	8-5
9	Setting PRIMENET-related PRIMOS.COMI Commands	9-1
	START_DSM	9-1
	COMM_CONTROLLER	9-1
	START_NET	9-3
	ADDISK	9-4
	CAB	9-5
10	Configuring File Transfer Service	10-1
	Introduction	10-1
	FTS Access Rights	10-2
	FTSQ* Directory Size	10-3
	FTGEN Commands	10-3
	FTGEN Subcommands	10-4
	General FTGEN Commands	10-5
	Configuring File Transfer Servers	10-6

	Configuring File Transfer Queues	10-13
	Configuring Local and Remote Sites	10-18
	FTS Configuration Session	10-23
	Recovering From an Invalid Database	10-26
	Shutting Down FTS	10-27
11	Configuring NETLINK	11-1
	The NETLINK Configuration File	11-1
	Errors in the NETLINK Configuration File	11-2
A	CONFIG_NET Error Messages	A-1
	Glossary	GL-1
	Index	Index-1

About This Book

Purpose

The *PRIMENET Planning and Configuration Guide* explains how to plan, install, and configure a PRIMENET™ network and the optional File Transfer Service (FTS). Although it is written for Rev. 22.0 of PRIMENET, it does describe how to configure mixed-Rev. networks that contain nodes running older software.

Audience

This guide is for Network and System Administrators responsible for installing and configuring PRIMENET and FTS.

Organization

The *PRIMENET Planning and Configuration Guide* contains ten chapters, an appendix, and a glossary, which are summarized below.

Chapter 1 — PRIMENET Overview

Describes the PRIMENET services and types of transmission media, and provides guidelines to help you plan your network.

Chapter 2 — Installing PRIMENET Software

Provides procedures for installing PRIMENET, FTS, and the LAN300 Network Management Facility. Also lists the access rights required for network processes and explains how to protect the network-related directories.

Chapter 3 — PRIMENET Security

Describes PRIMENET's security system and explains how to protect data in various special situations.

Chapter 4 — PRIMENET Network Configuration

Explains when to create a global configuration file and when to use different configuration files in the same network. Also discusses PRIMENET addresses.

Chapter 5 — Preparing to Configure Your PRIMENET Network

Presents two examples of preparing for configuration, along with a checklist of questions you should answer before using CONFIG_NET, the PRIMENET configuration program.

Chapter 6 — Configuring Your PRIMENET Network

Explains how to use CONFIG_NET to create, edit, or display a PRIMENET configuration file.

Chapter 7 — Sample PRIMENET Configurations

Shows the CONFIG_NET dialog to create, edit, or list more than a dozen sample configurations, along with diagrams and explanatory notes.

Chapter 8 — Setting PRIMENET-related CONFIG Directives

Discusses how to set the PRIMENET-related directives in the system CONFIG file.

Chapter 9 — Setting PRIMENET-related PRIMOS.COMI Commands

Explains how to modify the PRIMOS.COMI file, which is executed during system coldstart.

Chapter 10 — Configuring File Transfer Service

Describes how to create the configuration file for File Transfer Service (FTS).

Chapter 11 — Configuring NETLINK

Describes how to create the NETLINK Configuration file.

Appendix A — CONFIG_NET Error Messages

Lists and explains the CONFIG_NET error messages.

PRIMENET Glossary

Defines PRIMENET terminology. These terms are printed in boldface type the first time they are described in the text.

Related Documentation

These documents provide related information:

- *User's Guide to Prime Network Services* (DOC10115-1LA)
- *Operator's Guide to Prime Networks* (DOC10114-1LA and its update, UPD10114-11A)

- *Programmer's Guide to Prime Networks* (DOC10113-1LA and its update, UPD10113-11A)
- *DSM User's Guide* (DOC10061-2LA)
- *NTS Planning and Configuration Guide* (DOC10159-1LA and its update, UPD10159-11A)
- *NTS User's Guide* (DOC10117-2LA)
- *PRIMOS TCP/IP Guide* (DOC10155-3LA)
- *PRIMOS User's Guide* (DOC4130-5LA)
- *ICS User's Guide* (DOC10094-1LA and its update, UPD10094-11A)
- *System Administrator's Guide, Volume I: System Configuration* (DOC10131-2LA)
- *System Administrator's Guide, Volume II: Communication Lines and Controllers* (DOC10132-2LA)
- *System Administrator's Guide, Volume III: System Access and Security* (DOC10133-2LA)
- *Subroutines Reference V: Event Synchronization* (DOC10213-1LA)
- *Operator's Guide to System Commands* (DOC9304-4LA)
- *System Administrator's Guide, Rev. 19.0* (DOC5037-190)
- *PRIMENET Guide, Rev. 19.0* (DOC3710-190)

The following chart shows where to find the information you need in the Prime networks document set. There is a column for each network product and a row for each functional activity. For example, to find information on monitoring and controlling PRIMENET, refer to the *Operator's Guide to Prime Networks*.

	PRIMENET	NTS	WSI300
Configuration	PRIMENET Planning and Configuration Guide	NTS Planning and Configuration Guide	
Installation		LTS300 Installation Guide	PRIMOS TCP/IP Guide
Monitoring and Control	Operator's Guide to Prime Networks		
Using the Software	User's Guide to Prime Network Services	NTS User's Guide	
Programming	Programmer's Guide to Prime Networks		

Prime Documentation Conventions

The following conventions are used in command formats, statement formats, and in examples throughout this document. Examples illustrate the uses of these commands and statements in typical applications.

<i>Convention</i>	<i>Explanation</i>	
UPPERCASE	In command formats, words in uppercase indicate the names of commands, options, statements, and keywords. Enter them in either uppercase or lowercase.	CONFIG_NET
lowercase	In command formats, words in lowercase indicate variables for which you must substitute a suitable value.	PASSWORD password
Abbreviations in format statements	If an uppercase word in a command format has an abbreviation, either the abbreviation is underscored or the name and abbreviation are placed within braces.	<u>LOGOUT</u> {SET_QUOTA} SQ}
Brackets []	Brackets enclose a list of one or more optional items. Choose none, one, or more of these items.	LD [-BRIEF -SIZE]
Braces { }	Braces enclose a list of items. Choose one and only one of these items.	CLOSE {filename ALL}
Braces within brackets [{ }]	Braces within brackets enclose a list of items. Choose either none or only one of these items; do not choose more than one.	BIND [{pathname options}]
Vertical bars 	Vertical bars enclose a list of two or more options. Choose one or more of these options.	OUTPUT filename TTY
Ellipsis ...	An ellipsis indicates that the preceding item may be entered more than once on the command line.	SHUTDN pdev-1 [...pdev-n]

<i>Convention</i>	<i>Explanation</i>	
Hyphen —	Wherever a hyphen appears as the first character of an option, it is a required part of that option.	LIST -SITE -ALL
<i>Bold italics</i> in examples	In examples, user input is in bold italics but system prompts and output are not.	Option: 2
<i>Italics</i> in messages	In messages, text in italics indicates a variable for which the program substitutes the appropriate value.	Unknown PSDN: <i>name</i>

PRIMENET Overview

This chapter summarizes **PRIMENET**'s major services and briefly describes the various types of communication lines that you can configure.

For complete information on PRIMENET's services and how to use them, and for a full description of communication lines, refer to these guides:

- *User's Guide to Prime Network Services*
- *Operator's Guide to Prime Networks*
- *Programmer's Guide to Prime Networks*

PRIMENET Services

PRIMENET includes five major services:

- Remote login
- The NETLINK utility
- File Transfer Service (FTS), a separately priced product
- Remote File Access (RFA)
- The Interprocess Communications Facility (IPCF)

These services allow users to access and process files that reside on remote nodes, transfer files between nodes, and log in to remote nodes. In most cases, PRIMENET makes network usage completely transparent to users and applications. For example, users can attach to directories on remote nodes as though the directories were on a local disk.

Remote Login

PRIMENET's **remote login** service allows users to log in to a remote node from a local terminal without logging in to the local node first. To do this, the user issues the **LOGIN** command with the **-ON** option, followed by the name of the remote node. For example,

```
LOGIN -ON SYSA
```

For further information on the LOGIN command format, refer to the *User's Guide to Prime Network Services* or the *Prime User's Guide*.

Remote login works only when the following two conditions are met:

- The two nodes are connected by a network path, either directly, or through one or more **gateway nodes**.
- The remote login access right is assigned between the two nodes in the PRIMENET configuration file. (Access rights are assigned in the PRIMENET configuration file with CONFIG_NET, the PRIMENET configuration program.)

For example, if users on Node A are to log in to Node B, you must assign Node A remote login access to Node B. In some cases, you may want to assign remote login access symmetrically, so that users on each of two nodes can log in to the other node.

In the sample configuration shown in Figure 1-1, users on Node A can log in to Node C. In this case, remote login access is assigned as part of the **gateway access** from Node A to Node C.

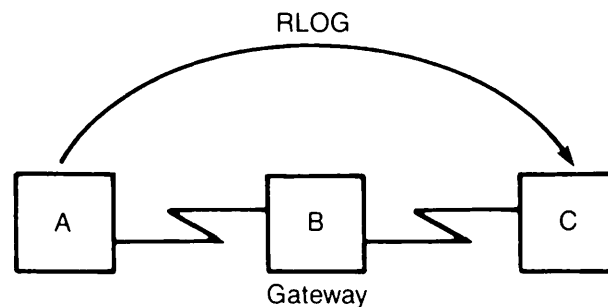


Figure 1-1
Remote Login

In all cases, a user must have a valid user ID on the remote node in order to log in there. On a given node, the NRUSR directive in the CONFIG file determines the maximum number of remote users that can be connected at a time. (The NRUSR directive is discussed in Chapter 8, Setting PRIMENET-related CONFIG Directives.)

NETLINK Utility

PRIMENET's **NETLINK** utility allows the user to:

- Log in to any Prime node that is part of a PRIMENET network.
- Gain terminal access to any node (Prime or non-Prime) across a PSDN if that node adheres to the **CCITT Packet Assembler/Disassembler (PAD)** protocols: **X.3**, **X.28**, and **X.29**.
- Control X.3 (terminal) parameters to tailor terminal handling characteristics.
- Have up to six concurrent remote login sessions on the same or different nodes.
- Switch between concurrent remote login sessions without logging out.
- Transfer files between Prime and non-Prime nodes. File transfers between two Prime nodes are generally accomplished with either the **COPY** command (which uses PRIMENET's Remote File Access (RFA) services) or File Transfer Service (FTS).

To enable NETLINK between two Prime nodes, you must use **CONFIG_NET** to assign IPCF access rights between the nodes. You must also ensure that the **NRUSR CONFIG** directive is set to a value greater than zero on the remote node. For more information on NRUSR, refer to Chapter 8, Setting PRIMENET-related CONFIG Directives. NETLINK's remote login facility works even if remote login access is not configured between the communicating nodes. Refer to Chapter 3, PRIMENET Security, for more information.

Remote File Access (RFA)

PRIMENET's **Remote File Access (RFA)** method allows users and application programs to access files on remote nodes as though the files were local. For example, remote files can be copied, edited, and otherwise manipulated exactly as if they resided on the local node. The user or application sees no difference between attaching to a directory on the local node and attaching to a directory on a remote node.

Remote File Access is enabled by assigning RFA access between nodes during network configuration. It is implemented internally with the **Network Process Extension (NPX)** facility. RFA works as follows:

1. A process requests access to a file on another node. This process is called a **master**.
2. On the node being accessed, the call is received by a process called an **NPX slave**. A slave is a phantom that is dedicated to receiving calls from masters on remote nodes.
3. The slave performs the requested operation on its node, returning data to the master.

All of this is transparent to the user.

On each node in the network, the **System Administrator** uses the **NSLUSR CONFIG** directive to configure the number of slaves allowed on a system. The System Administrator must also use the **ADDISK** command on the local system to indicate the location of the remote disk to be

accessed by RFA. Otherwise, PRIMENET cannot "see" the remote disk. For more information on CONFIG directives, see Chapter 8, Setting PRIMENET-related CONFIG Directives, or the *System Administrator's Guide, Volume I: System Configuration*.

File Transfer Service (FTS)

File Transfer Service (FTS) is a separately priced product that transfers files between networked Prime nodes. FTS is an alternative to the PRIMOS® COPY command, which uses PRIMENET's Remote File Access method to copy files between Prime nodes.

A major advantage of FTS over the COPY command is that FTS can transfer files to or from a disk that your node cannot access through Remote File Access. Furthermore, you can submit a file transfer request to FTS even if the remote node involved (or the line to it) is down. FTS holds the request in a queue until the transfer can be performed. You can direct FTS to create a log of the transfer and to notify the sender and/or receiver of the transfer.

The Network Administrator and/or the System Administrator is responsible for several tasks regarding FTS; for example, assigning ACL rights to the FTS servers and using the FTGEN utility to configure the FTS system. These tasks are described in Chapter 2, Installing PRIMENET Software, Chapter 3, PRIMENET Security, and Chapter 10, Configuring File Transfer Service.

Information on how to transfer files with FTS is also included in the *User's Guide to Prime Network Services*. The *Operator's Guide to Prime Networks* explains how to monitor and control FTS.

Interprocess Communications Facility (IPCF)

Interprocess Communications Facility (IPCF) is a set of subroutines that can be called from application programs. With these subroutines, users can establish connections and pass data over them, using the industry-standard X.25 protocol. A user can, for example, develop an application that consists of several different modules, with each module running as a separate user on a different node. The modules can then exchange data across the network. IPCF subroutines are designed to run on 50 Series™ CPUs in V-mode, I-mode, or IX-mode only. Note that nodes must have IPCF access to each other in order to use IPCF subroutines. All network access rights are assigned with the CONFIG_NET program, which is described in Chapter 6, Configuring Your PRIMENET Network. For information on using the IPCF routines, refer to the *Programmer's Guide to Prime Networks*.

Types of PRIMENET Communications Lines

The first part of network configuration is defining the network topology, that is, defining the types of communications lines used in your network and the nodes to which they are connected. Each type of physical transmission medium in a network is called a **subnetwork**. For example, a network might contain a half-duplex subnetwork, a RINGNET™ subnetwork, and two LAN300

subnetworks. CONFIG_NET, the PRIMENET configuration program, helps you to define your network's topology by asking you a series of questions at the beginning of the configuration session. This section describes the types of subnetworks over which PRIMENET can run.

Systems in a PRIMENET network can be connected by one or more of the following means:

- Ring network (RINGNET)
- IEEE 802.3 Local Area Network (LAN300)
- Full-duplex synchronous line
- Half-duplex synchronous line
- Packet Switching Data Network (PSDN)
- Gateway node

In the case where two nodes are connected by more than one subnetwork, PRIMENET attempts communications based on this priority order:

1. RINGNET
2. First LAN300 in the configuration connecting the nodes
3. Second LAN300
4. Synchronous lines
5. PSDN

Whether you are setting up your own network or joining an existing one, your Customer Support Center can help you decide which types of lines to use. Your decision will be influenced by factors such as cost, available hardware, the distance between nodes, expected frequency of network use, and, in the case of an existing network, the types of lines already in use in the network. You need to know whether any of the nodes on your network are connected to PSDNs, which nodes (if any) use leased lines to communicate, and so on.

All of PRIMENET's services operate in exactly the same way over any type of line. Any differences are handled at the hardware and protocol levels. Thus, the type of line is transparent to users. However, network programmers can specify line type when establishing a virtual circuit with certain IPCF subroutines. For more information, refer to the *Programmer's Guide to Prime Networks*.

The PRIMENET Ring Network (RINGNET)

A PRIMENET ring network (RINGNET) is a **Local Area Network (LAN)** composed of computer systems that are connected by twin-axial cable in a ring configuration. Each system is logically connected to all other systems on the ring. A token circulates around the ring, in one direction, at a rate of 10 megabits per second. (Data throughput will be lower.) If one node is disabled for any reason, the rest of the ring is not affected as long as the distance between *active* nodes does not exceed 750 feet (3280 feet if a RINGNET repeater is used).

On the hardware level, RINGNET is controlled by the **PRIMENET Node Controller (PNC or PNC II)**. All the nodes in the ring must be in close physical proximity because of the nature of the electrical connection. The maximum distance between any two adjacent active nodes is 750 feet, unless a RINGNET repeater is used. The use of a **repeater** can increase this distance up to 3280 feet, or 1 kilometer.

Each node on a ring must be assigned a **ring node ID**, which is a number from 1 through 247 that uniquely identifies the node. Ring node IDs are assigned during network configuration.

IEEE 802.3 Local Area Networks (LAN300s)

IEEE 802.3 Local Area Networks (**LAN300s**) are a new bus-based transmission medium that supports PRIMENET. All PRIMENET services run unchanged on LAN300s, including Remote Login, NETLINK, Network Process Extension (NPX) facility, and Interprocess Communications Facility (IPCF) except for minor differences in IPCF subroutines to accommodate differences in the physical transmission medium. (These differences are explained in the *Programmer's Guide to Prime Networks*.) As many as 256 PRIMENET nodes can be attached to each LAN300.

PRIMENET and **Network Terminal Service (NTS)** can run concurrently on the same LAN300 and hosts. (A LAN300 can be dedicated solely to NTS as well.) NTS is a separate network product that allows large numbers of terminals to communicate with any host on the network; it does not support host-to-host communications. NTS terminals are attached to **LAN Terminal Server 300s (LTS300s)** instead of hosts. NTS also supports TCP/IP for PRIMOS, a product that allows communications between 50 Series hosts, other Prime hosts, and non-Prime systems running a TCP/IP (Transmission Control Protocol/Internet Protocol) product. A fourth product, the LAN300 Network Management Facility, provides service functions to the LAN300. These functions are LHC300 downline load and upline dump, LTS300 downline load, error and event reporting, statistics gathering, status commands, and a diagnostic loopback capability.

NTS has its own configuration file, created with CONFIG_NTS. Although NTS and PRIMENET and their configurations are completely separate and do not share the same database, you should use the host name given by the SYSNAM CONFIG directive in both configurations. For consistency and to avoid confusion, you should use the same names for LAN300s and **LAN Host Controller 300s (LHC300s)** in both configuration files, where applicable. LHC300s are the controller boards that connect 50 Series hosts to a LAN300; they are described further under LAN300 Topology in this chapter. For complete information on NTS configuration, refer to the *NTS Planning and Configuration Guide*.

LAN300 Topology: Most LAN300 networks consist of one or more 500-meter segments of coaxial cable, joined by local or remote repeaters. A local repeater is a single microprocessor-based box that connects two cable segments, making a segment as long as 1000 meters. A **remote repeater** consists of two microprocessor-based boxes joined by a fiber optic cable that can be as long as 1000 meters.

A **LAN Multiport Transceiver 300 (LMT300 or fanout unit)** allows a maximum of sixteen hosts to be attached to a cable segment via the same cable tap. (Two multiport units can be cascaded, or cabled to each other. Each unit supports eight hosts.) Taps are also called **medium access units**, or MAUs. Alternately, LMT300s allow a maximum of sixteen hosts to be connected into a network that does not contain a coaxial cable at all. Such a network is a cableless LAN300.

A **LAN Host Controller 300 (LHC300)** is a controller board that plugs into the backplane of a 50 Series computer. This board connects the Prime host to a cable tap or multiport unit. LHC300 configuration information includes the LHC300 name, the host in which it is inserted, and the LAN300 to which it is attached.

A **LAN Terminal Server 300 (LTS300)** is a terminal server for Network Terminal Service (NTS) that supports up to eight terminals, serial printers, or other asynchronous devices.

Non-Prime hosts running software conforming to the **International Organization for Standardization (ISO) DP8880/2** standard can exchange packets with Prime hosts over a LAN300. ISO DP8880/2 specifies X.25 1984 running on Logical Link Control Level 2 (LLC2). Configuration of a non-Prime host entails giving its Media Access Control (MAC) and Link Service Access Point (LSAP) address, specifying the highest logical channel number that can be used for virtual circuits, setting the default window and packet sizes, and indicating the restart procedures used by the host.

LAN300 Configuration Guidelines: Observe the following general guidelines when deciding on the topology of your LAN300 networks. Figure 1-2 is a sample LAN300 network topology that illustrates many of these guidelines.

- A single local repeater provides a maximum node separation of 1000 meters, because it connects two 500-meter (maximum) segments. An example is the separation of NodeA and NodeF in Figure 1-2.
- A remote repeater allows for a maximum of 2000 meters between two nodes, as illustrated by NodeD and NodeJ in Figure 1-2. This is because a remote repeater consists of two boxes separated by a 1000-meter (maximum) fiber optic cable, with each box also attached to a 500-meter (maximum) cable segment.
- There can be a maximum of two repeaters of any type between any two nodes in the network. The maximum distance between nodes in a network, 3500 meters, is achieved by combining two remote repeaters and three cable segments.
- The maximum length of a coaxial cable segment is 500 meters. It can contain as many as 100 MAUs, spaced at least 2.5 meters apart.
- A LAN300 can contain as many as 1024 nodes, but a maximum of 256 of them can be running PRIMENET.
- A Prime host can be connected to a maximum of seven local area networks. There are also limits for each type of network: it can be connected to as many as two LAN300s running PRIMENET, four LAN300s running NTS, two LAN300s running WSI300, and only one RINGNET network. (The combined maximum number of NTS and WSI300 networks is four.) Of course, the number of networks a host can support

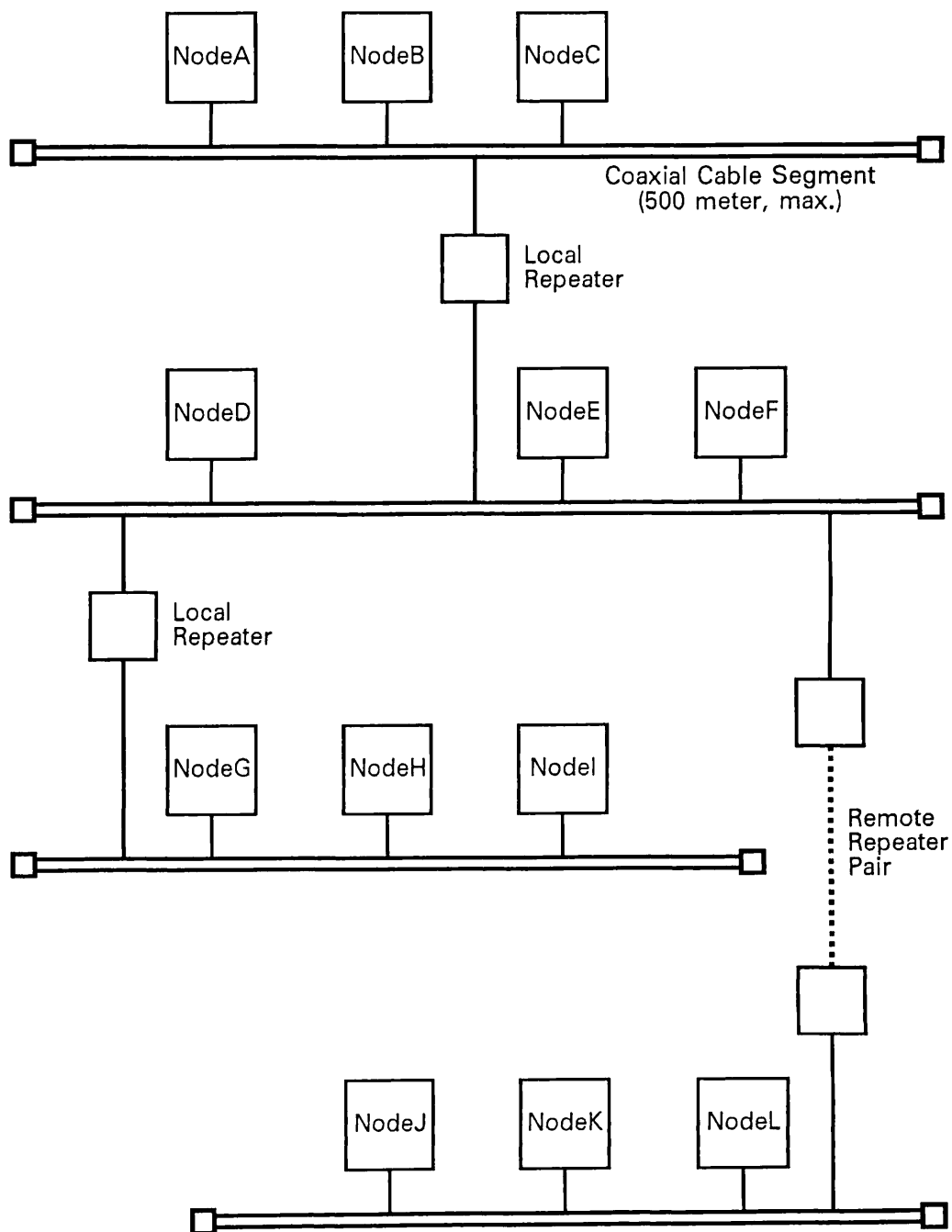


Figure 1-2
Sample LAN300 Network Topology

depends on its CPU size and the number of board slots available in its backplane. (In the maximum configuration of seven local area networks, there would be a separate controller board for each network.)

- A maximum of seven network controller boards can be inserted into the backplane of a Prime host. This can include one PRIMENET Node Controller (PNC or PNC II) for RINGNET and as many as six LHC300s. A maximum of two of these LHC300s can run PRIMENET, as many as four can run NTS, and as many as two can run WSI300.
- Although you can run NTS and PRIMENET concurrently on an LHC300, this limits the number of NTS connections to 32. In addition, both networks count toward the maximum number of networks for the host. For example, a host with two LHC300s running NTS and PRIMENET concurrently could have at most two more LHC300s running only NTS and one PNC for RINGNET.
- TCP/IP for PRIMOS requires a dedicated LHC300; it cannot be run concurrently on an LHC300 with any other product. There can be a maximum of two LHC300s in a host running TCP/IP for PRIMOS; they can be connected to the same or different LAN300s.
- As many as four LHC300s running NTS can be connected to the same LAN300 (or different LAN300s), but each LHC300 in the host running PRIMENET must be connected to a different LAN300.

Multiple LAN300s

There are occasions when you might want to divide your machine population into multiple LAN300 networks. One reason might be to improve network performance by dividing one large overused LAN300 network into smaller networks of machines that frequently communicate with each other. If you plan to use both PRIMENET and NTS, you could run PRIMENET on one LAN300 and NTS on the other. This would result in better network performance than if you ran both products concurrently on the same LAN300. Additionally, a separate LAN300 for NTS would allow more NTS users to be connected to the host at the same time — 128 NTS users per LHC300 dedicated solely to NTS.

Another reason for creating multiple LAN300s is to improve security. You could restrict access to sensitive machines by placing them on a separate LAN300.

A third reason is to provide a highly reliable connection between your computers by installing two separate LAN300s between machines. This would improve reliability but not performance because PRIMENET currently does not provide load balancing between multiple LAN300s. When two nodes are connected by alternate routes, PRIMENET attempts communications across the routes based on the priority order listed in the section entitled Types of PRIMENET Communications Lines in this chapter. In the case of multiple LAN300 routes, PRIMENET first attempts communications on the first one listed in the configuration file.

Full-duplex Synchronous Lines

In a PRIMENET environment, a **full-duplex synchronous line** is a dedicated, leased line between two Prime nodes, between a Prime node and a PSDN, or between a Prime node and a non-Prime node running X.25 1984 software. Full-duplex PRIMENET lines are permanent links between the nodes they connect, and they cannot be reallocated for purposes other than PRIMENET while PRIMENET is running.

PRIMENET's full-duplex synchronous lines use CCITT X.25 Level 2 protocol with either **High-speed Data Link Control (HDLC)** or **Binary Synchronous Communications (BSC)** character framing (ASCII or EBCDIC). Your Prime Customer Support Center can help you determine which type of framing to use. In general, we recommend HDLC with **Link Access Protocol Balanced (LAPB)** because it is becoming the preferred standard.

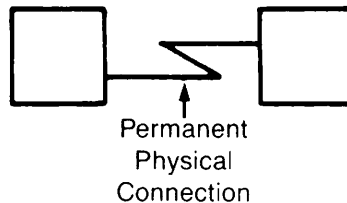


Figure 1-3
Full-duplex PRIMENET Line

Half-duplex Synchronous Lines

PRIMENET's **half-duplex (HDX)** synchronous lines are temporary dialup telephone connections between Prime nodes. A node that has a half-duplex line can use the line to call other nodes, just as you can use a telephone to call different people. Figures 1-3 and 1-4 illustrate the differences between full-duplex and half-duplex lines.

A half-duplex line is a connection over which data travels in only one direction at a time. This type of communication contrasts with the full-duplex mode, where both nodes can send and receive signals at the same time.

A half-duplex PRIMENET connection between two nodes is made when the calling node dials out on one of its half-duplex lines and the receiving node accepts the call on one of its half-duplex lines. A modem is required at each end of the connection.

At each end of a half-duplex PRIMENET link, system operators enter commands to make and break the connection. If a node expects an incoming call, the operator readies a line to receive the call by starting it up in **passive mode**. To make a call, an operator starts up a half-duplex line in **active mode** and dials a remote site. Once a call is successfully answered, the connection functions just like any other PRIMENET link. When communication is complete, an operator may break the connection. Thus, a half-duplex PRIMENET connection exists only for the duration of the phone call between two nodes.

When you configure your network, CONFIG_NET asks you to list all the network's half-duplex nodes. A half-duplex node is a node that has one or more half-duplex PRIMENET lines. Each

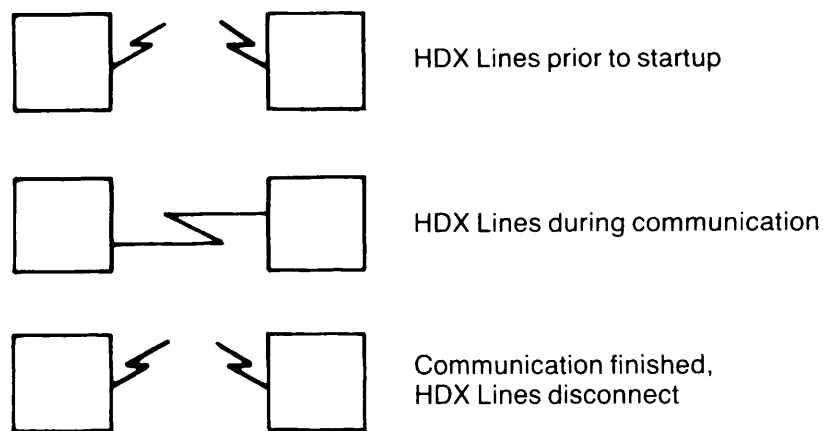


Figure 1-4
Half-duplex PRIMENET Line

half-duplex node can call any other half-duplex node as long as the appropriate access rights are configured between the nodes. The half-duplex nodes and their half-duplex lines make up the network's half-duplex subnetwork.

PRIMENET's half-duplex communication uses **BSC-ASCII framing**. Half-duplex lines are supported by MDLC (Multiline Data Link Controller) and ICS3 (Intelligent Communications Subsystem 3) controllers.

Operator commands to control and monitor half-duplex lines are described in the *Operator's Guide to Prime Networks*.

Synchronous Line Restrictions

The following rules govern the use of half-duplex and full-duplex synchronous lines in a PRIMENET network:

- A maximum of three synchronous lines can be active on a system at a time. Thus, if your system has more than three synchronous lines configured, you can only use three of them at a time for PRIMENET communications.
- Only one full-duplex line at a time can be active between two nodes.
- A node and a PSDN cannot have more than one full-duplex point-to-point synchronous line active at a time.

- A node may be connected to no more than two different PSDNs. If a node is connected to two different PSDNs, a different full-duplex line must be used for each connection.
- Only one half-duplex connection at a time can be active between two nodes.

Packet Switching Data Networks (PSDNs)

Any Prime system with PRIMENET and the X.25 option can be connected to one or two different **Packet Switching Data Networks (PSDNs)**. PSDNs connect Prime systems with both Prime and non-Prime systems. Connections to PSDNs are made over full-duplex synchronous lines; these lines are supported on the following controllers:

- MDLC
- ICS1 (Rev. 19.3 and later)
- ICS2 (Rev. 20.0 and later)
- ICS3 (Rev. 20.1 and later)

Each network node that has access to a PSDN is assigned one or more PSDN addresses by the **PSDN Administrator**. You need to know the PSDN addresses of the nodes on your network when you configure the network.

PRIMENET currently supports many PSDNs around the world. Call your Prime Customer Support Center for more information.

International Communications Over Packet Switching Data Networks

If your network is to be used for international communications, for example, from the U.S. to France, you may not be able to use Remote File Access (RFA). Network congestion and X.25 facilities handling through an international PSDN gateway can interfere with RFA. Since FTS provides strong error-recovery capabilities, you should use it to transfer data through an international PSDN gateway.

Gateway Nodes

At Rev. 19.3 and later, two Prime nodes can be connected by a series of intermediate nodes rather than by a direct link. A connection over a chain or path of direct links is called a **route-through** connection or a **gateway** connection. Each intermediate node, or **gateway node**, runs a process called the **Route-through Server**.

The Route-through Server routes data through the gateway nodes from the originating node to the destination node. For each route-through connection, the server allocates the necessary virtual circuits and transparently passes the data to the next node on the path to the destination

node. Although the route-through process is transparent to the user, the Route-through Server can be monitored by the system operator, as described in the *Operator's Guide to Prime Networks*.

When you configure a network, you can define the following nodes:

- Gateway nodes
- Nodes that have access to other nodes through a gateway connection

The Route-through Server uses this information to determine the route from the sending node to the receiving node.

Guidelines for Using Gateway Service

The Route-through Server uses two virtual circuits for every route-through user. This reduces the number of virtual circuits available for remote users and slaves on a gateway node. If the number of route-through users on a gateway node exceeds 82, the attempt to place the route-through call will be rejected.

When implementing route-through on your network, use the following guidelines:

- Configure no more than two intermediate gateway nodes.
- Configure only one route-through path between two nodes. Alternate routing is not supported.
- Do not configure Remote File Access (RFA) across a gateway node.
- Configure only one gateway node between a node and a PSDN connection.
- If a route-through path includes a PSDN, the PSDN must support subaddressing or multiple addresses per PSDN line.
- If a route-through path on your network includes a PSDN, you can access only those nodes on the PSDN whose names and addresses you include in the network configuration file.

Generally, route-through service is best used for the low throughput and low response time requirements of remote login, NETLINK, and FTS.

Applications using IPCF subroutines should not use fast select calls when making a connection across a gateway node running pre-Rev. 21.0 PRIMENET. (Rev. 21.0 PRIMENET *does* support fast select calls across gateway nodes.) For more information, refer to the *Programmer's Guide to Prime Networks*.

Installing PRIMENET Software

This chapter explains how to install Prime network products. It also outlines the Access Control List (ACL) rights you must assign to the network server processes so that they can operate properly. The information covered includes:

- Installing Prime network products
- Setting ACLs for PRIMENET, FTS, and ISC
- Configuring DSM for LAN300 Network Management

Installing Prime Network Products

Prime provides a set of CPL and command files for installing network products on a system. If your network includes a LAN300, run `NETWORK_MGT.INSTALL.CPL`. To install File Transfer Service, run `FTS.INSTALL.COMI`, which installs the files described in the section entitled Contents of the FTSQ* Directory, later in this chapter. To install PRIMENET, run `PRINET.INSTALL.COMI`. This command file installs the files described in the next section, Contents of the PRIMENET Directory.

Contents of the PRIMENET Directory

PRIMENET* is a top-level directory that must exist on the system disk (on the COMDEV pack) at system startup. This directory contains all files needed to run PRIMENET; these files are used by the network servers during the startup and operation of PRIMENET. Remote File Access (RFA) slaves also use the PRIMENET* directory. The PRIMENET* directory must contain the following files and be accessible to network servers in order for the servers to run properly:

- `SLAVE.COMI`, a command input file that initiates the startup of slaves on the system.
- `NETWORK_SERVER.COMI` and `NETMAN.SAVE`, files that `START_NET` runs to initialize NETMAN, the PRIMENET server process that is described in the next section.
- `ISCNSR.CPL`, a file that `START_NET` runs to initialize the ISC network server, `ISC_NETWORK_SERVER`. The ISC network server supports remote ISC; that is, ISC sessions conducted over PRIMENET.

- ISC_NETWORK_SERVER.RUN, the program executed by the ISC network server.
- PRIMENET.CONFIG, the default name of the PRIMENET configuration file. (PRIMENET* is the default directory; the PRIMENET configuration file can be stored elsewhere.)
- RT.COMI and RT_SERVER.SAVE, files that initialize the Route_Through server if the node is configured as a gateway node.

Contents of the FTSQ* Directory

The FTSQ* directory contains the following files:

- FTS database files
- Log files of user requests
- *server_name*.LOG, which contains startup and shutdown messages from the file transfer server phantom
- FTP.SEG, an executable file for the file transfer server phantom processes
- FTS help files
- All FTS run-time files and directories

Contents of the DSM* Directory

If your node is running Distributed Systems Management (DSM), the DSM* directory must contain DSM*>LOGS>NETWORKS>NETWORK.LOG, the default name of the network log file. (This file is described in the *DSM User's Guide*.)

Setting ACLs for PRIMENET, FTS, and ISC

This section describes the ACL settings and ACL groups required for PRIMENET, FTS, and ISC to operate correctly. It contains this information:

- PRIMENET-related ACL Settings
- ISC-related ACL Settings
- FTS-related ACL Settings
- LAN300 Network Management ACL Group
- Summary of PRIMENET-related ACL Settings

PRIMENET-related ACL Settings

This section specifies the Access Control List (ACL) rights that you must assign to certain processes and users on your system in order for PRIMENET to work correctly. These processes and users, which are listed below, allow systems in a network to interact with each other. All of the network-related ACL settings, including those required for FTS, are summarized in the section entitled Summary of PRIMENET-related ACL Settings, later in this chapter.

- Network Server Process (NETMAN)
- Supervisor Terminal Process (SYSTEM)
- The Route-through Server (RT_SERVER)

NETMAN: Network activity is handled by a network server process called NETMAN. NETMAN appears on the STATUS USERS list as an NSP (Network Server Process). NETMAN does not have to be registered in the user validation file. However, NETMAN comes from the system pool of phantom processes, so your system must have at least one phantom available for NETMAN's use. The NPUSR CONFIG directive sets the number of phantom processes on a system; for more information, refer to Chapter 8, Setting PRIMENET-related CONFIG Directives.

If NETMAN does not have UR access rights to PRIMENET*, the network does not start up. This is because NETMAN either does not start up or starts up and logs out, or because START_NET cannot bring up PRIMENET. When PRIMENET fails to startup, PRIMOS displays the message Network Server logged out during network startup on the supervisor terminal.

Supervisor Terminal Process (SYSTEM): The supervisor terminal process (SYSTEM) must have ALURWX access to PRIMENET*. SYSTEM also needs Read access to the PRIMENET configuration file, which is named PRIMENET.CONFIG by default. (Your configuration file might have a different name.)

System or Network Administrator: The System Administrator or Network Administrator must have Write access to the PRIMENET configuration file and ALL access to PRIMENET*.

Route-through Server (RT_SERVER): The Route-through Server (RT_SERVER) is a process that allows a system to act as a "gateway" for communication between nodes not directly connected through a ring, PSDN, or synchronous line. RT_SERVER does not have to be registered in the user validation file. However, RT_SERVER comes from the system pool of phantom processes, so if your system is a gateway node, you must have at least one phantom available for RT_SERVER's use. The NPUSR directive in your system's CONFIG file sets the number of phantom processes. For more information, refer to Chapter 8, Setting PRIMENET-related CONFIG Directives.

You must give RT_SERVER UR access rights to the PRIMENET* directory.

NETLINK: All NETLINK users must have U access to PRIMENET*, UR access to PRIMENET*>NETLINK to be able to read the NETLINK Configuration file, and UR access to PRIMENET*>SIT_TEXT_DBS to be able to read NETLINK's text message files. This is done by setting \$REST:U for PRIMENET* and \$REST:UR for PRIMENET*>NETLINK and PRIMENET*>SIT_TEXT_DBS. The System Administrator or Network Administrator must have ALL access to PRIMENET*>NETLINK and W (write) access to NETLINK.CONFIG in that directory.

SLAVE\$: Give SLAVE\$ UR access to PRIMENET*.

\$REST: Give \$REST U access to PRIMENET*.

ISC-related ACL Settings

In order for remote ISC to operate properly, you must ensure that the ISC Network Server, ISC_NETWORK_SERVER, is assigned ALL ACL rights to the PRIMENET*>JOURNALS directory and U (at least) ACL rights to PRIMENET*.

FTS-related ACL Settings

In order for FTS to operate properly, you must ensure that these processes are assigned appropriate ACL rights to the FTSQ* directory:

- YTSMAN, the file transfer manager
- The file transfer servers

YTSMAN: YTSMAN, the file transfer manager, must have ALL access rights to the FTSQ* directory.

File Transfer Servers: The file transfer server(s) must have ALL access rights to the FTSQ* directory in order for File Transfer Service to operate. A maximum of eight file transfer servers may be configured and named during the FTOP operation. Furthermore, users and the FTS servers need certain access rights to source and destination directories; these rights are described in Chapter 10, Configuring File Transfer Service.

LAN300 Network Management ACL Group

If your network includes a LAN300, use EDIT_PROFILE to create an ACL group called .NETWORK_MGT\$ and include the appropriate network operators and administrators. Only the members of this group and User 1 are allowed to use the LAN300 network management commands: LIST_LHC_STATUS, LIST_LTS_STATUS, and LOOPBACK. For more information on EDIT_PROFILE and PRIMOS security in general, see the *System Administrator's Guide, Volume III: System Access and Security*.

Summary of PRIMENET-related ACL Settings

The access rights to PRIMENET* and FTSQ* that each process or group must have are as follows:

<i>Process or Group</i>	<i>Access to PRIMENET*</i>	<i>Access to FTSQ*</i>	<i>Access to PRIMENET*> JOURNALS</i>	<i>Access to PRIMENET*> NETLINK</i>	<i>Access to PRIMENET*> SIT_TEXT_DBS</i>
NETMAN	UR				
SYSTEM	ALURWX				
RT_SERVER	UR				
SLAVES\$	UR				
\$REST	U	NONE		UR	UR
Network Administrator	ALL	ALL		ALL	
YTSMAN		ALL			
FTS servers		ALL			
ISC_NETWORK_ SERVER	U		ALL		

Configuring DSM for LAN300 Network Management

We recommend that you configure the Distributed Systems Management (DSM) Unsolicited Message facility to handle LAN300 network management event messages. Otherwise, these event messages are placed in the default log on the local system, DSM*>LOGS>UMH>DEFAULT.LOG. It is better to have them sent to private logs in the NETWORK_MGT* directory. Using CONFIG_UM, create three private logs in the NETWORK_MGT* directory: NMSR.LOG, DLL.LOG, and ULD.LOG. The example below illustrates this procedure:

```
CONFIG_UM NMSR -SEL
```

```
CONFIG_UM Rev. 21.0.26 Copyright (c) 1987, Prime Computer, Inc.
```

```
Product Name: NMSR
```

```
Product Name: <RETURN>
```

```
Severity -ANY;
```

```
Destination: LOGGER NETWORK_MGT*>NMSR.LOG -PLOG
```

```
Destination: <RETURN>
```

```
Do you wish to edit this selection ? NO
```

```
Configuring NMSR on EN.P86.
```

```
Completed OK
```

CONFIG_UM DLL -SEL

CONFIG_UM Rev. 21.0.26 Copyright (c) 1987, Prime Computer, Inc.

Product Name: **CONTROLLER_DLL**

Product Name: **<RETURN>**

Severity **-ANY**

Destination: **LOGGER NETWORK_MGT*>DLL.LOG -PLOG**

Destination: **<RETURN>**

Do you wish to edit this selection ? **NO**

Configuring NMSR on EN.P86.

Completed OK

CONFIG_UM ULD -SEL

CONFIG_UM Rev. 21.0.26 Copyright (c) 1987, Prime Computer, Inc.

Product Name: **CONTROLLER_ULD**

Product Name: **<RETURN>**

Severity **-ANY**

Destination: **LOGGER NETWORK_MGT*>ULD.LOG -PLOG**

Destination: **<RETURN>**

Do you wish to edit this selection ? **NO**

Configuring NMSR on EN.P86.

Completed OK

PRIMENET Security

Before configuring your network, you should consider the degree of security required between each pair of nodes. CONFIG_NET, the PRIMENET configuration program, prompts you to assign access rights between nodes. Before you respond to these prompts, you should consider the following factors:

- General security considerations
- Node-to-node access rights
- Non-Prime node access rights guidelines
- Symmetry requirements
- Node-to-node passwords
- Forced user validation
- Controlling remote file access
- Controlling remote logins
- Security considerations with NETLINK
- Half-duplex passwords
- Security considerations over a gateway link
- Controlling access from PSDNs and dialup terminal lines

In addition to using CONFIG_NET to set security for your network, you should also take the following steps:

- Set network-related ACLs. (See Chapter 2, Installing PRIMENET Software.)
- Ensure that your network's System Administrators and users protect their files by means of ACLs. (See the *Prime User's Guide*.)
- Set up FTS security. (See Chapter 10, Configuring File Transfer Service.)

General Security Considerations

Most security breaches occur when you fail to take simple precautions. For example, carelessness about user IDs and passwords can result in unauthorized access to your network. The System and/or Network Administrator should adequately protect a node's services and data from unauthorized access. This is especially true if one or more nodes are connected to a PSDN.

PRIMOS and PRIMENET offer basic protection mechanisms that help you establish and maintain effective network security. To protect a node from unauthorized entry, you should use the following password mechanisms:

- User passwords (discussed in the *System Administrator's Guide, Volume III: System Access and Security*)
- External login program (discussed in the *System Administrator's Guide, Volume III: System Access and Security*)
- Node-to-node passwords (discussed in this chapter)
- FTS passwords (discussed in Chapter 10, Configuring File Transfer Service)
- HDX passwords (discussed in this chapter)

If you create or add your own service that is accessible through PRIMENET, protect it in a similar way. For example, ensure that this service has its own password mechanism.

There are also other features that you should use to make your node more secure. For example, EDIT_PROFILE (discussed in the *System Administrator's Guide, Volume III: System Access and Security*) allows you to:

- Prevent users from selecting a null password.
- Set minimum password length.
- Create project profiles in conjunction with user passwords.

Furthermore, you should use ACLs to limit access to specific disks, directories, and files on a node. You should also encourage users on your node to adequately protect their directories and files with ACLs. (Refer to the *System Administrator's Guide, Volume III: System Access and Security* and the *Prime User's Guide* for more information.)

Finally, you need to maintain security as you add nodes and services to your network. Refer to this section each time you expand your network.

Node-to-node Access Rights

When you configure your network, CONFIG_NET prompts you to describe each network node. In particular, you need to specify which types of access each node has to each other node.

The following are the PRIMENET access rights; they define a node's access *to* another node.

<i>Access Right</i>	<i>Meaning</i>
NONE	No access at all
IPCF	Access by means of Interprocess Communication Facility (IPCF) sub-routines only
RLOG	Remote login (or remote log-through) and IPCF
RFA	Remote File Access (RFA) and IPCF
ALL	IPCF, RLOG, and RFA

NONE

The node is not allowed to access the other node. If Node X has no access to Node Y, then Node X prevents its users and processes from calling Node Y. NONE is the default access on the network; you must explicitly configure all access rights. NONE is the only access right that prohibits use of the IPCF subroutines.

Note

An exception to the statement above is that any node that is *directly* connected to a PSDN (as opposed to being connected through a gateway) can access any other node on the PSDN through NETLINK or the IPCF subroutines, regardless of the access configured between the two nodes. If NONE access is configured, the calling node must use the called node's PSDN address rather than the node name in making the call. For more information about this exception and how to guard against it, see the section entitled Controlling Access from PSDNs and Dialup Terminal Lines in this chapter.

IPCF

Allows processes on a node to communicate with processes on another node through IPCF subroutine calls. IPCF is sufficient access to allow NETLINK, File Transfer Service (FTS), and InterServer Communications (ISC) to function between two nodes. If two nodes are to communicate via intervening gateway node(s), IPCF must be enabled between each pair of nodes in the path.

If you assign IPCF access from one node to another, CONFIG_NET automatically assigns IPCF access in the opposite direction. IPCF is the only access that you can configure from a Prime node to a non-Prime node. RLOG, RFA, and ALL automatically enable IPCF access. In other words, NONE is the only access right that prohibits use of the IPCF subroutines.

Note

If you enable IPCF access between nodes, users on either node can use NETLINK to log in remotely to the other node, regardless of whether or not you configured RLOG access to either node. Refer to Security Considerations With NETLINK, later in this chapter.

RLOG

Allows a user to log in to a remote node by means of the `-ON` option of the LOGIN command. The user need not log in to the local node or even have a user ID on the local node. The user must simply have a valid ID and password on the remote node. RLOG and IPCF are the only access rights you should configure from a non-Prime node to any other node.

RFA

Permits a user to access files on a remote node without logging in there. Like IPCF access, RFA is always assigned symmetrically between two nodes. If you assign Node X RFA access to Node Y, CONFIG_NET automatically assigns Node Y RFA access to Node X, even if you do not explicitly do so yourself. For a fuller discussion of this symmetry requirement and its implications, refer to Symmetry Requirements, later in this chapter. Do not assign RFA access to or from a non-Prime node.

ALL

Allows all types of access: IPCF, RLOG, and RFA.

Other Considerations

Note that you can assign the same access rights in various ways. For example, assigning ALL access is the same as assigning RFA and RLOG; assigning RLOG is the same as assigning RLOG and IPCF.

A node honors a request for network service only if the proper access is specified through CONFIG_NET. For example, suppose you have assigned RLOG access (but not RFA access) from Node R to Node S. If a user on Node R tries to access a file on Node S without logging in to Node S, Node R rejects the outgoing request.

Specifying Access Rights With CONFIG_NET

This section provides an example of the CONFIG_NET dialog that prompts you for a node's access rights. Chapter 6, Configuring Your PRIMENET Network, fully explains all of the access rights prompts.

CONFIG_NET prompts you for a node's access rights in several steps. For example, consider the configuration shown in Figure 3-1.

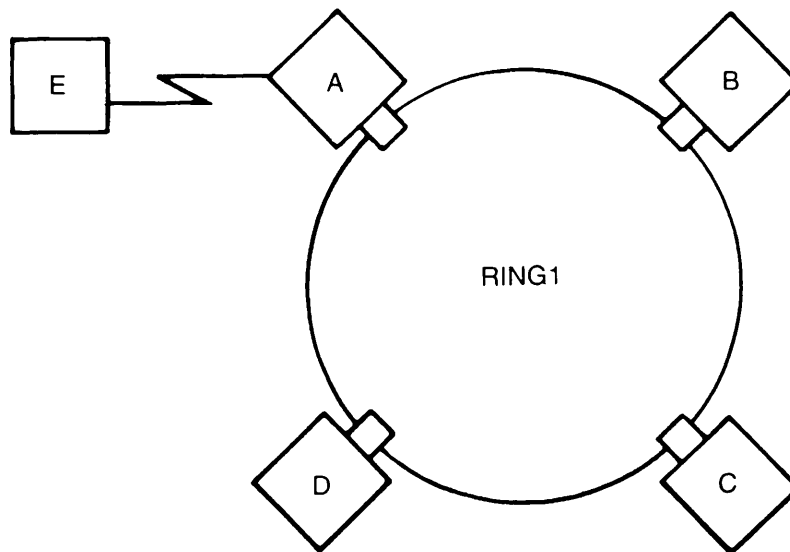


Figure 3-1
Access Rights on a Network

RING1 is composed of Nodes A, B, C, and D. In addition, Node A is connected by a full-duplex line (FDX1) to Node E. Suppose you want to allow Node A's users to log in to Nodes B, C, and D and to access files remotely on Nodes C and E. When you describe Node A, part of your dialog with CONFIG_NET would proceed as follows. (Pressing <RETURN> selects the default value, which is the first one in parenthesis following the prompt. Entering a semicolon after the input forces CONFIG_NET to move to the next prompt instead of repeating the previous one.)

```

Describe Node A
Ring node ID for A on RING1 1, <1-247>
: <RETURN>
Access rights from A via RING1
(NONE, RFA, RLOG, IPCF, ALL): RLOG;
Force user validation(NO, YES)? <RETURN>
Enter nodes accessible from A via RING1 with this access
(NONE, ALL, <node names>, <network names>): B,C,D;
  
```

```
Access rights from A via RING1
(NONE, RFA, RLOG, IPCF, ALL): RFA;
Force user validation(NO, YES)? <RETURN>
Enter nodes accessible from A via RING1 with this access
(NONE, ALL, <node names>, <network names>): C;
Access rights from A via RING1
(NONE, RFA, RLOG, IPCF, ALL): NONE
Node-node password between A and B
(NONE, YES, <password>): <RETURN>
Node-node password between A and C
(NONE, YES, <password>): <RETURN>
Node-node password between A and D
(NONE, YES, <password>): <RETURN>
.
.
.
.
.
Access rights from A via FDX1
(NONE, RFA, RLOG, IPCF, ALL): RFA;
Force user validation(NO, YES)? <RETURN>
Enter nodes accessible from A via FDX1 with this access
(NONE, ALL, <node names>, <network names>): E;
Access rights from A via FDX1
(NONE, RFA, RLOG, IPCF, ALL): NONE
Node-node password between A and E
(NONE, YES, <password>): <RETURN>
```

Non-Prime Node Access Rights Guidelines

When configuring a network containing non-Prime nodes (nodes running non-PRIMENET X.25 1984 software), specify only the following access rights for non-Prime nodes:

- To a non-Prime node: IPCF
- From a non-Prime node: IPCF and RLOG

Symmetry Requirements

PRIMENET's node-to-node access rights are configured for one node at a time. For example, configuring access between Node A and Node B consists of two steps: configuring A's access to B, and configuring B's access to A.

As mentioned earlier in this chapter, CONFIG_NET enforces symmetry in the assignment of RFA and IPCF access between two nodes. For example, suppose you assign RFA (and thus, automatically, IPCF) access from Node A to Node B, and then you configure no access (NONE) from Node B to Node A. CONFIG_NET overrides your decision and assigns RFA and IPCF access from Node B to Node A. You are not warned of this enforced symmetry. However, you can use CONFIG_NET's LIST facility to list all configured access rights between nodes. (For more information on the LIST facility, see Chapter 6, Configuring Your PRIMENET Network.) This list includes any RFA or IPCF access configured automatically by CONFIG_NET.

Remote Naming

Remote naming is a security feature that allows the identity (user name, project, and groups) of a process running on one node to be communicated to another node. Remote naming is used by two Prime network services: Network Process Extension (NPX), which supports Remote File Access (RFA), and InterServer Communications (ISC). Both NPX and ISC use remote naming to check the identity of the user or server that is requesting their services across the network.

ISC Use of Remote Naming

ISC is a kernel facility that provides *sessions* through which any two PRIMOS servers can synchronize their operations and exchange messages. (For a full description of ISC, refer to the *Subroutines Reference Guide, Volume V*.) In the case where ISC is being used over a network (remote ISC), remote naming provides the *target* server with identity information about the *client* server that is attempting to establish a session. The target server uses this identity information to decide whether or not to comply with the request. Remote naming also provides identity information to the client server, so that it can determine whether the target server can actually be trusted to supply the requested service.

NPX Use of Remote Naming

NPX uses the identity information provided by remote naming to activate a *slave* process on the target node, which runs on behalf of the *master* process on the source node. The slave process uses the identity information provided by remote naming as its user ID. Note that NPX *activates* a slave process, whereas ISC provides coordination and communications between *already-active* processes.

Limitations of Remote Naming

The remote naming facility, while useful, has some serious limitations. How can the slave process or target server tell whether or not the remote name really comes from the kernel or merely from a user-written emulator? What if the name given matches that of another user on the target node? Node-to-node passwords and forced user validation, described in the sections that follow, provide the additional security needed to prevent the problems described above.

Node-to-node Passwords

In a previous section, we raised the possibility of a remote name being provided by a user-written emulator instead of the kernel of the source node. You can prevent such security breaches by using node-to-node passwords, which are sometimes referred to as *ring 0 passwords*. Node-to-node passwords are established with CONFIG_NET, the PRIMENET configuration program, and are subsequently known only to the kernels of the two nodes. They are transparent to PRIMENET users. When the target NPX or ISC process receives identity information in a message that also contains the node-to-node password, it assumes that the identity information also comes from the kernel and is therefore legitimate.

Whenever you configure any access rights between two nodes, for example from A and B, CONFIG_NET displays a prompt similar to the following:

```
Node-node password between A and B
(NONE, YES, <password>):
```

You can enter a password of your choosing or enter YES to have CONFIG_NET randomly generate one for you. In either case, the password is used both when A calls B and when B calls A. When you later configure B's access to A, CONFIG_NET does not prompt you for the node-to-node password again, because node-to-node passwords are always symmetrical and the password is already in place. You can change node-to-node passwords with the Edit mode of CONFIG_NET, as described in Chapter 6, Configuring Your PRIMENET Network.

Caution

For security purposes, CONFIG_NET generates different random node-to-node passwords each time it is run. Hence, if you use multiple configuration files in your network, you should supply your own node-to-node passwords to ensure consistency.

CONFIG_NET's LIST mode can be used to display your network's node-to-node passwords. This means that anyone who is allowed to read the network configuration file and execute CONFIG_NET has access to these passwords. Be sure to use ACLs to protect both the network configuration file and the use of CONFIG_NET.

At this point, you may be wondering why CONFIG_NET prompts you about the node-to-node password for any type of access rights between nodes, whereas NPX applies only to RFA access, and remote ISC needs only IPCF access rights. Recall from the previous discussion of access rights that when you configure RFA, RLOG, or ALL, you also implicitly configure IPCF access. You are therefore opening up the possibility of security breaches through ISC, because ISC needs only IPCF access. CONFIG_NET automatically prompts you about both protective measures — node-to-node passwords and forced user validation.

Forced User Validation

Another security issue is that the user name sent by remote naming could match a user name on the target node. In that case, the remote user would acquire all of the ACL rights of the user with the same name on the target node. This is a real possibility when forced user validation is not in effect, because remote naming sends the user or process ID from the *source node* (the local ID). When forced user validation is in effect, however, the user or process must first add a *remote ID* with the ARID command. (See the *Prime User's Guide* for details.) This ID is remote in the sense that it must be listed in the System Administrator's Directory (SAD) of the target (remote) node. (For more information about the SAD, see the *System Administrator's Guide, Volume III: System Access and Security*.) When forced user validation is configured from one node to another, remote naming sends this remote ID rather than the local ID.

CONFIG_NET always prompts you about forced user validation, regardless of the type of access you configure. This is because configuring ALL, RLOG, or RFA also implicitly configures IPCF access, which allows remote ISC to function. Thus, whenever you configure any type of access between nodes, you are opening up the possibility of security breaches by means of ISC. You can prevent this possibility by forcing user validation.

Deciding About Forced User Validation

You should force user validation if:

- Security between nodes is a strong concern, and/or
- The two nodes do not coordinate user IDs; that is, IDs are not unique across the two nodes.

For example, suppose nodes P and Q are configured for RFA access but do not coordinate user IDs. Harry Rosen has ID HARRY on Node P, while Harry Smith has ID HARRY on Node Q. If you do not force user validation, then when Harry Smith attaches to a directory on Node P, the slave acquires user ID HARRY and receives all of Harry Rosen's ACL rights. Harry Smith can then access any files that Harry Rosen can. This situation cannot be circumvented by assigning different passwords to the two Harrys, because password checking is bypassed.

You need not force user validation if:

- Security between nodes is not a strong concern, *and*
- User IDs uniquely identify users across the two nodes. (This means that Harry Smith on Node Q and Harry Rosen on Node P are assigned different IDs, such as HARRY_S and HARRY_R.)]

Even with coordination of IDs, if you do not demand full user validation, you are trusting that masters or ISC servers are valid users who are authorized to access the target node.

As Network Administrator, you should confer with individual System Administrators to decide which nodes will coordinate IDs. When two nodes do coordinate IDs, the System Administrators

must inform one another of all new IDs on their nodes. The simplest way to handle ID coordination is for one person (for example, the Network Administrator) to take sole charge of assigning IDs.

The EDIT_PROFILE command VERIFY_USER can help you find out which IDs have already been assigned on a given node. (Refer to the *System Administrator's Guide, Volume III: System Access and Security* for information on EDIT_PROFILE. EDIT_PROFILE is the utility that allows System Administrators to add, change, and delete information about users and their attributes on a node.)

In most cases, you should configure forced user validation symmetrically because ID coordination is symmetric and security needs are often symmetric.

Controlling Remote File Access

To control remote file access effectively, you need to understand how the Network Process Extension (NPX) facility masters and slaves work. (For a brief introduction to masters and slaves, refer to Chapter 1, PRIMENET Overview.)

A master can have no more than one slave on a given remote node at one time. All of the master's operations on the remote node are handled by that one slave. However, a single master can have slaves on as many as 15 remote nodes simultaneously. Furthermore, many masters on one node can simultaneously call their corresponding slaves on another node. On each node whose files can be accessed remotely, the System Administrator must use the NSLUSR directive in the CONFIG file to set the maximum number of slaves on the node.

A slave is dedicated to its calling master process while the master is attached to the remote node. Slaves that are not being used by masters remain dormant, using minimal node resources, until they are called. A dormant slave has no user ID and does not appear on the STATUS USERS list. However, a slave that has been called by a master takes on a user ID and becomes a full-fledged user, appearing on the STATUS USERS list.

The issues of which IDs a node's slaves acquire and how they acquire them are very important for node security. If forced user validation is in effect, before calling a slave, a master must use the ADD_REMOTE_ID (ARID) command to specify a user ID that is valid on the slave's node (a remote ID). The slave then takes on this ID and logs in to its node in the standard way, going through the user validation process. Forced user validation provides the highest level of security for an RFA-accessible node, especially when used with a node-to-node password.

If forced user validation is not in effect, the slave inherits its master's ID and ACL rights without going through the normal login and user validation process. In either case, the slave acquires the access rights associated with its new user ID.

The following sections describe forced user validation for RFA access and explain when it should be used. In this discussion, *master node* refers to the node that is accessing a remote node's files, and *slave node* refers to the node whose files are being accessed. Note that these terms apply only to a given remote file access request at a given moment. Since RFA is a

symmetric access right, either node can take the role of master. In fact, users on both nodes might use remote file access simultaneously, so that each node is a master node for some requests and a slave node for others at the same time.

Forcing User Validation for RFA Access

If you force user validation, the following steps must occur before remote file access can take place:

- Before issuing a command that requires remote file access, a user or process on the master node must issue the `ADD_REMOTE_ID` (ARID) command. On the ARID command line, the user must specify a user ID and password that are valid on the remote node. (A project name can also be specified.) The ID is used by any slave(s) on the remote node subsequently called by the user on the master node. (For information on the ARID command, refer to the *Prime User's Guide*.)
- When a user or process on the master node requests a remote file access, the slave goes through a complete login sequence on the remote node, using the user ID and password specified in the ARID command. Thus, the slave takes on the user ID specified by the master in the ARID command.
 - If the login is successful, the slave also acquires the ACL rights assigned to that ID, if any.
 - If the login fails, the master receives an error message and remote file access does not take place.

Note

Users who access remote files frequently may find it convenient to incorporate the ARID command into their `LOGIN.CPL` files using the `-PROMPT` option. If `-PROMPT` is specified, ARID asks for the user's password on the remote node. Thus, the user's password on the remote node does not (and *should not*) appear in the user's `LOGIN` file.

If you force user validation, the System Administrator of the slave node must supply users on the master node with valid user IDs to add.

Not Forcing User Validation for RFA Access

If you do not force user validation, the following steps must occur before a remote file access takes place:

- The calling user (master) can still issue the ARID command before making the remote call. In this case, slave login occurs just as in the case of forced user validation.

- If the master does not issue the ARID command, the slave takes on the same user ID as the master. This ID need not be a valid ID on the slave node because the slave bypasses the standard login procedure. A special, fast login takes place; neither validation nor password checking occurs. The master does not pass a user password to the slave. The only security check that occurs involves the node-to-node password (discussed in a previous section). However, if the slave node uses ACLs, the slave acquires any ACL rights associated with the master's ID. If there are none, the slave acquires only the default access rights given to the \$REST ACL group.

Note

On nodes that use directory passwords rather than ACLs, slaves' access rights are governed by standard password protection rules. (Masters supply directory passwords when they attach to the remote node.)

Controlling Remote Logins

A user who wants to log in to a remote node must have a valid user ID on the remote node. System Administrators can use different methods for supplying IDs to remote users, depending upon the degree of security required between nodes. For a full description of user IDs, profiles, and projects, see the *System Administrator's Guide, Volume III: System Access and Security*.

- If security is not a strong concern, a System Administrator might inform remote System Administrators and/or remote users of some of the existing IDs on the local node that they can use.
- If security is a relatively strong concern, a System Administrator might set up a pool of guest IDs (and perhaps a project) with limited ACL rights for use by remote users.
- If security is a very strong concern, a System Administrator might decide that each remote user who wishes to log in to the local node must be assigned a unique user ID and User Profile.

As Network Administrator, you might want to decide on a global plan for managing remote logins. On the other hand, individual System Administrators on your network might want to make policy decisions themselves, on a node-by-node basis.

Once you enable remote login by means of CONFIG_NET, each System Administrator must use the NRUSR CONFIG directive to control the maximum number of simultaneous remote users on his or her node. The NRUSR directive is described in Chapter 8, Setting PRIMENET-related CONFIG Directives.

Note

Whether or not forced user validation is in effect between two nodes does not affect Remote Login. The user must always supply an ID and password that are valid on the remote node.

Security Considerations With NETLINK

The NETLINK utility allows users on a PRIMENET network to connect to remote nodes on the same network. A user on Node A can connect to Node B via NETLINK as long as IPCF access is enabled between each pair of adjacent nodes in the path from A to B.

Once connected to Node B via NETLINK, a user from Node A can log in to Node B, regardless of whether RLOG access is assigned between A and B. Furthermore, the user can issue the LOGIN -ON command to log in to a node that is connected to Node B, without first logging in to Node B itself. Thus, NETLINK allows a user to reach nodes that are not directly connected to the local node, even when the intervening nodes are not gateway nodes. (Of course, a user must always have a valid user ID in order to log in to any node.)

Note

Whether or not forced user validation is in effect between two nodes has no effect on NETLINK operation.

Half-duplex Passwords

Since PRIMENET's half-duplex communication occurs over dialup lines, it is possible for any node with a modem to dial into a half-duplex node and pretend to be a valid network node. We strongly recommend that you use half-duplex passwords to protect against this possibility.

Each time you configure access from one half-duplex node to another, CONFIG_NET asks whether you want to assign incoming and outgoing half-duplex passwords. For example, if you assign access from Node A to Node B via a half-duplex line, CONFIG_NET asks you for the following information:

- A's incoming HDX password from B
- A's outgoing HDX password to B

If you assign these passwords, CONFIG_NET automatically sets up the following additional passwords:

- B's outgoing HDX password to A, which is defined to be the same as A's incoming HDX password from B
- B's incoming HDX password from A, which is defined to be the same as A's outgoing HDX password to B

Whenever Node A initiates half-duplex communication with Node B, Node A provides its outgoing password to Node B. Node B checks to be sure that the password it receives matches its stored incoming password from Node A. If the passwords do not match, it rejects the call. When Node B initiates half-duplex communication with Node A, a similar verification occurs. Once you assign half-duplex passwords, they are transparent to the user; PRIMENET uses them internally.

You can choose your own half-duplex passwords or let CONFIG_NET generate random passwords for you. You can also change half-duplex passwords through the Edit mode of CONFIG_NET, as described in Chapter 6, Configuring Your PRIMENET Network.

Security Considerations Over a Gateway Link

Gateway access between nodes is assigned with CONFIG_NET. The gateway access rights are identical to the standard access rights, and forced user validation and node-to-node passwords work in the same way that they do for standard node-to-node access. The requirements and cautions that apply to gateway access are identical to those for the node-to-node access described above.

Note that a user either on a Prime node or accessing a Prime node from a Packet Switching Data Network (PSDN) can call a gateway node directly and thereby reach other nodes in the network. If you have not secured each node with the proper security features provided by PRIMOS and PRIMENET, unauthorized access to your network is possible. It is your responsibility to deter unauthorized access on your network by using the security mechanisms that are discussed in General Security Rules earlier in this chapter. Also, if you create or add your own service that is accessible through PRIMENET, you should protect it in a similar way.

Controlling Access From PSDNs and Dialup Terminal Lines

You should consider carefully what types of network access to grant to a node that:

- Is directly connected to a PSDN, *or*
- Can be reached indirectly through a PSDN or through a dialup terminal line (that is, can be accessed by remote users with terminals and modems).

Rule 1: A Node Directly Connected to a PSDN

Any node that is *directly* connected to a PSDN (as opposed to being connected through a gateway) can access any other node on the PSDN through NETLINK or the IPCF subroutines, *even if no access is explicitly configured between the two nodes.*

If no access is configured, the calling node must use the called node's PSDN address rather than the node name in making the call. The called node may be directly or indirectly connected to the PSDN. (If the called node is indirectly connected, the calling node uses the called node's indirect address. Indirect addresses are described in Chapter 4, PRIMENET Network Configuration.)

Thus, if Node X is directly connected to a PSDN, users on Node X can call any node whose PSDN address they know. If Node Y is connected directly or indirectly to a PSDN, users on any node that is directly connected to the PSDN may call Node Y, provided they know Node Y's address.

A node that is connected *indirectly* to a PSDN cannot call another node on the PSDN unless IPCF access is configured between the nodes. IPCF access is also required for any call that uses a node name rather than an address.

Because of the foregoing, it is important that you carefully protect all files on nodes with PSDN addresses. Assess the need for gateway access to PSDNs carefully. Impose strong login restrictions on all PSDN-accessible nodes.

Rule 2: A Node Accessed via a PSDN or Dialup Line

A user accessing a node through a PSDN or dialup terminal line has the same rights to your network as the node has. For example, in Figure 3-2, Node B is connected to a ring and to a PSDN.

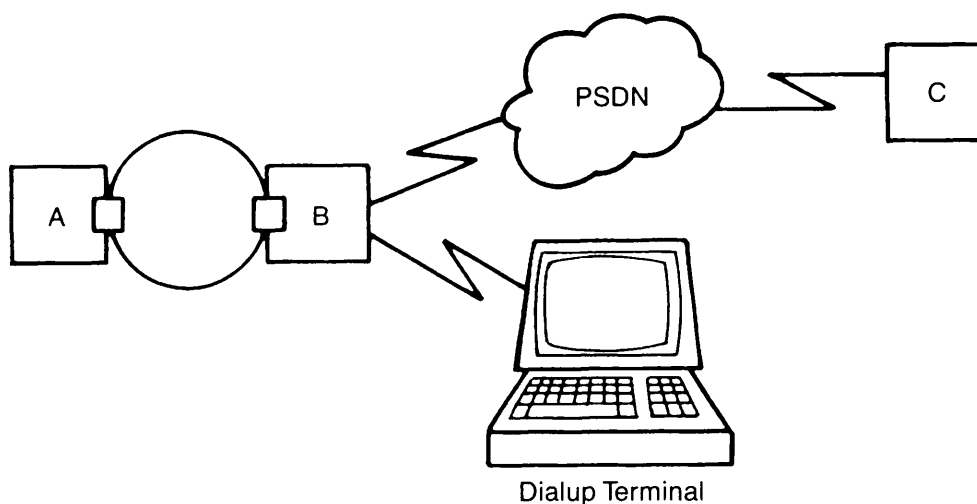


Figure 3-2
Access From a PSDN

If you permit users on Node B to log in to Node A remotely, any user connecting to Node B through the PSDN (for example, from Node C) or through a dialup terminal line can also log in to Node A by using the `LOGIN -ON A` command. This is true even if Node A does not have a PSDN address. Similarly, if you assign Node B RFA access to Node A, then PSDN or terminal

line users who can log in to Node B will be able to access Node A's files. If A does not have a PSDN address, you can protect Node A by restricting Node B's access to A, for example, by disabling RLOG access from B to A.

Thus, imposing strict login requirements on Node B is not sufficient; to secure the network, you must also restrict access from B to all other nodes. You will probably want to increase login security on any node that B can access and force user validation if RFA is enabled between B and any other node. You may even want to use external login programs to impose additional login restrictions on the nodes of a PSDN-accessible network. Be sure that all important files on the network are well protected by ACLs.

Note

Dialup terminal line does *not* refer to a half-duplex line. Half-duplex lines are node-to-node connections, whereas dialup terminal lines are terminal-to-node lines.

Security on Pre-Rev. 19.3 Nodes

If your network contains pre-Rev. 19.3 nodes, refer to the Rev. 19.0 *System Administrator's Guide* and Rev. 19.0 *PRIMENET Guide* for the following information on network security prior to Rev. 19.3:

- Controlling remote logins
- Controlling remote users' access to disks on your node
- Controlling remote users' access to your node's files
- Using NETCFG to set access rights
- Setting up security for FTS

CONFIG_NET prompts you for the names of the pre-Rev. 19.3 nodes in your network. For more information on pre-Rev. 19.3 nodes, refer to the section entitled Specifying Addresses to CONFIG_NET in Chapter 4, PRIMENET Network Configuration, and to the section entitled Defining the Network Topology in Chapter 6, Configuring Your PRIMENET Network.

PRIMENET Network Configuration

In order for a PRIMENET network to operate properly, each network node must have certain information. For example, each node must know:

- What nodes are on the network.
- What kinds of communication links are being used.
- What types of access are allowed between nodes.
- Whether the network is connected to any Packet Switching Data Networks (PSDNs).

This kind of information makes up the **network configuration** and is stored in a binary file called the **network configuration file**.

CONFIG_NET, the PRIMENET configuration program, enables you to create a *global* network configuration file. That is, in most cases, you can run CONFIG_NET on any node to define the entire network at one time. You can then copy this file to each node on the network.

CONFIG_NET uses a series of questions and menus to guide you in supplying the required information. It uses your responses to generate the network configuration. Creating the network configuration file by running CONFIG_NET is called *configuring the network*.

Before using CONFIG_NET, you should plan your network carefully and gather all of the necessary information. This chapter and Chapter 5, *Preparing to Configure Your PRIMENET Network*, provide information on configuration planning. This chapter also explains how to determine the addresses in your network. Chapter 5 contains a list of questions you should answer before running CONFIG_NET. After reading this chapter and answering the questions in Chapter 5, you will be ready to configure your network according to the instructions presented in Chapter 6, *Configuring Your PRIMENET Network*. Chapter 7, *Sample PRIMENET Configurations*, presents examples of various configurations, with the corresponding CONFIG_NET dialog.

The Network Configuration File

Unless you specify otherwise, CONFIG_NET names the network configuration file PRIMENET.CONFIG and places it in your current working directory. You may want to create the file in the PRIMENET* directory (or copy it there when configuration is complete). When the system operator brings up PRIMENET on a node with the START_NET command,

START_NET looks for the network configuration file and uses it to produce the PRIMENET database. Unless the operator specifies an alternate configuration file, START_NET looks for the file PRIMENET*>PRIMENET.CONFIG.

The PRIMENET database lists the correct nodename for each remote node on the network, indicates which remote nodes have access to the local node, and specifies the remote nodes that the local node can access. START_NET also sets aside buffer space for each remote node with which the local node will communicate. (It does not set aside buffer space for other nodes.) Nodes in route-through paths use the PRIMENET database to determine where to route data.

In some cases you may want to create several different network configuration files. For instance, you might want to store various hypothetical configurations for future use or keep a copy of an older configuration for reference. To avoid confusion, keep these alternate configuration files in a different directory from that of the currently active configuration file.

Global Configuration

The file that CONFIG_NET generates is called a **global** configuration file because it contains information about all the nodes, connections, access rights, and security restrictions in the network. In most cases, you run CONFIG_NET once to create the configuration file, and then distribute a copy to each node on the network.

The START_NET command is issued separately on each node of the network. The operator cannot issue the START_NET command successfully until the network configuration file is in place. START_NET does not interrupt operation of the node on which it is issued.

As a general guideline, identical configuration files should be used on all nodes in a network for the following reasons:

- Using the same configuration file throughout the network ensures that all nodes have the same picture of the network. For example, if a node-to-node password is in effect between two nodes, both nodes are certain to have the same password recorded in their configuration files. Also, there is no confusion over access rights between nodes.
- Creating the network configuration may require a significant amount of planning. It is usually easiest to run CONFIG_NET once for the whole network.
- CONFIG_NET checks that the file it generates is internally consistent and that it adheres to certain configuration rules. (These checks are explained in more detail in the section entitled Verification in Chapter 6, Configuring Your PRIMENET Network.) If different nodes use different files, CONFIG_NET cannot detect inconsistencies between these files. Such inconsistencies can prevent nodes from communicating with one another.

However, sometimes this guideline does not apply; in certain special cases, different configuration files are used on different nodes of the network. These cases are described in the next section.

Using Different Configuration Files in the Same Network

You must use more than one configuration file in the following four situations:

1. If your network contains one or more pre-Rev. 19.3 nodes
2. If your network contains one or more pre-Rev. 21.0 nodes
3. If your network contains a PSDN gateway
4. If you lack certain information about one or more network nodes

These situations are described below.

Mixed-Rev. Networks With Pre-Rev. 19.3 Nodes

Pre-Rev. 19.3 nodes cannot use CONFIG_NET's global configuration file. For a pre-Rev. 19.3 node, you must create a separate configuration file with the NETCFG utility, which is described briefly later in this chapter and fully in the Rev. 19.0 *System Administrator's Guide*. Thus, a pre-Rev. 19.3 node has its own configuration file. (However, CONFIG_NET does prompt you to identify and describe the pre-Rev. 19.3 nodes in the global configuration file. The global configuration file is used in all the *post*-Rev. 19.3 nodes.)

Caution

You must define all pre-Rev. 19.3 nodes as such when you configure your network. This allows CONFIG_NET to prompt you for necessary information about addresses used by old nodes. If you fail to identify a pre-Rev. 19.3 node, problems such as call collisions, inoperative synchronous lines, or remote file access errors could result. For more information about configuring old nodes, refer to *Specifying Addresses in a Mixed-Rev. Network*, later in this chapter.

Mixed-Rev. Networks With Pre-Rev. 21.0 Nodes

Observe these considerations if any nodes in your network are using pre-Rev. 21.0 PRIMENET, CONFIG_NET, or START_NET:

- Pre-Rev. 21.0 nodes cannot run Rev. 21.0 CONFIG_NET.
- Pre-Rev. 21.0 nodes using pre-Rev. 21.0 CONFIG_NET can still use X.25 1984 features, but you must use Rev. 21.0 CONFIG_NET and PRIMENET if Prime nodes are to communicate with non-Prime nodes over FDX or LAN300 links.

- Rev. 21.0 CONFIG_NET can read configuration files created with earlier versions of CONFIG_NET. This allows you to edit your existing configuration files when adding LAN300 functionality to your network. However, when you edit (for any reason) a configuration file created with an earlier version of CONFIG_NET, you must enter Create mode during the session. In Create mode, CONFIG_NET automatically prompts you about the new features: LAN300s and non-Prime nodes. (Answer NONE if you are not using these features.) If you do not go into Create mode, CONFIG_NET rejects the configuration as invalid when you attempt to save it.
- Pre-Rev. 21.0 CONFIG_NET cannot read configuration files created or edited by Rev. 21.0 CONFIG_NET.
- Rev. 21.0 START_NET can start PRIMENET using any valid configuration file, regardless of the revision of CONFIG_NET with which it was created. You do not need to update your old configuration file if you are not using the new Rev. 21.0 features such as LAN300s, communication with non-Prime nodes, and setting the maximum number of virtual circuits on a node.
- Pre-Rev. 21.0 START_NET cannot start PRIMENET with a configuration file created with Rev. 21.0 CONFIG_NET.

Therefore, if you are upgrading some nodes in the network to Rev. 21.0, while leaving other nodes at earlier revision levels, you must use two network configuration files: one file for the Rev. 21.0 nodes and another for the pre-Rev. 21.0 nodes. This is because pre-Rev. 21.0 START_NET cannot read configuration files created with Rev. 21.0 CONFIG_NET. Although you must still explicitly mark pre-Rev. 19.3 nodes in the Rev. 21.0 configuration file, you do not have to specially mark nodes running a revision between 19.3 and 21.0. For more information on pre-Rev. 19.3 nodes, refer to Mixed-Rev. Networks with Pre-Rev. 19.3 Nodes in this chapter.

PSDN Gateways

A connection between two PSDNs is called a **PSDN gateway**. If your network contains a PSDN gateway (as, for example, the one illustrated in Figure 4-1), you cannot use one global configuration file for the whole network. Instead, you must create separate configuration files for the parts of the network on either side of the gateway. Refer to Chapter 7, Sample PRIMENET Configurations, for an example of configuring a network with a PSDN gateway.

Unknown Configuration Information

If you do not have some of the configuration information for a particular node, you can enter UNKNOWN for that information in the global configuration file, then later create a complete configuration file for the node in question.

For example, suppose Node A is connected to another node by a full-duplex synchronous line. For some reason you do not know all the details about SYSA's end of that line. (Perhaps SYSA's administrator is on vacation the day that you configure the network.) When CONFIG_NET asks

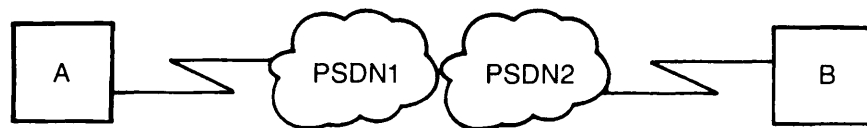


Figure 4-1
PSDN Gateway

you for the synchronous line number (on SYSA) of the line, you may need to answer UNKNOWN. But the copy of the configuration file that is actually used on SYSA must contain the synchronous line number; "UNKNOWN" is not sufficient. Thus, you might need to copy your completed configuration file to SYSA and have a System Administrator on SYSA edit it to include the synchronous line number. SYSA's configuration file will then be different from the files used on the other nodes, but this difference will not affect network operation.

Guidelines for Using Multiple Configuration Files

If you do use different configuration files on different network nodes, remember that PRIMENET does not check that the files are consistent. You must therefore make sure that all ring node IDs, nodenames, synchronous line numbers, node-to-node passwords, half-duplex passwords, and so on are defined the same way in all of the configuration files used in the network.

If you need to change the configuration file on a given node, you can use the Edit mode of CONFIG_NET, which is described in Chapter 6, Configuring Your PRIMENET Network. When you have finished editing the file, issue the STOP_NET command to *stop the network* (that is, remove the node from the network without shutting the node down), then issue the START_NET command to restart the network with the new configuration file. In most cases, you should copy the new file to the nodes that had copies of the old file. Keep in mind that changing one configuration file in the network without changing the others in the same way is not generally recommended, except in one of the four situations listed earlier.

CONFIG_NET Versus the NETCFG Utility

Prior to Rev. 19.3, PRIMENET did not use global configuration files. Each node had its own unique network configuration file that described only the lines and nodes directly connected to that node. The System or Network Administrator on each node ran the NETCFG utility to create that node's configuration file.

You must use NETCFG to edit the configuration files of nodes running PRIMOS revisions earlier than Rev. 19.3. NETCFG is described in the Rev. 19.0 *System Administrator's Guide*. Refer also to the section entitled Specifying Addresses to CONFIG_NET, later in this chapter, and to the section entitled Defining the Network Topology, in Chapter 6, Configuring Your PRIMENET Network.

Specifying Addresses to CONFIG_NET

CONFIG_NET asks you to supply an address for a node under the following circumstances:

- The node is a Prime or non-Prime node connected to a PSDN.
- The node can access a PSDN indirectly through a gateway node. In this case, CONFIG_NET prompts you for an **indirect PSDN address**.
- The node is a non-Prime node connected to a LAN300, or a Prime node connected to a LAN300 in a network that contains non-Prime nodes. In this case, CONFIG_NET prompts you for the node's **LAN300 address**.
- The node can be accessed by a non-Prime node on a LAN300 indirectly (through a gateway node). In this case, CONFIG_NET prompts you for an **indirect LAN300 address**.
- The node is a non-Prime node connected to a full-duplex line, or a Prime node connected to a non-Prime node by a full-duplex line. In this case, CONFIG_NET prompts you for the node's **FDX address**.
- The node can be accessed by a non-Prime node on a full-duplex line indirectly (through a gateway node). In this case, CONFIG_NET asks for an **indirect FDX address**.
- The node is part of a mixed-Rev. network, can be accessed by a pre-Rev. 19.3 node, and has more than one address.

The following sections describe how to determine the correct address to supply to CONFIG_NET in each of these situations.

Specifying PSDN Addresses

If your network connects to one or more PSDNs, for each PSDN you must decide:

- The name of the PSDN
- The name of each node directly connected to the PSDN
- The PSDN address(es) of each such node

The PSDN Administrator is responsible for assigning PSDN addresses to all nodes that connect to the PSDN. If you do not know the necessary PSDN addresses, contact your PSDN Administrator.

Note

A PSDN address must not begin with 9999.

Specifying Indirect PSDN Addresses

If your network contains one or more nodes that can access a PSDN indirectly (through a gateway), for each of those nodes you must know:

- The name of the node
- The name of the PSDN
- The node's *indirect* PSDN address (explained below)
- The name of the gateway node that is connected to the PSDN and will route PSDN data to and from the node in question
- The number of the synchronous line that connects the gateway node to the PSDN (and that is used to route data to the node in question)

Each combination of the form nodeA-gateway-PSDN requires a unique indirect address for *nodeA*. You can assign an indirect address in two ways:

- Using multiple addressing
- Using subaddresses

If a PSDN supports multiple addressing, you can ask the PSDN Administrator to assign multiple addresses to the gateway node: one for the gateway node itself, and one for each node that connects to the PSDN through the gateway. As data for a particular address is received, the gateway node routes it to the correct node. The PSDN sees only the gateway node with its multiple addresses; the PSDN need not know about the indirectly connected nodes.

If a PSDN supports subaddresses, you can create an indirect address by starting with the gateway node's assigned PSDN address and adding a numeric suffix. Use a different suffix for each node that accesses the PSDN through that gateway. For example, if the gateway's PSDN address is 311061755555, you might assign the indirect addresses 31106175555511 and 31106175555522, respectively, to two nodes that access the PSDN through the gateway. Check with the PSDN Administrator to find out about any specific rules for creating subaddresses.

For examples of configurations using indirect addresses, refer to Chapter 7, Sample PRIMENET Configurations.

Note

The subaddress that you append to the PSDN address must not end in a 0.

Specifying LAN300 Addresses

CONFIG_NET asks for the LAN300 addresses of non-Prime nodes on LAN300 networks and of Prime nodes on LAN300s in networks that contain non-Prime nodes.

LAN300 Addresses for Prime Nodes: CONFIG_NET prompts you for the addresses of Prime nodes on LAN300 networks that contain non-Prime nodes primarily because some non-Prime nodes require a source address in incoming calls. Check with the administrator of the non-Prime node for specific requirements because some machines require a null source address in incoming calls, others require a specific address, and still others only look for a valid address.

The default value, NONE, causes the Prime host to omit its Level 3 address from its Call Request packets. This is acceptable for communication with most non-Prime hosts. For incoming calls, Prime hosts configured with the default value allow themselves to be called by either a null address (no Level 3 address) or the address automatically generated for them by CONFIG_NET. (CONFIG_NET automatically generates a Level 3 address beginning with "9999," based on the node's name). You can override this automatically generated address by entering one or more alternate addresses in response to the CONFIG_NET prompt. In that case, the Prime node inserts one of your addresses in its Call Request packets and accepts only those incoming calls with one of your addresses.

LAN300 Addresses for Non-Prime Nodes: The first address prompt for a non-Prime node queries you for the node's Level 3 (packet level) address(es). In most cases, it is acceptable to give a non-Prime node a null address by entering NULL at the CONFIG_NET prompt. However, if a non-Prime node is to communicate with another non-Prime node through a gateway, they must be able to accept non-null addresses, and you must give a network address for each node. This is because the gateway needs the addresses for routing.

When you are configuring a non-Prime node on a LAN300, CONFIG_NET also prompts you for the node's MAC and LSAP address. Both of these are Level 2 (link level) addresses. The MAC (Media Access Control) address identifies the node attached to the LAN300, whereas the LSAP (Link Service Access Point) identifies the particular service on that node. Check with the administrator of the non-Prime node to obtain this information.

The format for the 12-hex-digit MAC address is *nn-nn-nn-nn-nn-nn*. The optional LSAP address is two hex digits, which are preceded with a plus sign (+) and appended to the end of the MAC address: *nn-nn-nn-nn-nn-nn+nn*.

Specifying Indirect LAN300 Addresses

CONFIG_NET prompts you for a node's indirect LAN300 address when it can be accessed by a non-Prime node on a LAN300 that is indirectly connected via a gateway node. Figure 4-2 illustrates this situation.

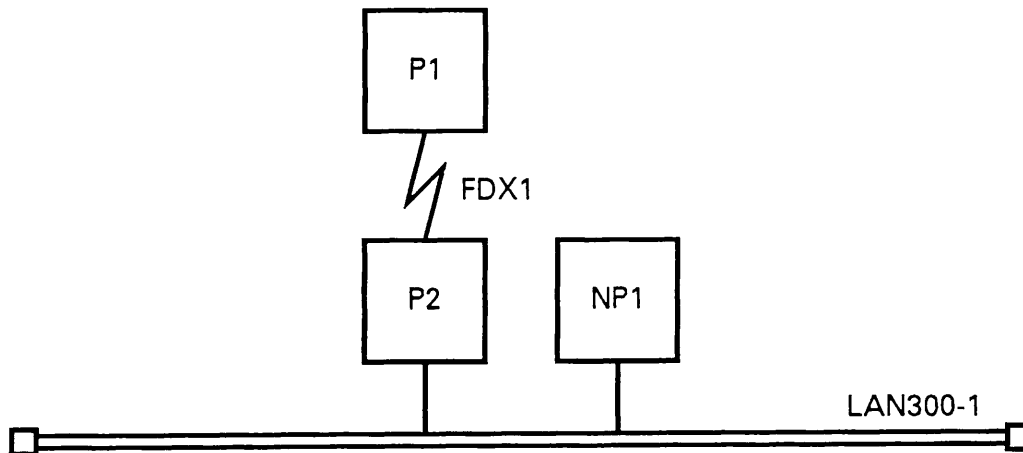


Figure 4-2
Indirectly Connected Non-Prime Node on a LAN300

P1 and P2 are Prime nodes attached to a full-duplex line, FDX1, whereas NP1 is a non-Prime node attached to LAN300-1. P2 is also attached to LAN300-1, and it serves as a gateway between P1 and NP1. During configuration, you must define P1's indirect LAN300 address, because NP1 needs an address to use in order to reach P1 through the gateway node, P2.

Specifying FDX Addresses

CONFIG_NET asks for the FDX addresses of non-Prime nodes attached to FDX lines and of Prime nodes attached to a non-Prime node by an FDX line.

FDX Addresses for Prime Nodes: CONFIG_NET prompts you for the Level 3 (packet level) address(es) of Prime nodes that are connected to a non-Prime node by an FDX line primarily because some non-Prime nodes require a source address in incoming calls. Check with the administrator of the non-Prime node for specific requirements because some machines require a null source address in incoming calls, others require a specific address, and still others only look for a valid address.

The default value, NONE, causes the Prime host to omit its Level 3 address from its Call Request packets. This is acceptable for communication with most non-Prime hosts. For incoming calls, Prime hosts configured with the default value allow themselves to be called by

either a null address (no Level 3 address) or the address automatically generated for them by CONFIG_NET. (CONFIG_NET automatically generates a Level 3 address beginning with "9999," based on the node's name). You can override this automatically generated address by entering one or more alternate addresses in response to the CONFIG_NET prompt. In that case, the Prime node inserts one of your addresses in its Call Request packets and accepts only those incoming calls with one of your addresses.

CONFIG_NET then prompts you for the synchronous line number on the node to be used for the FDX line.

FDX Addresses for Non-Prime Nodes: The first address prompt for a non-Prime node queries you for the node's Level 3 (packet level) address(es). In most cases, it is acceptable to give a non-Prime node a null address by entering NULL at the CONFIG_NET prompt. However, if a non-Prime node is to communicate with another non-Prime node through a gateway, they must be able to accept non-null addresses, and you must give a network address for each node. This is because the gateway needs the addresses for routing.

CONFIG_NET then prompts you for the synchronous line number on the node to be used for the the FDX line. You may leave the synchronous line number unknown for non-Prime nodes because it is unlikely that a non-Prime node could read a Prime configuration file.

When you are configuring a non-Prime node on an FDX line, CONFIG_NET also prompts you for the Link Access Protocol Balanced (LAPB) address for the node. This is a Level 2 (link level) address. The LAPB address is used in command frames sent from the Prime node to the non-Prime node. It may be 1 or 3; the default is 3. This default assumes that the non-Prime acts as DTE (Data Terminal Equipment). Non-Prime nodes that are PADs (Packet Assemblers/Disassemblers) normally act as DCE (Data Communications Equipment) and should be configured as X.25 PSDNs.

Specifying Indirect FDX Addresses

CONFIG_NET prompts you for a node's indirect FDX address when it can be accessed by a non-Prime node on an FDX that is indirectly connected via a gateway node. Figure 4-3 illustrates this situation.

NP1 is a non-Prime node attached to a Prime node named P1 by FDX1, a full-duplex line. P1 is also attached to LAN300-1, and it serves as a gateway node between NP1 and P2, another Prime node on the LAN300. During configuration, you must define P2's indirect FDX address because NP1 needs an address to use in order to reach P2 through the gateway node, P1.

Specifying Addresses in a Mixed-Rev. Network

When you configure your network, CONFIG_NET asks you to identify any pre-Rev. 19.3 nodes. If your network contains any of these nodes, you may need to run the NETCFG utility on each of them in order to obtain certain information that CONFIG_NET requires. This section explains why you may need to run NETCFG, and it provides an example.

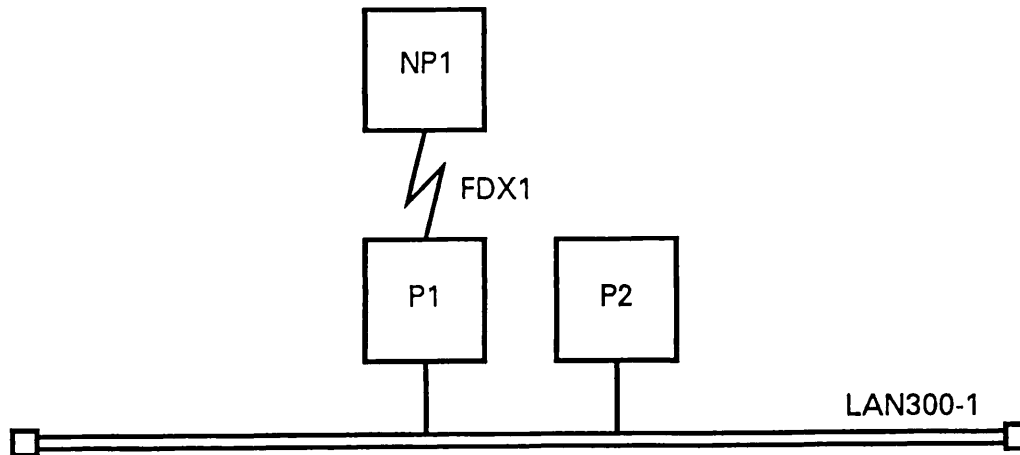


Figure 4-3
Indirectly Connected Non-Prime Node on an FDX

Prior to Rev. 19.3, each node was identified by only one address. If the node was connected to a PSDN, it was known by its PSDN address. If the node was not connected to a PSDN, it was known by its PRIMENET address.

As of Rev. 19.3, a node can have more than one address. Thus, a node might be identified by both a PSDN address and a PRIMENET address.

If your network contains both old nodes (Rev. 19.3 or earlier) and new nodes (*post*-Rev. 19.3), you may have the situation in which one or more old nodes communicate with a multiply addressed new node. But an old node cannot recognize multiple addresses. Each old node can use only one address to identify the new node. Furthermore, CONFIG_NET requires that all old nodes use the *same* address for the new node. CONFIG_NET issues the following prompt:

```
What address do old nodes have configured for node new_node
(<PSDN-address>, <PRIMENET-address>, <address>)
```

where *new_node* is the name of the multiply addressed new node. On the second line of the prompt, CONFIG_NET displays the new node's PSDN address(es), if any, as well as its PRIMENET address. (A PRIMENET address can be recognized by the fact that it starts with 9999.)

To answer this prompt, you must run NETCFG on each old node that communicates with *new_node* to see what address the old node uses for *new_node*. You must make sure that all the old nodes that communicate with *new_node* agree on *new_node*'s address. Enter the agreed-upon address response to the CONFIG_NET prompt shown above. This agreed-upon address is sometimes called a **compatibility address**.

To display an old node's configuration, issue the NETCFG command on the old node. Answer YES in response to the Review old network configuration? prompt. When the configuration is displayed, look for the line with the name of the new node. If the column labeled Addr contains a number, that number is a PSDN address; enter this address in response to the CONFIG_NET prompt. If you do not see a number in the Addr column, the old node uses a PRIMENET address to identify the new node; choose the PRIMENET address in response to the CONFIG_NET prompt.

If different old nodes disagree on a new node's address, you must create new network configurations on the old nodes and correct the disagreement. To create a new configuration on an old node, answer YES in response to the NETCFG prompt, Create new network configuration? Refer to the 19.0 *System Administrator's Guide* for detailed instructions for using NETCFG.

For example, suppose SYSB is a new node with a TELENET address (311061766666) and a PRIMENET address (99990402010880). Suppose SYSA is an old node that communicates with SYSB. The CONFIG_NET prompt looks like this:

```
What address do old nodes have configured for node SYSB
(311061766666, 99990402010880, <address>)
```

To answer this prompt, you need to run NETCFG on SYSA. If you have not already done so, you can use FAST_SAVE to save your incomplete CONFIG_NET configuration, run NETCFG on SYSA to obtain the address, then continue with CONFIG_NET. Your NETCFG session on SYSA might look like this:

```
OK, NETCFG
Review old network configuration? YES

Rev    19.0 network configuration file

Ring Net
      Name          Addr          Ring ID   FAM INFO   RLOG
-----
*ME*  SYSA          1
      SYSB          311061766666    2   II/VALID.   No
                                Node-Node password: SECRET

Create new network configuration? NO
```

In this case, you would answer 311061766666 in response to the NETCFG prompt. On the other hand, if your NETCFG session looked like this:

OK, **NETCFG**

Review old network configuration? **YES**

Rev 19.0 network configuration file

Ring Net

	Name	Addr	Ring ID	FAM INFO	RLOG
	-----	-----	-----	-----	----
ME	SYSA		1		
	SYSB		2	II/VALID.	No

Node-Node password: SECRET

Create new network configuration? **NO**

then you would answer 99990402010880 in response to the CONFIG_NET prompt, indicating that the PRIMENET address is used.

Note

If you supply CONFIG_NET with an address that does not actually match the address used by old node(s), problems such as call collisions, inoperative synchronous lines, or remote file access errors could result.

Preparing to Configure Your PRIMENET Network

This chapter uses two examples to illustrate how to prepare your network configuration. This chapter also provides a configuration checklist, which lists all the information you need to have on hand to configure your network. Before using CONFIG_NET, you should draw a sketch of your network, review this checklist, and answer all the questions that pertain to your network.

Preparing for Configuration: Example One

Suppose you are in charge of a network with the following elements:

- Two half-duplex nodes: A and B, each with one half-duplex line
- A full-duplex line connecting A with a third node, C
- A ring connecting A with a fourth node, D
- A full-duplex line connecting A with TELENET
- A fifth node, E, accessible to A through TELENET

As the first step in preparing your configuration, make a rough sketch of the network. This helps you keep track of your network's topology as you answer CONFIG_NET's prompts. In your sketch, include all rings, LAN300s, full-duplex lines, half-duplex lines, and PSDNs. Also include all nodes, labeling each with its name. Show which nodes are connected, and by which lines. For example, show which nodes are on each ring, which nodes are connected by full-duplex lines, and so on. For the network outlined above, you might draw a picture like the one in Figure 5-1.

Note that the full-duplex line, FDX1, is drawn between Nodes A and C, but that the half-duplex lines on Nodes A and B are not connected to one another in the drawing. This difference reflects the fact that full-duplex connections are permanent, whereas half-duplex connections are temporary.

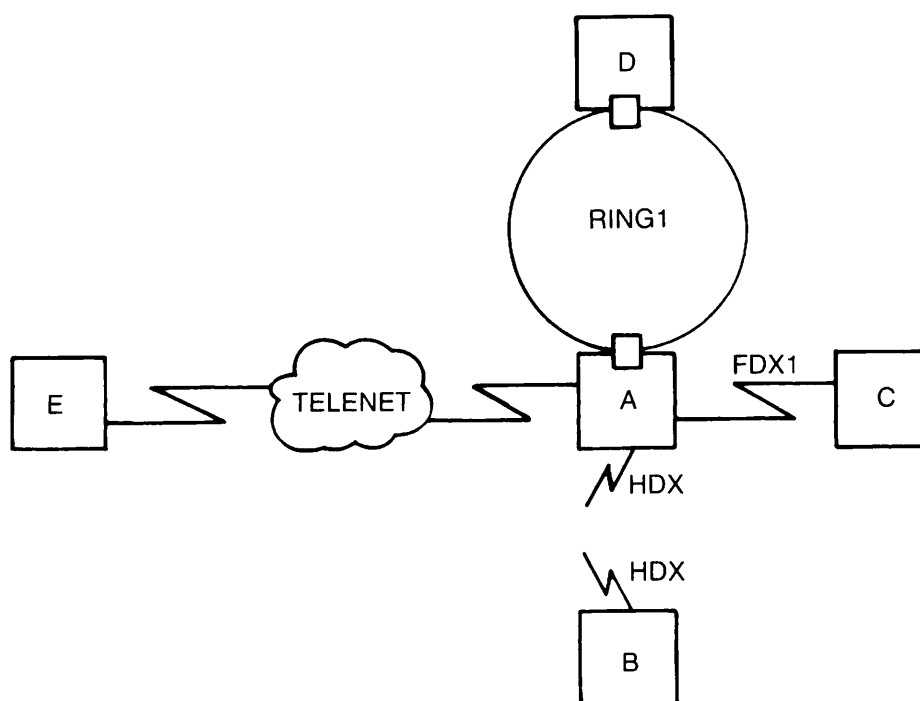


Figure 5-1
Network Sketch for Example One

Once you have a general network sketch, focus on detailed information about each node and connection. For the network in this example, answer the questions listed below. (Sample answers are supplied here.)

- What is Node A's TELENET address?

311061799999

- What is Node E's TELENET address?

311061788888

- Is Node A a gateway node?

Yes

- Which pairs of nodes communicate through Node A (using Node A as a gateway)?

B and C
 B and D
 B and E
 C and D
 C and E
 D and E

(Nodes A, B, and C are explicitly granted access to Node E. Node D is not, but Node E is able to call Node D over TELENET for reasons discussed below.)

Review the guidelines in Chapter 1, PRIMENET Overview, on configuring access over a gateway node. In particular, you should not configure RFA over a gateway.

- Which nodes have indirect TELENET addresses?

Node B — 31106179999903
 Node C — 31106179999902
 Node D — 31106175559901

(The fact that Node D is assigned a TELENET address allows Node E to call Node D over TELENET even though no access is explicitly configured between them. This point is discussed in more detail below.)

- What types of access does each node have to each other node? Do you want to enable forced user validation? Do you want to assign node-to-node passwords?

Table 5-1 shows all access rights in the network. FUV indicates that forced user validation is in effect. N-NP indicates that a node-to-node password is assigned.

Table 5-1
Access Rights on Sample Network One

<i>Nodes</i>	<i>Link Type</i>	<i>Access Rights</i>		
A to B	via HDX	IPCF		
A to C	via FDX1	RFA	FUV	N-NP
A to D	via RING1	ALL	FUV	N-NP
A to E	via TELENET	IPCF		
B to A	via HDX	RLOG		
B to C	via gateway	RLOG		
B to D	via gateway	IPCF		
B to E	via gateway	IPCF		
C to A	via FDX1	RFA	FUV	N-NP
C to B	via gateway	IPCF		
C to D	via gateway	RLOG		
C to E	via gateway	IPCF		

Table 5-1
Access Rights on Sample Network One – Continued

<i>Nodes</i>	<i>Link Type</i>	<i>Access Rights</i>
D to A	via RING1	ALL FUV N-NP
D to B	via gateway	IPCF
D to C	via gateway	RLOG
D to E	via gateway	NONE
E to A	via TELENET	IPCF
E to B	via gateway	IPCF
E to C	via gateway	IPCF
E to D	via gateway	NONE

Nodes A, B, and C are granted IPCF access to Node E. Since IPCF access is symmetric, Node E automatically has IPCF access to Nodes A, B, and C, even if this access is not explicitly granted to E. No access is configured between Nodes D and E.

Because Node A is directly connected to TELENET, it does not *need* IPCF access to Node E in order to connect to Node E. Similarly, because Node E is directly connected to TELENET, Node E does not need IPCF access to Nodes A, B, C, and D in order to access those nodes. As Chapter 3, PRIMENET Security, explains, a node that is directly connected to a PSDN may call any other node on the PSDN as long as it uses the called node's PSDN address in making the call.

Node D will not be able to call Node E, because Node D is not directly connected to TELENET and no access is configured between D and E.

- What is the ring node ID of each node on RING1?

Node A: 1

Node D: 2

- What is the logical line number of FDX1 at each end (that is, on Node A and on Node C)?

On Node A: 0

On Node C: 0

- Does FDX1 use LAP or LAPB protocol?

LAPB

- Does FDX1 use HDLC framing or bisynchronous framing? If bisynchronous framing is used, is the framing character set ASCII or EBCDIC?

FDX1 uses HDLC framing.

- On Nodes A and B, which logical synchronous line numbers (0 through 7) are assigned to half-duplex lines?

On Node A: 2

On Node B: 0

- Do you want to assign half-duplex passwords between Nodes A and B?

Yes

- What are the logical line numbers of the full-duplex lines connecting Nodes A and E to TELENET?

On Node A: 1

On Node E: UNKNOWN

- What are the protocol, framing, default packet size, default window size, and highest logical channel number (LCN) for virtual circuits on the line connecting Node A to TELENET?

Protocol: LAPB

Framing: HDLC

Default packet size (in bytes): 128

Default window size for line: 2

Highest LCN for virtual circuits: 4095

- Are any of the nodes running pre-Rev. 19.3 software?

No

- Are any of the nodes non-Prime nodes (running non-PRIMENET X.25 software)?

No

As you answer questions like these, you may want to add information to your sketch. For example, you might find it useful to draw in access rights, PSDN addresses, and logical line numbers. The example presented above appears again as Create Mode Example 8 in Chapter 7, Sample PRIMENET Configurations. That section presents the CONFIG_NET dialog that configures this network.

Preparing for Configuration: Example Two

Suppose you are responsible for configuring the network illustrated in Figure 5-2, which has these elements:

- A LAN300 named LAN300-1 with three nodes: P1, P2, and NP1
- A full-duplex line, FDX1, connecting P2 with a fourth node, NP2

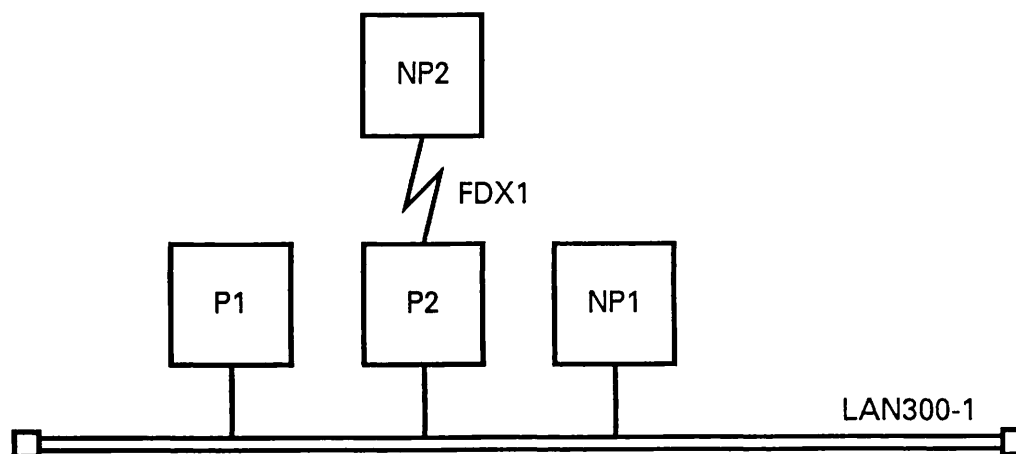


Figure 5-2
Network Sketch for Example Two

To prepare for configuring this network, you need to answer these questions:

- Are there any nodes running pre-Rev. 19.3 software?
No
- Are there any non-Prime nodes?
Yes, NP1 and NP2
- Does Node P2 serve as a gateway node?
Yes
- Which pairs of nodes communicate through Node P2 (using Node P2 as a gateway)?
P1 and NP2
NP1 and NP2
- What types of access does each node have to each other node? Do you want to enable forced user validation? Do you want to assign node-to-node passwords?

Table 5-2 shows all access rights in the network. FUV indicates that forced user validation is in effect. N-NP indicates that a node-to-node password is assigned.

Table 5-2
Access Rights on Sample Network Two

<i>Nodes</i>	<i>Link Type</i>	<i>Access Rights</i>
P1 to P2	via LAN300-1	ALL FUV N-NP
P1 to NP1	via LAN300-1	IPCF
P1 to NP2	via gateway	IPCF
P2 to P1	via LAN300-1	ALL
P2 to NP1	via LAN300-1	IPCF
P2 to NP2	via FDX1	IPCF
NP1 to P1	via LAN300-1	NONE
NP1 to P2	via LAN300-1	NONE
NP1 to NP2	via gateway	IPCF
NP2 to P1	via gateway	RLOG, IPCF
NP2 to P2	via FDX	NONE
NP2 to NP1	via gateway	IPCF

IPCF access is explicitly granted between these pairs of nodes: P1 to NP1, P1 to NP2, P2 to NP1, P2 to NP2, NP1 to NP2, NP2 to P1, and NP2 to NP1. Since IPCF access is symmetric (automatically granted in the reverse direction), IPCF access is automatically granted between all the nodes in the network.

- Does NP1 or NP2 require a source address in incoming calls?

No

- What is the indirect FDX1 address for node P1? (This is the address NP2 uses to call Node P1 through the gateway node P2. See Specifying Indirect FDX Addresses in Chapter 4, PRIMENET Network Configuration, for more information.)

999800000001

- What is the indirect LAN300-1 address for node NP2? (This is the address P1 and NP1 use to call Node NP2 through the gateway node P2. For more information, see Specifying Indirect LAN300 Addresses in Chapter 4, PRIMENET Network Configuration.)

999800000012

- What is the MAC + LSAP address for NP1?

11-22-33-44-55-66+CO

- What are the LHC300 logical device numbers for PRIMENET support on LAN300-1 for Nodes P1, P2, and NP1?

Node P1: 0

Node P2: 0

Node NP1: Unknown

- What is the highest logical channel number for virtual circuits on the line from Node NP1 to LAN300-1?

4095

- What is the default window size for the line from Node NP1 to LAN300-1?

7

- What is the default packet size (in bytes) for the line from Node NP1 to LAN300-1?

512

- Does Node NP1 act as Data Communications Equipment (DCE) or as Data Terminal Equipment (DTE), or does it use dynamic determination?

Dynamic determination

- Does Node NP1 use ISO 8881 procedures (drop idle links)?

Yes

- What is the LAPB address for NP2?

1

- What are the synchronous line numbers on Nodes P2 and NP2 for FDX1?

Node P2: 1

Node NP2: Unknown

- Does FDX1 use LAPB or LAP protocol?

LAPB

- Does FDX1 use HDLC, BSC-ASCII, or BSC-EBCDIC framing?

HDLC

- What is the highest logical channel number for virtual circuits on the line from Node NP2 to FDX1?

4095

- What is the default window size for the line from Node NP2 to FDX1?

7

- What is the default packet size (in bytes) for the line from Node NP2 to FDX1?

128

- Does Node NP2 act as a DCE or as a DTE, or does it use dynamic determination?

DCE

- Does Node NP2 use ISO 8881 procedures (drop idle links)?

No

The preceding example appears again as Example 9 of Create Mode Examples in Chapter 7, Sample PRIMENET Configurations. That section presents the CONFIG_NET dialog that configures this network.

Configuration Checklist

Listed below are questions that you should answer before using CONFIG_NET to configure your network. The answers to these questions, together with a sketch of your network, should prepare you adequately for the process of configuration.

Disregard any questions that do not pertain to your network. For example, if your network does not have any connections to PSDNs, you need not worry about PSDN-related questions.

These questions assume that you have read Chapter 1, PRIMENET Overview, Chapter 3, PRIMENET Security, and Chapter 4, PRIMENET Network Configuration. If you have trouble answering any of the questions after reading those chapters, consult your Prime Customer Support Center. For questions regarding PSDNs (for example, PSDN addresses and line characteristics), consult your PSDN Administrator.

General Questions

The following questions pertain to your network as a whole:

- Do you share the responsibility of network configuration with another administrator? Or, do you use more than one global network configuration file? (Chapter 4, PRIMENET Network Configuration, discusses networks that require more than one configuration file.)

If so, be sure that ring node IDs, access rights, node-to-node passwords, half-duplex passwords, and full-duplex line characteristics (framing and protocol) are assigned consistently. That is, all configuration files should agree about these aspects of the network. If you share responsibility with another administrator, you should plan the configuration together.

- Does your network contain any systems that are post-Rev. 19.3 but pre-Rev. 21.0?

If so, you need a separate configuration file for these nodes. You must ensure that the configuration file for these nodes is consistent with the new configuration file for Rev. 21.0 nodes. All information must match, including ring node IDs, access rights, passwords, and so on. For more information on pre-Rev. 21.0 nodes, refer to *Mixed-Rev. Networks with Pre-Rev. 21.0 Nodes* in Chapter 4, *PRIMENET Network Configuration*.

- Does your network contain any pre-Rev. 19.3 systems?

If so, the information that you supply to CONFIG_NET must be consistent with the information in the old nodes' configuration file. That is, the nodes should agree on ring node IDs, access rights, passwords, and full-duplex line characteristics.

You should also take note of any network addresses (for example, PSDN addresses) that occur in the old nodes' configuration files. To understand the reason for this, refer to the explanation and examples in the section entitled *Specifying Addresses in a Mixed-Rev. Network* in Chapter 4, *PRIMENET Network Configuration*. That section shows you how to display the configuration file on a pre-Rev. 19.3 system. For more details about network configuration prior to Rev. 19.3, refer to the Rev. 19.0 *System Administrator's Guide*.

Note

When you configure your network, CONFIG_NET asks you to list any pre-Rev. 19.3 nodes on the network. Be sure to list *all* pre-Rev. 19.3 nodes. If you omit one or more of them, problems such as call collisions, inoperative synchronous lines, or remote file access errors could result.

- What is the network topology? That is, what systems are connected to each other, and by what types of network links (rings, LAN300s, full-duplex lines, half-duplex lines, PSDNs)?

This question is best answered with a sketch, as described in the example at the beginning of this chapter.

- What are the node names of all the systems on your network?

A node's name must be the name given by its SYSNAM CONFIG directive. This name can be one to six characters long, with the same restrictions as PRIMOS filenames.

- Which nodes are non-Prime nodes?
- Are any nodes in your network connected to PSDNs? If so, which nodes? Which PSDNs?

Caution

It is very important that you configure *all* of your network's connections to PSDNs. For example, if a pre-Rev. 19.3 node is connected to a PSDN, describing that connection in the old node's NETCON file is not sufficient; CONFIG_NET must also know about it. If you do not tell CONFIG_NET about all of the network's PSDN connections, PSDN addresses may not be assigned properly. In that case, problems such as call collisions, inoperative synchronous lines, or remote file access errors could result.

- Which nodes, if any, are gateway nodes (nodes on which the Route-through Server is running)?
- Which pairs of nodes (if any) communicate through a path of one or more gateway nodes?

Questions for Rings

If your network contains one or more rings, answer these questions for each ring:

- Which nodes are on the ring?
- What is the ring node ID of each node on the ring?

When you configure the network, CONFIG_NET asks whether you want to accept the pre-set (default) ring node ID or assign a different one. The ring node ID is a number from 1 through 247. On a given ring, each node must have a unique ring node ID.

Question for LAN300s

If your network contains one or more LAN300s, answer this question for each LAN300: Which nodes are on the LAN300?

Questions for Full-duplex Lines

The following questions apply to each full-duplex line connecting two Prime systems on your network:

- What is the logical line number of the line at each end (that is, on each of the two nodes the line connects)?

Each synchronous line on a Prime node, full-duplex or half-duplex, must be assigned a unique logical line number from 0 through 7. You do not need to know the synchronous line number for a non-Prime node. Refer to Synchronous Line Restrictions in Chapter 1, PRIMENET Overview, to find out about restrictions on the number of synchronous lines allowed. Does the line use LAP or LAPB protocol?

- Does the line use HDLC framing or bisynchronous framing? If bisynchronous framing is used, is the framing character set ASCII or EBCDIC?

Questions for Half-duplex Lines and Nodes

Answer the following questions if your network includes nodes with half-duplex lines:

- Which nodes have half-duplex lines? How many half-duplex lines does each of these nodes have?
- On each of these nodes, which logical synchronous line numbers are assigned to half-duplex lines?

Each synchronous line on a node, full-duplex or half-duplex, must be assigned a unique logical line number from 0 through 7. Refer to Chapter 1, PRIMENET Overview, to find out about restrictions on the number of synchronous lines allowed. For each pair of nodes that communicate over HDX lines, do you want to assign incoming and/or outgoing HDX passwords?

Questions for Prime-to-PSDN Full-duplex Lines

Answer the following questions for each full-duplex line connecting a Prime system to a PSDN:

- What is the logical line number of the line on the Prime system?

Each synchronous line, full-duplex or half-duplex, must be assigned a unique logical line number from 0 through 7. Does the line use LAP or LAPB protocol?

- Does the line use HDLC framing or bisynchronous framing? If bisynchronous framing is used, is the framing character set ASCII or EBCDIC?
- What packet size and window size did you subscribe to?
- What is the highest logical channel number used to identify a virtual circuit on the line? (Different PSDNs may require different ways of numbering virtual circuits on a line.)

If you do not know the answers to the last four questions, contact the PSDN Administrator.

Questions for Each Node

Answer the following questions for each node:

- Is it on a ring?
- Is it on a LAN300 (or two LAN300s)?
- What is the logical device number of the LHC300 connecting it to each LAN300?
- Does it have full-duplex connection(s)?
- Does it have half-duplex line(s)?
- What are the synchronous line numbers for the full-duplex and half-duplex connections?
- Does it communicate with other nodes through gateway nodes (that is, over indirect connections)? Which nodes?
- Can it be accessed indirectly by a non-Prime node on an FDX line (through a gateway node)? If so, what is its indirect FDX address?
- Can it be accessed indirectly by a non-Prime node on a LAN300 (through a gateway node)? If so, what is its indirect LAN300 address?
- Is it directly connected to a PSDN? Which PSDN? What is the node's PSDN address?
- Does it have indirect access to a PSDN (through a gateway node)? If so, then:
 - What is the node's indirect PSDN address?
 - Which gateway node is directly connected to the PSDN and routes data to the node in question?
 - On that gateway node, which synchronous line connects to the PSDN and is used to route data to the node in question?
- Does it communicate with non-Prime nodes that require a source address in incoming calls? If so, what are its LAN300 and/or FDX address(es)?
- Does the node have more than one address? If so, and if the network includes any "old" (pre-Rev. 19.3) nodes, which one of the multiple addresses is recognized and used by the old nodes? For more information, see *Specifying Addresses in a Mixed-Rev. Network* in Chapter 4, PRIMENET Network Configuration.
- What type(s) of access will the node have:
 - To each other node on the same ring?
 - To each other node on the same LAN300(s)?
 - To each other node accessible by a full-duplex line?
 - To each other node accessible by a half-duplex line?
 - To each other node accessible through a PSDN?
 - To each other node accessible over a gateway connection?

- For each node that the node can access, do you want to:
 - Force user validation?
 - Assign a node-to-node password?

Additional Questions for Non-Prime Nodes

For each non-Prime node on your network, answer these questions in addition to the questions in the section entitled Questions for Each Node.

- Is the non-Prime node attached to a LAN300? If so, what is its MAC + LSAP address? What is the name of the LAN300?
- Is the non-Prime node attached to a full-duplex line? If so, what is its LAPB address? What is the name of the full-duplex line?
- Does the non-Prime node require a particular source address to be used in incoming calls from a Prime node?
- What addresses are required to connect to applications on the non-Prime node?
- What addresses are required for the non-Prime node to connect to applications on Prime nodes?
- What is the highest logical channel number for virtual circuits on the non-Prime node's link to the LAN300, FDX line, or PSDN?
- What are the default window and packet sizes for the non-Prime node's link to the LAN300, FDX line, or PSDN?
- Does the non-Prime node act as a DCE or as a DTE, or does it use dynamic determination (as specified in ISO DP8208)?
- Does the node use ISO 8881 procedures (drop idle links)?

Configuring Your PRIMENET Network

This chapter explains how to configure your network with CONFIG_NET, the PRIMENET configuration program. This chapter assumes that your network hardware is in place, that you have read the preceding chapters of this book, that you have prepared a sketch of your network, and that you have answered the questions in the configuration checklist presented in Chapter 5, Preparing to Configure Your PRIMENET Network.

This chapter presents these topics:

- Invoking CONFIG_NET
- Displaying help information
- Using CONFIG_NET
- Verification
- Creating a configuration
- Defining the network topology
- Providing per-node information
- Editing a configuration
- Strategies for editing your network
- Special editing features
- Listing a configuration
- Saving and validating a configuration
- Quickly saving a configuration
- Terminating CONFIG_NET

CONFIG_NET's error messages are listed and described in Appendix B.

Caution

Before you configure your network, be sure you understand the configuration guidelines and restrictions described in Chapter 1, PRIMENET Overview, as well as the security guidelines discussed in Chapter 3, PRIMENET Security.

Invoking CONFIG_NET

The CONFIG_NET command invokes CONFIG_NET. It has this format:

```
CONFIG_NET [pathname] [-HELP  
                     -NO_WAIT]
```

where the optional *pathname* is the pathname of an existing PRIMENET configuration file. The options have these meanings:

- | | |
|-----------------|---|
| -HELP | Displays the CONFIG_NET command syntax. |
| -NO_WAIT | Causes CONFIG_NET to display listing information without stopping. If you do not use this option, CONFIG_NET stops and displays the - MORE- - prompt after every screen of information. Press <input type="button" value="Return"/> to view the next screen, or enter N, NO, Q, or QUIT to terminate the display. |

When you specify a pathname, CONFIG_NET attempts to read the network configuration from the specified file, and displays an error message if it is unreadable. Once CONFIG_NET is satisfied that the specified file is consistent, or if you did not specify a file, it displays the **option prompt**:

```
Create, Edit, Quit, Save, Fast_Save, List, or Help?
```

Displaying Help Text

To display HELP text at any time during a CONFIG_NET session, press -P, then enter HELP in response to the option prompt. For example,

```
Create, Edit, Quit, Save, Fast_Save, List, or Help? HELP
```

CONFIG_NET displays this HELP message:

CREATE mode is an interactive question/answer session which should be used to create a new network configuration, or to complete a configuration which was partially entered or edited.

EDIT mode is used to make changes to an existing network configuration.

QUIT will exit CONFIG_NET without saving the configuration information.

SAVE writes the configuration information into a disk file.

FAST_SAVE writes the configuration to disk without validation.

LIST mode is used to display the existing configuration information.

CONFIG_NET also has HELP descriptions for each Edit menu. These menus are discussed in the section entitled Editing a Configuration.

Using CONFIG_NET

CONFIG_NET has two major modes of operation: **Create mode** and **Edit mode**. In Create mode, CONFIG_NET displays a series of questions to help you create a new configuration or supply information about a new configuration object, such as a new node or a new subnetwork. In Edit mode, CONFIG_NET presents a menu-driven interface that allows you to add, delete, or modify configuration information. The LIST facility displays all or part of the configuration on your screen, which is useful when you cannot remember previously entered information. The HELP facility explains CONFIG_NET's prompts and menus.

You can switch between Create and Edit modes or use the LIST or HELP facility at any time during a CONFIG_NET session by summoning the option prompt:

Create, Edit, Quit, Save, Fast_Save, List, or Help?

Whenever you invoke CONFIG_NET, your session begins with the option prompt. To summon the option prompt at any time during a configuration session, press **Ctrl-P**. If you summon the option prompt while answering a Create mode prompt, CONFIG_NET returns you to the same place when you reenter Create mode. At the option prompt, you can enter any one of these responses:

<i>Response</i>	<i>Result</i>
CREATE	Puts you in Create mode, or returns you to Create mode at the same place in the configuration where you left.
EDIT	Puts you in Edit mode to add, modify, or delete existing configuration information.

<i>Response</i>	<i>Result</i>
QUIT	Terminates CONFIG_NET without saving the configuration on disk.
SAVE	Fully validates the data in the configuration, then writes it on disk. If CONFIG_NET detects errors, it notifies you and gives you the option to write the file on disk anyway.
FAST_SAVE	Writes the configuration to disk without first validating it.
LIST	Displays all or part of the configuration.
HELP	Displays an explanation of the responses to the option prompt.

Verification

CONFIG_NET checks your configuration data for errors at the following times:

- When you enter Create mode
- Continuously as you work within Create mode
- When you enter the SAVE response to the option prompt

CONFIG_NET verifies the configuration whenever you enter Create mode, regardless of whether you are just beginning to work on an existing configuration or returning from Edit or List mode. If CONFIG_NET detects erroneous, inconsistent, or incomplete information, it automatically starts Create mode at the point where it detects the problem. CONFIG_NET then prompts you for the required information.

As you work in Create mode, CONFIG_NET examines your input. If you supply an improper entry, CONFIG_NET repeats the prompt so that you can correct the error.

Finally, when you enter the SAVE response at the option prompt, CONFIG_NET examines the configuration data for consistency. If the file is inconsistent or incomplete, CONFIG_NET warns you:

```
Configuration errors detected.  
Do you wish to save it anyway?
```

You may want to save the file (write it on disk) at this point. Then, to find out which information is missing or incorrect, enter Create mode. CONFIG_NET prompts you for the required information.

CONFIG_NET checks your data for such errors as:

- Incorrect syntax
- Incorrect range
- Incorrect type of data (for example, numbers supplied when an alphanumeric string is required)

- More than one node with the same name, address, or ring node ID
- Too many lines connected to one node
- One node defined to be on more than one ring
- One node defined to be on more than two LAN300s
- Rings, LAN300s, or FDX lines with only one node configured
- Access rights granted where no physical connection is defined
- Conflicting access rights
- Two nodes configured to have gateway access, where one or more of the intervening nodes has no Route-through Server
- Two nodes configured to have gateway access, where the path connecting them includes an adjacent pair of nodes that cannot access one another with at least the IPCF subroutines

Creating a Configuration

The next two sections, Defining the Network Topology and Providing Per-Node Information, list and describe the prompts that CONFIG_NET displays when you are creating a configuration or adding a new configuration object. To enter create mode, enter CREATE at the option prompt. The Create mode dialog has two parts. In the first part, CONFIG_NET prompts you to describe the general physical layout, or topology, of the network. In the second part, CONFIG_NET prompts you for specific information about each node in the network. CONFIG_NET checks your input continuously as you work in Create mode.

CONFIG_NET Prompts

CONFIG_NET prompts consist of question followed by a list of the possible answers enclosed in parentheses. The first item in the list is the default value; to choose it, press without entering any data. For example, pressing after the following prompt:

```
Ring node ID for A on RING1 (1, <1-247>):
```

assigns the default ring node ID (1) to Node A.

When you type an entry and press in response to a prompt that can accept multiple answers, CONFIG_NET repeats the list of choices. To go on to the next prompt, press in response to the repeated prompt. For example,

```
Enter nodes connected to RING1
(NONE, <node names>):  A
(NONE, <node names>):
Enter nodes connected to FDX1
(NONE, <node names>):
```

To enter more than one answer, you may either use separate lines:

```
Enter nodes connected to RING1
(NONE, <node names>):  A
(NONE, <node names>):  B
(NONE, <node names>):
Enter nodes connected to FDX1
(NONE, <node names>):
```

or include multiple answers on the same line, separated by commas, as shown below. You do not need to include spaces after the commas.

```
Enter nodes connected to RING1
(NONE, <node names>):  A,B
(NONE, <node names>):
Enter nodes connected to FDX1
(NONE, <node names>):
```

To suppress repetition of a prompt, enter a semicolon (;) after your last entry. For example:

```
Enter nodes connected to RING1
(NONE, <node names>):  A, B;
Enter nodes connected to FDX1
(NONE, <node names>):
```

Options that appear in angle brackets (< >) require a specific response, such as a nodename or a subnetwork name. In the example shown below, you would enter the names of the nodes running non-PRIMENET X.25 software.

```
Enter nodes running non-Primenet X.25 software
(NONE, <node names>):
```

The CONFIG_NET prompts query you about two categories of information: Network Topology and Per-Node Information.

Defining the Network Topology

CONFIG_NET asks you the following questions to help you define the network topology. CONFIG_NET uses this information to determine how many nodes are on the network and how the nodes are connected.

- Name the nodes connected to each ring in the network. Node names can be as many as six characters long.
- Name the nodes connected to each LAN300 in the network.
- Indicate which pairs of nodes are connected by full-duplex lines.

- Name all nodes that have half-duplex lines.
- Name all PSDNs that can be accessed from your network, and indicate which nodes are connected to each PSDN.
- Identify any gateway nodes in the network.
- Identify any pre-Rev. 19.3 nodes in the network.
- Identify any nodes in the network running non-PRIMENET X.25 software (non-Prime nodes).

Ring Definition

CONFIG_NET assigns the names RING1, RING2, and so on to the rings in your configuration, incrementing the integers in order. You can change the name with CONFIG_NET's Edit mode. This prompt queries you for the nodes connected to each ring in your network:

```
Enter nodes connected to RING1
(NONE, <node names>):
```

Enter the names of the nodes on the (first) ring, RING1. If your network does not include any rings, enter NONE or press . Since this prompt can accept multiple answers, CONFIG_NET repeats the list of choices until you press as an answer or terminate your entry with a semicolon (;). CONFIG_NET automatically queries you about the next ring after you have entered the maximum number of nodes allowed on a ring, 247.

CONFIG_NET continues to issue this prompt, incrementing the ring number each time. When you have configured all of your network's rings, enter NONE or press without entering data. CONFIG_NET then queries you about LAN300s.

Note

Each ring can have a maximum of 247 nodes. A given node can be on only one ring.

LAN300 Definition

CONFIG_NET assigns the names LAN300-1, LAN300-2, and so on to the LAN300s in your configuration, incrementing the integers in order. You can change the name with CONFIG_NET's Edit mode. You must ensure that this name matches the one used for the LAN300 in your NTS configuration file, if you have one. Otherwise, if you attempt to start PRIMENET while NTS is already running on the LAN300, START_NET detects the naming inconsistency and does not start PRIMENET. START_NTS also checks for LAN300 name consistency when you attempt to start NTS on a LAN300 on which PRIMENET is already running.

The following prompt queries you for the nodes connected to each LAN300 in your network:

```
Enter nodes connected to LAN300-1
(NONE, <node names>):
```


Enter the names of the nodes on the (first) LAN300, LAN300-1. If your network does not include any LAN300s, enter NONE or press . Since this prompt can accept multiple answers, CONFIG_NET repeats the list of choices until you press as an answer or terminate your entry with a semicolon (;). CONFIG_NET automatically queries you about the next LAN300 after you have entered the maximum number of nodes allowed on a LAN300, 256.

CONFIG_NET continues to issue this prompt, incrementing the LAN300 number each time. When you have defined all of your network's LAN300s, enter NONE or press without entering data. CONFIG_NET then queries you about full-duplex lines.

Note

Each LAN300 can have a maximum of 256 PRIMENET nodes. A given node can be on only two LAN300s (for PRIMENET).

Full-duplex Definition

CONFIG_NET assigns the names FDX1, FDX2, and so on to the full-duplex lines in your configuration, incrementing the integers in order. You can change the name with CONFIG_NET's Edit mode. The following prompt queries you for the nodes connected to each full-duplex point-to-point line in your network:

```
Enter nodes connected to FDX1
(NONE, <node names>):
```

Enter the names of the two nodes connected by the (first) full-duplex line, FDX1. If your network does not include any full-duplex lines, enter NONE or press .

CONFIG_NET continues to issue this prompt, incrementing the line number each time. When you have defined all of your network's full-duplex lines, enter NONE or press without entering data. CONFIG_NET then queries you about half-duplex lines.

Note

You must observe the synchronous line restrictions described in Synchronous Line Restrictions in Chapter 1.

Half-duplex Definition

The following prompt queries you about the half-duplex nodes in your network:

```
Enter nodes connected to HDX
(NONE, <node names>):
```

Enter the names of all half-duplex nodes on your network, that is, the nodes that have one or more half-duplex lines. If none of the nodes in your network has half-duplex lines, enter NONE or press . CONFIG_NET then queries you about your network's Packet Switching Data Network (PSDN) connections.

Note

You must observe the synchronous line restrictions described in Synchronous Line Restrictions in Chapter 1, PRIMENET Overview.

Packet Switching Data Network Definition

The following prompt queries you about the PSDNs to which your network is connected:

```
Enter packet switching data network names
(NONE, <PSDN names>):
```

If your network includes one or more PSDN connections, enter the names of the PSDNs. The following PSDNs are supported: AUSTPAC, DATAPAC, DDN, IS8208, ITAPAC, PSS, SAPONET, TELENET, TELEPAC, TRANSPAC, and TYMNET. If you want to connect to a PSDN that is not included in this list, use the name X.25.

Note

Later in the dialog, CONFIG_NET asks you for default window size, packet size, and highest logical channel number to be used for a virtual circuit on the PSDN connection you have just defined. If you specified X.25 as your PSDN, you must be especially careful to enter the correct values for these parameters, as the CONFIG_NET defaults for X.25 may not be appropriate for your PSDN.

If your network does not include any connections to PSDNs, enter NONE or press . CONFIG_NET then queries you about your network's gateway nodes.

If you entered one or more PSDN names, CONFIG_NET issues the following prompt for each PSDN:

```
Enter nodes connected to PSDN
(NONE, <node names>):
```

where *PSDN* is a PSDN name you entered in response to the previous prompt. Enter the names of the node(s) that are *directly* connected to *PSDN* via full-duplex lines. Do not include nodes that are connected indirectly, via gateways. A node can be connected to two different PSDNs, but each node can support only *one* connection to a given PSDN.

Note

It is very important to configure *all* of your network's connections to PSDNs. For example, if a pre-Rev. 19.3 node is connected to a PSDN, describing that connection in the old node's NETCON file is not sufficient; CONFIG_NET must also know about it. If you do not tell CONFIG_NET about all of the network's PSDN connections, PSDN addresses may not be assigned properly. In that case, problems such as call collisions, inoperative synchronous lines, or remote file access errors could result.

Gateway Definition

The following prompt queries you about the gateway nodes in your network:

```
Enter gateway nodes  
(NONE, <node names>):
```

Enter the names of your network's gateway nodes. Include only those nodes that route data. Do not include nodes that have gateway access but are not themselves gateways.

If your network does not include any gateway nodes, enter NONE or press Return. CONFIG_NET then queries you about your network's pre-Rev. 19.3 nodes.

Note

You cannot connect two different gateway nodes to the same PSDN. For other restrictions concerning gateway nodes, refer to Guidelines for using Gateway Service in Chapter 1, PRIMENET Overview.

Pre-Rev. 19.3 Node Definition

The following prompt queries you about your network's pre-Rev. 19.3 nodes, that is, nodes that are running pre-Rev. 19.3 PRIMOS.

```
Enter nodes running old (pre-rev-19.3) PRIMOS  
(NONE, <node names>):
```

Enter the names of any pre-Rev. 19.3 nodes on your network. Press Return or enter NONE if your network does not contain pre-Rev. 19.3 nodes.

Note

Be sure to list *all* of your network's pre-Rev. 19.3 nodes. If you omit one or more of them, problems such as call collisions, inoperative synchronous lines, or remote file access errors could result.

Non-Prime Node Definition

The following prompt queries you about your network's non-Prime nodes, that is, the nodes running non-PRIMENET X.25 software. These non-Prime nodes can be attached to LAN300s, FDX lines, or PSDNs.

```
Enter nodes running non-Primenet X.25 software  
(NONE, <node names>):
```

Enter the names of the non-Prime nodes on your network, such as PADs and non-Prime hosts. Define X.25 packet switches as PSDNs because they have a routing function.

This completes the topology definition part of the Create mode dialog. Next, CONFIG_NET queries you for information about each node in the configuration.

Providing Per-node Information

Once you have defined your network's topology, CONFIG_NET asks for information about each node. Having a sketch of your network on hand can help you to answer these questions quickly and accurately. For a complete list of the information required by CONFIG_NET, refer to the configuration checklist in Chapter 5, Preparing to Configure Your PRIMENET Network.

Prompts about a particular node are introduced with the following message:

```
Describe node node name
```

where *node name* is the name of one of the nodes you entered in the first part of the CREATE dialog, the network topology definition. CONFIG_NET issues different prompts for each node, depending on the types of communications lines to which the node is connected. For example, if a node is connected to a ring, CONFIG_NET asks for the ring node ID. If the node also has a full-duplex line, CONFIG_NET asks about the characteristics of that line; and so on.

This section lists all of CONFIG_NET's per-node prompts, grouped by category as follows:

- The **per-node prompt for rings** appears if the node is connected to a ring.
- The **per-node prompt for LAN300s** appears if the node is connected to a LAN300.
- **Per-node prompts for full-duplex lines** appear if the node has one or more full-duplex lines.
- **Per-node prompts for half-duplex lines** appear if the node has one or more half-duplex lines.
- **Per-node prompts for PSDNs** appear if the node is directly connected to a PSDN, or if the node could be connected to a PSDN indirectly (through gateway nodes).
- **Universal per-node prompts** appear for all nodes, both Prime and non-Prime. These prompts ask about access rights, forced user validation, and node-to-node passwords for each node with which the node can communicate.
- **Per-node prompts for non-Prime nodes** appear for nodes marked as non-Prime nodes (those running non-PRIMENET X.25 software).

In all of the following prompts, *node name* is the node that appeared in the most recent Describe node message on your screen; *ring*, *LAN300*, *fdx*, and *PSDN* are the names of a ring, a LAN300, a full-duplex line, or a PSDN, respectively.

Per-node Prompt for Rings

The following prompt appears if the node is attached to a ring:

```
Ring node ID for node name on ring (default_ID, 1-247):
```

In this prompt, *ring* is the name of the ring to which *node name* is connected (RING1, RING2, etc.). The ring node ID is the node's Level 2 (link level) address. CONFIG_NET supplies default values for all ring node IDs. To accept the default, press (or enter the value of *default_ID*). Alternatively, you may override the default by entering a number from 1 through 247. If you enter an ID that is already in use on *ring*, CONFIG_NET repeats the prompt.

Note

If you use different configuration files on different ring nodes, be sure that the IDs are assigned consistently in the different files.

Per-node Prompts for LAN300s

For each LAN300 to which the node is attached, CONFIG_NET issues this prompt:

```
LHC logical device number for Primenet support for node name  
on LAN300 (UNKNOWN, <0-7>):
```

In this prompt, *LAN300* is the name of (one of) the LAN300(s) to which *node name* is connected. Enter the logical device number of the LHC300 by which *node name* is attached to *LAN300*. The LHC300's logical device number is assigned by an LHC directive in the node's CONFIG file, which is executed at cold start. (For more information on the LHC CONFIG directive, refer to Chapter 8, Setting PRIMENET-related CONFIG Directives.)

If you do not know the LHC300 logical device number, press or enter UNKNOWN. Note that if you answer UNKNOWN, you cannot use this version of the network configuration file on *node name*. The network configuration file used on *node name* must contain the LHC300 logical device numbers for all of *node name*'s LHC300s. If you enter an LHC300 logical device number that is already in use on *node name*, CONFIG_NET displays an error message and repeats the prompt.

Per-node Prompts for Full-duplex Lines

For each full-duplex line to which the node is attached, CONFIG_NET issues the following prompts:

```
Synchronous line number on node name for fdx  
(UNKNOWN, <0-7>):
```

In this prompt, *fdx* is a full-duplex line to which *node name* is attached (FDX1, FDX2, and so on). Enter the logical synchronous line number assigned to *fdx* on *node name*. If you do not

know which logical line number *node name* uses for *fdx*, press or enter UNKNOWN. Note that if you answer UNKNOWN, you cannot use this version of the network configuration file on *node name*. The network configuration file used on *node name* must contain the logical line numbers for *node name*'s full-duplex lines.

```
Protocol for line fdx
(LAPB, LAP):
```

Enter the protocol used on line *fdx*. We recommend the default protocol, LAPB (Link Access Protocol Balanced), because it is the most recent international standard. However, since LAPB was not supported prior to Rev. 19.3, you must specify LAP when one of the nodes on *fdx* is a pre-Rev. 19.3 node.

```
Framing for full-duplex line fdx
(HDLC, BSC-ASCII, BSC-EBCDIC)
```

Enter the framing used on line *fdx*. We recommend the default framing type, HDLC, because it is the most recent international protocol. Note that the ICS1 supports HDLC framing only.

For each line, CONFIG_NET prompts you for the framing and protocol only once. For example, if FDX1 connects Nodes A and B, the framing and protocol prompts for FDX1 appear in the per-node dialog for Node A or Node B, but not both.

Per-node Prompts for Half-duplex Lines

CONFIG_NET issues the following prompt if the node is a half-duplex node:

```
Synchronous line numbers for connections to the half-duplex network
(UNKNOWN, <0-7>):
```

Enter the logical synchronous line number(s) assigned to the half-duplex line(s) on *node name*. If you do not know which logical line number(s) *node name* uses for half-duplex communication, press or enter UNKNOWN. Note, however, that if you answer UNKNOWN, you cannot use this version of the network configuration file on *node name*. The network configuration file that is used on *node name* must contain the logical line number(s) for *node name*'s half-duplex line(s).

The following pair of prompts is repeated for each half-duplex node that *node name* can access via half-duplex lines:

```
node name's incoming HDX password from node node1
(NONE, YES, <password>):
```

```
node name's outgoing HDX password to node1
(NONE, YES, <password>):
```

Half-duplex passwords are described in Chapter 3, PRIMENET Security.

These prompts do not appear if the passwords in question have already been defined.

Note

When you ask CONFIG_NET to generate an HDX password for you, enter the entire word YES. If you enter Y or YE only, CONFIG_NET takes Y or YE to be your choice of a password.

Press or enter NONE if you do not want to assign a password. Answer YES if you want CONFIG_NET to generate a random password for you; in this case, CONFIG_NET displays the following statement:

Generated password is *nnnnnn*

Alternatively, you can enter your own password.

Caution

For security purposes, CONFIG_NET generates different random HDX passwords each time it is run. Thus, if you use multiple configuration files in your network, supply your own HDX passwords to ensure consistency.

Per-node Prompts for PSDNs

CONFIG_NET issues the following prompts for each PSDN to which the node is directly connected:

Enter *PSDN* addresses for *node name*
(NONE, PSDN addresses):

Enter the PSDN addresses for *node name* on *PSDN*.

Note

A PSDN address cannot begin with 9999.

Synchronous line numbers for *PSDN* address *nnnnnnnnnnnnnnnn*
(UNKNOWN, 0-7):

Enter the logical line number of *node name*'s synchronous line for *PSDN* address *nnnnnnnnnnnnnnnn*. If you do not know which logical line number(s) *node name* uses for that address, press or enter UNKNOWN. Note, however, that if you answer UNKNOWN,

you cannot use this version of the network configuration file on *node name*. The network configuration file that is used on *node name* must contain the logical line number(s) for *node name*'s PSDN connections.

One synchronous line can support more than one PSDN address. Thus, you can specify the same logical line number for two (or more) different addresses. However, only one full-duplex line can be used at a time to connect a given node to a given PSDN.

Protocol for line *line number* to PSDN
(LAPB, LAP):

Enter the protocol used on line *line number* to PSDN.

Framing for line *line number* to PSDN
(HDLC, BSC-ASCII, BSC-EBCDIC):

Enter the framing used on line *line number* to PSDN.

Highest logical channel number for line *line number* to PSDN
(2047, <1-2047>):

Enter the highest logical channel number that can be used for a virtual circuit on line *line number*. Ask the PSDN Administrator for this information. Prime supports a maximum of 900 virtual circuits at Rev. 21.0. However, the number you supply here is not the number of virtual circuits on the line, but the highest number used to *identify* a virtual circuit on the line.

Different PSDNs may require different ways of numbering virtual circuits on a line. For example, numbering sometimes begins with zero. In this case, if a line supported 16 virtual circuits, the circuits would be numbered 0 through 15, and you would enter 15 in response to the above prompt. (If you entered 16, call requests from your system over that line would fail.) Check with your PSDN Administrator to find out how many virtual circuits your line supports and how they are numbered.

Default window size for line *line number* to PSDN
(2, <1-7>):

Enter the default window size for line *line number* to PSDN. Consult your PSDN Administrator for this information.

Default packet size (in bytes) for line *line number* to PSDN
(256, <16-256>):

Enter the default packet size (in bytes) for line *line number* to PSDN. Consult your PSDN Administrator for this information.

Observe these considerations when configuring the default window size and default packet size:

- The window and packet size for incoming remote login calls are limited by the size of the buffers allocated for remote login lines (remote buffers). The default window size times the default packet size cannot exceed the size of remote buffers on the

Prime node. Remote buffer sizes are set with the REMBUF directive in the node's CONFIG file, or by the CAB command on Rev. 22.0 nodes. For more information on REMBUF, see Chapter 8 of this manual, Setting PRIMENET-related CONFIG Directives, and Appendix A of the *Programmer's Guide to Prime Networks*. For more information on CAB, see Chapter 9 of this manual, Setting PRIMENET-related PRIMOS.COMI Commands.

- Window size and packet size are no longer restricted to 2 and 128, respectively, for remote login calls. All of the values listed above are now acceptable.
- Window size and packet size can now be negotiated on a per-call basis for remote login calls.
- Some PSDNs impose packet and window size restrictions. Check with your PSDN representative for more information.

CONFIG_NET issues the following prompt if *node name* may be connected to *PSDN* indirectly, via gateway nodes.

```
Indirect PSDN address for node node name
(NONE, <address>):
```

Enter *node name*'s indirect *PSDN* address. Press or enter NONE if *node name* has no indirect *PSDN* address. Refer to Chapter 4, PRIMENET Network Configuration, for information on indirect addresses.

If you enter an address, CONFIG_NET issues the following two prompts:

```
Gateway node which will route address address
from PSDN to node node name
(NONE, <nodenames>):
```

In this prompt, *address* is the address you entered in response to the previous prompt. Enter the gateway node that will receive calls for *address* from the PSDN and route them through to *node name*.

```
Lines on node gateway for routing PSDN address address
for node node name
(UNKNOWN, <0-7>): 0;
```

In this prompt, *gateway* is the name of the gateway node you specified in the previous prompt. Enter the logical line number of the synchronous line on *gateway* connecting *gateway* with *PSDN*.

Universal Per-node Prompts

This section describes CONFIG_NET's universal per-node prompts, which query you about access rights, forced user validation, and node-to-node passwords. CONFIG_NET issues each of

these prompts for each subnetwork to which the node is attached. The prompts are presented in the following sections:

- Access Rights Prompt
- Forced User Validation Prompt
- Access Rights Companion Prompt
- Node-to-Node Password Prompt
- Gateway Access Rights Prompts

Access Rights Prompt: These prompts query you for the access rights from a node *to* the other nodes in the network. They are repeated for each subnetwork to which the node is attached.

Access rights from *node name* via $\left\{ \begin{array}{l} \textit{ring} \\ \textit{LAN300} \\ \textit{fdx} \\ \textit{HDX} \\ \textit{PSDN} \end{array} \right\}$

(NONE, RFA, RLOG, IPCF, ALL):

This prompt assigns some of *node name*'s access rights. Note that these are access rights *from* the node *node name*. That is, this prompt defines the access rights that *node name*'s users have to other systems — specifically, to the systems that *node name* reaches via the ring *ring*, via the LAN300 *LAN300*, via the full-duplex line *fdx*, via half-duplex (HDX) lines, or via the PSDN *PSDN*. For example,

Access rights from SYSA via RING1
(NONE, RFA, RLOG, IPCF, ALL):

Access rights from NODEA via LAN300-1
(NONE, RFA, RLOG, IPCF, ALL):

Access rights from B via FDX3
(NONE, RFA, RLOG, IPCF, ALL):

Access rights from NODEC via HDX
(NONE, RFA, RLOG, IPCF, ALL):

Access rights from D via TELENET
(NONE, RFA, RLOG, IPCF, ALL):

The first example concerns the rights that SYSA users have to use other systems via RING1. It does not concern rights that users of other systems have to SYSA. For definitions of the access rights, refer to Chapter 3, PRIMENET Security.

Forced User Validation Prompt: After querying you for access rights, CONFIG_NET issues the following prompt:

```
Force user validation(NO, YES)?
```

Specifying YES enhances the security of the systems that are to be accessed with RFA. (Chapter 3, PRIMENET Security, describes forced user validation in detail.) For example,

```
Access rights from B via FDX1
(NONE, RFA, RLOG, IPCF, ALL): RFA;
Force user validation(NO, YES)? YES
Enter nodes accessible from B via FDX1 with this access
(NONE, ALL, <node names>): C;
```

Each Force user validation? prompt applies only to the systems you name in answer to the next prompt. In the above example, forced user validation will apply when System B accesses System C's files remotely over FDX1. (Slaves on System C will be required to go through the standard validation process.)

Access Rights Companion Prompt: The access right prompt is always followed by this companion prompt:

```
Enter nodes accessible from node name via  $\left\{ \begin{array}{l} \text{ring} \\ \text{LAN300} \\ \text{fdx} \\ \text{HDX} \\ \text{PSDN} \end{array} \right\}$  with this access
```

(NONE, ALL, node names):

Enter the names of the nodes to which the access you just specified applies. For example, suppose you want users on SYSA to be able to log in to any system on RING2. Here is how the CONFIG_NET dialog would go:

```
Access rights from SYSA via RING2
(NONE, RFA, RLOG, IPCF, ALL): RLOG;
Enter nodes accessible from SYSA via RING2 with this access
(NONE, ALL, node names): ALL;
```

Note that in this case, ALL refers to all the nodes on RING2 — not all the nodes on the network. As another example, suppose NODEB communicates with NODEP and NODEQ over half-duplex lines, and you want NODEB to access these nodes with the IPCF subroutines only. Your dialog would look like this:

```
Access rights from NODEB via HDX
(NONE, RFA, RLOG, IPCF, ALL): IPCF;
Enter nodes accessible from NODEB via HDX with this access
(NONE, ALL, node names): NODEP, NODEQ;
```

This pair of prompts is repeated until you press or enter NONE in response to the first of the pair. Thus, you can assign *node name* different combinations of access rights to different remote nodes on the same ring, PSDN, and so on. For example,

```
Access rights from B via HDX
(NONE, RFA, RLOG, IPCF, ALL): IPCF;
Enter nodes accessible from B via HDX with this access
(NONE, ALL, <node names>): E;
Access rights from B via HDX
(NONE, RFA, RLOG, IPCF, ALL): RLOG;
Enter nodes accessible from B via HDX with this access
(NONE, ALL, <node names>): F,G;
Access rights from B via HDX
(NONE, RFA, RLOG, IPCF, ALL):
```

Note that full-duplex lines are unique in that *node name* can reach only one other node via a given full-duplex line. Thus, to respond to the prompt

```
Enter nodes accessible from node name via fdx with this access
(NONE, ALL, <node names>):
```

you must either enter the name of the node which *node name* reaches via *fdx*, or enter ALL, which has the same effect. For example, if FDX1 connects SYSC and SYSD, to answer the prompt

```
Enter nodes accessible from SYSC via FDX1 with this access
(NONE, ALL, <node names>):
```

you must enter either SYSD or ALL.

When you are specifying the access rights from a node via a PSDN, the second prompt includes the <network names> option:

```
Enter nodes accessible from node name via PSDN with this access
(NONE, ALL, <node names>, <network names>):
```

This allows you to enter a network name, such as FDX1, thereby giving the access right to all the nodes on the network. This is faster than entering the node names one at a time.

Node-to-node Password Prompt: CONFIG_NET displays the following prompt if you have not already defined a node-to-node password between the *node name* and *node1*:

```
Node-node password between node name and node1
(NONE, YES, password):
```

Press or enter NONE if you do not want to assign a node-to-node password for *node name* and *node1*. Answer YES if you want CONFIG_NET to generate a random password for you; in this case, CONFIG_NET displays the following statement:

Generated password is **nnnnnn**

Alternatively, you can enter your own password of as many as 32 characters. For more information on node-to-node passwords, refer to Chapter 3, PRIMENET Security.

Note

When you ask CONFIG_NET to generate a node-to-node password for you, enter the entire word YES. If you enter Y or YE only, CONFIG_NET takes Y or YE to be your choice of a password.

Caution

For security purposes, CONFIG_NET generates different random node-to-node passwords each time it is run. Thus, if you use multiple configuration files in your network, supply your own node-to-node passwords to ensure consistency.

CONFIG_NET's LIST mode displays your network's node-to-node passwords. This means that anyone who is allowed to read the network configuration file and execute CONFIG_NET has access to these passwords. Be sure to use ACLs to protect both the network configuration file and the use of CONFIG_NET.

Gateway Access Rights Prompts: These prompts query you for a node's access and access rights to other nodes across gateways.

The following prompt defines gateway access:

Gateway access from *node name*
(NONE, RFA, RLOG, IPCF, ALL):

This prompt defines the access rights that *node name*'s users will have to the systems that *node name* reaches through gateway nodes. Enter one or more access rights. This prompt is always followed (though not necessarily immediately) by the following companion prompt:

Enter nodes accessible from *node name* via gateway with this access
(NONE, ALL, node names):

Enter the names of the nodes to which the access rights you specified in the last prompt apply. We strongly recommend that you do not enter ALL in response to the second prompt. Note that these prompts ask about access *over* a gateway, not *to* the gateway. For example, in Figure 6-1, Node A has "gateway access" to Node C, but not to Node B; Node B is the gateway.

Note

Do not configure RFA access over a gateway. For information on other restrictions related to gateway nodes, refer to Guidelines for Using Gateway Service in Chapter 1, PRIMENET Overview.

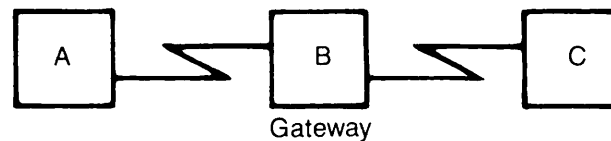


Figure 6-1
Gateway Access

Recall from Chapter 3, PRIMENET Security, that IPCF access is required between each pair of systems in a route-through path. Thus, in Figure 6-1, you would need to assign IPCF access between Node A and Node B, and also between Node B and Node C. (However, these rights are not gateway access rights, since they apply to adjacent systems.) Chapter 7, Sample PRIMENET Configurations, presents a more complex example with two gateway nodes in a route-through path.

In the configuration shown in Figure 6-2, suppose SYSA uses gateway nodes to communicate with SYSB, SYSC, and SYSD.

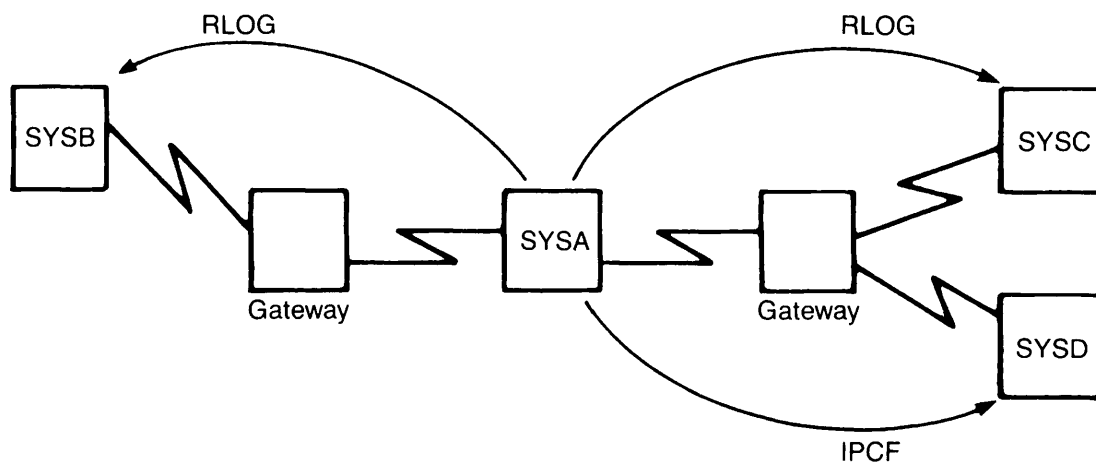


Figure 6-2
Assigning Gateway Access

If you wanted to allow SYSA users to log in to SYSB and SYSC, but wanted to allow only IPCF access from SYSA to SYSD, part of your dialog would look like this:

```

Gateway access from SYSA
(NONE, RFA, RLOG, IPCF, ALL): RLOG;
Enter nodes accessible from SYSA via gateway with this access
(NONE, ALL, node names): SYSB, SYSC;
Gateway access from SYSA
(NONE, RFA, RLOG, IPCF, ALL): IPCF;
Enter nodes accessible from SYSA via gateway with this access
(NONE, ALL, node names): SYSD;
Gateway access from SYSA
(NONE, RFA, RLOG, IPCF, ALL):
  
```

Per-node Prompts for Networks Containing Non-Prime Nodes

This section describes the prompts that appear for Prime nodes on LAN300s or FDX lines that include non-Prime nodes.

LAN300 and FDX Address Prompts: One of these prompts appears if the node can be directly accessed by a non-Prime node on the same LAN300 or FDX network.

Enter *LAN300* addresses for *node name*
(NONE, <*network name* addresses>):

Enter *fdx* addresses for *node name*
(NONE, <*network name* addresses>):

CONFIG_NET prompts you for the Level 3 (packet level) addresses of Prime nodes on networks that contain non-Prime nodes primarily because some non-Prime nodes require a source address in incoming calls. Check with the administrator of the non-Prime node for specific requirements because some machines require a null source address in incoming calls, others require a specific address, and still others only look for a valid address.

The default value, NONE, causes the Prime host to omit its Level 3 address from its Call Request packets. This is acceptable for communication with most non-Prime hosts. For incoming calls, Prime hosts configured with the default value allow themselves to be called by either a null address (no Level 3 address) or the Level 3 address automatically generated for them by CONFIG_NET. (CONFIG_NET automatically generates an address beginning with 9999, based on the node's name).

You can override the automatically generated address by entering one or more alternate addresses in response to the CONFIG_NET prompt. In that case, the Prime node inserts one of your addresses in its Call Request packets and accepts only those incoming calls with one of your addresses. To terminate your input and move on to the next prompt, press Return to select the default value, NONE.

Indirect LAN300 and FDX Address Prompts: One of these prompts appears if the node can be called by a non-Prime node on a LAN300 or FDX line indirectly (through a gateway node). (For a full discussion of indirect addresses, see the section entitled Specifying Addresses to CONFIG_NET in Chapter 4, PRIMENET Network Configuration.)

Indirect *LAN300* address for node *node name*
(NONE, <*LAN300* addresses>):

Indirect *fdx* address for node *node name*
(NONE, <*fdx* addresses>):

Enter the address that the non-Prime node uses to reach the node being configured through the gateway node. If you specify an indirect address, CONFIG_NET displays one of these prompts:

Gateway node which will route address *address* from *LAN300*
to node *node name*
(NONE, <node names>):

Gateway node which will route address *address* from *fdx*
to node *node name*
(NONE, <node names>):

Enter the name of the gateway node through which the non-Prime node calls the node being configured. Next, CONFIG_NET displays one of these prompts, depending on whether the non-Prime node is on an FDX line or a LAN300:

```
Line on node node name for routing fdx name address address
for node node name:
(UNKNOWN, <0-7>):
```

```
LHC logical device number on node node name for
routing LAN300 name address address for node node name:
(UNKNOWN, <0-7>):
```

Enter the line number or LHC300 logical device number on the gateway node that is used for routing calls from the non-Prime node (with the indirect FDX target address just specified) to the node being configured.

Per-node Prompt for Networks Containing Pre-Rev. 19.3 Nodes

The following prompt appears if *node name* has been assigned more than one address, and if the network contains one or more pre-Rev. 19.3 nodes.

```
What address do old nodes have configured for node node name
(<PSDN-address>, <PRIMENET-address>, <address>)
```

Enter the address used by "old" (pre-Rev. 19.3) nodes to identify *node name*. For more information about pre-Rev. 19.3 nodes and multiple addresses, refer to Chapter 4, PRIMENET Network Configuration.

Per-node Prompts for Non-Prime Nodes

When you are configuring a non-Prime node (a node running non-PRIMENET X.25 software), CONFIG_NET displays the following prompts in addition to the universal per-node prompts.

Addressing Prompts: The following prompts query you for the Level 3 and Level 2 addresses for the non-Prime node.

```
Enter LAN300 addresses for node name
(NONE, <network name addresses>, NULL):
```

```
Enter fdx addresses for node name
(NONE, <network name addresses>, NULL):
```

This prompt queries you for the non-Prime node's Level 3 (packet level) address(es). In most cases, it is acceptable to give a non-Prime node a *null address* by entering NULL at the

CONFIG_NET prompt. However, if a non-Prime node is to communicate with another non-Prime node through a gateway, the non-Prime nodes must be able to accept non-null addresses, and you must give a network address for each node. This is because the gateway needs the addresses for routing. To terminate your input and move on to the next prompt, press to select the default value, NONE.

This prompt appears for a non-Prime node on a LAN300, after the Level 3 network address prompt:

MAC (+LSAP) address for node *node name* on LAN300

Enter the non-Prime node's 12-hex-digit Media Access Control (MAC) address in the format *nn-nn-nn-nn-nn-nn*. Optionally, include the node's Link Service Access Point (LSAP) address, which is used to call a particular application on the non-Prime node. The LSAP address is two hex digits, which you precede with a plus sign (+) and append to the end of the MAC address: *nn-nn-nn-nn-nn-nn+nn*. Both of these are Level 2 (link level) addresses.

This prompt appears for a non-Prime node on an FDX line, after the Level 3 network address prompt:

LAP(B) address for node *node name* on *fdx* (3, 1):

Enter the LAPB address used in command frames sent from the Prime to the non-Prime node. The legal values are 1 and 3; the default value is 3. This is a Level 2 (link level) address.

One of these prompts appear if the node can be called by a non-Prime node on a LAN300 or FDX line indirectly (through a gateway node). (For a full discussion of indirect addresses, see the section entitled SPECIFYING ADDRESSES TO CONFIG_NET in Chapter 4, PRIMENET Network Configuration.)

Indirect LAN300 address for node *node name*
(NONE, <LAN300 addresses>):

Indirect *fdx* address for node *node name*
(NONE, <*fdx* addresses>):

Enter the address that the non-Prime node uses to reach the node being configured through the gateway node. If you specify an indirect address, CONFIG_NET displays one of these prompts:

Gateway node which will route address *address* from LAN300
to node *node name*
(NONE, <node names>):

Gateway node which will route address *address* from *fdx*
to node *node name*
(NONE, <node names>):

Enter the name of the gateway node through which the non-Prime node calls the node being configured. Next, CONFIG_NET displays one of these prompts, depending on whether the non-Prime node is on an FDX line or a LAN300:

Line on node *node name* for routing *fdx name* address *address*
for node *node name*
(UNKNOWN, <0-7>):

LHC logical device number on node *node name* for
routing *LAN300 name* address *address* for node *node name*
(UNKNOWN, <0-7>):

Enter the line number or LHC300 logical device number on the gateway node that is used for routing calls from the non-Prime node (with the indirect FDX target address just specified) to the node being configured.

Additional Prompts: CONFIG_NET displays the following additional prompts for non-Prime nodes before querying you about access rights.

Highest logical channel number for VCs on line *number* to
network name
(4095, <1-4095>):

Enter the highest logical channel number to be used for a virtual circuit on the line from the non-Prime node to the FDX, LAN300, or PSDN. The default value is 4095. Note that this is the highest logical channel number to be used to *identify* a virtual circuit, not the maximum number of virtual circuits.

Default window size for line *number* to *network name*
(2, <1-7>):

Enter the default window size for the line from the non-Prime node to the FDX, LAN300, or PSDN. The default window size is the maximum number of outstanding, unacknowledged packets allowed. The legal range is 1 through 7; the default value is 2. We recommend a window size of 7 for lines running at 9600 bps and a window size of 4 for lines running at 4800 bps. Before setting this parameter, see the discussion on default packet and window sizes below.

Default packet size (in bytes) for line *number* to *network name*
(*max*, <16-*max*>):

Enter the default packet size (in bytes) for the line from the non-Prime node to the FDX, LAN300, or PSDN. The default value is the maximum value, which is 256 bytes for FDX links and 512 for LAN300 links. The legal values are 16, 32, 64, 128, and 256 for FDX links, and 16, 32, 64, 128, 256, and 512 bytes for LAN300 links.

When you configure the default window size and default packet size, observe these considerations:

- The window and packet size for incoming remote login calls are limited by the size of the buffers allocated for remote login lines (remote buffers). The default window size times the default packet size cannot exceed the size of remote buffers on the Prime node. Remote buffer sizes are set with the REMBUF directive in the node's CONFIG file, or by the CAB command on Rev. 22.0 nodes. For more information on REMBUF, see Chapter 8 of this manual, Setting PRIMENET-related CONFIG Directives, and Appendix A of the *Programmer's Guide to Prime Networks*. For more information on CAB, see Chapter 9 of this manual, Setting PRIMENET-related PRIMOS.COMI Commands.
- Window size and packet size are no longer restricted to 2 and 128, respectively, for remote login calls. All of the values listed above are now acceptable.
- Window size and packet size can now be negotiated on a per-call basis for remote login calls.
- Some PSDNs impose packet and window size restrictions. Check with your PSDN Administrator for more information.

Determine DTE/DCE for node *node name* on *network name line number*
(DYNAMIC, DTE, DCE) :

This prompt asks if the non-Prime node acts as Data Communications Equipment (DCE) or as Data Terminal Equipment (DTE), or if it uses dynamic determination to establish its role. Ask the non-Prime system's administrator about this, or have the line analyzed with a datascopes to determine this information. If the two systems are to negotiate which will be DTE and which will be DCE, set this parameter to DYNAMIC determination. If you cannot find out whether the non-Prime node acts as a DTE or as a DCE, you can set this parameter to DYNAMIC, so long as the non-Prime node conforms to X.25 1980 or X.25 1984.

Does node *node name* on *network name line number* use
ISO 8881 procedures
(NO, YES) :

Answering YES to this prompt causes the line from the LAN300 to the non-Prime node to be dropped after a time (default 90 seconds) when no circuits are open. (An idle FDX link is not dropped). Contact the administrator of the non-Prime system to find out how the non-Prime node behaves.

Editing a Configuration

CONFIG_NET's Edit mode allows you to add, modify, or delete sections of your PRIMENET configuration file. Editing functions are available through one main menu and several submenus. The main menu allows you to choose *which* part of the configuration to edit; the submenus allow you to choose the addition, modification, or deletion to be made.

Before you edit your network configuration, plan your work carefully. Make a list of all additions, deletions, and other modifications you plan to make. Read through this entire section, which includes important information about editing strategy. Make a backup copy of your current configuration file.

After you have edited and saved your configuration, issue the `STOP_NET` command to remove your system from the network; then issue the `START_NET` command to restore the system to the network with the new configuration. (The `START_NET` and `STOP_NET` commands do not interrupt local system operation. These commands are described in the *Operator's Guide to Prime Networks*.)

Remember to copy the edited configuration file to other network nodes as necessary. It is important that all configuration files in the network be consistent, if not exactly the same. After copying a new configuration file to a node, use `STOP_NET` to remove the node from the network, then use `START_NET` to restore the node to the network with the new configuration file.

`CONFIG_NET`'s Edit mode consists of a set of menus. This section describes each menu and explains how to:

- Enter Edit mode
- Select a menu
- Add new objects to your configuration
- Modify existing objects in your configuration
- Delete objects from your configuration
- Enable/disable Data Set Status (DSS) interrupts
- Set the maximum frame size for a node on a ring

In the context of this discussion, a configuration *object* may be a node, a connection, an access right, a subnetwork (such as a ring, LAN300, a full-duplex line, or a half-duplex network), a PSDN address, a password, or any other part of the network description.

When adding new objects such as nodes and subnetworks to your configuration, it is wise use the Edit menus only to add the new object before switching into Create mode. In Create mode, `CONFIG_NET` prompts you for all the needed information, eliminating the possibility that you will forget something.

Editing examples appear in Chapter 7, Sample PRIMENET Configurations.

Notes

Rev. 21.0 CONFIG_NET can read configuration files created with earlier versions of CONFIG_NET. This allows you to edit your existing configuration files when adding LAN300 functionality to your network. However, when you edit (for any reason) a configuration file created with an earlier version of CONFIG_NET, you must enter Create mode during the session. In Create mode, CONFIG_NET automatically prompts you about the new features: LAN300s and non-Prime nodes. (Answer NONE if you are not using these features.) If you do not go into Create mode, CONFIG_NET rejects the configuration as invalid when you attempt to save it.

Pre-Rev. 21.0 CONFIG_NET cannot read configuration files created or edited by Rev. 21.0 CONFIG_NET.

Rev. 21.0 START_NET can start PRIMENET using any valid configuration file, regardless of the revision of CONFIG_NET with which it was created. You do not need to update your old configuration file if you are not using the new Rev. 21.0 features such as LAN300s, communication with non-Prime nodes, and setting the maximum number of virtual circuits on a node.

Entering EDIT Mode

To edit an existing configuration file, include the configuration file's pathname on the CONFIG_NET command line, then enter EDIT in response to the option prompt.

If you are already in CONFIG_NET, press -P to summon the option prompt, then enter EDIT:

```
Create, Edit, Quit, Save, Fast_Save, List, or Help? EDIT
```

The Edit Mode Menus

The Edit mode menus allow you to add, modify, and delete portions of the network configuration. One main menu leads to seven different submenus (including a HELP display). From the main menu, you choose which portion of your configuration you want to change. CONFIG_NET then supplies the appropriate submenu, from which you choose the desired modifications. When Edit mode starts, CONFIG_NET displays the main Edit menu, shown in Figure 6-3.

At the main Edit menu, enter the appropriate number to select the part of the configuration you want to edit, or press to leave Edit mode. Each selection has a submenu which lists the editing choices for that part of the configuration.

```
Edit Mode
What would you like to edit?

(0) HELP      (for assistance)
(1) NODE
(2) RING
(3) FDX       (full duplex synchronous Prime-to-Prime links)
(4) PSDN      (public data network)
(5) HDX       (half duplex network)
(6) LAN300    (IEEE 802.3 LAN)

Enter carriage return to leave Edit mode

What would you like to edit:
```

Figure 6-3
Main EDIT Menu

Displaying HELP Information: To display general editing information, choose option 0 (HELP). The general HELP display is shown in Figure 6-4.

EDIT mode allows you to change information for any node or network which is already configured.

You can also add new nodes and networks by:

- 1) specifying the type of the item you want to add (node, ring, full duplex synchronous Prime-to-Prime line, or Packet Switching Data Network, HDX, or LAN300) to this Edit Mode menu,
- and 2) when asked for the name of the item, specifying a name which is not already used for a node or network in the configuration.

Figure 6-4
HELP Display

Editing Nodes, Rings, FDX Lines, PSDNs, and LAN300s: If you choose option 1 (NODE), option 2 (RING), option 3 (FDX), option 4 (PSDN), or option 6 (LAN300), CONFIG_NET prompts you for the name of the node, ring, full-duplex line, PSDN, or LAN300 that you want to edit. (CONFIG_NET does not prompt you for the name of the half-duplex subnetwork because there can be only one half-duplex subnetwork in a configuration.) For example,

```
Edit Mode
```

```
What would you like to edit?
```

```
(0) HELP      (for assistance)
(1) NODE
(2) RING
(3) FDX       (full-duplex synchronous Prime-to-Prime links)
(4) PSDN      (packet switching data network)
(5) HDX       (half-duplex network)
(6) LAN300    (IEEE 802.3 LAN)
```

```
Enter carriage return to leave Edit mode
```

```
What would you like to edit: 2
```

```
Ring name (NONE, <ring name>): RING3
```

If you supply a name that already exists in the configuration, CONFIG_NET displays the appropriate submenu. Each submenu offers a choice of editing options and a specialized HELP display. Pressing in response to a submenu prompt returns you to the main Edit menu. The Node, Ring, FDX, PSDN, and LAN300 submenus and their associated HELP displays are shown in Figures 6-5 through 6-14.

If you enter the name of an object that has not yet been defined in the configuration, CONFIG_NET adds the object to the configuration. When you are adding a new node, CONFIG_NET prompts you for the name of the physical network (subnetwork) to which the new node is attached. When you enter the subnetwork name, CONFIG_NET redisplay the main Edit menu. Press -P to display the option prompt, then enter CREATE to switch to Create mode. CONFIG_NET automatically prompts you for the needed information about the new object, eliminating the possibility that you will omit something. This strategy for adding new objects is discussed in more detail in the section entitled Adding a New Node to the Network, later in this chapter.

Select a node editing option.

- (0) HELP (for assistance)
- (1) Delete this node
- (2) Change the name of this node
- (3) Modify this node's access information
- (4) Change node-node passwords for this node
- (5) Change HDX passwords for this node
- (6) Change this node's status as a gateway node
- (7) Add a PSDN address for this node
- (8) Delete a PSDN address for this node
- (9) Change a PSDN address for this node
- (10) Change this node's rev. status
- (11) Change this node's compatibility address
- (12) Change a LAN300 Host Controller for this node
- (13) Mark non-Prime node
- (14) Change non-Prime source address
- (15) Change maximum number of VCs for this node

Enter carriage return for the top level edit menu.

Figure 6-5
Node Submenu

The following options are allowed for editing a node:

- (1) Delete this node:
Removes the node completely from the configuration.
- (2) Change the name of this node:
Changes the name to a newly specified name.
- (3) Modify this node's access information:
Changes the access allowed between two nodes.
- (4) Change node-node passwords for this node:
Changes the node-node password used during Remote File Accesses to ensure that the remote system is allowed such access.
- (5) Change HDX passwords for this node:
Changes the incoming & outgoing passwords for half duplex connections.

Figure 6-6
HELP Information for the Node Submenu

- (6) Change this node's status as a gateway node:
Allows a node to be upgraded to a gateway node.
- (7) Add a PSDN address for this node:
Configures another Packet Switching Data Network address for this node.
- (8) Delete a PSDN address for this node:
Removes a Packet Switching Data Network address which was configured for this node.
- (9) Change a PSDN address for this node:
Removes a previously configured Packet Switching Data Network address for this node, and replaces it with the newly specified address.
- (10) Change this node's rev. status:
Allows a node to be upgraded when it is no longer running a version of PRIMOS prior to rev 19.3.
- (11) Change this node's compatibility address:
Changes the address which this node uses when communicating with nodes running pre-rev-19.3 PRIMOS.
- (12) Change a LAN300 Host Controller number for this node:
Changes a LAN300 Host Controller (LHC) logical device number for Primenet support for this node on a particular LAN300.
- (13) Mark non-Prime node:
A non-Prime node may be directly connected to an FDX line. This option may be used to mark a given node as running Primenet or not running Primenet.
- (14) Change non-Prime source address:
The default source address for used for communicating with directly connected non-Prime nodes is null. This option may be used to set the source address to be used for calls to non-Primes from this node.
- (15) Change the maximum number of VCs for this node:
The maximum number of virtual circuits that may be established for this node. If this number is not specified, the system default will be used.

Figure 6-6
HELP Information for the Node Submenu - Continued

Select option.

- (0) HELP (for assistance)
- (1) Remove ring from the configuration
- (2) Change the name of this ring
- (3) Add a node to this ring
- (4) Remove a node from this ring
- (5) Change ring node ID for a node on this ring
- (6) Set maximum frame size for a node on this ring

Enter carriage return for the top level edit menu.

Figure 6-7
Ring Submenu

The following options are allowed for editing a ring:

- (1) Remove ring from the configuration:
Deletes the ring, but not the nodes configured on the ring.
- (2) Change the name of this ring:
Changes the name of the ring.
This option is useful for changing the name from the configurator default to something more useful to the network administrator.
- (3) Add a node to this ring:
Add a new or existing node to this ring.
- (4) Remove a node from this ring:
Removes the node from the ring, but does not delete it from the configuration file. Use EDIT NODE to delete a node completely.
- (5) Change ring node ID for a node on this ring:
Changes the ring node ID assigned to a node on the ring.
- (6) Set maximum frame size for a node on this ring:
Allows packets larger than the default packet size to be sent between nodes on the ring.

Figure 6-8
HELP Information for Ring Submenu

```

Select desired change.

(0) HELP   (for assistance)
(1) Remove this link from the configuration
(2) Change the name of this link
(3) Add a node to this link
(4) Remove a node from this link
(5) Change synchronous line numbers
(6) Set LAP or LAPB protocol
(7) Set HDLC or Bisync framing
(8) Enable/Disable DSS interrupts
(9) Change LAP(B) address (non-Prime nodes)
(10) Change highest LCN (non-Prime nodes)
(11) Change default packet size (non-Prime nodes)
(12) Change default window size (non-Prime nodes)
(13) Change restart options (non-Prime nodes)

Enter carriage return for the top level edit menu.
    
```

Figure 6-9
FDX Submenu

The following options are allowed for editing a Full Duplex Synchronous Prime-to-Prime line:

- (1) Remove this link from the configuration:
Deletes the FDX line, but not the nodes configured on the line.
- (2) Change the name of this link:
Changes the name of the FDX link.
This option is useful for changing the name from the configurator default to something more useful to the network administrator.
- (3) Add a node to this link:
Add a new or existing node to the FDX line.
Remember that there should only be two nodes configured on a full duplex synchronous Prime-to-Prime line.
- (4) Remove a node from this link:
Removes the node from the line, but does not delete it from the configuration file. Use EDIT NODE to delete a node completely.

Figure 6-10
HELP Information for FDX Submenu

- (5) Change synchronous line number:
Changes the synchronous line number on one (or each) of the nodes for the Prime-to-Prime link.
- (6) Set LAP or LAPB protocol:
Changes the protocol used over the synchronous line to the PSDN.
- (7) Set HDLC or Bisync framing:
Changes the framing used over the synchronous line to the PSDN.
- (8) Enable/Disable DSS interrupts:
Changes the Data Set Status parameters configured.
- (9) Change Level II Address (non-Prime nodes):
Sets the LAP(B) address for a non-Prime node. This is ignored for Prime nodes.
- (10) Change highest LCN (non-Prime nodes):
Sets the highest logical channel number for a non-Prime node. This is ignored for a Prime node.
- (11) Change default packet size (non-Prime nodes):
Sets the default packet size for a link to a non-Prime node. This is ignored for a Prime node.
- (12) Change default window size (non-Prime nodes):
Sets the default packet size for a link to a non-Prime node. This is ignored for a Prime node.
- (13) Change restart options (non-Prime nodes):
The non-Prime node may be the DTE or DCE at Level III. In addition, restarts may be required by the non-Prime whenever there are no VCs active, in accordance with ISO DP 8881.

Figure 6-10
HELP Information for FDX Submenu - Continued

Select option.

- (0) HELP (for assistance)
- (1) Remove this PSDN from the configuration
- (2) Add a node to this PSDN
- (3) Remove a node from this PSDN
- (4) Add a line to this PSDN
- (5) Remove a line to this PSDN
- (6) Change synchronous line numbers
- (7) Set LAP or LAPB protocol
- (8) Set HDLC or Bisync framing
- (9) Enable/Disable DSS interrupts
- (10) Change highest LCN for a link to this PSDN
- (11) Change default packet size for a link to this PSDN
- (12) Change default window size for a link to this PSDN

Enter carriage return for the top level edit menu.

Figure 6-11
PSDN Submenu

The following options are allowed for editing a Packet Switching Data Network:

- (1) Remove this PSDN from the configuration:
Deletes the PSDN, but not the nodes configured on the PSDN.
- (2) Add a node to this PSDN:
Adds a new or existing node to the PSDN.
- (3) Remove a node from this PSDN:
Removes the node from the PSDN, but does not delete it from the configuration file. Use EDIT NODE to delete a node completely.
- (4) Add a line to this PSDN:
Specifies an additional synchronous line connecting a node to the PSDN.
- (5) Remove a line to this PSDN:
Deletes a synchronous line connecting a node to the PSDN.
This does not delete the node from the PSDN. If this is the only line connecting the node to the PSDN, CREATE mode will query you for another synchronous line.
- (6) Change synchronous line numbers:
Changes the line number for the synchronous line connecting the node to the PSDN.
- (7) Set LAP or LAPB protocol:
Changes the protocol used over the synchronous line to the PSDN.
- (8) Set HDLC or Bisync framing:
Changes the framing used over the synchronous line to the PSDN.
- (9) Enable/Disable DSS interrupts:
Changes the Data Set Status parameters configured.
- (10) Change highest LCN for a link to this PSDN:
Sets the highest logical channel number for calls from a given node to this PSDN.
- (11) Change default packet size for a link to this PSDN:
Sets the default packet size for a link to calls from a given node to this PSDN.
- (12) Change default window size for a link to this PSDN:
Sets the default packet size for a link to calls from a given node to this PSDN.

Figure 6-12
HELP Information for PSDN Submenu

Select option.

- (0) HELP (for assistance)
- (1) Remove this LAN300 from the configuration
- (2) Change the name of this LAN300
- (3) Add a node to this LAN300
- (4) Remove a node from this LAN300
- (5) Change MAC address (non-Prime nodes)
- (6) Change highest LCN (non-Prime nodes)
- (7) Change default packet size (non-Prime nodes)
- (8) Change restart options (non-Prime nodes)

Enter carriage return for the top level edit menu.

Figure 6-13
LAN300 Submenu

The following options are allowed for editing a LAN300:

- (1) Delete this LAN300 from the configuration:
Deletes the LAN300, but not the Primenet nodes configured on the LAN300.
- (2) Change the name of this LAN300:
Changes the name of the LAN300. This option is useful for changing the name from the configurator default to something more useful to the network administrator.
- (3) Add a node to this LAN300:
Adds a new or existing node to the LAN300.
- (4) Remove a node from this LAN300:
Removes the Prime node from the LAN300, but does not delete it from the configuration file. Use EDIT NODE to delete a node completely.
- (5) Change MAC Address (non-Prime nodes):
Sets the MAC address for a non-Prime node. This is ignored for Prime nodes.
- (6) Change highest LCN (non-Prime nodes):
Sets the highest logical channel number for a non-Prime node. This is ignored for a Prime node.
- (7) Change default packet size (non-Prime nodes):
Sets the default packet size for a link to a non-Prime node. This is ignored for a Prime node.
- (8) Change default window size (non-Prime nodes):
Sets the default packet size for a link to a non-Prime node. This is ignored for a Prime node.
- (9) Change restart options (non-Prime nodes):
The non-Prime node may be the DTE or DCE at Level III. In addition, restarts may be required by the non-Prime whenever there are no VCs active, in accordance with ISO DP 8881.

Figure 6-14
HELP Information for LAN300 Submenu

Editing the Half-duplex Network: If you choose option 5 (HDX) from the main Edit menu, and if your network already contains at least one half-duplex node, CONFIG_NET displays the half-duplex submenu (see Figures 6-15 and 6-16). If your network does not contain any half-duplex nodes, CONFIG_NET issues the following prompt when you select option 5 (HDX) from the main Edit menu:

```
The half-duplex network does not exist.  
Do you wish to create it?
```

If you answer anything but Y, YE, or YES, you are returned to the main Edit menu. If you answer Y, YE, or YES, CONFIG_NET displays this message:

```
The half-duplex network has been created.
```

and then displays the half-duplex submenu to allow you to define the half-duplex nodes and lines. The most efficient way to add the lines and nodes is to leave Edit mode and enter Create mode. (To do this, press **Ctrl**-P and then answer CREATE in response to the option prompt.) In Create mode, CONFIG_NET prompts you for the needed information. Alternatively, you can use Edit mode to add half-duplex nodes and lines.

```
Edit Half Duplex Network  
  
(0) HELP  (for assistance)  
(1) Delete the entire HDX network  
(2) Add a node to the HDX network  
(3) Remove a node from the HDX network  
(4) Change a synchronous line number  
(5) Add a synchronous line number  
(6) Delete a synchronous line number  
  
Enter carriage return for the top level edit menu.
```

Figure 6-15
HDX Submenu

Edit Half Duplex Network options include:

- (1) Delete the entire HDX network:
Removes all of the half duplex network, but not the nodes configured as part of the HDX network. Use EDIT NODE to delete a node completely.
- (2) Add a node to the HDX network:
Adds a new or existing node to the half duplex network.
- (3) Remove a node from the HDX network:
Removes the node from the half duplex network. This option will not delete it from the configuration file. Use EDIT NODE to delete a node completely.
- (4) Change a synchronous line number:
Changes a synchronous line number which a node may use for half duplex dial-up connections.
- (5) Add a synchronous line number:
Adds a synchronous line number which a node may use for half duplex dial-up connections.
- (6) Delete a synchronous line number:
Deletes a synchronous line number which a node may use for half duplex dial-up connections.

Figure 6-16
HELP Information for HDX Submenu

Strategy for Adding Objects to a Configuration

In general, the most efficient way to add objects to your configuration is to have Create mode do most of the work. Use Edit mode only to add the objects, then switch into Create mode. In Create mode, CONFIG_NET automatically prompts you for all of the information it needs. This strategy minimizes the chance that you will forget to provide necessary information.

In many cases, you *can* use Edit mode to add all information without returning to Create mode. However, we recommend that you rely solely on Edit mode only if you are experienced with editing your configuration. If you forget to provide certain information, CONFIG_NET issues the following message the next time you enter Create mode or attempt to save the configuration on disk:

Configuration errors detected.

When CONFIG_NET detects omissions as you enter Create mode, it automatically prompts you for the missing information. If CONFIG_NET detects omissions when you attempt to save your configuration on disk, CONFIG_NET informs you that there are errors, then allows you to save the configuration anyway. You can then go into Create mode to supply the missing information.

As another general strategy, always add a new subnetwork *before* adding the new nodes (if any) that are members of that subnetwork. For example, if you want to add a new ring with four nodes, first add the ring itself, then add the four nodes.

The following sections describe how to make several common types of additions to your configuration. For examples of editing sessions, refer to Chapter 7, Sample PRIMENET Configurations.

Adding a New Node to the Network

To add a new node to the network, follow these steps:

1. Choose the NODE option from the main Edit menu. Enter the name of the new node. CONFIG_NET displays this prompt:

```
Physical network attached to node name
(NONE, <pnet name>):
```

Enter the name of a subnetwork that connects *node name* to the rest of the network. If *node name* is connected to more than one subnetwork, simply choose one. CONFIG_NET displays the main Edit menu.

2. Transfer to Create mode. CONFIG_NET prompts you for information about *node name*, including its connection to the subnetwork you specified. Answer all prompts.
3. If *node name* is connected to more than one subnetwork, return to Edit mode to add *node name* to all appropriate subnetworks, as described below.

Adding a Node to a Subnetwork

To add a new or existing node to a subnetwork, use the submenu for that subnetwork. For example, use the Ring submenu to add a node to a ring or use the HDX submenu to add a node to the HDX subnetwork. If the node is not already defined in your configuration, CONFIG_NET adds the node to the entire network and to the subnetwork at the same time. After you have added the node, transfer to Create mode and answer all prompts.

Adding a Non-Prime Node

To add a non-Prime node to your configuration, first add it to the appropriate subnetwork as you would an ordinary node. Then, return to the Edit Node menu and select Mark non-Prime node. When CONFIG_NET asks if the node is running non-PRIMENET X.25 software, answer YES. Next, press **Ctrl**-P and enter CREATE at the option prompt. CONFIG_NET prompts you for the needed information.

Adding a Subnetwork

To add an entirely new subnetwork (such as a half-duplex network, a PSDN, a ring, a LAN300, or a full-duplex line), you must add the subnetwork itself *and* add any of its nodes that are not already defined in the configuration. For example, to add a new RINGNET to your configuration, select option 2, "RING" from the main Edit menu. When prompted, enter the name of the new network, then transfer to Create mode. CONFIG_NET prompts you for the remaining information, including node names and access rights over the new subnetwork.

Adding a PSDN Address for a Node

To add a PSDN address for a node, choose the NODE option from the main Edit menu. From the Node submenu, select option 7, Add a PSDN address for this node. CONFIG_NET prompts you for the name of the PSDN and the new address.

Adding a Half-Duplex Line

Before you can add a half-duplex line to a node, you must first define the node to be part of the HDX subnetwork. To do so, select option 2 from the HDX submenu, Add a node to the HDX network, then enter Create mode. CONFIG_NET prompts you for the line number and access rights. An alternate method is to select option 5 from the HDX submenu, Add a synchronous line number. CONFIG_NET prompts you for the name of the node. If the node you specify already has one or more half-duplex lines, CONFIG_NET lists them, then prompts you for the new logical line number.

Adding Gateway Nodes or Access

Adding gateway nodes or access to an existing network requires special care. For instructions, refer to the section, Strategy for Changing Gateway Access, later in this chapter.

Strategy for Modifying Objects in a Configuration

Use the Edit mode submenus to modify the characteristics of existing portions of your configuration. This section explains how to perform several common modifications. For specific examples, refer to Chapter 7, Sample PRIMENET Configurations.

Changing Access Rights

To change NodeX's access to other node(s), follow these steps:

1. Select the NODE option from the main Edit menu. CONFIG_NET prompts you for the node to edit.
2. Enter NodeX. CONFIG_NET displays the Node submenu.
3. Select option 3, Modify this node's access information. CONFIG_NET prompts you for link (subnetwork) for which you want to modify NodeX's access.
4. Enter the name of the subnetwork; for example, *RING2* or *FDX1*. CONFIG_NET displays the menu illustrated in Figure 6-17.

```
Modify Access for Node A over RING1
Select access changes.

(0) HELP  (for assistance)
(1) No Access
(2) IPCF access
(3) No IPCF access
(4) Remote File Access
(5) No Remote File Access
(6) Remote Log-Through Access
(7) No Remote Log-Through Access
(8) Forced User Validation
(9) No Forced User Validation

Enter a LIST of access modes.
```

Figure 6-17
Edit Access Menu

5. At the option prompt, enter the number corresponding to (one of) the access right(s) you want to assign. As CONFIG_NET repeats the option prompt, select the other access rights you want to assign, one at a time. When you are finished, press without entering a number. CONFIG_NET then prompts you for the nodes on the subnetwork that are to be given this access *from* NodeX.

6. Enter the appropriate node names. Note that this prompt asks about NodeX's access to other nodes. CONFIG_NET then prompts you for the nodes on the subnetwork that are to be given this access *to* NodeX.
7. Enter the appropriate node names. Note that this prompt asks about other nodes' access to NodeX.
8. Steps 5, 6, and 7 are repeated until you press or -P at Step 5 instead of entering access rights.

If you add RFA access, you may want to use the Node submenu to add a node-to-node password. Alternately, you can go into Create mode; CONFIG_NET prompts you for the node-to-node password. (See Changing Passwords, below.)

Note

Be especially careful when changing access over a gateway node. Refer to the section, Strategy for Changing Gateway Access, later in this chapter.

Changing Passwords

To change, add, or delete a node-to-node or half-duplex password between two nodes, select the NODE option from the main Edit menu. When CONFIG_NET prompts you for the node to be edited, enter either node's name. Next, select option 4, Change node-node passwords for this node, or option 5, Change HDX passwords for this node. CONFIG_NET prompts you for the necessary information.

Changing a Ring Node ID

To change the ring node ID of a ring node, choose the RING option from the main Edit menu. From the Ring submenu, choose option 5, Change ring node ID for a node on this ring. CONFIG_NET prompts you for the necessary information.

Changing the Protocol of a Full-duplex Line

To change the protocol of a full-duplex line, choose the FDX option from the main Edit menu. From the FDX submenu, choose option 6, Set LAP or LAPB protocol. CONFIG_NET prompts you for the necessary information.

Changing Logical Line to PSDN

To change the logical line number of a full-duplex synchronous line that connects a node to a PSDN, choose the PSDN option from the main Edit menu. From the PSDN submenu, choose option 6, Change synchronous line numbers. CONFIG_NET prompts you for the node name and the new logical line number.

Changing a Half-duplex Line Number

To change the logical line number of a half-duplex line, choose the HDX option from the main Edit menu. From the HDX submenu, choose option 4, Change a synchronous line number. CONFIG_NET asks for the name of the node whose line you want to change. When you enter the name of an HDX node, CONFIG_NET lists that node's existing HDX lines, asks which line you want to change, then prompts you for the new line number.

Changing an LHC300 Logical Device Number

To change the logical device number of the LAN Host Controller300 (LHC300) that connects a node to a LAN300 network, select the NODE option from the main Edit menu. CONFIG_NET displays the Node submenu. Select option (12), Change a LAN Host Controller number for this node. Because each node may be attached to two LAN300s, CONFIG_NET displays this prompt:

Existing LAN300 name (NONE, <LAN300 name>):

Enter the name of the LAN300 to which the LHC300 is attached. Use the NONE prompt if you change your mind and decide not to change the LHC300 logical device number. CONFIG_NET displays error messages and reprompts you if you enter a LAN300 that is not configured, or a LAN300 to which the LHC300 is not attached. After you have entered the LAN300 name, CONFIG_NET prompts you for the new LHC300 logical device number. If you enter a logical device number that is already configured on the node, CONFIG_NET displays an error message and repeats the prompt.

Indicating Non-Prime Nodes

After adding a non-Prime node (a node running non-Prime X.25 software) to your configuration, you must indicate that it is a non-Prime node. To do this, select option 13 from the Node submenu, Mark non-Prime node. CONFIG_NET displays this prompt:

Is node *node name* running Primenet (TM)
(NO, YES) ?

Answer NO. Next, press until the option prompt appears, then enter CREATE. CONFIG_NET prompts you for the additional information needed for non-Prime nodes.

Changing a Node's Network Address

For nodes on networks that contain non-Prime nodes, CONFIG_NET prompts for each node's network address and defaults the address to NULL if none is given. This is because some non-Prime nodes require calling (source) addresses in incoming calls. For this reason, a node's network address is referred to as its **non-Prime source address**. To change a node's network address, select option 14 from the Node submenu, Change non-Prime source address. CONFIG_NET prompts you for the new source address.

Changing the Maximum Number of Virtual Circuits for a Node

To set the maximum number of virtual circuits that a node can support at the same time, select option 15 from the Node submenu, Change maximum number of VCs for this node. CONFIG_NET prompts you for the new maximum.

Strategy for Deleting Objects From a Configuration

To delete an object from your network, you must first make a selection from the Edit menu. Your choice is determined by your goal. For example, if you want altogether to delete a node from the network, select NODE; if you want to delete a node only from one ring, select RING.

You can delete the following items from your network:

- Node
- Ring
- LAN300
- Full-duplex line between nodes
- Full-duplex line to a PSDN
- PSDN
- Half-duplex subnetwork
- Half-duplex line (from a node)
- Node from a ring, LAN300, full-duplex line, PSDN, or half-duplex subnetwork
- PSDN address of a node
- Node-to-node password
- Half-duplex password

Observe these guidelines when deleting portions of your configuration:

- To completely delete a node from the network and all subnetworks, choose the **NODE** option from the main Edit menu. When prompted, enter the name of the node you want to delete. From the Node submenu, choose option 1, **Delete this node**. CONFIG_NET deletes the node and automatically removes the other nodes' access rights to the deleted node.
- To delete a node from a subnetwork (ring, LAN300, full-duplex line, half-duplex network, or PSDN), select the subnetwork from the main Edit menu. Then, select the **Remove a Node** option from the submenu. CONFIG_NET removes the node from the subnetwork you are editing, but the node remains on all other subnetworks to which it belongs. For example, suppose SYSB is connected to a ring and to a PSDN. To remove SYSB's PSDN connection without affecting its ring membership, use option 3 of the PSDN submenu, **Remove a node from this PSDN**.
- To delete a subnetwork, you must first delete all of its nodes. For example, to delete a full-duplex line between nodes, you must first use option 4 of the FDX submenu, **Remove a node from this link**, to delete both nodes from the line, then select option 1 of the FDX submenu, **Remove this link from the configuration**, to remove the line itself. Similarly, to delete a PSDN, you must first use the PSDN submenu to remove all nodes from the PSDN, then use the PSDN submenu to remove the PSDN itself.

In addition to these general guidelines, the following instructions may be helpful:

- To remove a full-duplex line to a PSDN, select option 5 of the PSDN submenu, **Remove a line to this PSDN**.
- To remove a half-duplex line from a node, select option 6 of the HDX submenu, **Delete a synchronous line number**. CONFIG_NET prompts you for the node name and the number of the line to be removed.
- To remove the PSDN address of a node, use option 8 of the Node submenu, **Delete a PSDN address for this node**.
- To remove a node-to-node or half-duplex password between two nodes, use option 4 (**Change node-node passwords for this node**) or option 5 (**Change HDX passwords for this node**) of the Node submenu. When CONFIG_NET prompts you for the new password, press or enter NONE.
- To remove a node from a LAN300, select option 4, **Remove a node from this LAN300**, from the LAN300 submenu. CONFIG_NET prompts you for the name of the node to be removed.

Note

Be especially careful when deleting a gateway node or gateway access. For more information, refer to *Strategy for Changing Gateway Access* below.

For examples of deletions, refer to Chapter 7, *Sample PRIMENET Configurations*.

Strategy for Changing Gateway Access

This section provides special instructions for changing gateway access on your network.

Granting New Gateway Access Through an Existing Gateway

To add gateway access between existing nodes through an existing gateway, follow these steps:

1. Use the Node submenu to delete all nodes to which you will be granting new gateway access.
2. Use the main Edit menu to add back the nodes you deleted in Step 1.
3. Transfer to Create mode. In Create mode, CONFIG_NET prompts you for the necessary information about each new node, including its gateway access rights. Be sure to enter all of the information that the configuration originally contained, in addition to the new gateway access information.

Changing Access Over an Existing Gateway

To change access rights between two systems that already communicate via a gateway, follow the three steps under Granting New Gateway Access Through an Existing Gateway, above.

Changing an Existing Node Into a Gateway Node

To change an existing node into a gateway node, follow these steps:

1. Select the NODE option from the main Edit menu. When prompted, enter the name of the node that is to become a gateway.
2. Select option 6 from the Node submenu, Change this node's status as a gateway node. CONFIG_NET asks if the node is a gateway node.
3. Enter YES.
4. Grant gateway access to the nodes that are to communicate through the new gateway, as described Granting New Gateway Access Through an Existing Gateway, above.

Adding a New Gateway Node

To add a new node to the network and configure it a gateway node, follow these steps:

1. Add the node in the usual way, as described in Strategy for Adding Objects to a Configuration, above.
2. Enter Edit mode. Follow the instructions provided in Changing an Existing Node Into a Gateway Node, above.

Removing a Node's Gateway Function

To remove a node's gateway function, follow these steps:

1. Select the **NODE** option from the main Edit menu. When prompted, enter the name of the node that is to lose its gateway status.
2. Select option 6 of the Node submenu, **Change this node's status as a gateway node**. **CONFIG_NET** asks whether the node is a gateway node.
3. Enter **NO**.
4. For each pair of systems that communicated via the former gateway node, you must either add a new gateway that they can use, or remove their gateway access to one another, as described below.

Removing Gateway Access

To remove gateway access between two nodes, follow these steps:

1. Use the Node submenu to delete the nodes.
2. Use the main Edit menu to add the nodes back.
3. Transfer to Create mode. In Create mode, **CONFIG_NET** prompts you for information about each new node, including its gateway access rights. Reenter all information about the nodes, but do not enable gateway access.

Deleting a Gateway Node

Delete a gateway node as you would any other node. For each pair of nodes that used the gateway, you must remove the nodes' gateway access rights to one another.

Special Editing Features

CONFIG_NET allows you to enable or disable Data Set Status (DSS) interrupts and to set frame size on a ring. The following sections explain these procedures.

Enabling or Disabling DSS Interrupts

Edit mode allows you to enable or disable DSS interrupts for FDX and PSDN lines. This Edit mode feature is intended primarily for communications specialists. By default, DSS interrupts are enabled, meaning that the CPU is interrupted on Data Set Status changes. Disabling DSS interrupts prevents the CPU from being interrupted. This option is useful when a PSDN or FDX line runs through a modem eliminator.

When you select option 8 from the FDX submenu or option 9 from the PSDN submenu (Enable/Disable DSS Interrupts), CONFIG_NET issues these prompts:

```
Enable Data Set Status interrupts (NO, YES):  
Data Set Pattern (3, <0-15>):  
Data Set Order (3, <0-7>):
```

As usual, the first number in the parentheses is the default answer, which you can choose by pressing .

The following information may help you determine the correct data set pattern and data set order:

- Data set pattern

Specify a number (0-15) for the data set leads, which must be high to transmit or receive. The bits that make up this number, *wxyz*, have the meanings shown below. The pin number is the RS-232 pin number. The default bit setting is 0011 (decimal 3).

- w* Default is 0; see your Prime CSR before changing
- x* Carrier Detect bit (pin 8); default is 0
- y* Clear-To-Send bit (pin 5); default is 1
- z* Data-Set-Ready bit (pin 6); default is 1, data set ready

- Data set order

Specify a number (0-7) for the data set order to be issued before transmitting. The bits that make up this number, *xyz*, have the meanings shown below. The pin number is the RS-232 pin number. The default bit setting is 011 (decimal 3).

- x* Default is 0; see your Prime CSR before changing
- y* Request-To-Send bit (pin 4); default is 1
- z* Data-Terminal-Ready bit (pin 20); default is 1, data terminal ready

Note

Data set pattern bit *w* and data set order bit *x* also control the settings of certain pins. These settings are not documented here because they are hardware dependent. Consult your Prime Customer Support Representative (CSR) before changing either of these bits from its default value (0).

Setting Frame Size on a Ring

Option 6 of the Ring submenu, Set maximum frame size for a node on this ring, allows you to change the size of a node's Level 2 RINGNET frames. In some cases, you can improve performance by increasing the frame size.

Different nodes on a ring can use different frame sizes. When two nodes transfer data over a ring, PRIMENET uses the smaller of the two frame sizes supported on the two nodes. This flexibility allows you to assign frame sizes according to the amount and type of traffic flowing between specific nodes. For example, if two nodes exchange many large files, you may improve performance by increasing the frame size on both nodes.

However, increasing a node's frame size also increases the amount of buffer space reserved by PRIMENET on that node. For example, if you increase the frame size from 256 words to 512 words, you double the amount of buffer space allocated and wired. If you have a very large network configuration file and attempt to increase the frame size to 1024 words, you could possibly run out of buffer space. Thus, you should increase the frame size only if you have good reason to do so. You must weigh the disadvantages of increased memory usage against the advantages of increased throughput. Contact your Prime Customer Support Center for more information.

Displaying a Configuration

CONFIG_NET's LIST facility allows you to display all or part of your network configuration at any time during a CONFIG_NET session. The LIST facility is useful for checking your work during a session, or for displaying the contents of a configuration file that you have just selected for editing.

To use the LIST facility, press **Ctrl**-P to summon the option prompt, then enter LIST. CONFIG_NET displays this prompt:

```
What object would you like to list?  
(ALL, RINGS, LAN300S ,FDX, HDX, PSDNS, NODES, <node or network name>):
```

The options have the following meanings:

ALL	All information currently in the configuration file
RINGS	Information about all currently configured rings
LAN300S	Information about all currently configured LAN300s
FDX	Information about all currently configured full-duplex lines
HDX	Information about all currently configured half-duplex nodes and lines
PSDNS	Information about all currently configured network connections to PSDNs

NODES	Same as ALL: all information currently in the configuration file
node or network name	All current information on the specified node or network.

Examples of using the LIST facility appear in Chapter 7, Sample PRIMENET Configurations.

Saving and Validating a Configuration

You can validate your configuration and save it on disk at any time during the CONFIG_NET session by pressing -P and then entering SAVE in response to the option prompt.

If CONFIG_NET detects errors or omissions, it displays this message and prompt before continuing:

```
Configuration errors detected.  
Do you wish to save it anyway?
```

If you enter NO, CONFIG_NET repeats the option prompt. If you enter YES, or if CONFIG_NET detects no errors in your configuration, you are prompted:

```
Save file name (PRIMENET.CONFIG, <filename>):
```

(If you specified a filename when you invoked CONFIG_NET, that filename appears as the default instead of PRIMENET.CONFIG.) You can enter any valid filename, or press to select the default filename. CONFIG_NET saves the configuration on disk with the filename you specified, then displays the option prompt.

Quickly Saving a Configuration

To quickly save your configuration on disk at any time during a CONFIG_NET session, press -P and then enter FAST_SAVE or FS in response to the option prompt. CONFIG_NET warns you that it will not check the information in the configuration, and prompts you for confirmation to proceed. If you enter YES, CONFIG_NET displays this prompt:

```
Save file name (PRIMENET.CONFIG, <filename>):
```

(If you specified a filename when you invoked CONFIG_NET, that filename appears as the default instead of PRIMENET.CONFIG.) You can enter any valid filename, or press to select the default filename. CONFIG_NET saves the configuration file on disk with the filename you specified, then repeats the option prompt. During a Create or Edit mode session, you should save your configuration file frequently. Frequent saves preserve your work in the event of a system crash or terminal problem.

There are two situations when FAST_SAVE is useful:

- When you want to partially define a configuration, then save it quickly to be completed later.
- When you have been informed that the system is coming down in five minutes for a cold start. A normal save operation with full validation could take longer than five minutes.

Terminating CONFIG_NET

To terminate CONFIG_NET, press **Ctrl**-P and then enter QUIT in response to the option prompt. The QUIT option ends the CONFIG_NET session without saving any modifications that you may have made since the last save. If you have made modifications, CONFIG_NET asks you to confirm that you want to quit, then returns you to PRIMOS.

Sample PRIMENET Configurations

This chapter is divided into three sections:

- Create mode examples
- Edit mode examples
- List mode examples

These sections contain examples that show you how to create, edit, and list various sample network configurations. This chapter assumes that you have read Chapter 4, PRIMENET Network Configuration, and Chapter 6, Configuring Your PRIMENET Network.

The examples in this chapter use nine sample network configurations:

- Two nodes on a ring.
- Four nodes connected in a chain by full-duplex lines, including two gateway nodes.
- A half-duplex subnetwork of four nodes, one of which is also connected to a fifth node by a full-duplex line.
- Two nodes on a ring with one node connected to a PSDN and a third node directly connected to the PSDN. This example illustrates the use of indirect addressing with one gateway node.
- One node connected to two PSDNs. Each PSDN also has another node connected to it.
- A network with two nodes connected via a PSDN gateway.
- A mixed-Rev. network.
- A network with a ring, a full-duplex line, a half-duplex subnetwork, and a PSDN connection.
- A network with a non-Prime node and two Prime nodes on a LAN300, and a second non-Prime node connected via a full-duplex line to a Prime gateway node.

The examples contain sketches of the configurations, along with dialog notes that explain the CONFIG_NET dialog.

Create Mode Examples

This section shows how to configure the nine sample networks listed above. Each example includes a brief explanation, an illustration of the network, and a listing of the Create mode dialog. Portions of the dialog that require special attention are numbered. For comments on the numbered portions of dialog, refer to the dialog notes below the boxed illustrations.

Because this section contains **CREATE** examples, **CONFIG_NET** is invoked without a pathname in the command line.

Example 1: Simple Ring Configuration

In this example, two nodes, A and B, are connected over a ring as shown in Figure 7-1. The nodes have RLOG access to the other.

```
OK, CONFIG_NET
[CONFIG_NET Rev. 22.0 Copyright (c) 1987, Prime Computer, Inc.]

Create, Edit, Quit, Save, Fast_Save, List, or Help? CREATE
Enter nodes connected to RING1
① (NONE, <node names>): A,B;
  {
Enter nodes connected to RING2
(NONE, <node names>):
Enter nodes connected to LAN300-1
(NONE, <node names>):
② { Enter nodes connected to FDX1
(NONE, <node names>):
Enter nodes connected to HDX
(NONE, <node names>):
Enter packet switching data network names
(NONE, <PSDN names>):
  }
```

Dialog Notes

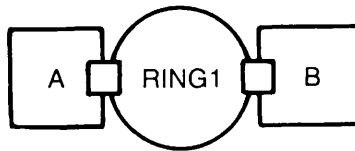


Figure 7-1. Simple Ring Configuration

① Semicolon suppresses repetition of RING1 prompt.

② Select default value (NONE) by pressing only

Enter gateway nodes
 (NONE, <node names>):
 Enter nodes running old (pre-rev-19.3) PRIMOS
 (NONE, <node names>):
 Enter nodes running non-Primenet X.25 software
 (NONE, <node names>):

- ③ Describe Node A
 Ring node ID for A on RING1 (1, <1-247>):
 Access rights from A via RING1
 (NONE, RFA, RLOG, IPCF, ALL): **RLOG;**
 Force user validation(NO, YES)?
- ④ Enter nodes accessible from A via RING1 with this access
 (NONE, ALL, <node names>, <network names>): **ALL;**
- ⑤ Access rights from A via RING1
 (NONE, RFA, RLOG, IPCF, ALL):
 Node-node password between A and B
 (NONE, YES, <password>):
- ⑥ Gateway access from A
 (NONE, RFA, RLOG, IPCF, ALL):

Describe Node B
 Ring node ID for B on RING1 (2, <1-247>):
 Access rights from B via RING1
 (NONE, RFA, RLOG, IPCF, ALL): **RLOG;**
 Force user validation(NO, YES)?

- ⑦ Enter nodes accessible from B via RING1 with this access
 (NONE, ALL, <node names>, <network names>): **A;**
 Access rights from B via RING1
 (NONE, RFA, RLOG, IPCF, ALL):
 Gateway access from B
 (NONE, RFA, RLOG, IPCF, ALL):
 All required configuration data has been supplied.

Create, Edit, Quit, Save, Fast_Save, List, or Help?

Dialog Notes

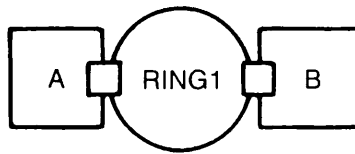


Figure 7-1. Simple Ring Configuration

- ③ Default ring node ID (1) is chosen.
- ④ If you add a node to a RING1, Node A will have RLOG access to it unless you explicitly change the access through Edit mode.
- ⑤ Access right prompt is always repeated. This allows you to specify access rights for other nodes or exceptions to the access right you just specified.
- ⑥ Gateway access prompt always appears unless node is an "old" node.
- ⑦ If you add a node to RING1, Node B will have RLOG access to it unless you explicitly change the access through Edit mode. Note that A is an acceptable abbreviation for ALL.

Example 2: Full-duplex Lines With Gateways

The network in this example, illustrated in Figure 7-2, contains four nodes connected by full-duplex lines. Two of these nodes (B and C) are gateway nodes. Nodes A and D are granted RLOG access to one another, communicating through the path formed by Nodes B and C. IPCF access is required between all pairs of nodes in the route-through path.

```
OK, CONFIG_NET
[CONFIG_NET Rev. 22.0 Copyright (c) 1987, Prime Computer, Inc.]

Create, Edit, Quit, Save, Fast_Save, List, or Help? CREATE
Enter nodes connected to RING1
(NONE, <node names>):
Enter nodes connected to LAN300-1
(NONE, <node names>):
8 { Enter nodes connected to FDX1
    (NONE, <node names>): A,B;
    Enter nodes connected to FDX2
    (NONE, <node names>): B,C;
    Enter nodes connected to FDX3
    (NONE, <node names>): C,D;
    Enter nodes connected to FDX4
    (NONE, <node names>):
    Enter nodes connected to HDX
    (NONE, <node names>):
    Enter packet switching data network names
    (NONE, <PSDN names>):
    Enter gateway nodes
    (NONE, <node names>): B,C;
    Enter nodes running old (pre-rev-19.3) PRIMOS
    (NONE, <node names>):
    Enter nodes running non-Primenet X.25 software
    (NONE, <node names>):

Describe Node A
Synchronous line number on A for FDX1
(UNKNOWN, <0-7>): 0
9 { Protocol for line FDX1
    (LAPB, LAP):
    Framing for full duplex line FDX1
    (HDLC, BSC-ASCII, BSC-EBCDIC):
10 { Access rights from A via FDX1
    (NONE, RFA, RLOG, IPCF, ALL): IPCF;
    Force user validation(NO, YES)?
    Enter nodes accessible from A via FDX1 with this access
    (NONE, ALL, <node names>, <network names>): B;
    Access rights from A via FDX1
    (NONE, RFA, RLOG, IPCF, ALL):
```

Dialog Notes

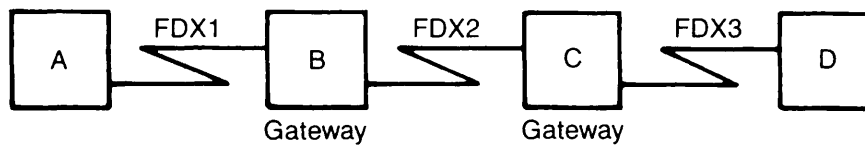


Figure 7-2. Full-duplex Lines With Gateways

- ⑧ Enter all nodes connected to full-duplex lines.
- ⑨ Press to select default values.
- ⑩ IPCF access must be assigned between all pairs of nodes in the route-through path.


```

Node-node password between A and B
(NONE, YES, <password>):

11 { Gateway access from A
    (NONE, RFA, RLOG, IPCF, ALL): IPCF;
    Force user validation(NO, YES)?
    Enter nodes accessible from A via gateway with this access
    (NONE, ALL, <node names>, <network names>): C;
    Gateway access from A
    (NONE, RFA, RLOG, IPCF, ALL): RLOG;
    Force user validation(NO, YES)?

    Enter nodes accessible from A via gateway with this access
    (NONE, ALL, <node names>, <network names>): D;
    Gateway access from A
    (NONE, RFA, RLOG, IPCF, ALL):
    Node-node password between A and C
    (NONE, YES, <password>):
    Node-node password between A and D
    (NONE, YES, <password>):

    Describe Node B
    Synchronous line number on B for FDX1
    (UNKNOWN, <0-7>): 0

    12 { Access rights from B via FDX1
        (NONE, RFA, RLOG, IPCF, ALL): IPCF;
        Force user validation(NO, YES)?
        Enter nodes accessible from B via FDX1 with this access
        (NONE, ALL, <node names>, <network names>): A;

        Access rights from B via FDX1
        (NONE, RFA, RLOG, IPCF, ALL):
        Synchronous line number on B for FDX2
        (UNKNOWN, <0-7>): 1
        Protocol for line FDX2
        (LAPB, LAP):
        Framing for full duplex line FDX2
        (HDL, BSC-ASCII, BSC-EBCDIC):

        13 { Access rights from B via FDX2
            (NONE, RFA, RLOG, IPCF, ALL): IPCF;
            Force user validation(NO, YES)?
            Enter nodes accessible from B via FDX2 with this access
            (NONE, ALL, <node names>, <network names>): C;

            Access rights from B via FDX2
            (NONE, RFA, RLOG, IPCF, ALL):
            Node-node password between B and C
            (NONE, YES, <password>):

            14 { Gateway access from B
                (NONE, RFA, RLOG, IPCF, ALL): IPCF;
                Force user validation(NO, YES)?
                Enter nodes accessible from B via gateway with this access
                (NONE, ALL, <node names>, <network names>): D;

                Gateway access from B
                (NONE, RFA, RLOG, IPCF, ALL):

```

Dialog Notes

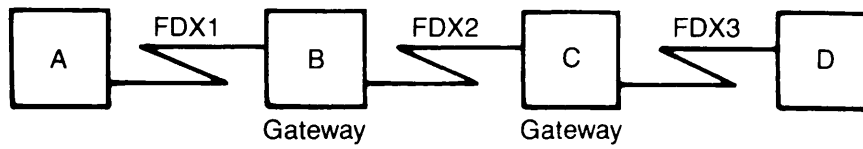


Figure 7-2. Full-duplex Lines With Gateways

- ⑪ - ⑭ IPCF access must be assigned between all pairs of nodes in the route-through path.

Node-node password between B and D
(NONE, YES, <password>):

Describe Node C
Synchronous line number on C for FDX2
(UNKNOWN, <0-7>): 0

- ⑮ { Access rights from C via FDX2
(NONE, RFA, RLOG, IPCF, ALL): **IPCF**;
Force user validation(NO, YES)?
Enter nodes accessible from C via FDX2 with this access
(NONE, ALL, <node names>, <network names>): **B**;

Access rights from C via FDX2
(NONE, RFA, RLOG, IPCF, ALL):
Synchronous line number on C for FDX3
(UNKNOWN, <0-7>): 1
Protocol for line FDX3
(LAPB, LAP):
Framing for full duplex line FDX3
(HDLC, BSC-ASCII, BSC-EBCDIC):

- ⑯ { Access rights from C via FDX3
(NONE, RFA, RLOG, IPCF, ALL): **IPCF**;
Force user validation(NO, YES)?
Enter nodes accessible from C via FDX3 with this access
(NONE, ALL, <node names>, <network names>): **D**;

Access rights from C via FDX3
(NONE, RFA, RLOG, IPCF, ALL):
Node-node password between C and D
(NONE, YES, <password>):

- ⑰ { Gateway access from C
(NONE, RFA, RLOG, IPCF, ALL): **IPCF**;
Force user validation(NO, YES)?
Enter nodes accessible from C via gateway with this access
(NONE, ALL, <node names>, <network names>): **A**;
Gateway access from C
(NONE, RFA, RLOG, IPCF, ALL):

Describe Node D
Synchronous line number on D for FDX3
(UNKNOWN, <0-7>): 0

- ⑱ { Access rights from D via FDX3
(NONE, RFA, RLOG, IPCF, ALL): **IPCF**;
Force user validation(NO, YES)?
Enter nodes accessible from D via FDX3 with this access
(NONE, ALL, <node names>, <network names>): **C**;

Access rights from D via FDX3
(NONE, RFA, RLOG, IPCF, ALL):

- ⑲ { Gateway access from D
(NONE, RFA, RLOG, IPCF, ALL): **IPCF**;
Force user validation(NO, YES)?
Enter nodes accessible from D via gateway with this access
(NONE, ALL, <node names>, <network names>): **B**;

Dialog Notes

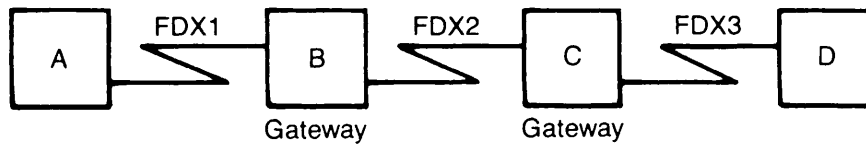


Figure 7-2. Full-duplex Lines With Gateways

- ⑮ - ⑲ IPCF access must be assigned between all pairs of nodes in the route-through path.

②0 { Gateway access from D
(NONE, RFA, RLOG, IPCF, ALL): *RLOG*;
Force user validation(NO, YES)?
Enter nodes accessible from D via gateway with this access
(NONE, ALL, <node names>, <network names>): *A*;
Gateway access from D
(NONE, RFA, RLOG, IPCF, ALL):
All required configuration data has been supplied.

Create, Edit, Quit, Save, Fast_Save, List, or Help?

Dialog Notes

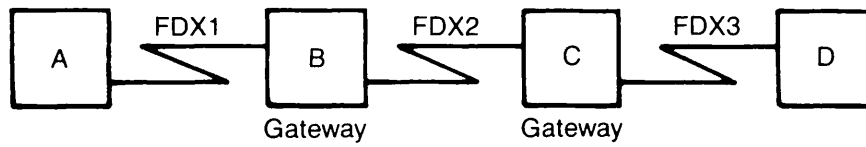


Figure 7-2. Full-duplex Lines With Gateways

- ② Nodes A and D are not directly connected; you define access through the gateway nodes.

Example 3: Half-duplex and Full-duplex Lines

Figure 7-3 shows a network with four half-duplex nodes (A, B, C, and D). Node B has two half-duplex lines, and each of Nodes A, C, and D has one half-duplex line. In addition, Node D is connected by a full-duplex line to a fifth node, E.

In this network, Node D is a gateway that routes communications between Node E and Node B. Node B is *not* configured as a gateway.

Figure 7-4 shows the access rights that are to be enabled between the various pairs of systems in this network.

```

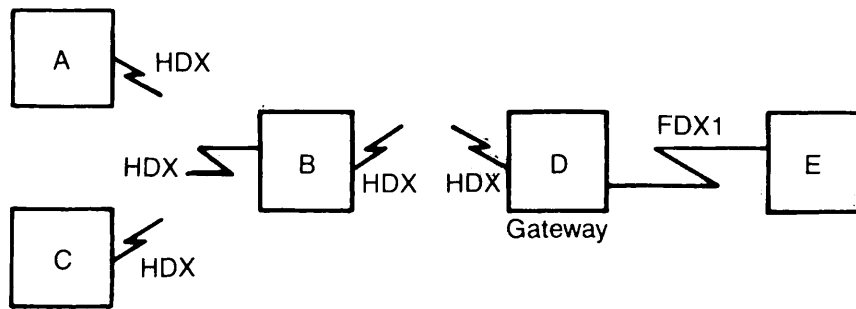
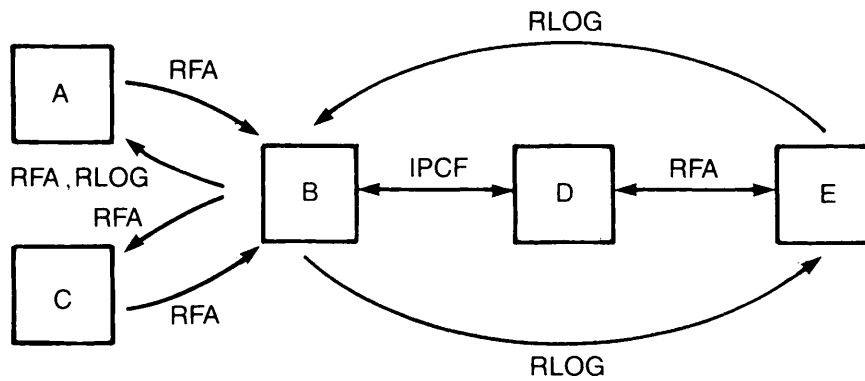
OK, CONFIG_NET
[CONFIG_NET Rev. 22.0 Copyright (c) 1987, Prime Computer, Inc.]

Create, Edit, Quit, Save, Fast_Save, List, or Help? CREATE
Enter nodes connected to RING1
(NONE, <node names>):
Enter nodes connected to LAN300-1
(NONE, <node names>):
Enter nodes connected to FDX1
(NONE, <node names>): D, E;
Enter nodes connected to FDX2
(NONE, <node names>):
Enter nodes connected to HDX
(21) (NONE, <node names>): A, B, C, D;
Enter packet switching data network names
(NONE, <PSDN names>):
Enter gateway nodes
(NONE, <node names>): D;
Enter nodes running old (pre-rev-19.3) PRIMOS
(NONE, <node names>):
Enter nodes running non-Primenet X.25 software
(NONE, <node names>):

Describe Node D
Synchronous line number on D for FDX1
(UNKNOWN, <0-7>): 0
Protocol for line FDX1
(LAPB, LAP):
Framing for full duplex line FDX1
(HDLC, BSC-ASCII, BSC-EBCDIC):
Access rights from D via FDX1
(NONE, RFA, RLOG, IPCF, ALL): RFA;
Force user validation(NO, YES)? YES
Enter nodes accessible from D via FDX1 with this access
(NONE, ALL, <node names>, <network names>): E;
Access rights from D via FDX1
(NONE, RFA, RLOG, IPCF, ALL):
Node-node password between D and E
(NONE, YES, <password>): YES

```

Dialog Notes

*Figure 7-3. Half-duplex and Full-duplex Lines**Figure 7-4. Access Rights*

- ②1 Enter names of all HDX nodes on the network.

Generated password is DHAZAN
Synchronous line numbers for connections to the half duplex network
(UNKNOWN, <0-7>): **1**;
Access rights from D via HDX
(NONE, RFA, RLOG, IPCF, ALL): **IPCF**;
Force user validation(NO, YES)?
Enter nodes accessible from D via HDX with this access
(NONE, ALL, <node names>, <network names>): **B**;
Access rights from D via HDX
(NONE, RFA, RLOG, IPCF, ALL):
D's incoming HDX password from B
(NONE, YES, <password>): **YES**
Generated password is ENQOCB
D's outgoing HDX password to B
(NONE, YES, <password>): **YES**
Generated password is EHAAZX
Node-node password between D and B
(NONE, YES, <password>):
Gateway access from D
(NONE, RFA, RLOG, IPCF, ALL):

Describe Node E
Synchronous line number on E for FDX1
(UNKNOWN, <0-7>): **0**
Access rights from E via FDX1
(NONE, RFA, RLOG, IPCF, ALL): **RFA**;
Force user validation(NO, YES)? **YES**
Enter nodes accessible from E via FDX1 with this access
(NONE, ALL, <node names>, <network names>): **D**;
Access rights from E via FDX1
(NONE, RFA, RLOG, IPCF, ALL):
Gateway access from E
(NONE, RFA, RLOG, IPCF, ALL): **RLOG**;
Force user validation(NO, YES)?
Enter nodes accessible from E via gateway with this access
(NONE, ALL, <node names>, <network names>): **B**;
Gateway access from E
(NONE, RFA, RLOG, IPCF, ALL):
Node-node password between E and B
(NONE, YES, <password>):

Describe Node A
Synchronous line numbers for connections to the half duplex network
(UNKNOWN, <0-7>): **0**;
Access rights from A via HDX
(NONE, RFA, RLOG, IPCF, ALL): **RFA**;
Force user validation(NO, YES)? **YES**
Enter nodes accessible from A via HDX with this access
(NONE, ALL, <node names>, <network names>): **B**;
Access rights from A via HDX
(NONE, RFA, RLOG, IPCF, ALL):

(22)

Dialog Notes

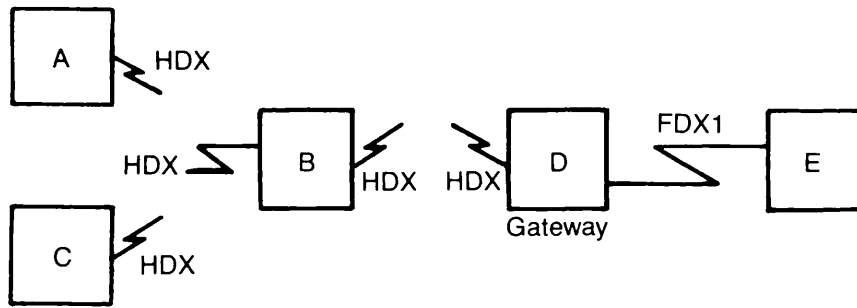


Figure 7-3. Half-duplex and Full-duplex Lines

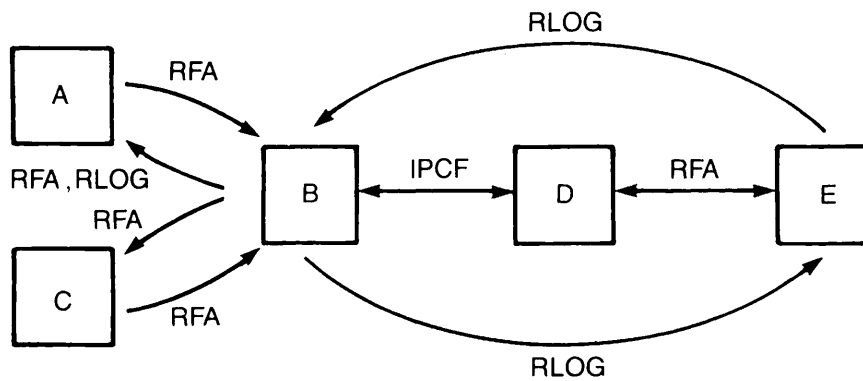


Figure 7-4. Access Rights

- ② Specify logical line number for the HDX line.

{
 23 { A's incoming HDX password from B
 (NONE, YES, <password>): **YES**
 Generated password is HAIGJO
 A's outgoing HDX password to B
 (NONE, YES, <password>): **YES**
 Generated password is HQGDTM
 Node-node password between A and B
 (NONE, YES, <password>): **YES**
 Generated password is HQKCIK
 Gateway access from A
 (NONE, RFA, RLOG, IPCF, ALL):

 Describe Node B
 Synchronous line numbers for connections to the half duplex network
 (UNKNOWN, <0-7>): **0,1;**
 Access rights from B via HDX
 (NONE, RFA, RLOG, IPCF, ALL): **RLOG,RFA;**
 Force user validation(NO, YES)? **YES**
 Enter nodes accessible from B via HDX with this access
 (NONE, ALL, <node names>, <network names>): **A;**
 Access rights from B via HDX
 (NONE, RFA, RLOG, IPCF, ALL): **RFA;**
 Force user validation(NO, YES)? **YES**
 Enter nodes accessible from B via HDX with this access
 (NONE, ALL, <node names>, <network names>): **C;**
 Access rights from B via HDX
 (NONE, RFA, RLOG, IPCF, ALL): **IPCF;**
 Force user validation(NO, YES)?
 Enter nodes accessible from B via HDX with this access
 (NONE, ALL, <node names>, <network names>): **D;**
 Access rights from B via HDX
 (NONE, RFA, RLOG, IPCF, ALL):
 {
 24 { B's incoming HDX password from C
 (NONE, YES, <password>): **YES**
 Generated password is JZDAOK
 B's outgoing HDX password to C
 (NONE, YES, <password>): **YES**
 Generated password is JYZSGX
 Node-node password between B and C
 (NONE, YES, <password>): **YES**
 Generated password is JPMCSO
 Gateway access from B
 (NONE, RFA, RLOG, IPCF, ALL): **RLOG;**
 Force user validation(NO, YES)?
 Enter nodes accessible from B via gateway with this access
 (NONE, ALL, <node names>, <network names>): **E;**
 Gateway access from B
 (NONE, RFA, RLOG, IPCF, ALL):

Dialog Notes

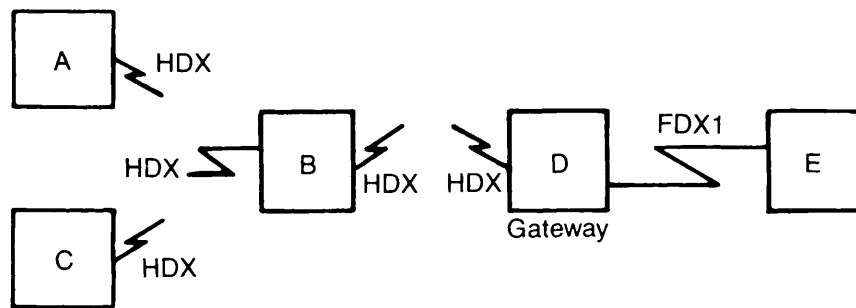


Figure 7-3. Half-duplex and Full-duplex Lines

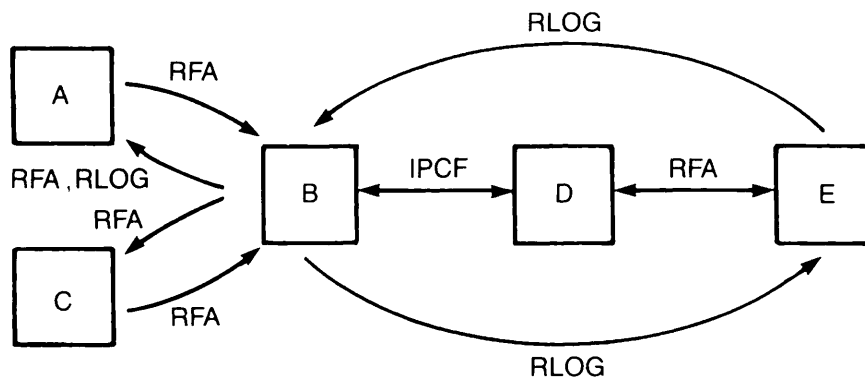


Figure 7-4. Access Rights

- ②③ Generate HDX passwords for Nodes A and B.
- ②④ Generate HDX passwords for Nodes C and B.

Describe Node C

Synchronous line numbers for connections to the half duplex network

(UNKNOWN, <0-7>): **0;**

Access rights from C via HDX

(NONE, RFA, RLOG, IPCF, ALL): **RFA;**

Force user validation(NO, YES)? **YES**

Enter nodes accessible from C via HDX with this access

(NONE, ALL, <node names>, <network names>): **B;**

Access rights from C via HDX

(NONE, RFA, RLOG, IPCF, ALL):

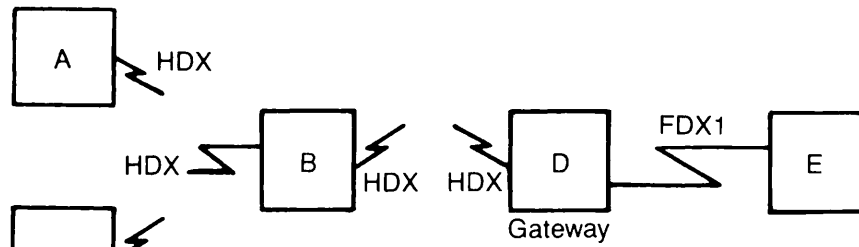
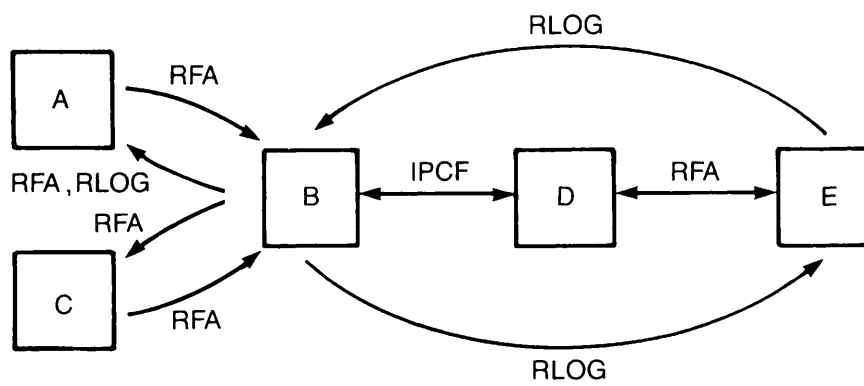
Gateway access from C

(NONE, RFA, RLOG, IPCF, ALL):

All required configuration data has been supplied.

Create, Edit, Quit, Save, Fast_Save, List, or Help?

Dialog Notes

*Figure 7-3. Half-duplex and Full-duplex Lines**Figure 7-4. Access Rights*

Example 4: Indirect PSDN Addressing With One Gateway Node

Figure 7-5 shows a network with two nodes, A and B, on a ring. Node B is directly connected to TELENET, with address 311055500999. It is also a gateway node that routes data between TELENET and Node A. Node A's indirect TELENET address is 31105550099901. A third node, C, is also directly connected to TELENET, with address 311055500888.

```
OK, CONFIG_NET
[CONFIG_NET Rev. 22.0 Copyright (c) 1987, Prime Computer, Inc.]

Create, Edit, Quit, Save, Fast_Save, List, or Help? CREATE
Enter nodes connected to RING1
(NONE, <node names>): A,B;
Enter nodes connected to RING2
(NONE, <node names>):
Enter nodes connected to LAN300-1
(NONE, <node names>):
Enter nodes connected to FDX1
(NONE, <node names>):
Enter nodes connected to HDX
(NONE, <node names>):
Enter packet switching data network names
(NONE, <PSDN names>): TELENET;
Enter nodes connected to TELENET
(NONE, <node names>): B,C;
Enter gateway nodes
(25) (NONE, <node names>): B;
Enter nodes running old (pre-rev-19.3) PRIMOS
(NONE, <node names>):
Enter nodes running non-Primenet X.25 software
(NONE, <node names>):

Describe Node A
Ring node ID for A on RING1 (1, <1-247>): 1
Access rights from A via RING1
(NONE, RFA, RLOG, IPCF, ALL): RLOG;
Force user validation(NO, YES)?
Enter nodes accessible from A via RING1 with this access
(NONE, ALL, <node names>, <network names>): B;
Access rights from A via RING1
(NONE, RFA, RLOG, IPCF, ALL):
Node-node password between A and B
(NONE, YES, <password>):
(26) Indirect TELENET address for node A
(NONE, <TELENET addresses>): 31105550099901;
Gateway node which will route address 31105550099901 from TELENET
to node A
(NONE, <node names>): B;
Lines on node B for routing TELENET address 31105550099901
for node A
(UNKNOWN, <0-7>): 0;
```

Dialog Notes

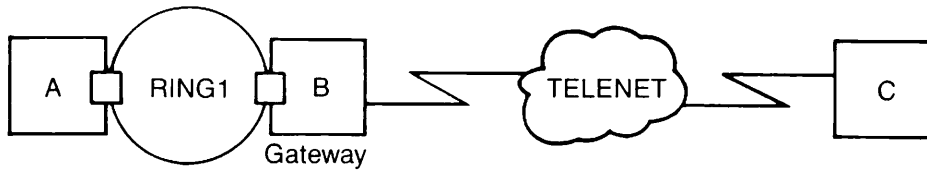


Figure 7-5. Indirect Addressing With One Gateway Node

②⑤ Node B is the gateway between Node A and TELENET.

②⑥ This indirect address combines Node B's PSDN address and a unique subaddress.


```

(27) { Gateway access from A
      (NONE, RFA, RLOG, IPCF, ALL): IPCF;
      Force user validation(NO, YES)? NO
      Enter nodes accessible from A via gateway with this access
      (NONE, ALL, <node names>, <network names>): C;

      Gateway access from A
      (NONE, RFA, RLOG, IPCF, ALL):
      Node-node password between A and C
      (NONE, YES, <password>):

      Describe Node B
      Ring node ID for B on RING1 (2, <1-247>): 2;
      Access rights from B via RING1
      (NONE, RFA, RLOG, IPCF, ALL): RLOG;
      Force user validation(NO, YES)?
      Enter nodes accessible from B via RING1 with this access
      (NONE, ALL, <node names>, <network names>): A;
      Access rights from B via RING1
      (NONE, RFA, RLOG, IPCF, ALL):
      Enter TELENET addresses for B
      (NONE, <TELENET addresses>): 311055500999;
      Synchronous line numbers for TELENET address 311055500999
      (UNKNOWN, <0-7>): 0;

(28) { Protocol for line SMLC00 to TELENET
      (LAPB, LAP):
      Framing for line SMLC00 to TELENET
      (HDLC, BSC-ASCII, BSC-EBCDIC):
      Highest logical channel number for VCs on line SMLC00 to TELENET
      (4095, <1-4095>): 4095
      Default window size for line SMLC00 to TELENET
      (2, <1-7>):
(29) { Default packet size (in bytes) for line SMLC00 to TELENET
      (256, <16-256>): 128
      Access rights from B via TELENET
      (NONE, RFA, RLOG, IPCF, ALL): IPCF;
      Force user validation(NO, YES)?
      Enter nodes accessible from B via TELENET with this access
      (NONE, ALL, <node names>, <network names>): C;
      Access rights from B via TELENET
      (NONE, RFA, RLOG, IPCF, ALL):
      Node-node password between B and C
      (NONE, YES, <password>):
      Indirect TELENET address for node B
      (NONE, <TELENET addresses>):
      Gateway access from B
      (NONE, RFA, RLOG, IPCF, ALL):

      Describe Node C
      Enter TELENET addresses for C
      (NONE, <TELENET addresses>): 311055500888;
      Synchronous line numbers for TELENET address 311055500888
      (UNKNOWN, <0-7>): 0;

```

Dialog Notes

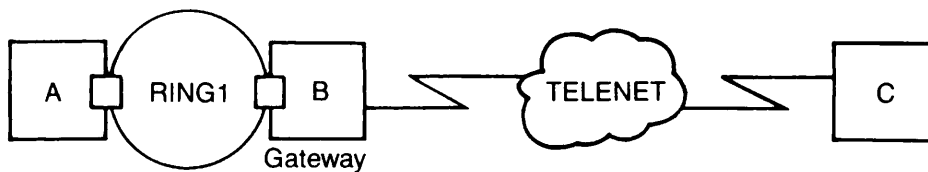


Figure 7-5. Indirect Addressing With One Gateway Node

- ②⑦ Node A is given IPCF access to Node C.
- ②⑧ Default value chosen by pressing .
- ②⑨ TELENET's default packet size is 128.

Protocol for line SMLC00 to TELENET
(LAPB, LAP):
Framing for line SMLC00 to TELENET
(HDLC, BSC-ASCII, BSC-EBCDIC):
Highest logical channel number for VCs on line SMLC00 to TELENET
(4095, <1-4095>): **255**
Default window size for line SMLC00 to TELENET
(2, <1-7>):
Default packet size (in bytes) for line SMLC00 to TELENET
(256, <16-256>): **128**
Access rights from C via TELENET
(NONE, RFA, RLOG, IPCF, ALL): **IPCF**;
Force user validation(NO, YES)?
Enter nodes accessible from C via TELENET with this access
(NONE, ALL, <node names>, <network names>): **B**;
Access rights from C via TELENET
(NONE, RFA, RLOG, IPCF, ALL):
Indirect TELENET address for node C
(NONE, <TELENET addresses>):
Gateway access from C
(NONE, RFA, RLOG, IPCF, ALL): **IPCF**;
Force user validation(NO, YES)?
Enter nodes accessible from C via gateway with this access
(NONE, ALL, <node names>, <network names>): **A**;
Gateway access from C
(NONE, RFA, RLOG, IPCF, ALL):
All required configuration data has been supplied.

Create, Edit, Quit, Save, Fast_Save, List, or Help?

Dialog Notes

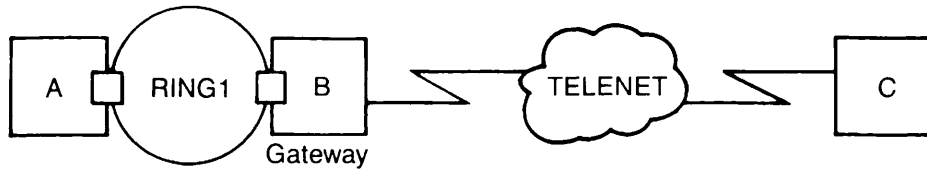


Figure 7-5. Indirect Addressing With One Gateway Node

Example 5: Multiple PSDN Connections

Figure 7-6 shows a network in which one node, SYSX, is connected to two different PSDNs, TYMNET and X.25. For an explanation of when to use "X.25" as a PSDN name, refer to the section entitled Packet Switching Data Network Definition in Chapter 6, Configuring Your PRIMENET Network. Two other nodes, SYSY and SYSZ, are connected to TYMNET and X.25, respectively.

```
OK, CONFIG_NET
[CONFIG_NET Rev. 22.0 Copyright (c) 1987, Prime Computer, Inc.]
```

```
Create, Edit, Quit, Save, Fast_Save, List, or Help? CREATE
Enter nodes connected to RING1
(NONE, <node names>):
Enter nodes connected to LAN300-1
(NONE, <node names>):
Enter nodes connected to FDX1
(NONE, <node names>):
Enter nodes connected to HDX
(NONE, <node names>):
Enter packet switching data network names
(NONE, <PSDN names>): TYMNET, X.25;
Enter nodes connected to TYMNET
(NONE, <node names>): SYSX, SYSY;
Enter nodes connected to X.25
(NONE, <node names>): SYSX, SYSZ;
Enter gateway nodes
(NONE, <node names>):
Enter nodes running old (pre-rev-19.3) PRIMOS
(NONE, <node names>):
Enter nodes running non-Primenet X.25 software
(NONE, <node names>):
```

```
Describe Node SYSX
Enter TYMNET addresses for SYSX
(30) (NONE, <TYMNET addresses>): 310655555;
Synchronous line numbers for TYMNET address 310655555
(UNKNOWN, <0-7>): 0;
Protocol for line SMLC00 to TYMNET
(LAPB, LAP):
Framing for line SMLC00 to TYMNET
(HDLC, BSC-ASCII, BSC-EBCDIC):
Highest logical channel number for VCs on line SMLC00 to TYMNET
(4095, <1-4095>): 4095
Default window size for line SMLC00 to TYMNET
(2, <1-7>):
Default packet size (in bytes) for line SMLC00 to TYMNET
(256, <16-256>): 128;
Access rights from SYSX via TYMNET
(NONE, RFA, RLOG, IPCF, ALL): IPCF;
Force user validation(NO, YES)?
Enter nodes accessible from SYSX via TYMNET with this access
(NONE, ALL, <node names>, <network names>): SYSY;
```

Dialog Notes

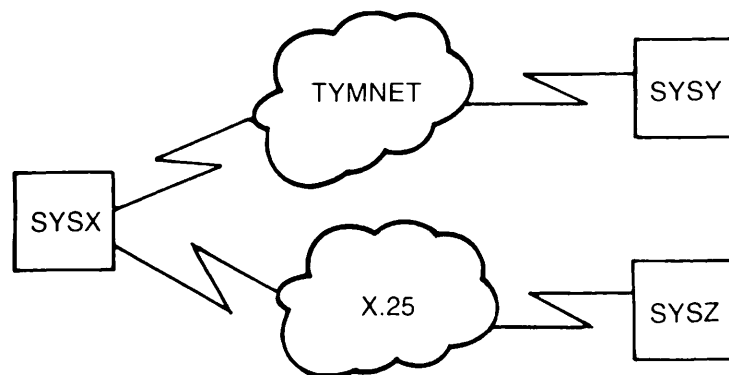


Figure 7-6. Multiple PSDN Connections

③⑩ This is SYSX's TYMNET address.

Access rights from SYSX via TYMNET
(NONE, RFA, RLOG, IPCF, ALL):
Node-node password between SYSX and SYSY
(NONE, YES, <password>):
Enter X.25 addresses for SYSX
(31) (NONE, <X.25 addresses>): **7777777777777777;**
Synchronous line numbers for X.25 address 7777777777777777
(32) (UNKNOWN, <0-7>): **1;**
Protocol for line SMLC01 to X.25
(LAPB, LAP):
Framing for line SMLC01 to X.25
(HDLC, BSC-ASCII, BSC-EBCDIC):
Highest logical channel number for VCs on line SMLC01 to X.25
(4095, <1-4095>): **4095**
Default window size for line SMLC01 to X.25
(2, <1-7>):
Default packet size (in bytes) for line SMLC01 to X.25
(256, <16-256>): **128;**
Access rights from SYSX via X.25
(NONE, RFA, RLOG, IPCF, ALL): **IPCF;**
Force user validation(NO, YES)?
Enter nodes accessible from SYSX via X.25 with this access
(NONE, ALL, <node names>, <network names>): **SYSZ;**
Access rights from SYSX via X.25
(NONE, RFA, RLOG, IPCF, ALL):
Node-node password between SYSX and SYSZ
(NONE, YES, <password>):
Gateway access from SYSX
(NONE, RFA, RLOG, IPCF, ALL):

Describe Node SYSY
Enter TYMNET addresses for SYSY
(33) (NONE, <TYMNET addresses>): **310622222;**
Synchronous line numbers for TYMNET address 310622222
(UNKNOWN, <0-7>): **0;**
Protocol for line SMLC00 to TYMNET
(LAPB, LAP):
Framing for line SMLC00 to TYMNET
(HDLC, BSC-ASCII, BSC-EBCDIC):
Highest logical channel number for VCs on line SMLC00 to TYMNET
(4095, <1-4095>): **4095**
Default window size for line SMLC00 to TYMNET
(2, <1-7>):
Default packet size (in bytes) for line SMLC00 to TYMNET
(256, <16-256>): **128;**
Access rights from SYSY via TYMNET
(NONE, RFA, RLOG, IPCF, ALL): **IPCF;**
Force user validation(NO, YES)?
Enter nodes accessible from SYSY via TYMNET with this access
(NONE, ALL, <node names>, <network names>): **SYSX;**

Dialog Notes

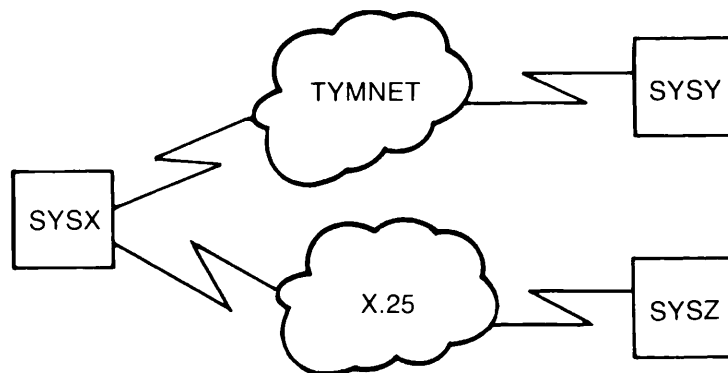


Figure 7-6. Multiple PSDN Connections

- ③① This is SYSX's X.25 address.
- ③② You assign a unique line number for each line you configure.
- ③③ This is SYSY's TYMNET address.

Access rights from SYSY via TYMNET

(NONE, RFA, RLOG, IPCF, ALL):

Gateway access from SYSY

(NONE, RFA, RLOG, IPCF, ALL):

Describe Node SYSZ

Enter X.25 addresses for SYSZ

34 (NONE, <X.25 addresses>): **88888888888888;**

Synchronous line numbers for X.25 address 88888888888888

(UNKNOWN, <0-7>): **0;**

Protocol for line SMLC00 to X.25

(LAPB, LAP):

Framing for line SMLC00 to X.25

(HDL, BSC-ASCII, BSC-EBCDIC):

Highest logical channel number for VCs on line SMLC00 to X.25

(4095, <1-4095>): **4095**

Default window size for line SMLC00 to X.25

(2, <1-7>):

Default packet size (in bytes) for line SMLC00 to X.25

(256, <16-256>): **128;**

Access rights from SYSZ via X.25

(NONE, RFA, RLOG, IPCF, ALL): **IPCF;**

Force user validation(NO, YES)?

Enter nodes accessible from SYSZ via X.25 with this access

(NONE, ALL, <node names>, <network names>): **SYSX;**

Access rights from SYSZ via X.25

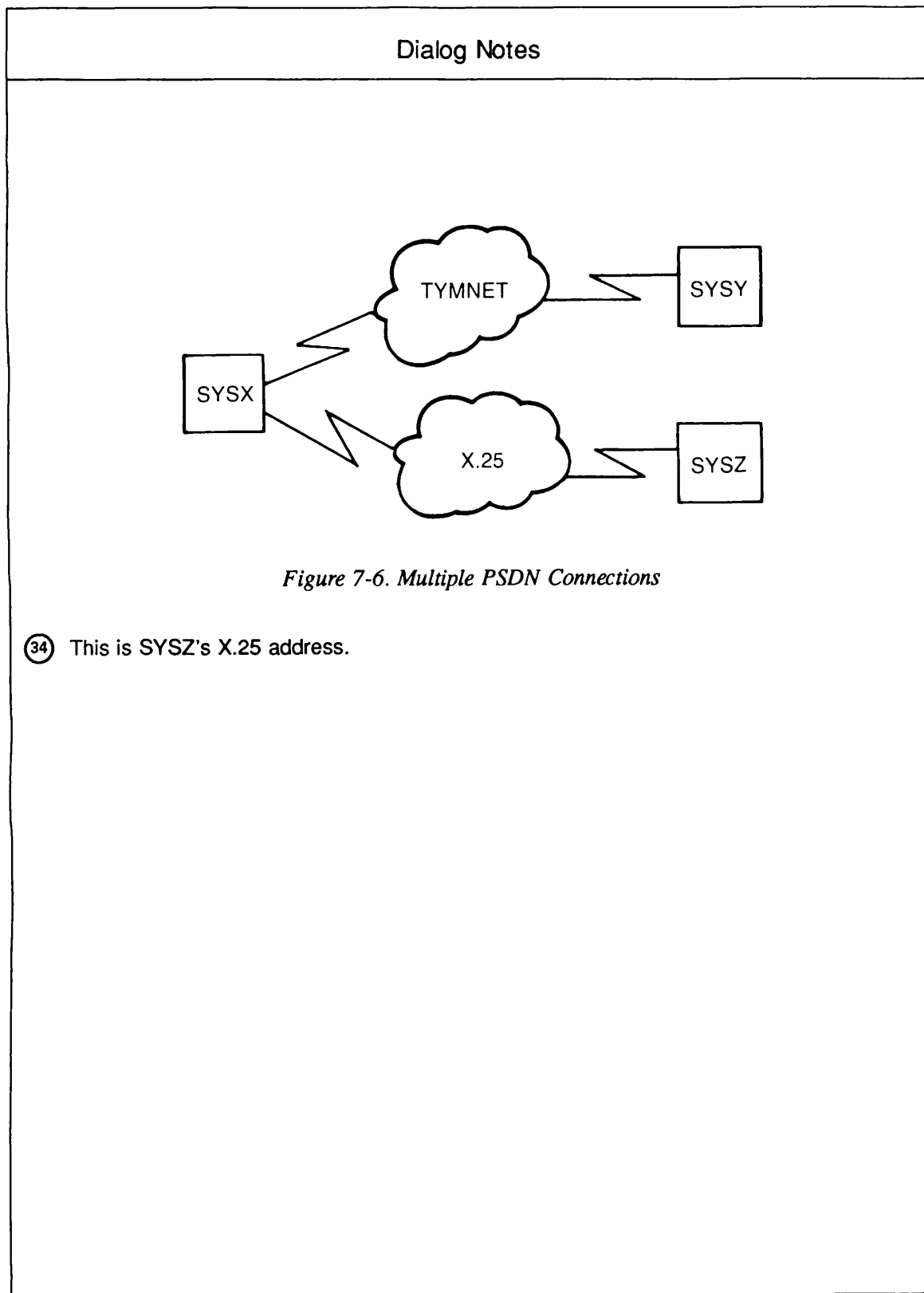
(NONE, RFA, RLOG, IPCF, ALL):

Gateway access from SYSZ

(NONE, RFA, RLOG, IPCF, ALL):

All required configuration data has been supplied.

Create, Edit, Quit, Save, Fast_Save, List, or Help?



Example 6: PSDN Gateway

As mentioned in the section entitled PSDN Gateways in Chapter 4, PRIMENET Network Configuration, a network with a PSDN gateway (a connection between two PSDNs) requires more than one global configuration file. This is because a different configuration file must be used on each side of the gateway. For example, in the configuration shown in Figure 7-7, Nodes A and B must have different configuration files. The CONFIG_NET dialogs for these two files are listed below. Note that Node A does not see the PSDN X.25 at all. From Node A's point of view, Node B is a TELENET node. Similarly, Node B sees X.25 but not TELENET, and treats Node A as a node on the X.25 PSDN.

DIALOG FOR CONFIGURATION FILE ON NODE A

```
OK, CONFIG_NET
[CONFIG_NET Rev. 22.0 Copyright (c) 1987, Prime Computer, Inc.]
```

```
Create, Edit, Quit, Save, Fast_Save, List, or Help? CREATE
```

```
Enter nodes connected to RING1
```

```
(NONE, <node names>):
```

```
Enter nodes connected to LAN300-1
```

```
(NONE, <node names>):
```

```
Enter nodes connected to FDX1
```

```
(NONE, <node names>):
```

```
Enter nodes connected to HDX
```

```
(NONE, <node names>):
```

```
Enter packet switching data network names
```

```
(NONE, <PSDN names>): TELENET;
```

```
Enter nodes connected to TELENET
```

```
(35) (NONE, <node names>): A,B;
```

```
Enter gateway nodes
```

```
(NONE, <node names>):
```

```
Enter nodes running old (pre-rev-19.3) PRIMOS
```

```
(NONE, <node names>):
```

```
Enter nodes running non-Primenet X.25 software
```

```
(NONE, <node names>):
```

```
Describe Node A
```

```
Enter TELENET addresses for A
```

```
(NONE, <TELENET addresses>): 311055511111;
```

```
Synchronous line numbers for TELENET address 311055511111
```

```
(UNKNOWN, <0-7>): 0;
```

```
Protocol for line SMLC00 to TELENET
```

```
(LAPB, LAP):
```

Dialog Notes

*Figure 7-7. PSDN Gateway*

- 35 B is treated as a TELENET node.

Framing for line SMLC00 to TELENET
(HDL, BSC-ASCII, BSC-EBCDIC):
Highest logical channel number for VCs on line SMLC00 to TELENET
(4095, <1-4095>): **4095**
Default window size for line SMLC00 to TELENET
(2, <1-7>):
Default packet size (in bytes) for line SMLC00 to TELENET
(256, <16-256>): **128;**
Access rights from A via TELENET
(NONE, RFA, RLOG, IPCF, ALL): **RLOG;**
Force user validation(NO, YES)?
Enter nodes accessible from A via TELENET with this access
(NONE, ALL, <node names>, <network names>): **B;**
Access rights from A via TELENET
(NONE, RFA, RLOG, IPCF, ALL):
Node-node password between A and B
(NONE, YES, <password>):
Gateway access from A
(NONE, RFA, RLOG, IPCF, ALL):

Describe Node B

Enter TELENET addresses for B

③⑥ (NONE, <TELENET addresses>): **77777777777777;**

Synchronous line numbers for TELENET address 77777777777777

③⑦ (UNKNOWN, <0-7>):

Access rights from B via TELENET

(NONE, RFA, RLOG, IPCF, ALL): **RLOG;**

Force user validation(NO, YES)?

Enter nodes accessible from B via TELENET with this access

(NONE, ALL, <node names>, <network names>): **A;**

Access rights from B via TELENET

(NONE, RFA, RLOG, IPCF, ALL):

Gateway access from B

(NONE, RFA, RLOG, IPCF, ALL):

All required configuration data has been supplied.

Create, Edit, Quit, Save, Fast_Save, List, or Help?

Dialog Notes



Figure 7-7. PSDN Gateway

- ③⑥ This is actually Node B's X.25 address.
- ③⑦ When you specify UNKNOWN, CONFIG_NET does not ask for the framing or protocol.

DIALOG FOR CONFIGURATION FILE ON NODE B

OK, CONFIG_NET
 [CONFIG_NET Rev. 22.0 Copyright (c) 1987, Prime Computer, Inc.]

Create, Edit, Quit, Save, Fast_Save, List, or Help? **CREATE**

Enter nodes connected to RING1

(NONE, <node names>):

Enter nodes connected to LAN300-1

(NONE, <node names>):

Enter nodes connected to FDX1

(NONE, <node names>):

Enter nodes connected to HDX

(NONE, <node names>):

Enter packet switching data network names

(NONE, <PSDN names>): **X.25;**

Enter nodes connected to X.25

(38) (NONE, <node names>): **A,B;**

Enter gateway nodes

(NONE, <node names>):

Enter nodes running old (pre-rev-19.3) PRIMOS

(NONE, <node names>):

Enter nodes running non-Primenet X.25 software

(NONE, <node names>):

Describe Node A

Enter X.25 addresses for A

(39) (NONE, <X.25 addresses>): **311055511111;**

Synchronous line numbers for X.25 address 311055511111

(UNKNOWN, <0-7>):

Access rights from A via X.25

(NONE, RFA, RLOG, IPCF, ALL): **RLOG;**

Force user validation(NO, YES)?

Enter nodes accessible from A via X.25 with this access

(NONE, ALL, <node names>, <network names>): **B;**

Access rights from A via X.25

(NONE, RFA, RLOG, IPCF, ALL):

Node-node password between A and B

(NONE, YES, <password>):

Gateway access from A

(NONE, RFA, RLOG, IPCF, ALL):

Describe Node B

Enter X.25 addresses for B

(NONE, <X.25 addresses>): **77777777777777;**

Synchronous line numbers for X.25 address 77777777777777

(UNKNOWN, <0-7>): **0;**

Protocol for line SMLC00 to X.25

(LAPB, LAP):

Framing for line SMLC00 to X.25

(HDLC, BSC-ASCII, BSC-EBCDIC):

Dialog Notes

*Figure 7-7. PSDN Gateway*

- ③⑧ A is treated as an X.25 node.
- ③⑨ This is actually Node A's TELENET address.

Highest logical channel number for VCs on line SMLC00 to X.25
(4095, <1-4095>): **4095**
Default window size for line SMLC00 to X.25
(2, <1-7>):
Default packet size (in bytes) for line SMLC00 to X.25
(256, <16-256>): **128;**
Access rights from B via X.25
(NONE, RFA, RLOG, IPCF, ALL): **RLOG;**
Force user validation(NO, YES)?
Enter nodes accessible from B via X.25 with this access
(NONE, ALL, <node names>, <network names>): **A;**
Access rights from B via X.25
(NONE, RFA, RLOG, IPCF, ALL):
Gateway access from B
(NONE, RFA, RLOG, IPCF, ALL):
All required configuration data has been supplied.

Create, Edit, Quit, Save, Fast_Save, List, or Help?

Dialog Notes

*Figure 7-7. PSDN Gateway*

Example 7: Mixed-Rev. Network

This example shows how to configure a mixed-Rev. network such as the one shown in Figure 7-8. Node A, an old node, is connected to Node B by a full-duplex line. Node B has two addresses: a TYMNET address, 310699999, and a PRIMENET address, 99990402010880. In the per-node dialog for Node B, CONFIG_NET asks which of these addresses is used by old nodes to identify Node B. For information about addresses in mixed-Rev. networks, refer to the section entitled Specifying Addresses in a Mixed-Rev. Network in Chapter 4, PRIMENET Network Configuration.

```
OK, CONFIG_NET
[CONFIG_NET Rev. 22.0 Copyright (c) 1987, Prime Computer, Inc.]
```

```
Create, Edit, Quit, Save, Fast_Save, List, or Help? CREATE
```

```
Enter nodes connected to RING1
```

```
(NONE, <node names>):
```

```
Enter nodes connected to LAN300-1
```

```
(NONE, <node names>):
```

```
Enter nodes connected to FDX1
```

```
(NONE, <node names>): A,B;
```

```
Enter nodes connected to FDX2
```

```
(NONE, <node names>):
```

```
Enter nodes connected to HDX
```

```
(NONE, <node names>):
```

```
Enter packet switching data network names
```

```
(NONE, <PSDN names>): TYMNET;
```

```
Enter nodes connected to TYMNET
```

```
(NONE, <node names>): B,C;
```

```
Enter gateway nodes
```

```
(NONE, <node names>):
```

```
Enter nodes running old (pre-rev-19.3) PRIMOS
```

```
(40) (NONE, <node names>): A;
```

```
Enter nodes running non-Primenet X.25 software
```

```
(NONE, <node names>):
```

```
Describe Node A
```

```
Synchronous line number on A for FDX1
```

```
(UNKNOWN, <0-7>): 0;
```

```
Protocol for line FDX1
```

```
(LAPB, LAP): LAP;
```

```
Framing for full duplex line FDX1
```

```
(HDLC, BSC-ASCII, BSC-EBCDIC): HDLC;
```

```
Access rights from A via FDX1
```

```
(NONE, RFA, RLOG, IPCF, ALL): IPCF;
```

```
Force user validation(NO, YES)?
```

```
Enter nodes accessible from A via FDX1 with this access
```

```
(NONE, ALL, <node names>, <network names>): B;
```

```
Access rights from A via FDX1
```

```
(NONE, RFA, RLOG, IPCF, ALL):
```

```
Node-node password between A and B
```

```
(NONE, YES, <password>):
```

Dialog Notes

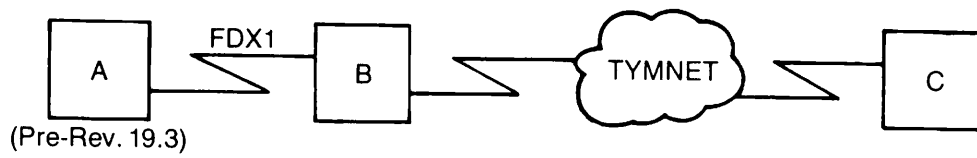


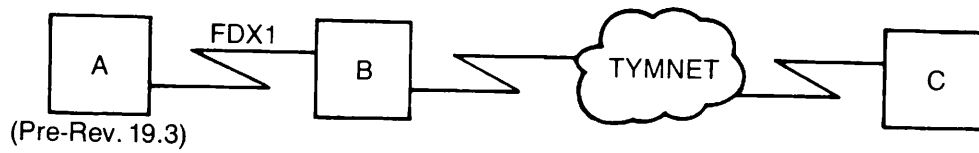
Figure 7-8. Mixed-Rev. Network

- ④ Identify A as a pre-Rev. 19.3 node.

Describe Node B
Synchronous line number on B for FDX1
(UNKNOWN, <0-7>): **0;**
Access rights from B via FDX1
(NONE, RFA, RLOG, IPCF, ALL): **IPCF;**
Force user validation(NO, YES)?
Enter nodes accessible from B via FDX1 with this access
(NONE, ALL, <node names>, <network names>): **A;**
Access rights from B via FDX1
(NONE, RFA, RLOG, IPCF, ALL):
Enter TYMNET addresses for B
(NONE, <TYMNET addresses>): **310699999;**
Synchronous line numbers for TYMNET address 310699999
(UNKNOWN, <0-7>): **1;**
Protocol for line SMLC01 to TYMNET
(LAPB, LAP):
Framing for line SMLC01 to TYMNET
(HDLC, BSC-ASCII, BSC-EBCDIC):
Highest logical channel number for VCs on line SMLC01 to TYMNET
(4095, <1-4095>): **4095**
Default window size for line SMLC01 to TYMNET
(2, <1-7>):
Default packet size (in bytes) for line SMLC01 to TYMNET
(256, <16-256>): **128;**
Access rights from B via TYMNET
(NONE, RFA, RLOG, IPCF, ALL): **RLOG;**
Force user validation(NO, YES)?
Enter nodes accessible from B via TYMNET with this access
(NONE, ALL, <node names>, <network names>): **C;**
Access rights from B via TYMNET
(NONE, RFA, RLOG, IPCF, ALL):
Node-node password between B and C
(NONE, YES, <password>):
Gateway access from B
(NONE, RFA, RLOG, IPCF, ALL):

Describe Node C
Enter TYMNET addresses for C
(NONE, <TYMNET addresses>): **310688888;**
Synchronous line numbers for TYMNET address 310688888
(UNKNOWN, <0-7>): **0;**
Protocol for line SMLC00 to TYMNET
(LAPB, LAP):
Framing for line SMLC00 to TYMNET
(HDLC, BSC-ASCII, BSC-EBCDIC):
Highest logical channel number for VCs on line SMLC00 to TYMNET
(4095, <1-4095>): **4095**
Default window size for line SMLC00 to TYMNET
(2, <1-7>):

Dialog Notes

*Figure 7-8. Mixed-Rev. Network*

Default packet size (in bytes) for line SMLC00 to TYMNET
(256, <16-256>): **128;**
Access rights from C via TYMNET
(NONE, RFA, RLOG, IPCF, ALL): **IPCF;**
Force user validation(NO, YES)?
Enter nodes accessible from C via TYMNET with this access
(NONE, ALL, <node names>, <network names>): **B;**
Access rights from C via TYMNET
(NONE, RFA, RLOG, IPCF, ALL):
Gateway access from C
(NONE, RFA, RLOG, IPCF, ALL):

Describe Node B

- (41) What address do old nodes have configured for node B
(310699999, 99990402010880, <address>):
All required configuration data has been supplied.

Create, Edit, Quit, Save, Fast_Save, List, or Help?

Dialog Notes

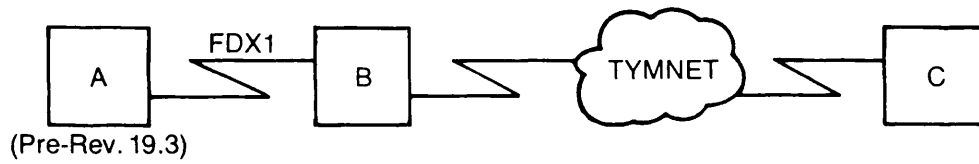


Figure 7-8. Mixed-Rev. Network

- ④ CONFIG_NET displays the PDSN and PRIMENET addresses. You indicate which address is specified for Node B in Node A's NETCON file.

Example 8: General Network Example

Figure 7-9 is a sketch of the network that was used as an example in Chapter 5, *Preparing to Configure Your PRIMENET Network*. This network has a ring, a full-duplex line, a half-duplex subnetwork, and a PSDN connection. Node A is a gateway node that routes data between the following pairs of indirectly connected nodes:

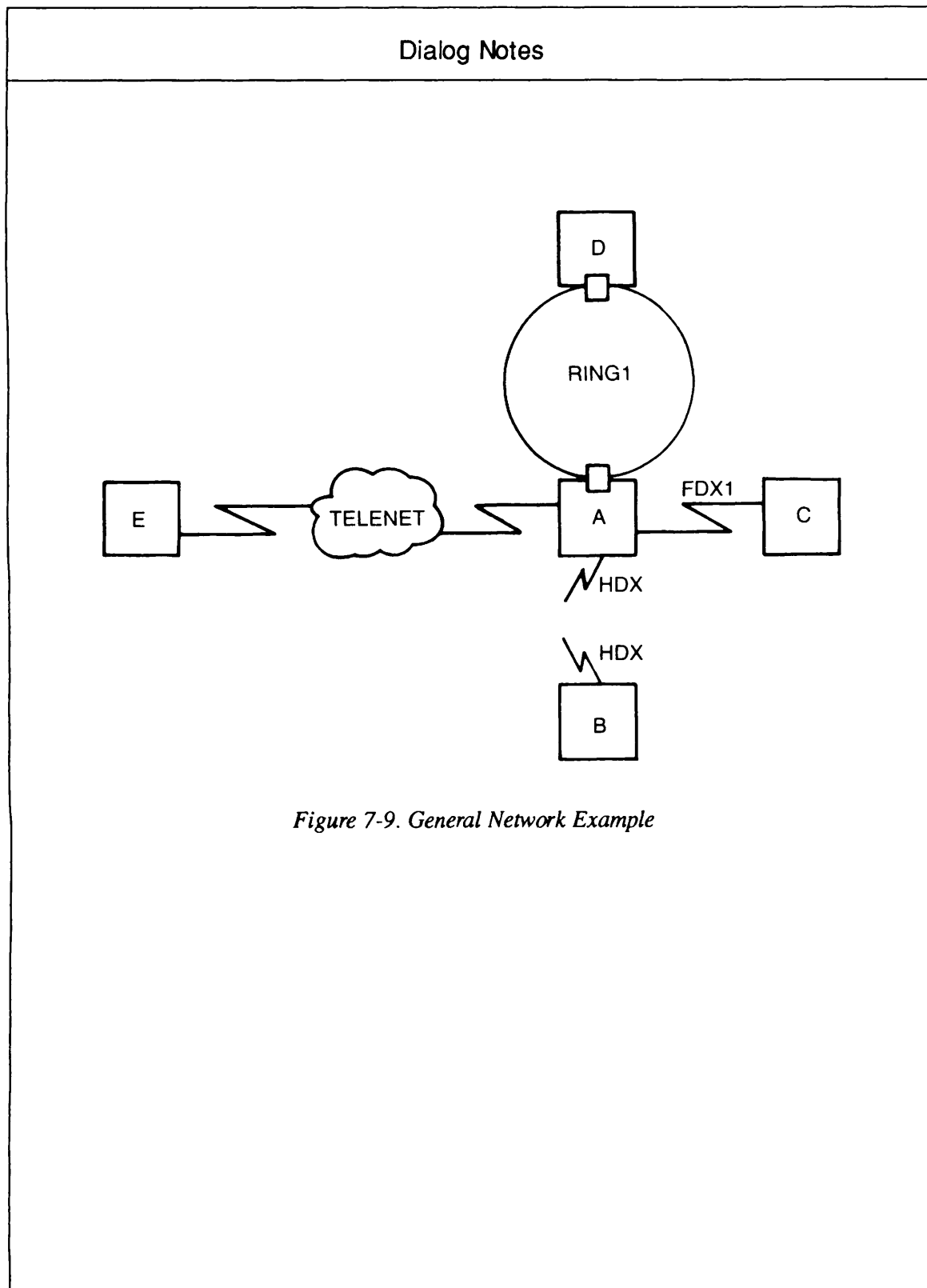
- B and C
- B and D
- B and E
- C and D
- C and E
- D and E

(Nodes A, B, and C will explicitly be granted access to Node E. Node D will not, but Node E will be able to call Node D over TELENET for reasons discussed below.)

Nodes A and E are directly connected to TELENET, with addresses 311055599999 and 311055588888, respectively. Nodes B, C, and D have indirect addresses formed by adding the suffixes 03, 02, and 01, respectively, to Node A's address. The fact that Node D is assigned a TELENET address will allow Node E to call Node D over TELENET even though no access is explicitly configured between them. This point is discussed in more detail below.

The following list indicates the access rights enabled in this network:

<i>Nodes</i>	<i>Link Type</i>	<i>Access</i>
A to B	via HDX	IPCF
A to C	via FDX1	RFA
A to D	via RING1	ALL
A to E	via TELENET	IPCF
B to A	via HDX	RLOG
B to C	via gateway	RLOG
B to D	via gateway	IPCF
B to E	via gateway	IPCF



<i>Nodes</i>	<i>Link Type</i>	<i>Access</i>
C to A	via FDX1	RFA
C to B	via gateway	\PCF
C to D	via gateway	RLOG
C to E	via gateway	PCF
D to A	via RING1i	ALL
D to B	via gateway	PCF
D to C	via gateway	RLOG
D to E	via gateway	NONE
E to A	via TELENET	PCF
E to B	via gateway	PCF
E to C	via gateway	PCF
E to D	via gateway	NONE

Notes

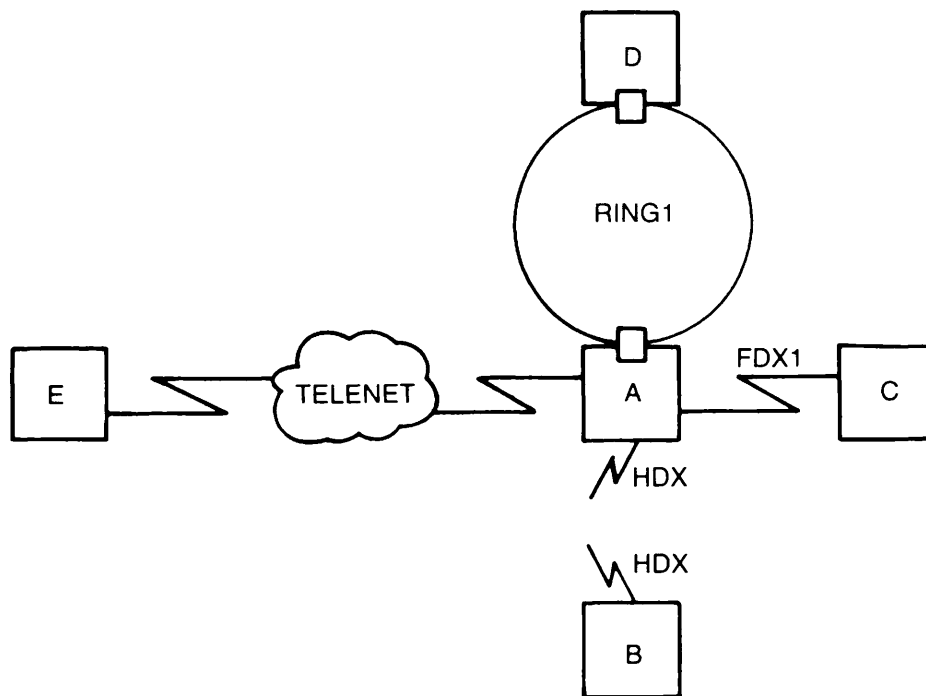
Nodes A, B, and C are granted PCF access to Node E. Because PCF access is symmetric, Node E will automatically have PCF access to Nodes A, B, and C (although in this example we will not configure this access explicitly). No access is configured between Nodes D and E.

Because Node A is directly connected to TELENET, it does not *need* PCF access to Node E in order to connect to Node E. Similarly, because Node E is directly connected to TELENET, Node E does not need PCF access to Nodes A, B, C, and D in order to access these nodes. As explained in Chapter 3, PRIMENET Security, a node that is directly connected to a PSDN may call any other node on the PSDN, as long as it uses the called node's PSDN address in making the call.

Node D will not be able to call Node E, since Node D is not directly connected to TELENET and no access is configured between D and E.

The CONFIG_NET dialog for this network is shown below.

Dialog Notes

*Figure 7-9. General Network Example*

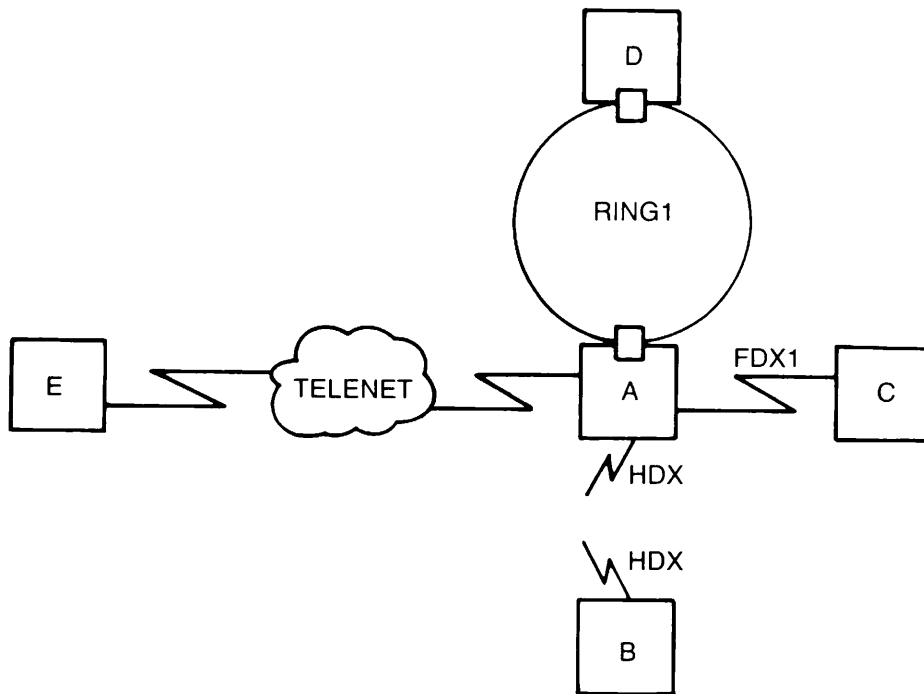
OK, CONFIG_NET
 [CONFIG_NET Rev. 22.0 Copyright (c) 1987, Prime Computer, Inc.]

Create, Edit, Quit, Save, Fast_Save, List, or Help? **CREATE**
 Enter nodes connected to RING1
 (NONE, <node names>): **A,D;**
 Enter nodes connected to RING2
 (NONE, <node names>):
 Enter nodes connected to LAN300-1
 (NONE, <node names>):
 Enter nodes connected to FDX1
 (NONE, <node names>): **A,C;**
 Enter nodes connected to FDX2
 (NONE, <node names>):
 Enter nodes connected to HDX
 (NONE, <node names>): **A,B;**
 Enter packet switching data network names
 (NONE, <PSDN names>): **TELENET;**
 Enter nodes connected to TELENET
 (NONE, <node names>): **A,E;**
 Enter gateway nodes
 (NONE, <node names>): **A;**
 Enter nodes running old (pre-rev-19.3) PRIMOS
 (NONE, <node names>):
 Enter nodes running non-Primenet X.25 software
 (NONE, <node names>):

(42) Describe Node A
 Ring node ID for A on RING1 (1, <1-247>): **1**
 Access rights from A via RING1
 (NONE, RFA, RLOG, IPCF, ALL): **ALL;**
 Force user validation(NO, YES)? **YES**
 Enter nodes accessible from A via RING1 with this access
 (NONE, ALL, <node names>, <network names>): **D;**
 Access rights from A via RING1
 (NONE, RFA, RLOG, IPCF, ALL):
 Node-node password between A and D
 (NONE, YES, <password>): **YES**
 Generated password is EKQORQ

(43) Synchronous line number on A for FDX1
 (UNKNOWN, <0-7>): **0**
 Protocol for line FDX1
 (LAPB, LAP):
 Framing for full duplex line FDX1
 (HDL, BSC-ASCII, BSC-EBCDIC):
 Access rights from A via FDX1
 (NONE, RFA, RLOG, IPCF, ALL): **RFA;**
 Force user validation(NO, YES)? **YES**
 Enter nodes accessible from A via FDX1 with this access
 (NONE, ALL, <node names>, <network names>): **C;**
 Access rights from A via FDX1
 (NONE, RFA, RLOG, IPCF, ALL):
 Node-node password between A and C
 (NONE, YES, <password>): **YES**
 Generated password is FNDLBQ

Dialog Notes

*Figure 7-9. General Network Example*

④② Define A's ring connection.

④③ Define A's FDX connection.

```

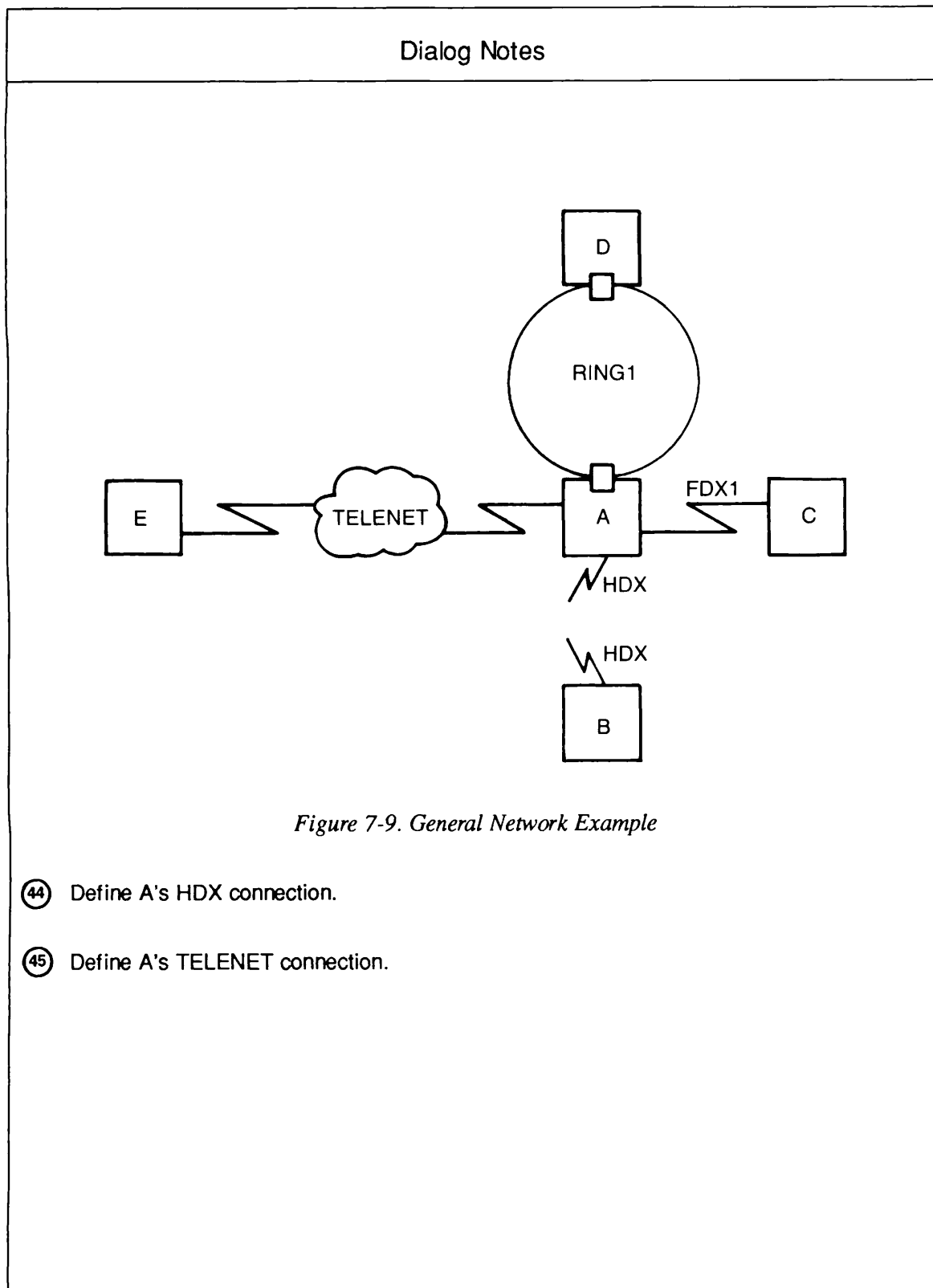
(44) { Synchronous line numbers for connections to the half duplex network
      (UNKNOWN, <0-7>): 2;
      Access rights from A via HDX
      (NONE, RFA, RLOG, IPCF, ALL): IPCF;
      Force user validation(NO, YES)? YES
      Enter nodes accessible from A via HDX with this access
      (NONE, ALL, <node names>, <network names>): B;
      Access rights from A via HDX
      (NONE, RFA, RLOG, IPCF, ALL):
      A's incoming HDX password from B
      (NONE, YES, <password>): YES
      Generated password is GCLGXT
      A's outgoing HDX password to B
      (NONE, YES, <password>): YES
      Generated password is GORZZA
      Node-node password between A and B
      (NONE, YES, <password>): YES
      Generated password is GUZHFQ

      Enter TELENET addresses for A
      (NONE, <TELENET addresses>): 311055599999;
      Synchronous line numbers for TELENET address 311055599999
      (UNKNOWN, <0-7>): 1;
      Protocol for line SMLC01 to TELENET
      (LAPB, LAP):
      Framing for line SMLC01 to TELENET
      (HDLC, BSC-ASCII, BSC-EBCDIC):
      Highest logical channel number for VCs on line SMLC01 to TELENET
      (4095, <1-4095>): 4095
      Default window size for line SMLC01 to TELENET
      (2, <1-7>):
(45) { Default packet size (in bytes) for line SMLC01 to TELENET
      (256, <16-256>): 128;
      Access rights from A via TELENET
      (NONE, RFA, RLOG, IPCF, ALL): IPCF;
      Force user validation(NO, YES)?
      Enter nodes accessible from A via TELENET with this access
      (NONE, ALL, <node names>, <network names>): E;
      Access rights from A via TELENET
      (NONE, RFA, RLOG, IPCF, ALL):
      Node-node password between A and E
      (NONE, YES, <password>):
      Indirect TELENET address for node A
      (NONE, <TELENET addresses>):

      Gateway access from A
      (NONE, RFA, RLOG, IPCF, ALL):

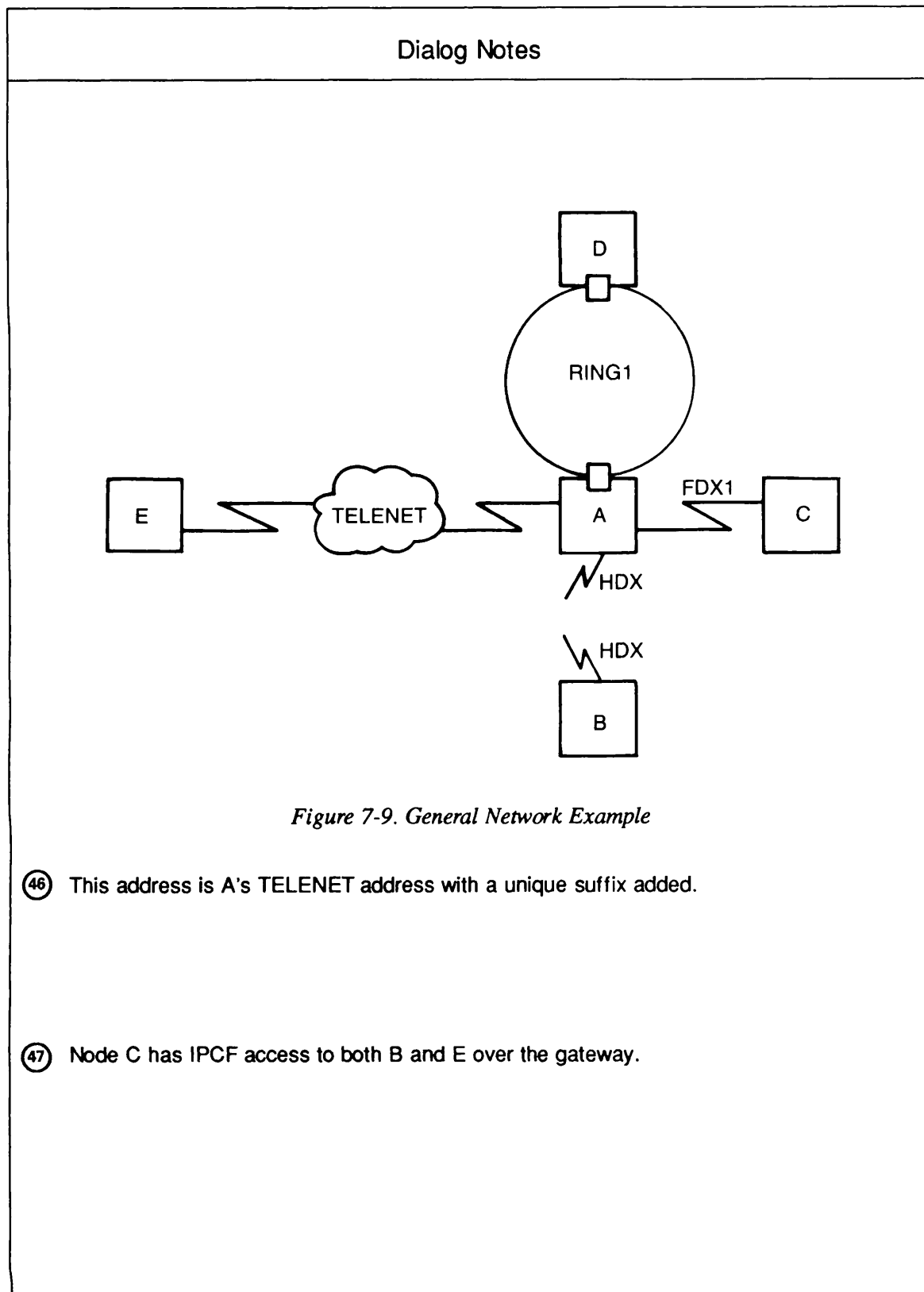
      Describe Node D
      Ring node ID for D on RING1 (2, <1-247>): 2;
      Access rights from D via RING1
      (NONE, RFA, RLOG, IPCF, ALL): ALL;
      Force user validation(NO, YES)? YES
      Enter nodes accessible from D via RING1 with this access
      (NONE, ALL, <node names>, <network names>): A;
      Access rights from D via RING1
      (NONE, RFA, RLOG, IPCF, ALL):

```



Indirect TELENET address for node D
 (46) (NONE, <TELENET addresses>): **31105559999901;**
 Gateway node which will route address 31105559999901 from TELENET
 to node D
 (NONE, <node names>): **A;**
 Lines on node A for routing TELENET address 31105559999901
 for node D
 (UNKNOWN, <0-7>): **1;**
 Gateway access from D
 (NONE, RFA, RLOG, IPCF, ALL): **IPCF;**
 Force user validation(NO, YES)?
 Enter nodes accessible from D via gateway with this access
 (NONE, ALL, <node names>, <network names>): **B;**
 Gateway access from D
 (NONE, RFA, RLOG, IPCF, ALL): **RLOG;**
 Force user validation(NO, YES)?
 Enter nodes accessible from D via gateway with this access
 (NONE, ALL, <node names>, <network names>): **C;**
 Gateway access from D
 (NONE, RFA, RLOG, IPCF, ALL):
 Node-node password between D and B
 (NONE, YES, <password>):
 Node-node password between D and C
 (NONE, YES, <password>):

 Describe Node C
 Synchronous line number on C for FDX1
 (UNKNOWN, <0-7>): **0;**
 Access rights from C via FDX1
 (NONE, RFA, RLOG, IPCF, ALL): **RFA;**
 Force user validation(NO, YES)? **YES**
 Enter nodes accessible from C via FDX1 with this access
 (NONE, ALL, <node names>, <network names>): **A;**
 Access rights from C via FDX1
 (NONE, RFA, RLOG, IPCF, ALL):
 Indirect TELENET address for node C
 (NONE, <TELENET addresses>): **31105559999902;**
 Gateway node which will route address 31105559999902 from TELENET
 to node C
 (NONE, <node names>): **A;**
 Lines on node A for routing TELENET address 31105559999902
 for node C
 (UNKNOWN, <0-7>): **1;**
 Gateway access from C
 (NONE, RFA, RLOG, IPCF, ALL): **IPCF;**
 Force user validation(NO, YES)?
 Enter nodes accessible from C via gateway with this access
 (NONE, ALL, <node names>, <network names>): **B,E;**
 Gateway access from C
 (NONE, RFA, RLOG, IPCF, ALL): **RLOG;**
 Force user validation(NO, YES)?
 Enter nodes accessible from C via gateway with this access
 (NONE, ALL, <node names>, <network names>): **D;**
 Gateway access from C
 (NONE, RFA, RLOG, IPCF, ALL):



Node-node password between C and B
 (NONE, YES, <password>):
 Node-node password between C and E
 (NONE, YES, <password>):

Describe Node B
 Synchronous line numbers for connections to the half duplex network
 (UNKNOWN, <0-7>): **0;**
 Access rights from B via HDX
 (NONE, RFA, RLOG, IPCF, ALL): **RLOG;**
 Force user validation(NO, YES)? **YES**
 Enter nodes accessible from B via HDX with this access
 (NONE, ALL, <node names>, <network names>): **A;**
 Access rights from B via HDX
 (NONE, RFA, RLOG, IPCF, ALL):
 Indirect TELENET address for node B
 (NONE, <TELENET addresses>): **31105559999903;**
 Gateway route which will route address 31105559999903 from TELENET
 to node B
 (NONE, <node names>): **A;**
 Lines on node A for routing TELENET address 31105559999903
 for node B
 (UNKNOWN, <0-7>): **1;**

(48)

Gateway access from B
 (NONE, RFA, RLOG, IPCF, ALL): **IPCF;**
 Force user validation(NO, YES)?
 Enter nodes accessible from B via gateway with this access
 (NONE, ALL, <node names>, <network names>): **D,E;**
 Gateway access from B
 (NONE, RFA, RLOG, IPCF, ALL): **RLOG;**
 Force user validation(NO, YES)?
 Enter nodes accessible from B via gateway with this access
 (NONE, ALL, <node names>, <network names>): **C;**
 Gateway access from B
 (NONE, RFA, RLOG, IPCF, ALL):
 Node-node password between B and E
 (NONE, YES, <password>):

Describe Node E
 Enter TELENET addresses for E
 (NONE, <TELENET addresses>): **311055588888;**
 Synchronous line numbers for TELENET address 311055588888
 (UNKNOWN, <0-7>):
 Access rights from E via TELENET
 (NONE, RFA, RLOG, IPCF, ALL):
 Indirect TELENET address for node E
 (NONE, <TELENET addresses>):
 Gateway access from E
 (NONE, RFA, RLOG, IPCF, ALL):
 All required configuration data has been supplied.

Create, Edit, Quit, Save, Fast_Save, List, or Help?

Dialog Notes

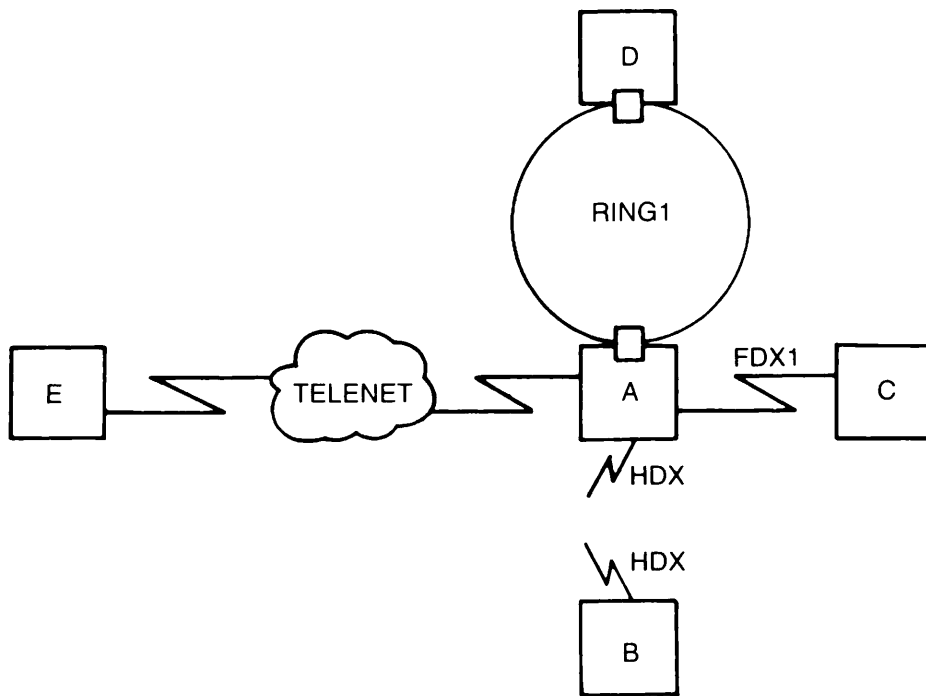


Figure 7-9. General Network Example

- ④ Node B has IPCF gateway access to D and E, and RLOG gateway access to C.

Example 9: LAN300 and Non-Prime Nodes

Figure 7-10 is a sketch of the network that was used as an example in Chapter 5, Preparing to Configure Your PRIMENET Network. This network has a LAN300, a full-duplex line, two non-Prime nodes, NP1 and NP2, and two Prime nodes, P1 and P2. Node P2 is a gateway node that routes data between the following pairs of indirectly connected nodes:

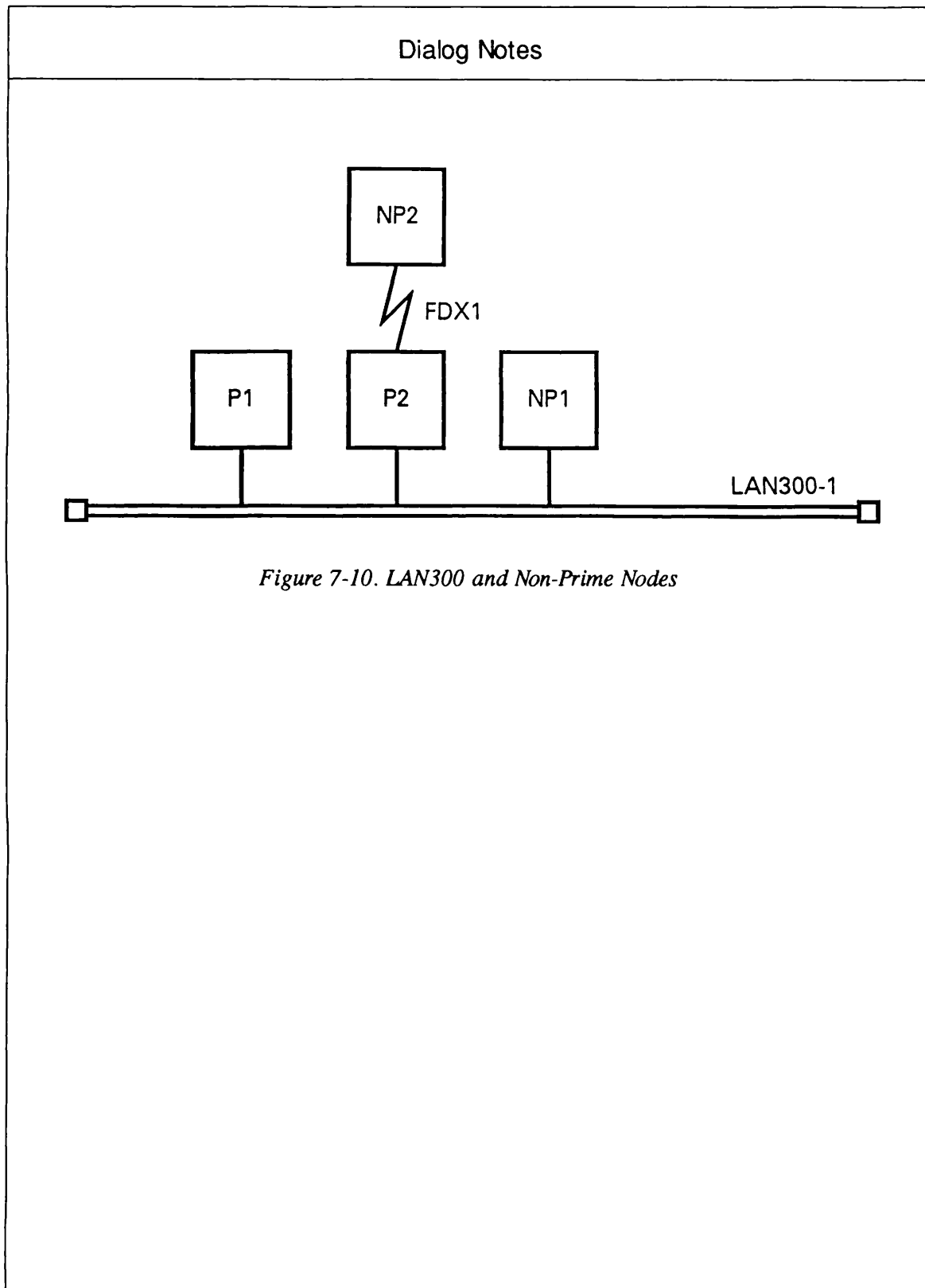
- P1 and NP2
- NP1 and NP2

Note that NP2 needs an indirect FDX address for NP1 in order to call it through gateway node P2. Likewise, P1 needs an indirect LAN300 address for NP2 in order to call it through gateway node P2.

This list indicates the access rights enabled in this network: IPCF access is explicitly granted between these pairs of nodes: P1 to NP1, P1 to NP2, P2 to NP1, P2 to NP2, NP1 to NP2, NP2 to P1, and NP2 to NP1. Since IPCF access is symmetric (automatically granted in the reverse direction), IPCF access is automatically granted between all the nodes in the network.

<i>Nodes</i>	<i>Link Type</i>	<i>Access</i>		
P1 to P2	via LAN300-1	ALL	FUV	N-NP
P1 to NP1	via LAN300-1	IPCF		
P1 to NP2	via gateway	IPCF		
P2 to P1	via LAN300-1	ALL		
P2 to NP1	via LAN300-1	IPCF		
P2 to NP2	via FDX1	IPCF		
NP1 to P1	via LAN300-1	NONE		
NP1 to P2	via LAN300-1	NONE		
NP1 to NP2	via gateway	IPCF		
NP2 to P1	via gateway	RLOG		
NP2 to P2	via FDX	NONE		
NP2 to NP1	via gateway	IPCF		

The CONFIG_NET dialog for this network is shown in Figure 7-33.



OK, CONFIG_NET

[CONFIG_NET Rev. 22.0 Copyright (c) 1987, Prime Computer, Inc.]

Create, Edit, Quit, Save, Fast_Save, List, or Help? **CREATE**

Enter nodes connected to RING1

(NONE, <node names>):

(49) { Enter nodes connected to LAN300-1
(NONE, <node names>): **P1,P2,NP1;**
Enter nodes connected to LAN300-2
(NONE, <node names>):
Enter nodes connected to FDX1
(NONE, <node names>): **P2,NP2;**
Enter nodes connected to FDX2
(NONE, <node names>):
Enter nodes connected to HDX
(NONE, <node names>):
Enter packet switching data network names
(NONE, <PSDN names>):

(50) { Enter gateway nodes
(NONE, <node names>): **P2;**
Enter nodes running old (pre-rev-19.3) PRIMOS
(NONE, <node names>):

(51) { Enter nodes running non-Primenet X.25 software
(NONE, <node names>): **NP1,NP2;**

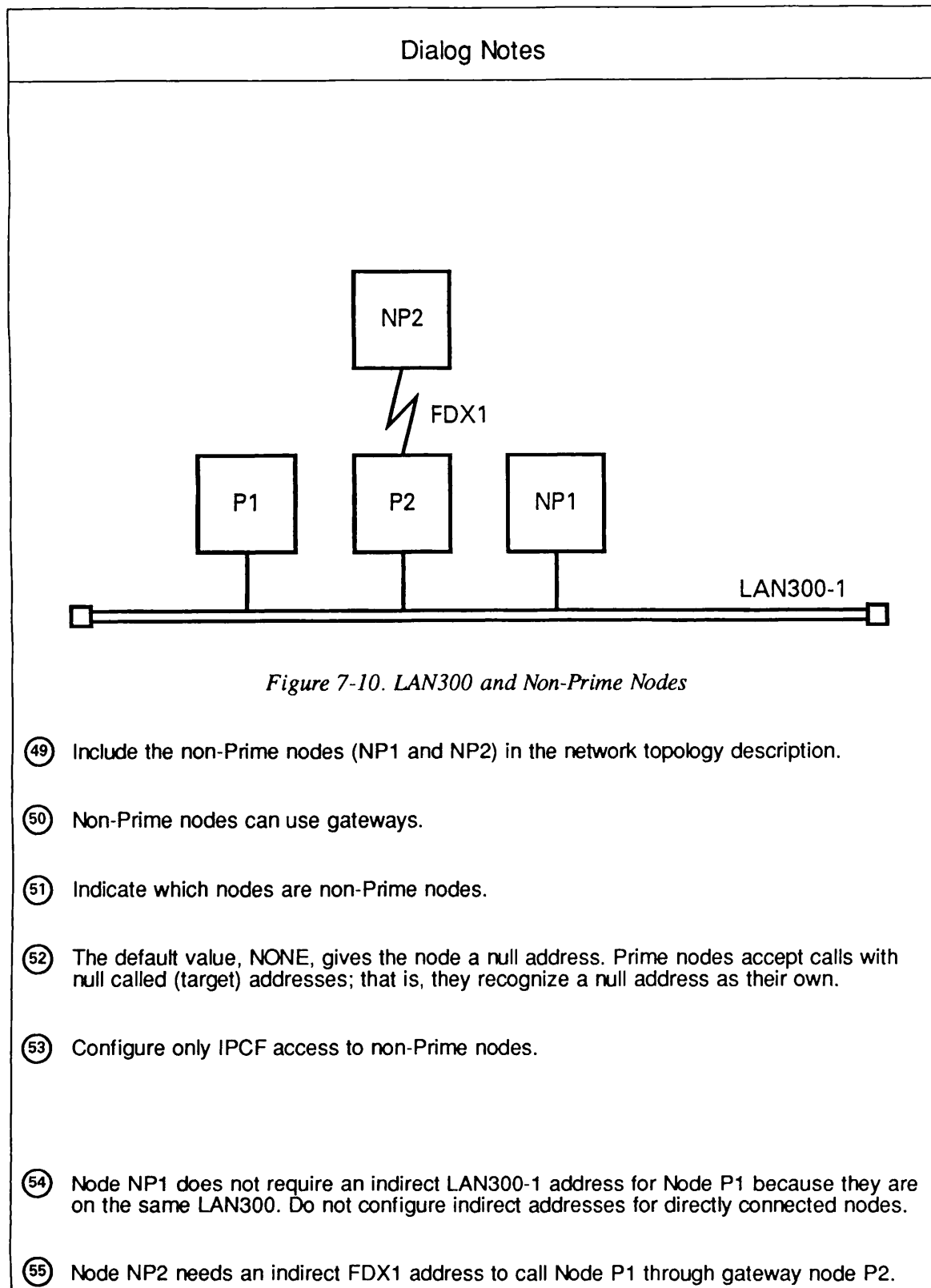
Describe Node P1

(52) { Enter LAN300-1 addresses for P1
(NONE, <LAN300-1 addresses>):
LHC logical device number for Primenet support for P1 on LAN300-1
(UNKNOWN, <0-7>): **0**
Access rights from P1 via LAN300-1
(NONE, RFA, RLOG, IPCF, ALL): **ALL**
Force user validation(NO, YES)? **NO**
Enter nodes accessible from P1 via LAN300-1 with this access
(NONE, ALL, <node names>, <network names>): **P2;**

(53) { Access rights from P1 via LAN300-1
(NONE, RFA, RLOG, IPCF, ALL): **IPCF;**
Force user validation(NO, YES)?
Enter nodes accessible from P1 via LAN300-1 with this access
(NONE, ALL, <node names>, <network names>): **NP1;**
Access rights from P1 via LAN300-1
(NONE, RFA, RLOG, IPCF, ALL):
Node-node password between P1 and P2
(NONE, YES, <password>): **YES**
Generated password is MZDGHR
Node-node password between P1 and NP1
(NONE, YES, <password>): **NO**

(54) { Indirect LAN300-1 address for node P1
(NONE, <LAN300-1 addresses>): **NONE**

(55) { Indirect FDX1 address for node P1
(NONE, <FDX1 addresses>): **999800000001;**

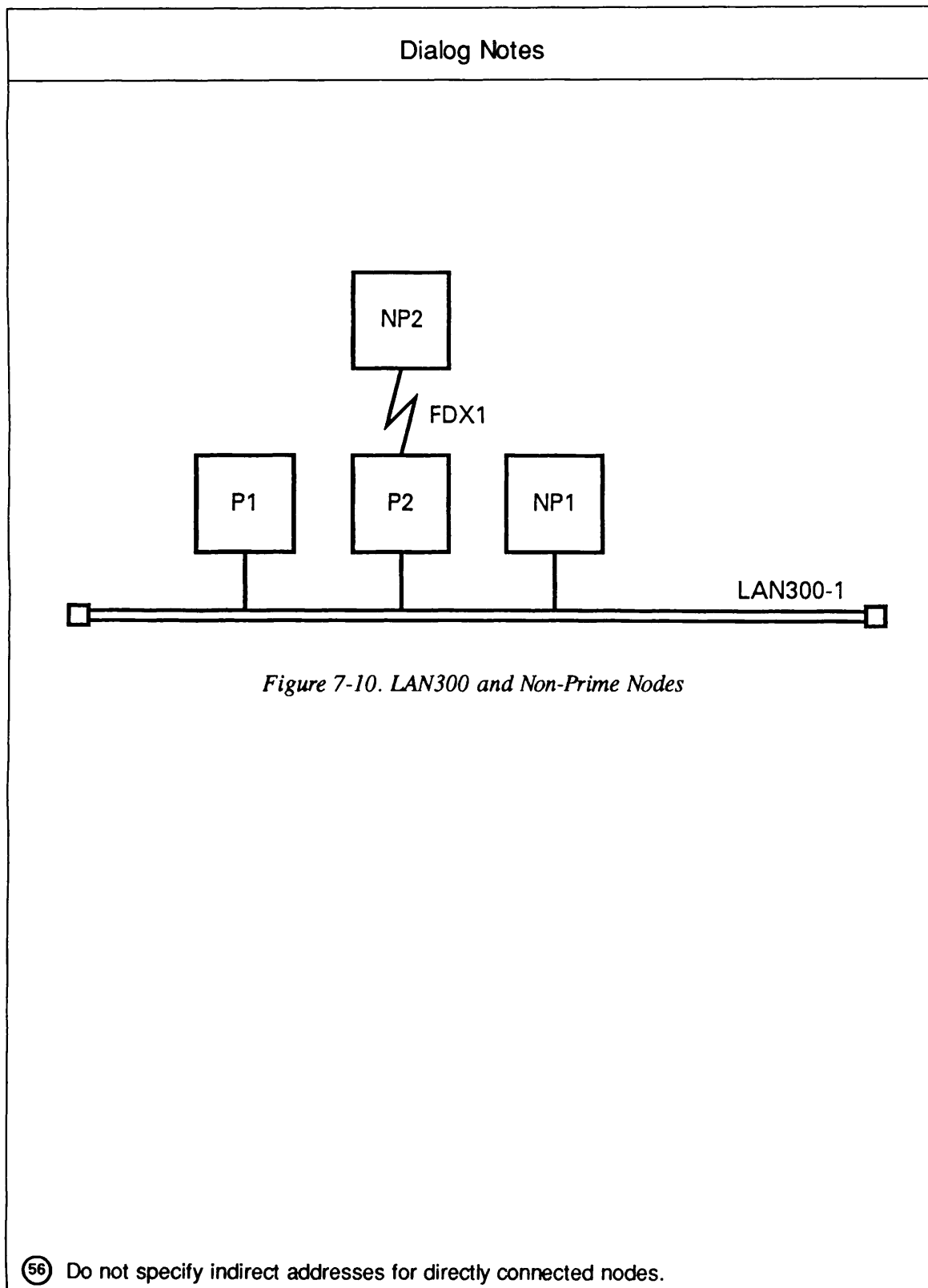



```

Gateway node which will route address 999800000001 from FDX1
to node P1
(NONE, <node names>): P2;
Lines on node P2 for routing FDX1 address 999800000001
for node P1
(UNKNOWN, <0-7>): 0
Gateway access from P1
(NONE, RFA, RLOG, IPCF, ALL): IPCF;
Force user validation(NO, YES)?
Enter nodes accessible from P1 via gateway with this access
(NONE, ALL, <node names>, <network names>): NP2;
Gateway access from P1
(NONE, RFA, RLOG, IPCF, ALL):
Node-node password between P1 and NP2
(NONE, YES, <password>):

Describe Node P2
Enter LAN300-1 addresses for P2
(NONE, <LAN300-1 addresses>):
LHC logical device number for Primenet support for P2 on LAN300-1
(UNKNOWN, <0-7>): 0
Access rights from P2 via LAN300-1
(NONE, RFA, RLOG, IPCF, ALL): ALL;
Force user validation(NO, YES)?
Enter nodes accessible from P2 via LAN300-1 with this access
(NONE, ALL, <node names>, <network names>): P1;
Access rights from P2 via LAN300-1
(NONE, RFA, RLOG, IPCF, ALL): IPCF;
Force user validation(NO, YES)?
Enter nodes accessible from P2 via LAN300-1 with this access
(NONE, ALL, <node names>, <network names>): NP1;
Access rights from P2 via LAN300-1
(NONE, RFA, RLOG, IPCF, ALL):
Node-node password between P2 and NP1
(NONE, YES, <password>):
Indirect LAN300-1 address for node P2
(NONE, <LAN300-1 addresses>):
Enter FDX1 addresses for P2
(NONE, <FDX1 addresses>):
Protocol for line FDX1
(LAPB, LAP):
Framing for full duplex line FDX1
(HDLC, BSC-ASCII, BSC-EBCDIC):
Access rights from P2 via FDX1
(NONE, RFA, RLOG, IPCF, ALL): IPCF;
Force user validation(NO, YES)?
Enter nodes accessible from P2 via FDX1 with this access
(NONE, ALL, <node names>, <network names>): NP2;
Access rights from P2 via FDX1
(NONE, RFA, RLOG, IPCF, ALL):
Node-node password between P2 and NP2
(NONE, YES, <password>):
(56) { Indirect FDX1 address for node P2
      { (NONE, <FDX1 addresses>):
        Gateway access from P2
        (NONE, RFA, RLOG, IPCF, ALL):

```

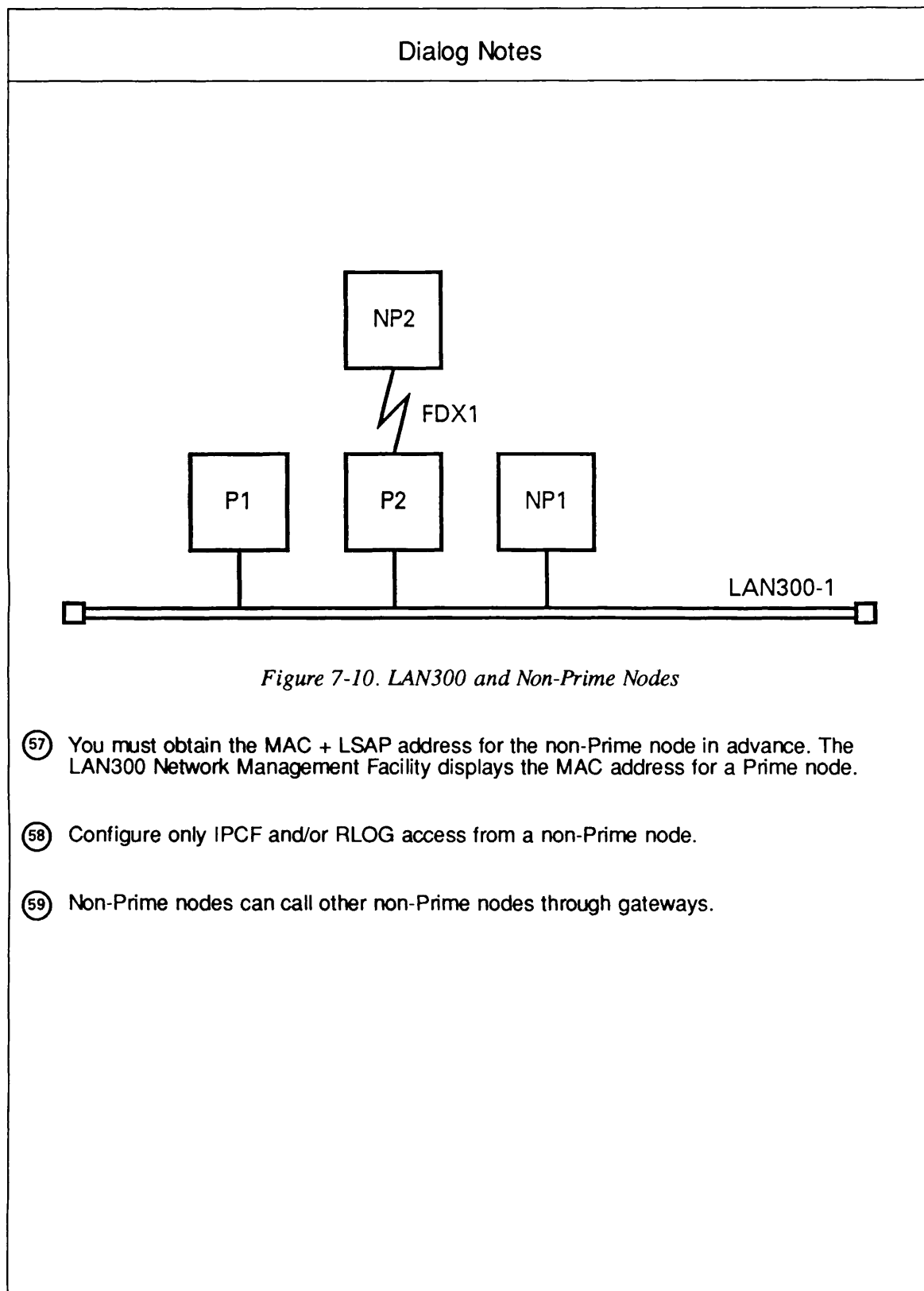


```

Describe Node NP1
Enter LAN300-1 addresses for NP1
(NONE, <LAN300-1 addresses>, NULL): 7777777777777777;
LHC logical device number for Primenet support for NP1 on LAN300-1
(UNKNOWN, <0-7>):
(57) MAC (+ LSAP) address for node NP1 on LAN300-1: 08-00-2F-44-55-66
Highest logical channel number for VCs on line .UNKNOWN to LAN300-1
(4095, <1-4095>):
Default window size for line .UNKNOWN to LAN300-1
(2, <1-7>): 7
Default packet size (in bytes) for line .UNKNOWN to LAN300-1
(512, <16-512>):
Determine DTE/DCE for node NP1 on LAN300-1 .UNKNOWN
(DYNAMIC, DTE, DCE):
Does node NP1 on LAN300-1 .UNKNOWN use ISO 8881 procedures
(NO, YES): YES
(58) Access rights from NP1 via LAN300-1
(NONE, RFA, RLOG, IPCF, ALL): RLOG;
Force user validation(NO, YES)?
Enter nodes accessible from NP1 via LAN300-1 with this access
(NONE, ALL, <node names>, <network names>): P1,P2;
Access rights from NP1 via LAN300-1
(NONE, RFA, RLOG, IPCF, ALL):
Indirect LAN300-1 address for node NP1
(NONE, <LAN300-1 addresses>):
Indirect FDX1 address for node NP1
(NONE, <FDX1 addresses>): 999800000002;
Gateway node which will route address 999800000002 from FDX1
to node NP1
(NONE, <node names>): P2;
(59) { Gateway access from NP1
      (NONE, RFA, RLOG, IPCF, ALL): IPCF;
      Force user validation(NO, YES)?
      Enter nodes accessible from NP1 via gateway with this access
      (NONE, ALL, <node names>, <network names>): NP2;
      Gateway access from NP1
      (NONE, RFA, RLOG, IPCF, ALL):
      Node-node password between NP1 and NP2
      (NONE, YES, <password>):

Describe Node NP2
Indirect LAN300-1 address for node NP2
(NONE, <LAN300-1 addresses>): 9998000000012;
Gateway node which will route address 9998000000012 from LAN300-1
to node NP2
(NONE, <node names>): P2;
Enter FDX1 addresses for NP2
(NONE, <FDX1 addresses>, NULL): 6666666666666666;
Synchronous line number on NP2 for FDX1
(UNKNOWN, <0-7>):
LAP(B) address for node NP2 on FDX1 (3, 1): 1
Highest logical channel number for VCs on line .UNKNOWN to FDX1
(4095, <1-4095>):
Default window size for line .UNKNOWN to FDX1
(2, <1-7>): 7

```



Default packet size (in bytes) for line .UNKNOWN to FDX1
(256, <16-256>): **128**
Determine DTE/DCE for node NP2 on FDX1 .UNKNOWN
(DYNAMIC,DTE,DCE): **DCE**
Does node NP2 on FDX1 .UNKNOWN use ISO 8881 procedures
(NO, YES): **NO**
Access rights from NP2 via FDX1
(NONE, RFA, RLOG, IPCF, ALL): **RLOG;**
Force user validation(NO, YES)?
Enter nodes accessible from NP2 via FDX1 with this access
(NONE, ALL, <node names>, <network names>): **P2;**
Access rights from NP2 via FDX1
(NONE, RFA, RLOG, IPCF, ALL):
Indirect FDX1 address for node NP2
(NONE, <FDX1 addresses>):
Gateway access from NP2
(NONE, RFA, RLOG, IPCF, ALL): **IPCF;**
Force user validation(NO, YES)?
Enter nodes accessible from NP2 via gateway with this access
(NONE, ALL, <node names>, <network names>): **NP1;**
Gateway access from NP2
(NONE, RFA, RLOG, IPCF, ALL):
All required configuration data has been supplied.

Create, Edit, Quit, Save, Fast_Save, List, or Help?

Dialog Notes

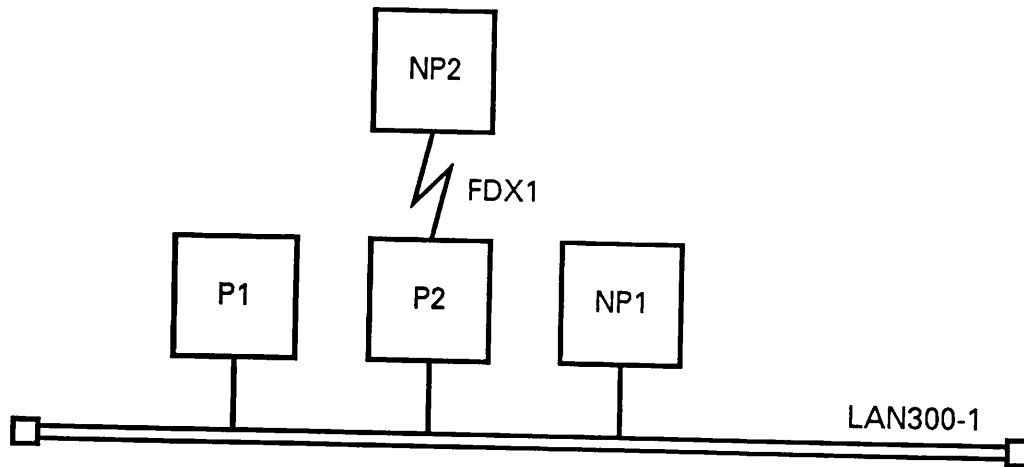


Figure 7-10. LAN300 and Non-Prime Nodes

Edit Mode Examples

This section contains examples of adding, modifying, and deleting portions of network configurations. The seven examples included here show how to:

- Add a ring to an existing network, connecting it by means of a full-duplex line
- Add a new node to a half-duplex subnetwork
- Change access rights between two existing nodes
- Change the characteristics of a full-duplex line to a PSDN
- Delete a node from a network
- Disable DSS interrupts for a full-duplex line
- Add a non-Prime node to a LAN300.

The examples in this section use the networks configured in the Create mode examples, earlier in this chapter. As in that section, portions of the dialog that require special attention are numbered. For comments on the numbered portions of dialog, refer to the Dialog Notes on the opposite pages.

Example 1: Adding a Ring and a Full-duplex Line

In this example, the network shown in Figure 7-1 is edited. A new ring, RING2, is added. RING2 has two nodes, C and D. Node C is connected to Node B by a new full-duplex line, FDX1. The result is shown in Figure 7-11.

This example illustrates the strategy of having Create mode do most of the work. The Administrator uses Edit mode only to add the objects RING2 and FDX1, then transfers to Create mode, where CONFIG_NET asks for all information needed for the new nodes.

```
OK, CONFIG_NET
[CONFIG_NET Rev. 22.0 Copyright (c) 1987, Prime Computer, Inc.]
```

```
Create, Edit, Quit, Save, Fast_Save, List, or Help? EDIT
```

```
Edit Mode
```

```
What would you like to edit?
```

- (0) HELP (for assistance)
- (1) NODE
- (2) RING
- (3) FDX (full duplex synchronous Prime-to-Prime links)
- (4) PSDN (packet switching data network)
- (5) HDX (half duplex network)
- (6) LAN300 (IEEE 802.3 Local Area Network)

Dialog Notes

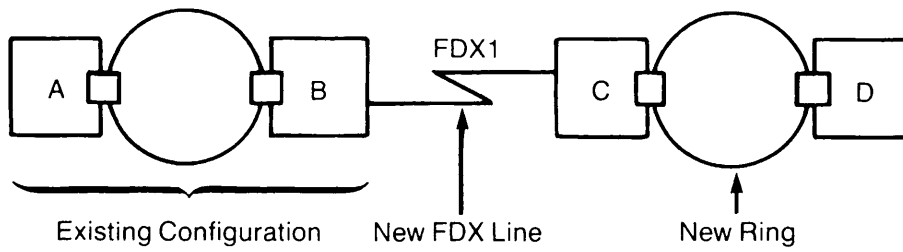


Figure 7-11. Adding a Ring and a Full-duplex Line

Enter carriage return to leave Edit mode

What would you like to edit: **2**

RING name

① (NONE, <RING name>): **RING2**

Unknown network has been added.

Edit Mode

What would you like to edit?

- (0) HELP (for assistance)
- (1) NODE
- (2) RING
- (3) FDX (full duplex synchronous Prime-to-Prime links)
- (4) PSDN (packet switching data network)
- (5) HDX (half duplex network)
- (6) LAN300 (IEEE 802.3 Local Area Network)

Enter carriage return to leave Edit mode

What would you like to edit: **3**

FDX name

② (NONE, <FDX name>): **FDX1**

Unknown network has been added.

Edit Mode

What would you like to edit?

- (0) HELP (for assistance)
- (1) NODE
- (2) RING
- (3) FDX (full duplex synchronous Prime-to-Prime links)
- (4) PSDN (packet switching data network)
- (5) HDX (half duplex network)
- (6) LAN300 (IEEE 802.3 Local Area Network)

Enter carriage return to leave Edit mode

What would you like to edit:

③ Create, Edit, Quit, Save, Fast_Save, List, or Help? **CREATE**

Enter nodes connected to RING2

(NONE, <node names>): **C,D;**

Enter nodes connected to FDX1

(NONE, <node names>): **C,B;**

Dialog Notes

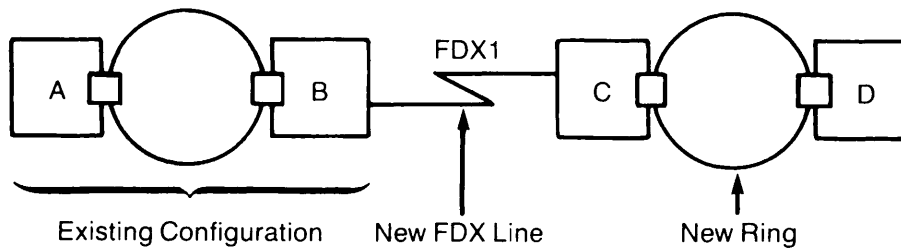


Figure 7-11. Adding a Ring and a Full-duplex Line

- ① Add the new ring.
- ② Add the new FDX line.
- ③ Transfer to Create mode.

- Describe Node B
- Synchronous line number on B for FDX1
(UNKNOWN, <0-7>): **0;**
- Protocol for line FDX1
(LAPB, LAP):
- Framing for full duplex line FDX1
(HDLC, BSC-ASCII, BSC-EBCDIC):
- ④ Access rights from B via FDX1
(NONE, RFA, RLOG, IPCF, ALL): **RLOG;**
- Force user validation(NO, YES)?
- Enter nodes accessible from B via FDX1 with this access
(NONE, ALL, <node names>, <network names>): **C;**
- Access rights from B via FDX1
(NONE, RFA, RLOG, IPCF, ALL):
- Node-node password between B and C
(NONE, YES, <password>):
- Describe Node C
- Ring node ID for C on RING2 (1, <1-247>):
- Access rights from C via RING2
(NONE, RFA, RLOG, IPCF, ALL): **RLOG;**
- Force user validation(NO, YES)?
- ⑤ Enter nodes accessible from C via RING2 with this access
(NONE, ALL, <node names>, <network names>): **ALL;**
- Access rights from C via RING2
(NONE, RFA, RLOG, IPCF, ALL):
- Node-node password between C and D
(NONE, YES, <password>):
- ⑥ Synchronous line number on C for FDX1
(UNKNOWN, <0-7>): **0;**
- Access rights from C via FDX1
(NONE, RFA, RLOG, IPCF, ALL): **RLOG;**
- Force user validation(NO, YES)?
- Enter nodes accessible from C via FDX1 with this access
(NONE, ALL, <node names>, <network names>): **B;**
- Access rights from C via FDX1
(NONE, RFA, RLOG, IPCF, ALL):
- Gateway access from C
(NONE, RFA, RLOG, IPCF, ALL):
- Describe Node D
- ⑦ Ring node ID for D on RING2 (2, <1-247>):
- Access rights from D via RING2
(NONE, RFA, RLOG, IPCF, ALL): **RLOG;**
- Force user validation(NO, YES)?
- Enter nodes accessible from D via RING2 with this access
(NONE, ALL, <node names>, <network names>): **ALL;**
- Access rights from D via RING2
(NONE, RFA, RLOG, IPCF, ALL):
- Gateway access from D
(NONE, RFA, RLOG, IPCF, ALL):
- All required configuration data has been supplied.

Create, Edit, Quit, Save, Fast_Save, List, or Help?

Dialog Notes

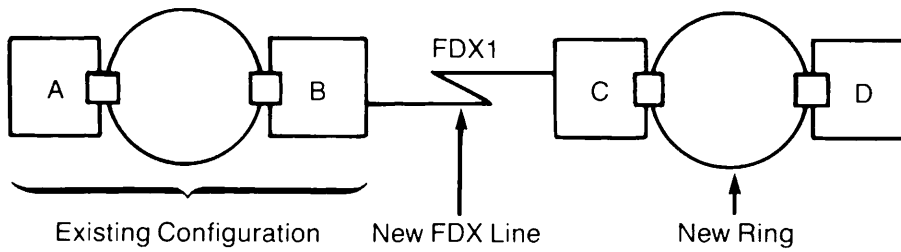


Figure 7-11. Adding a Ring and a Full-duplex Line

- ④ Add information about Node B's FDX1 connection.
- ⑤ Add information about Node C's RING2 connection.
- ⑥ Add information about Node C's FDX1 connection.
- ⑦ Add information about Node D's RING2 connection.

Example 2: Adding a Half-duplex Node

In this example, a new half-duplex node, F, is added to the network illustrated in Figure 7-3, resulting in the new configuration shown in Figure 7-12. Node F is given RLOG access to Node C, and Node C is given IPCF access to Node F. These changes are made in three steps:

1. From Edit mode, the half-duplex submenu is used to add the new node, F, to the half-duplex subnetwork and to the entire network at the same time.
2. The Administrator transfers to Create mode and answers questions about Node F, assigning Node F RLOG access to Node C.
3. The Administrator goes back into Edit mode to assign Node C IPCF access to Node F.

```
OK, CONFIG_NET
[CONFIG_NET Rev. 22.0 Copyright (c) 1987, Prime Computer, Inc.]
```

```
Create, Edit, Quit, Save, Fast_Save, List, or Help? EDIT
Edit Mode
What would you like to edit?
```

- (0) HELP (for assistance)
- (1) NODE
- (2) RING
- (3) FDX (full duplex synchronous Prime-to-Prime links)
- (4) PSDN (packet switching data network)
- (5) HDX (half duplex network)
- (6) LAN300 (IEEE 802.3 Local Area Network)

Enter carriage return to leave Edit mode

- ⑧ What would you like to edit: **5**
Edit Half Duplex Network

- (0) HELP (for assistance)
- (1) Delete the entire HDX network
- (2) Add a node to the HDX network
- (3) Remove a node from the HDX network
- (4) Change a synchronous line number
- (5) Add a synchronous line number
- (6) Delete a synchronous line number

Enter carriage return for the top level edit menu.

- ⑨ { Option: **2**
New node for HDX
(NONE, <node name>): **F**
F has been added to the HDX network

Dialog Notes

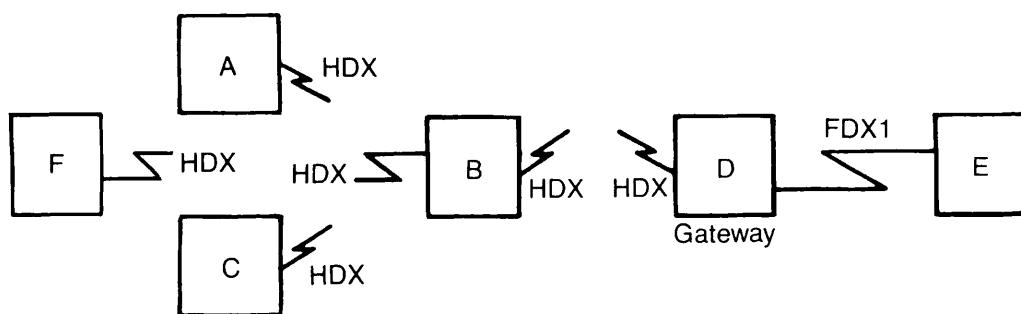


Figure 7-12. Adding a Half-duplex Node

⑧ Edit the HDX subnetwork.

⑨ Add the new HDX node.

Edit Half Duplex Network

- (0) HELP (for assistance)
- (1) Delete the entire HDX network
- (2) Add a node to the HDX network
- (3) Remove a node from the HDX network
- (4) Change a synchronous line number
- (5) Add a synchronous line number
- (6) Delete a synchronous line number

Enter carriage return for the top level edit menu.

- ⑩ { Option: **<CONTROL-P>**
 { Create, Edit, Quit, Save, Fast_Save, List, or Help? **CREATE**

Describe Node F

Synchronous line numbers for connections to the half duplex network
 (UNKNOWN, <0-7>): **0;**

- ⑪ { Access rights from F via HDX
 (NONE, RFA, RLOG, IPCF, ALL): **RLOG;**
 { Force user validation(NO, YES)?
 { Enter nodes accessible from F via HDX with this access
 (NONE, ALL, <node names>, <network names>): **C;**

Access rights from F via HDX
 (NONE, RFA, RLOG, IPCF, ALL):

- ⑫ { F's incoming HDX password from C
 (NONE, YES, <password>): **YES**
 { Generated password is MGSARJ
 { F's outgoing HDX password to C
 (NONE, YES, <password>): **YES**
 { Generated password is MERRIL

Gateway access from F

(NONE, RFA, RLOG, IPCF, ALL):

All required configuration data has been supplied.

- ⑬ Create, Edit, Quit, Save, Fast_Save, List, or Help? **EDIT**
 Edit Mode
 What would you like to edit?

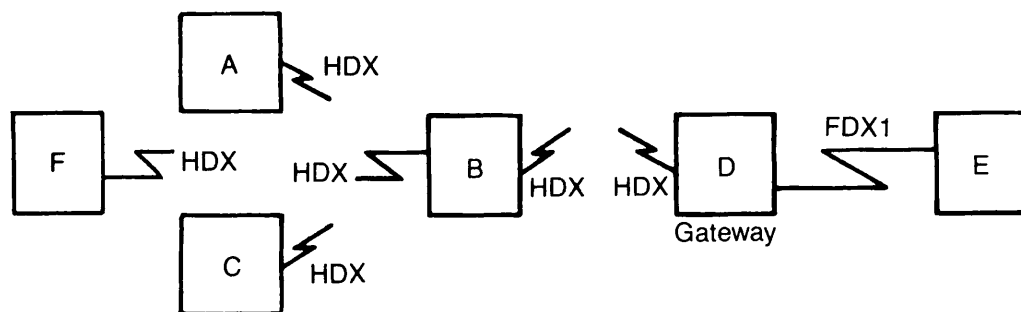
- (0) HELP (for assistance)
- (1) NODE
- (2) RING
- (3) FDX (full duplex synchronous Prime-to-Prime links)
- (4) PSDN (packet switching data network)
- (5) HDX (half duplex network)
- (6) LAN300 (IEEE 802.3 Local Area Network)

Enter carriage return to leave Edit mode

What would you like to edit: **1**

Node name (NONE, <node name>): **C**

Dialog Notes

*Figure 7-12. Adding a Half-duplex Node*

- ⑩ Transfer to Create mode.
- ⑪ Assign access from F to C.
- ⑫ Assign HDX passwords.
- ⑬ Return to Edit mode.

Edit Node C

Select a node editing option.

- (0) HELP (for assistance)
- (1) Delete this node
- (2) Change the name of this node
- (3) Modify this node's access information
- (4) Change node-node passwords for this node
- (5) Change HDX passwords for this node
- (6) Change this node's status as a gateway node
- (7) Add a network address for this node
- (8) Delete a network address for this node
- (9) Change a network address for this node
- (10) Change this node's rev. status
- (11) Change this node's compatibility address
- (12) Change a LAN300 Host Controller number for this node
- (13) Mark non-Prime node
- (14) Change non-Prime source address
- (15) Change maximum number of VCs for this node

Enter carriage return for the top level edit menu.

Option: 3

Modify access for which links on C

(NONE, <pnet name>): **HDX**

Modify Access for Node C over HDX

Select access changes.

- (0) HELP (for assistance)
- (1) No Access
- (2) IPCF access
- (3) No IPCF access
- (4) Remote File Access
- (5) No Remote File Access
- (6) Remote Log-Through Access
- (7) No Remote Log-Through Access
- (8) Forced User Validation
- (9) No Forced User Validation

(14) Enter a LIST of access modes.

Option: 2

Option:

Nodes to be given this access from C via HDX

(NONE, ALL, <node name>): **F**

(NONE, ALL, <node name>):

Nodes to be given this access to C via HDX

(NONE, ALL, <node name>):

Modify Access for Node C over HDX

Select access changes.

Dialog Notes

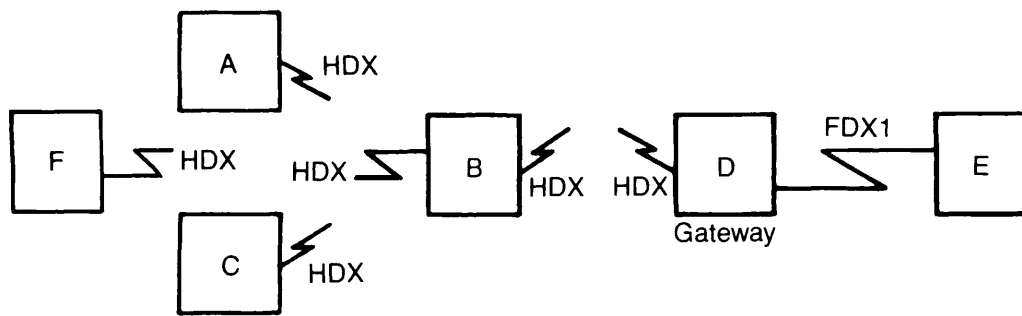


Figure 7-12. Adding a Half-duplex Node

- ⑭ Assign access from C to F.

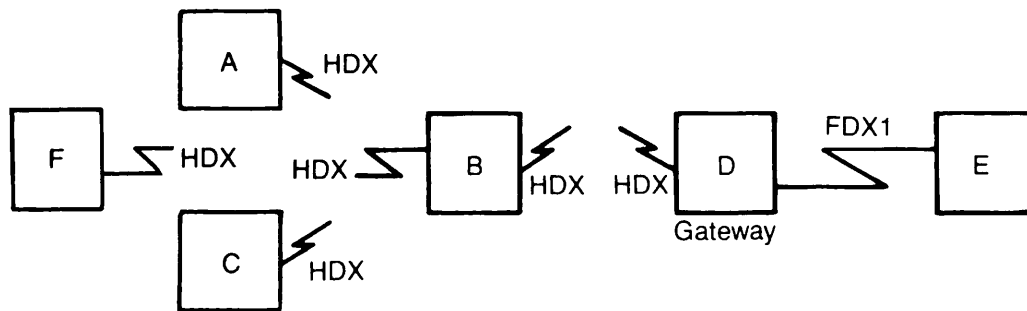
- (0) HELP (for assistance)
- (1) No Access
- (2) IPCF access
- (3) No IPCF access
- (4) Remote File Access
- (5) No Remote File Access
- (6) Remote Log-Through Access
- (7) No Remote Log-Through Access
- (8) Forced User Validation
- (9) No Forced User Validation

Enter a LIST of access modes.

Option: **<CONTROL-P>**

Create, Edit, Quit, Save, Fast_Save, List, or Help?

Dialog Notes

*Figure 7-12. Adding a Half-duplex Node*

Example 3: Changing Access Rights

In this example, the Administrator changes the access rights between Nodes A and C in the network in Figure 7-13. (This configuration is the same one that was created in Create mode Example 8, earlier in this chapter.) The nodes were originally configured with RFA access to one another; they are now assigned RLOG access instead.

```
OK, CONFIG_NET
[CONFIG_NET Rev. 22.0 Copyright (c) 1987, Prime Computer, Inc.]
```

```
Create, Edit, Quit, Save, Fast_Save, List, or Help? EDIT
Edit Mode
What would you like to edit?
```

- (0) HELP (for assistance)
- (1) NODE
- (2) RING
- (3) FDX (full duplex synchronous Prime-to-Prime links)
- (4) PSDN (packet switching data network)
- (5) HDX (half duplex network)
- (6) LAN300 (IEEE 802.3 Local Area Network)

```
Enter carriage return to leave Edit mode
```

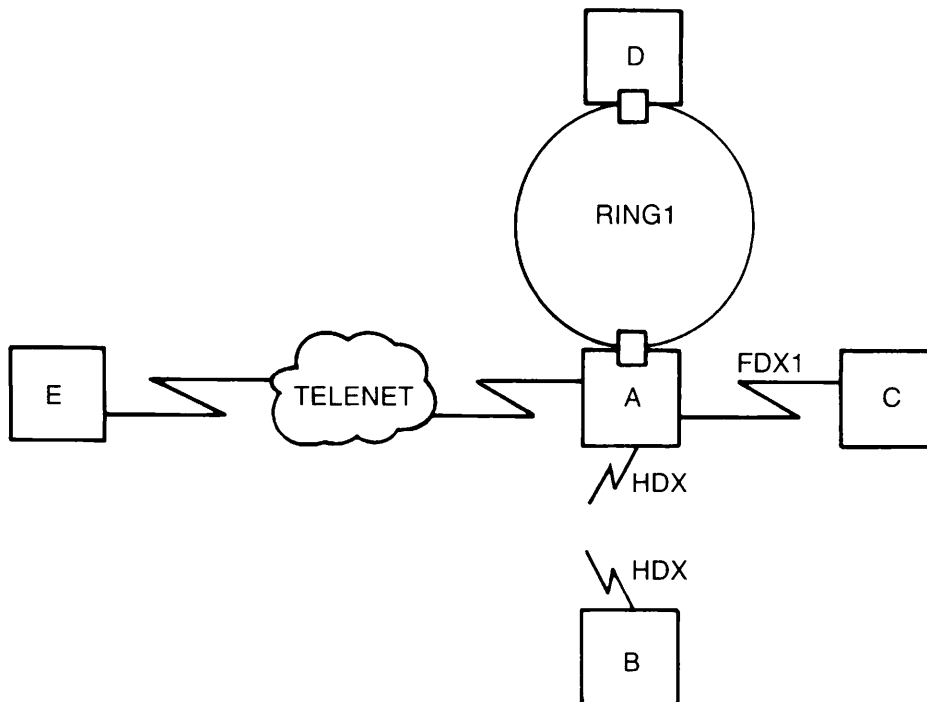
```
What would you like to edit: 1
(15) Node name (NONE, <node name>): A
Edit Node A
Select a node editing option.
```

- (0) HELP (for assistance)
- (1) Delete this node
- (2) Change the name of this node
- (3) Modify this node's access information
- (4) Change node-node passwords for this node
- (5) Change HDX passwords for this node
- (6) Change this node's status as a gateway node
- (7) Add a network address for this node
- (8) Delete a network address for this node
- (9) Change a network address for this node
- (10) Change this node's rev. status
- (11) Change this node's compatibility address
- (12) Change a LAN300 Host Controller number for this node
- (13) Mark non-Prime node
- (14) Change non-Prime source address
- (15) Change maximum number of VCs for this node

```
Enter carriage return for the top level edit menu.
```

```
(16) { Option: 3
      Modify access for which links on A
      (NONE, <pnet name>): FDX1
      Modify Access for Node A over FDX1
      Select access changes.
```

Dialog Notes

*Figure 7-13. General Network Example*

⑮ Edit Node A.

⑯ Edit Node A's access over FDX1.

- (0) HELP (for assistance)
- (1) No Access
- (2) IPCF access
- (3) No IPCF access
- (4) Remote File Access
- (5) No Remote File Access
- (6) Remote Log-Through Access
- (7) No Remote Log-Through Access
- (8) Forced User Validation
- (9) No Forced User Validation

Enter a LIST of access modes.

Option: 5

Option: 6

Option:

Nodes to be given this access from A via FDX1

(17) (NONE, ALL, <node name>): C;

Nodes to be given this access to A via FDX1

(18) (NONE, ALL, <node name>): C;

Modify Access for Node A over FDX1

Select access changes.

- (0) HELP (for assistance)
- (1) No Access
- (2) IPCF access
- (3) No IPCF access
- (4) Remote File Access
- (5) No Remote File Access
- (6) Remote Log-Through Access
- (7) No Remote Log-Through Access
- (8) Forced User Validation
- (9) No Forced User Validation

Enter a LIST of access modes.

Option: <CONTROL-P>

Create, Edit, Quit, Save, Fast_Save, List, or Help?

Dialog Notes

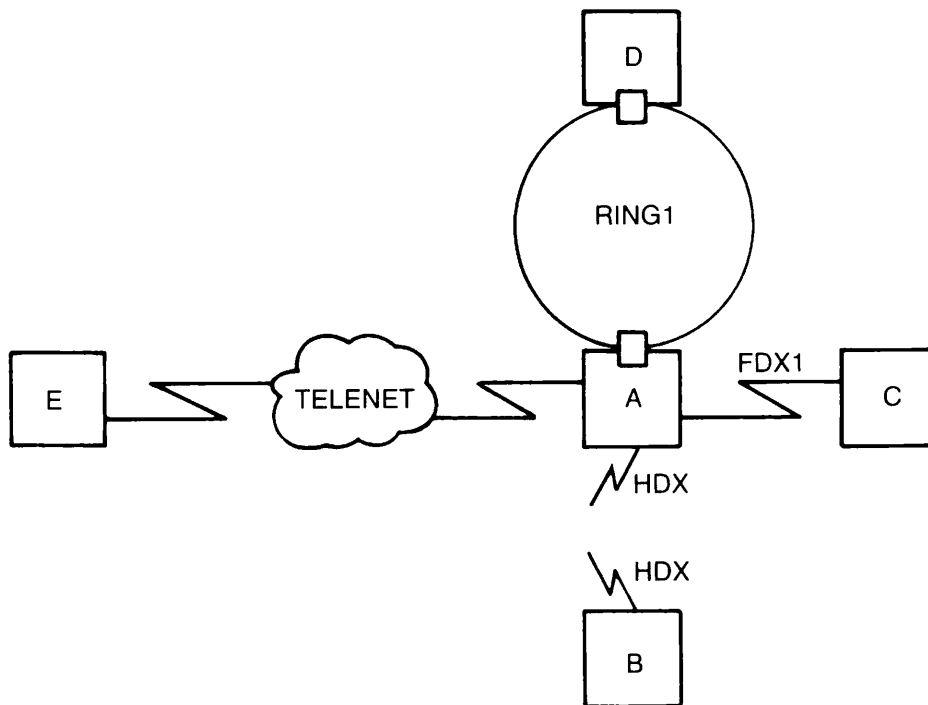


Figure 7-13. General Network Example

- ⑪ Change Node A's access to Node C.
- ⑫ Change Node C's access to Node A.

Example 4: Changing PSDN Line Characteristics

This example uses the configuration shown in Figure 7-14. (This configuration is the same one that was created in Create mode Example 5, earlier in this chapter.) The Administrator changes the logical line number and protocol of the line between Node SYSX and X.25. The logical line number is changed from 1 to 2, and the protocol from LAPB to LAP.

```
OK, CONFIG_NET
[CONFIG_NET Rev. 22.0 Copyright (c) 1987, Prime Computer, Inc.]
```

```
Create, Edit, Quit, Save, Fast_Save, List, or Help? EDIT
Edit Mode
What would you like to edit?
```

- (0) HELP (for assistance)
- (1) NODE
- (2) RING
- (3) FDX (full duplex synchronous Prime-to-Prime links)
- (4) PSDN (packet switching data network)
- (5) HDX (half duplex network)
- (6) LAN300 (IEEE 802.3 Local Area Network)

```
Enter carriage return to leave Edit mode
```

```
What would you like to edit: 4
```

```
PSDN name
```

```
(19) (NONE, <PSDN name>): X.25
```

```
Edit Packet Switching Data Network X.25
```

```
Select option.
```

- (0) HELP (for assistance)
- (1) Remove this PSDN from the configuration
- (2) Add a node to this PSDN
- (3) Remove a node from this PSDN
- (4) Add a line to this PSDN
- (5) Remove a line to this PSDN
- (6) Change synchronous line numbers
- (7) Set LAP or LAPB protocol
- (8) Set HDLC or Bisync framing
- (9) Enable/Disable DSS interrupts
- (10) Change highest LCN for a link to this PSDN
- (11) Change default packet size for a link to this PSDN
- (12) Change default window size for a link to this PSDN

```
Enter carriage return for the top level edit menu.
```

Dialog Notes

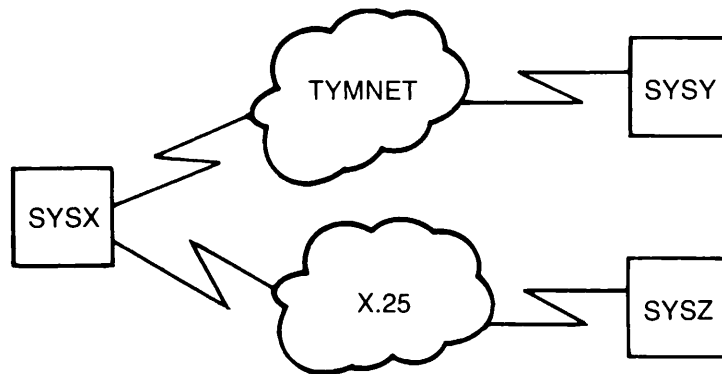


Figure 7-14. Multiple PSDN Connections

- ① Edit the X.25 PSDN.

- (20) { Option: 6
Node name (NONE, <node name>): **SYSX**
New line number
(NONE, <line number>): **2**
Edit Packet Switching Data Network X.25
Select option.
- (0) HELP (for assistance)
 - (1) Remove this PSDN from the configuration
 - (2) Add a node to this PSDN
 - (3) Remove a node from this PSDN
 - (4) Add a line to this PSDN
 - (5) Remove a line to this PSDN
 - (6) Change synchronous line numbers
 - (7) Set LAP or LAPB protocol
 - (8) Set HDLC or Bisync framing
 - (9) Enable/Disable DSS interrupts
 - (10) Change highest LCN for a link to this PSDN
 - (11) Change default packet size for a link to this PSDN
 - (12) Change default window size for a link to this PSDN

Enter carriage return for the top level edit menu.

- (21) { Option: 7
Node name (NONE, <node name>): **SYSX**
Protocol for line SMLC02 to X.25
(LAPB, LAP): **LAP**
Edit Packet Switching Data Network X.25
Select option.
- (0) HELP (for assistance)
 - (1) Remove this PSDN from the configuration
 - (2) Add a node to this PSDN
 - (3) Remove a node from this PSDN
 - (4) Add a line to this PSDN
 - (5) Remove a line to this PSDN
 - (6) Change synchronous line numbers
 - (7) Set LAP or LAPB protocol
 - (8) Set HDLC or Bisync framing
 - (9) Enable/Disable DSS interrupts
 - (10) Change highest LCN for a link to this PSDN
 - (11) Change default packet size for a link to this PSDN
 - (12) Change default window size for a link to this PSDN

Enter carriage return for the top level edit menu.

Option: **<CONTROL-P>**

Create, Edit, Quit, Save, Fast_Save, List, or Help?

Dialog Notes

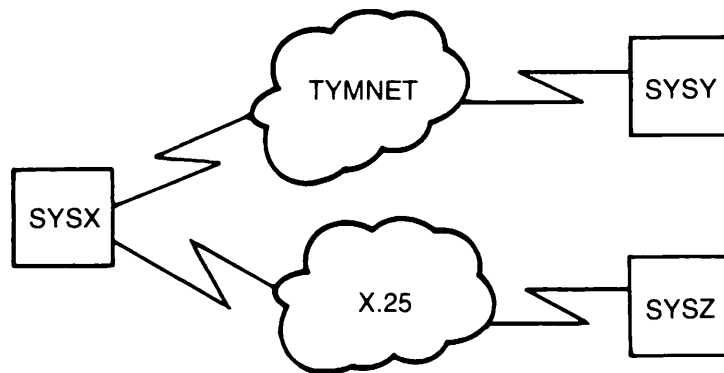


Figure 7-14. Multiple PSDN Connections

- ②① Change logical line number on SYSX.
- ②① Change framing of line from LAPB to LAP.

Example 5: Deleting a Node From a Network

In this example, the Administrator uses the Node submenu to delete Node A from the network illustrated in Figure 7-15. (This configuration is the same one that was created in Create mode Example 3, earlier in this chapter.) Note that the Administrator does not have to remove the access rights between Node A and Node B. When Node A is removed from the network, all access rights to and from A are automatically removed as well. The Administrator transfers to Create mode to ensure that no further information is required.

```
OK, CONFIG_NET
[CONFIG_NET Rev. 22.0 Copyright (c) 1987, Prime Computer, Inc.]
```

```
Create, Edit, Quit, Save, Fast_Save, List, or Help? EDIT
Edit Mode
What would you like to edit?
```

- (0) HELP (for assistance)
- (1) NODE
- (2) RING
- (3) FDX (full duplex synchronous Prime-to-Prime links)
- (4) PSDN (packet switching data network)
- (5) HDX (half duplex network)
- (6) LAN300 (IEEE 802.3 Local Area Network)

```
Enter carriage return to leave Edit mode
```

```
What would you like to edit: 1
Node name (NONE, <node name>): A
Edit Node A
Select a node editing option.
```

(22)

- (0) HELP (for assistance)
- (1) Delete this node
- (2) Change the name of this node
- (3) Modify this node's access information
- (4) Change node-node passwords for this node
- (5) Change HDX passwords for this node
- (6) Change this node's status as a gateway node
- (7) Add a network address for this node
- (8) Delete a network address for this node
- (9) Change a network address for this node
- (10) Change this node's rev. status
- (11) Change this node's compatibility address
- (12) Change a LAN300 Host Controller number for this node
- (13) Mark non-Prime node
- (14) Change non-Prime source address
- (15) Change maximum number of VCs for this node

```
Enter carriage return for the top level edit menu.
```

Dialog Notes

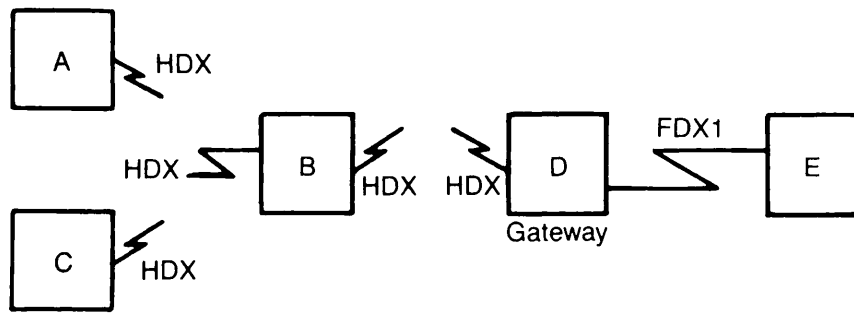


Figure 7-15. Half-duplex and Full-duplex Lines

② Edit Node A.

- ②③ Option: 1
Node deleted
Edit Mode
What would you like to edit?
- (0) HELP (for assistance)
 - (1) NODE
 - (2) RING
 - (3) FDX (full duplex synchronous Prime-to-Prime links)
 - (4) PSDN (packet switching data network)
 - (5) HDX (half duplex network)
 - (6) LAN300 (IEEE 802.3 Local Area Network)
- Enter carriage return to leave Edit mode
- ②④ { What would you like to edit: <CONTROL-P>
Create, Edit, Quit, Save, Fast_Save, List, or Help? **CREATE**
All required configuration data has been supplied.

Dialog Notes

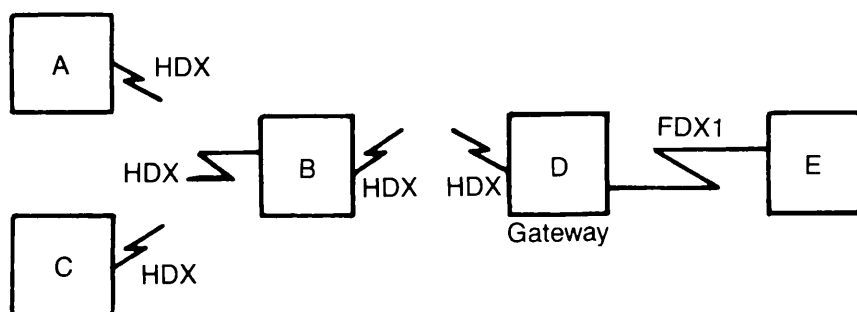


Figure 7-15. Half-duplex and Full-duplex Lines

②③ Delete Node A.

②④ Transfer to Create mode to ensure that no further configuration information is required.

Example 6: Disabling DSS Interrupts

This example shows how an Administrator could disable DSS (Data Set Status) interrupts at one end of a full-duplex line. The example uses the configuration shown in Figure 7-16. (This configuration is the same one that was used as Example 1 in Chapter 5, Preparing to Configure Your PRIMENET Network, and as Create mode Example 8, earlier in this chapter. DSS interrupts are disabled for FDX1 on Node C.

```
OK, CONFIG_NET
[CONFIG_NET Rev. 22.0 Copyright (c) 1987, Prime Computer, Inc.]
```

```
Create, Edit, Quit, Save, Fast_Save, List, or Help? EDIT
Edit Mode
What would you like to edit?
```

- (0) HELP (for assistance)
- (1) NODE
- (2) RING
- (3) FDX (full duplex synchronous Prime-to-Prime links)
- (4) PSDN (packet switching data network)
- (5) HDX (half duplex network)
- (6) LAN300 (IEEE 802.3 Local Area Network)

Enter carriage return to leave Edit mode

(25) What would you like to edit: **3**

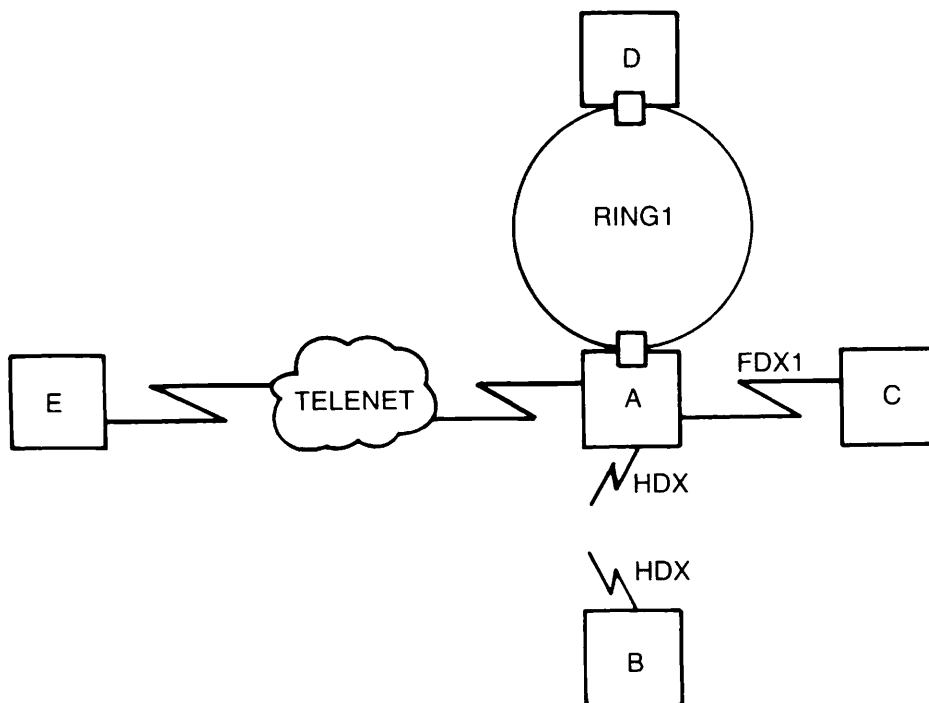
```
FDX name
(NONE, <FDX name>): FDX1
Edit Full Duplex Link FDX1
Select desired change.
```

- (0) HELP (for assistance)
- (1) Remove this link from the configuration
- (2) Change the name of this link
- (3) Add a node to this link
- (4) Remove a node from this link
- (5) Change synchronous line numbers
- (6) Set LAP or LAPB protocol
- (7) Set HDLC or Bisync framing
- (8) Enable/Disable DSS interrupts
- (9) Change LAP(B) address (non-Prime nodes)
- (10) Change highest LCN (non-Prime nodes)
- (11) Change default packet size (non-Prime nodes)
- (12) Change default window size (non-Prime nodes)
- (13) Change restart options (non-Prime nodes)

Enter carriage return for the top level edit menu.

```
(26) { Option: 8
      { Node name (NONE, <node name>): C
      { Enable Data Set Status interrupts (YES, NO): NO
      { Edit Full Duplex Link FDX1
      { Select desired change.
```

Dialog Notes

*Figure 7-16. General Network Example*

②⑤ Edit line FDX1.

②⑥ Disable DSS interrupts for Node C.

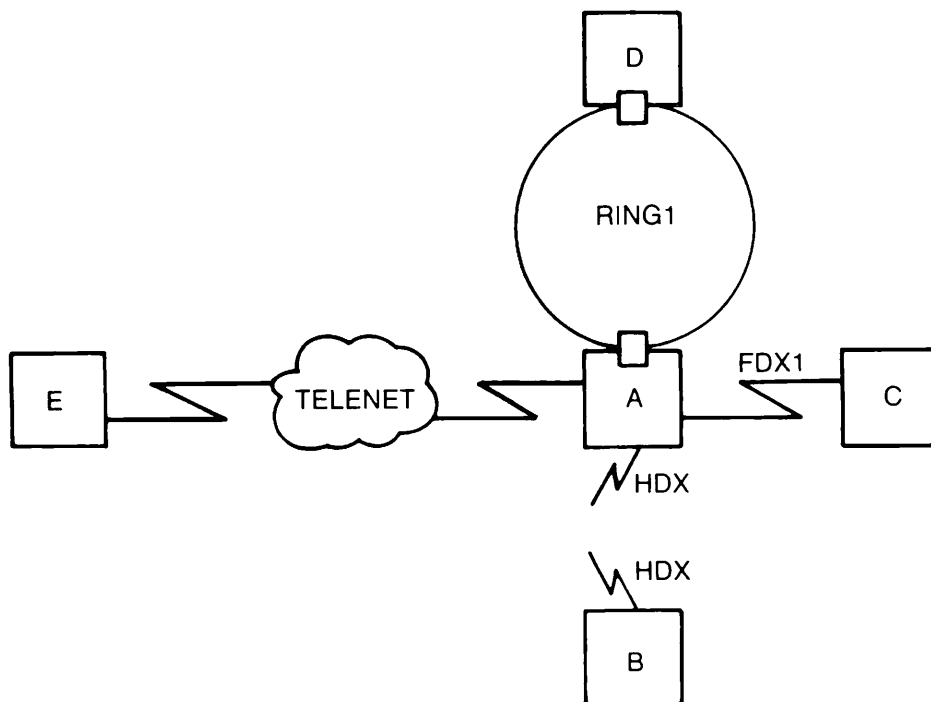
- (0) HELP (for assistance)
- (1) Remove this link from the configuration
- (2) Change the name of this link
- (3) Add a node to this link
- (4) Remove a node from this link
- (5) Change synchronous line numbers
- (6) Set LAP or LAPB protocol
- (7) Set HDLC or Bisync framing
- (8) Enable/Disable DSS interrupts
- (9) Change LAP(B) address (non-Prime nodes)
- (10) Change highest LCN (non-Prime nodes)
- (11) Change default packet size (non-Prime nodes)
- (12) Change default window size (non-Prime nodes)
- (13) Change restart options (non-Prime nodes)

Enter carriage return for the top level edit menu.

Option: **<CONTROL-P>**

Create, Edit, Quit, Save, Fast_Save, List, or Help?

Dialog Notes

*Figure 7-16. General Network Example*

Example 7: Adding a Non-Prime Node

In this example, a new non-Prime node, NP3, is added to the network illustrated in Figure 7-10, resulting in the new configuration shown in Figure 7-17. (NP3 is added to LAN300-1.) Node NP3 is given IPCF access to Node NP2, because it will communicate with that node through gateway node P2. Because NP2 is on an FDX line and must call NP3 through gateway node P2, an indirect FDX address is supplied for NP3. The addition is made in four steps:

1. From Edit mode, the LAN300 submenu is used to add the new node, NP3, to the LAN300 subnetwork and to the entire network at the same time.
2. The Administrator transfers to Create mode and answers questions about Node NP3, assigning Node NP3 IPCF access to Node NP2.
3. The Administrator goes back into Edit mode to indicate that Node NP3 is a non-Prime node.
4. The Administrator transfers to Create mode and answers questions related to non-Prime nodes.

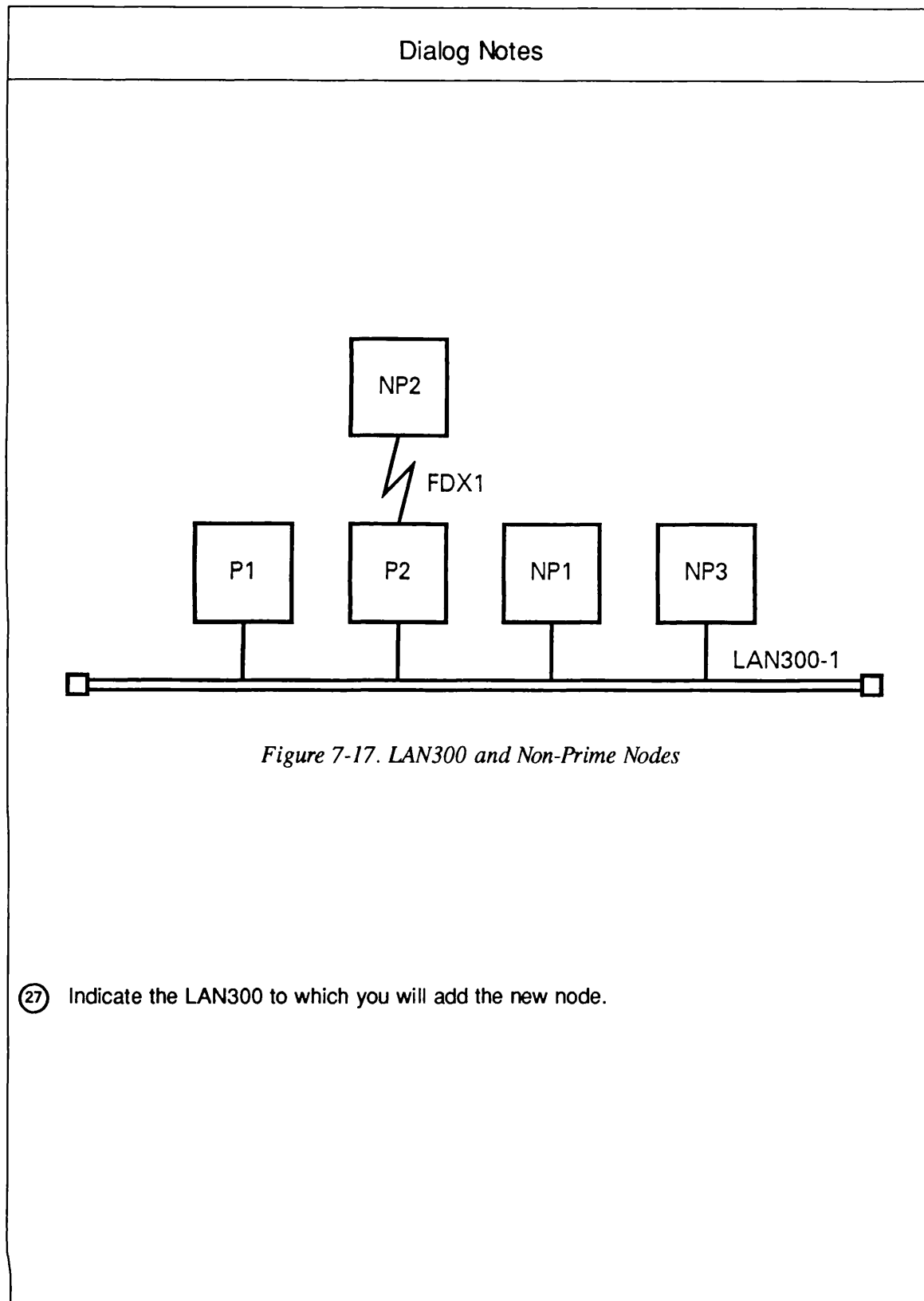
```
OK, CONFIG_NET
[CONFIG_NET Rev. 22.0 Copyright (c) 1987, Prime Computer, Inc.]
```

```
Create, Edit, Quit, Save, Fast_Save, List, or Help? EDIT
Edit Mode
What would you like to edit?
```

```
(0) HELP      (for assistance)
(1) NODE
(2) RING
(3) FDX       (full duplex synchronous Prime-to-Prime links)
(4) PSDN      (packet switching data network)
(5) HDX       (half duplex network)
(6) LAN300    (IEEE 802.3 Local Area Network)
```

```
Enter carriage return to leave Edit mode
```

```
(27) { What would you like to edit: 6
      LAN300 name
      (NONE, <LAN300 name>): LAN300-1
      Edit LAN300 LAN300-1
      Select option.
```



- (0) HELP (for assistance)
- (1) Remove this LAN300 from the configuration
- (2) Change the name of this LAN300
- (3) Add a node to this LAN300
- (4) Remove a node from this LAN300
- (5) Change MAC address (non-Prime nodes)
- (6) Change highest LCN (non-Prime nodes)
- (7) Change default packet size (non-Prime nodes)
- (8) Change default window size (non-Prime nodes)
- (9) Change restart options (non-Prime nodes)

Enter carriage return for the top level edit menu.

- (28) { Option: **3**
 New node for LAN300-1
 (NONE, <node name>): **NP3**
 Edit LAN300 LAN300-1
 Select option.

- (0) HELP (for assistance)
- (1) Remove this LAN300 from the configuration
- (2) Change the name of this LAN300
- (3) Add a node to this LAN300
- (4) Remove a node from this LAN300
- (5) Change MAC address (non-Prime nodes)
- (6) Change highest LCN (non-Prime nodes)
- (7) Change default packet size (non-Prime nodes)
- (8) Change default window size (non-Prime nodes)
- (9) Change restart options (non-Prime nodes)

Enter carriage return for the top level edit menu.

- (29) { Option: **<CONTROL-P>**
 Create, Edit, Quit, Save, Fast_Save, List, or Help? **CREATE**

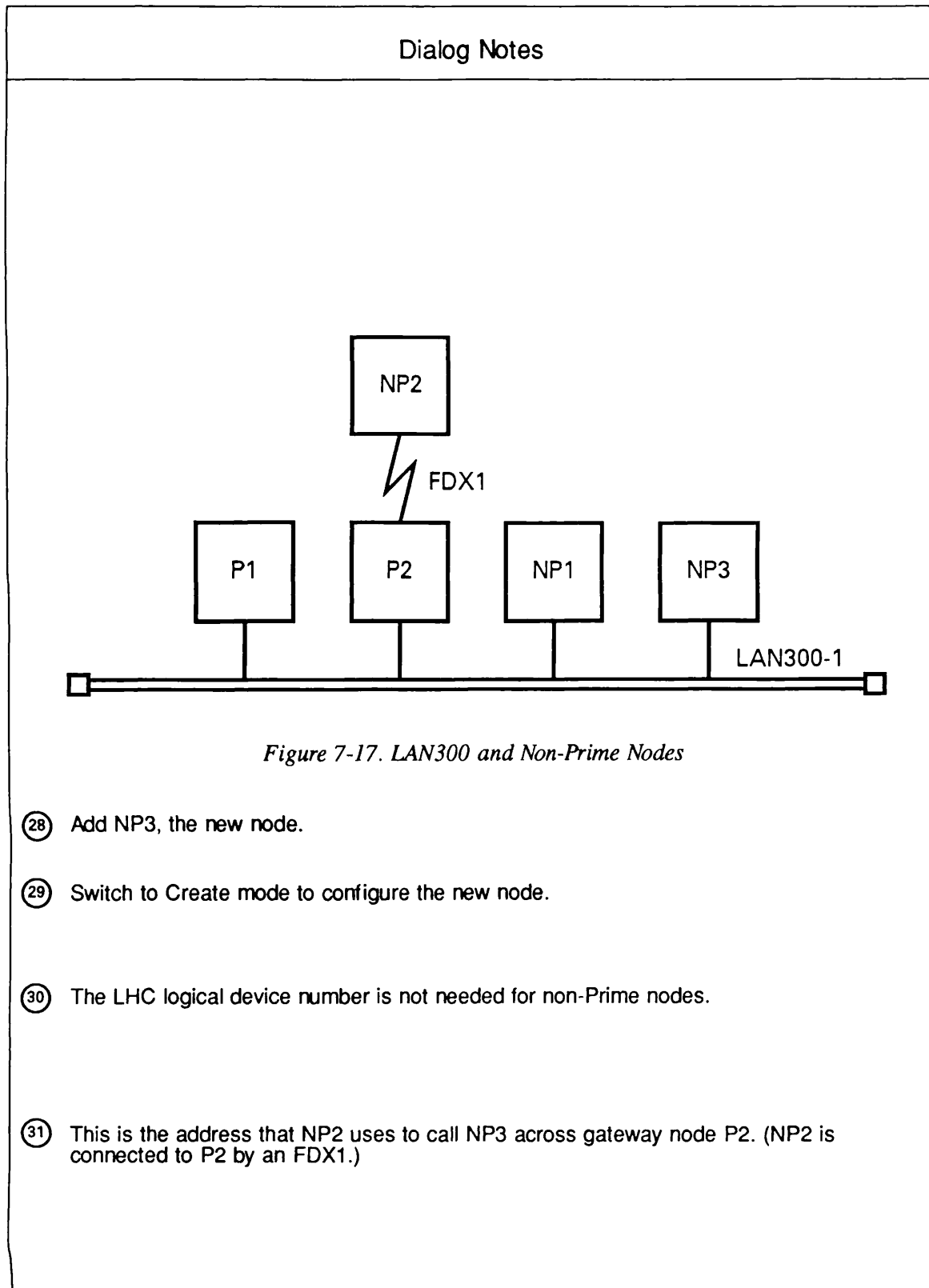
Describe Node NP3

No address is configured for line to LAN300-1

Enter LAN300-1 addresses for NP3

(NONE, <LAN300-1 addresses>):

- (30) { LHC logical device number for Primenet support for NP3 on LAN300-1
 (UNKNOWN, <0-7>):
- Indirect LAN300-1 address for node NP3
 (NONE, <LAN300-1 addresses>):
- (31) { Indirect FDX1 address for node NP3
 (NONE, <FDX1 addresses>): **999800000003;**
 Gateway node which will route address 999800000003 from FDX1
 to node NP3
 (NONE, <node names>): **P2;**



Gateway access from NP3
(NONE, RFA, RLOG, IPCF, ALL): **IPCF**;
Force user validation(NO, YES)?
Enter nodes accessible from NP3 via gateway with this access
(NONE, ALL, <node names>, <network names>): **NP2**;
Gateway access from NP3
(NONE, RFA, RLOG, IPCF, ALL):
Node-node password between NP3 and NP2
(NONE, YES, <password>):
All required configuration data has been supplied.

③ { Create, Edit, Quit, Save, Fast_Save, List, or Help? EDIT
Edit Mode

What would you like to edit?

- (0) HELP (for assistance)
- (1) NODE
- (2) RING
- (3) FDX (full duplex synchronous Prime-to-Prime links)
- (4) PSDN (packet switching data network)
- (5) HDX (half duplex network)
- (6) LAN300 (IEEE 802.3 Local Area Network)

Enter carriage return to leave Edit mode

What would you like to edit: **1**

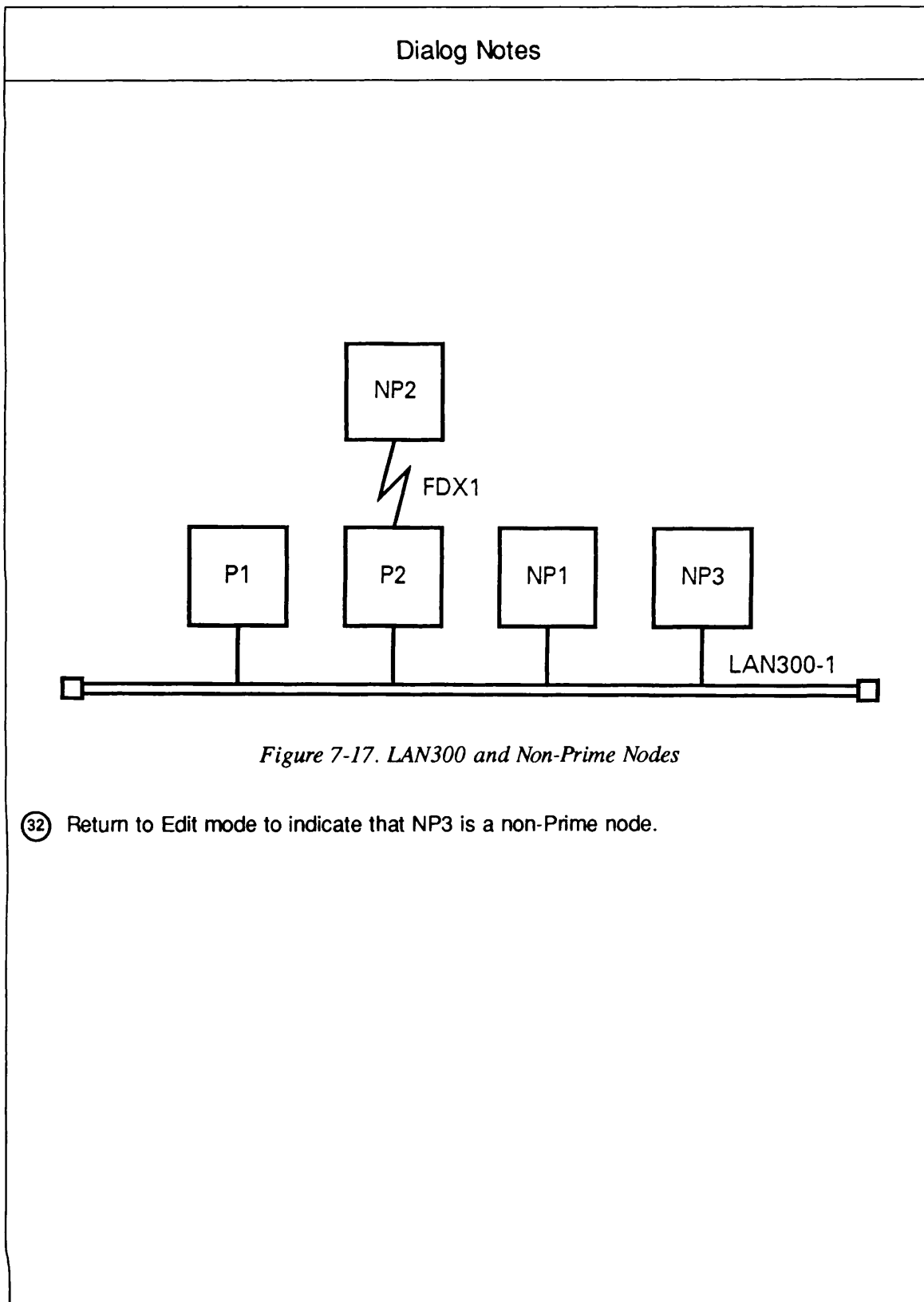
Node name (NONE, <node name>): **NP3**

Edit Node NP3

Select a node editing option.

- (0) HELP (for assistance)
- (1) Delete this node
- (2) Change the name of this node
- (3) Modify this node's access information
- (4) Change node-node passwords for this node
- (5) Change HDX passwords for this node
- (6) Change this node's status as a gateway node
- (7) Add a network address for this node
- (8) Delete a network address for this node
- (9) Change a network address for this node
- (10) Change this node's rev. status
- (11) Change this node's compatibility address
- (12) Change a LAN300 Host Controller number for this node
- (13) Mark non-Prime node
- (14) Change non-Prime source address
- (15) Change maximum number of VCs for this node

Enter carriage return for the top level edit menu.



- { Option: **13**
 33 { Is node NP3 running Primenet (TM)
 (NO, YES)? **NO**
 Edit Node NP3
 Select a node editing option.

 (0) HELP (for assistance)
 (1) Delete this node
 (2) Change the name of this node
 (3) Modify this node's access information
 (4) Change node-node passwords for this node
 (5) Change HDX passwords for this node
 (6) Change this node's status as a gateway node
 (7) Add a network address for this node
 (8) Delete a network address for this node
 (9) Change a network address for this node
 (10) Change this node's rev. status
 (11) Change this node's compatibility address
 (12) Change a LAN300 Host Controller number for this node
 (13) Mark non-Prime node
 (14) Change non-Prime source address
 (15) Change maximum number of VCs for this node

 Enter carriage return for the top level edit menu.
- { Option: **<CONTROL-P>**
 34 { Create, Edit, Quit, Save, Fast_Save, List, or Help? **CREATE**

 Describe Node NP3
 MAC (+ LSAP) address for node NP3 on LAN300-1: **08-00-2F-45-46-56**
 Highest logical channel number for VCs on line .UNKNOWN to LAN300-1
 (4095, <1-4095>):
 Default window size for line .UNKNOWN to LAN300-1
 (2, <1-7>): **7**
 Default packet size (in bytes) for line .UNKNOWN to LAN300-1
 (512, <16-512>):
 Determine DTE/DCE for node NP3 on LAN300-1 .UNKNOWN
 (DYNAMIC,DTE,DCE):
 Does node NP3 on LAN300-1 .UNKNOWN use ISO 8881 procedures
 (NO, YES): **YES**
 All required configuration data has been supplied.

 Create, Edit, Quit, Save, Fast_Save, List, or Help?

Dialog Notes

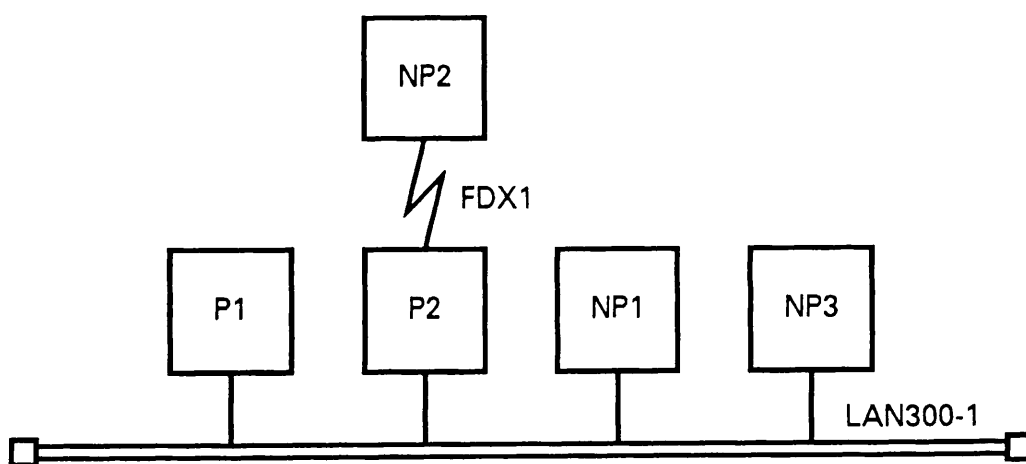


Figure 7-17. LAN300 and Non-Prime Nodes

- ③③ Indicate that NP3 is a non-Prime node (because it is not running PRIMENET).
- ③④ Return to Create mode to supply information needed for non-Prime nodes.

List Mode Examples

List mode allows you to view some or all of the information in a configuration. When you enter LIST in response to the Option Prompt, CONFIG_NET issues the following prompt:

```
What object would you like to list
ALL, RINGS, LAN300S, FDX, HDX, PSDNS, NODES,
<node or network name>:
```

The following examples indicate the contents of each type of List mode display.

The ALL Listing

The ALL listing for the configuration in Figure 7-9 is shown below.

```
OK, CONFIG_NET
CONFIG_NET Rev. 22.0 Copyright c 1987, Prime Computer, Inc.
Create, Edit, Quit, Save, Fast_Save, List, or Help? LIST
What object would you like to list
(ALL, RINGS, LAN300S, FDX, HDX, PSDNS, NODES,
  <node or network name>): ALL
Node A
  gateway
  Level_3_Address: 99990402067650
  Ring RING1   Ring Node ID: 1
    Access from node A
      Node D          RFA IPCF Remote Log Thru Validation
      Node-Node password: EKQORQ
  FDX FDX1 SMLC00 LAPB HDLC Interrupt/Pattern/Order=Yes/0011/0011
    Access from node A
      Node C          RFA Validation
      Node-Node password: FNDLBQ
  Half Duplex Network Lines: SMLC02
    Access from node A
      Node B          IPCF Validation
      Node-Node password: GUZHFQ
      Incoming half duplex password: GCLGXT
      Outgoing half duplex password: GORZZA
  PSDN TELENET
    Address: 311055599999 Lines: SMLC01
    SMLC01 LAPB HDLC 4095 2 128 Interrupt/Pattern/Order=Yes/0011/0011
      Access from node A
        Node E          IPCF
        Node-Node password:

Node D

Level_3_Address: 99990402015051
Ring RING1   Ring Node ID: 2
  Access from node D
    Node A          RFA IPCF Remote Log Thru Validation
    Node-Node password: EKQORQ
```

Gateway Access from node D
Node B IPCF
Node-Node password:
Node C Remote Log Thru
Node-Node password:
Indirect address: 3110555999901 Gateway: A

Node C

Level_3_Address: 99990402062911
FDX FDX1 SMLC00 LAPB HDLC Interrupt/Pattern/Order=Yes/0011/0011
Access from node C
Node A RFA Validation
Node-Node password: FLZRCL
Gateway Access from node C
Node D IPCF
Node-Node password:
Node B
Indirect address: 3110555999902 Gateway: A

Node B

Level_3_Address: 99990402010880
Half Duplex Network Lines: SMLC00
Access from node B
Node A IPCF Remote Log Thru Validation
Node-Node password: IZCXGB
Incoming half duplex password: IAZPKJ
Outgoing half duplex password: HMWDXE
Gateway Access from node B
Node D IPCF
Node-Node password:
Node E IPCF
Node-Node password:
Node C Remote Log Thru
Indirect address: 3110555999903 Gateway: A

Node E

PSDN TELENET
Address: 311055588888 Lines: unknown
Access from node E
Node A IPCF
Node-Node password:
Gateway Access from node E
Node B IPCF
Node-Node password:

Create, Edit, Quit, Save, Fast_Save, List, or Help?

The RINGS Listing

The RINGS listing for the configuration in Figure 7-11 is shown below.

```
Create, Edit, Quit, Save, Fast_Save, List, or Help? LIST
What object would you like to list
ALL, RINGS, LAN300S, FDX, HDX, PSDNS, NODES, <node or network name>): RINGS
```

```
Ring RING1
  Node  RingID
  A      1
  B      2
Ring RING2
  Node  RingID
  C      1
  D      2
```

```
Create, Edit, Quit, Save, Fast_Save, List, or Help?
```

The LAN300S Listing

The LAN300S listing for the configuration in Figure 7-10 is shown below.

```
Create, Edit, Quit, Save, Fast_Save, List, or Help? LIST
What object would you like to list
ALL, RINGS, LAN300S, FDX, HDX, PSDNS, NODES, <node or network name>): LAN300S
```

```
LAN300 LAN300-1
  Node  Address          Controller AddressII          maxLCN window
packet
P1      99990403179921  LHC00
P2      99990455721031  LHC00
NP1     77777777777777  unknown    08-00-2F-44-55-66+0C 4095    7    512
      ISO 8881 dynamic DxE
```

```
Create, Edit, Quit, Save, Fast_Save, List, or Help?
```

The FDX Listing

The FDX listing for the configuration in Figure 7-2 is shown below.

```
Create, Edit, Quit, Save, Fast_Save, List, or Help? LIST
What object would you like to list
ALL, RINGS, LAN300S, FDX, HDX, PSDNS, NODES, <node or network name>): FDX
```

```
FDX FDX1
  Node  Line Protocol Framing
  A      SMLC00 LAPB    HDLC    Interrupt/Pattern/Order=Yes/0011/0011
  B      SMLC00 LAPB    HDLC    Interrupt/Pattern/Order=Yes/0011/0011
```

```

FDX  FDX2
Node   Line Protocol Framing
B      SMLC01  LAPB    HDLC    Interrupt/Pattern/Order=Yes/0011/0011
C      SMLC00  LAPB    HDLC    Interrupt/Pattern/Order=Yes/0011/0011
FDX  FDX3
Node   Line Protocol Framing
C      SMLC01  LAPB    HDLC    Interrupt/Pattern/Order=Yes/0011/0011
D      SMLC00  LAPB    HDLC    Interrupt/Pattern/Order=Yes/0011/0011

Create, Edit, Quit, Save, Fast_Save, List, or Help?

```

The HDX Listing

The HDX listing for the configuration in Figure 7-3 is shown below.

```

Create, Edit, Quit, Save, Fast_Save, List, or Help?  LIST
What object would you like to list
ALL, RINGS, LAN300S, FDX, HDX, PSDNS, NODES, <node or network name>): HDX

Half Duplex
Node   Line
A      SMLC00
B      SMLC00
B      SMLC01
C      SMLC00
D      SMLC01

Create, Edit, Quit, Save, Fast_Save, List, or Help?

```

The PSDNS Listing

The PSDNS listing for the configuration in Figure 7-6 is shown below.

```

Create, Edit, Quit, Save, Fast_Save, List, or Help?  LIST
What object would you like to list
ALL, RINGS, LAN300S, FDX, HDX, PSDNS, NODES, <node or network name>): PSDNS

PSDN  TYMNET
Node   Address          Line Protocol Framing  maxLCN window packet
SYSX   310655555          SMLC00  LAPB    HDLC    4095   2    128
      Interrupt/Pattern/Order=Yes/0011/0011
SYSY   310622222          SMLC00  LAPB    HDLC    4095   2    128
      Interrupt/Pattern/Order=Yes/0011/0011
PSDN  X.25
Node   Address          Line Protocol Framing  maxLCN window packet
SYSX   7777777777777777  SMLC01  LAPB    HDLC    4095   2    128
      Interrupt/Pattern/Order=Yes/0011/0011
SYSZ   8888888888888888  SMLC00  LAPB    HDLC    4095   2    128
      Interrupt/Pattern/Order=Yes/0011/0011

Create, Edit, Quit, Save, Fast_Save, List, or Help?

```


The NODES Listing

The NODES listing for the configuration in Figure 7-1 is shown below.

```
Create, Edit, Quit, Save, Fast_Save, List, or Help? LIST
What object would you like to list
ALL, RINGS, LAN300S, FDX, HDX, PSDNS, NODES, <node or network name>): NODES
```

Node A

```
Level_3_Address: 99990402067650
Ring RING1      Ring Node ID: 1
    Access from node A
        Node B          Remote Log Thru
        Node-Node password:
```

Node B

```
Level_3_Address: 99990402010880
Ring RING1      Ring Node ID: 2
    Access from node B
        Node A          Remote Log Thru
```

```
Create, Edit, Quit, Save, Fast_Save, List, or Help?
```

The Specific Node or Network Listing

The following LIST mode session uses the configuration in Figure 7-8.

```
Create, Edit, Quit, Save, Fast_Save, List, or Help? LIST
What object would you like to list
ALL, RINGS, LAN300S, FDX, HDX, PSDNS, NODES, <node or network name>): TYMNET
```

PSDN TYMNET

Node	Address	Line	Protocol	Framing	maxLCN	window	packet
B	310699999	SMLC01	LAPB	HDLC	4095	2	128
Interrupt/Pattern/Order=Yes/0003/0003							
C	310688888	SMLC00	LAPB	HDLC	4095	2	128
Interrupt/Pattern/Order=Yes/0003/0003							

```
Create, Edit, Quit, Save, Fast_Save, List, or Help? LIST
What object would you like to list
(ALL, RINGS, LAN300S, FDX, HDX, PSDNS, NODES, <node or network name>): B
```

Node B

```
Compatibility Address: 310699999
FDX FDX1 SMLC00 LAP HDLC Interrupt/Pattern/Order=Yes/0003/0003
    Access from node B
        Node A          RFA not enabled
```

PSDN TYMNET

```
Address: 310699999          Lines: SMLC01
SMLC01 LAPB HDLC 4095 2 128 Interrupt/Pattern/Order=Yes/0003/0003
    Access from node B
        Node C          RFA not enabled          Remote Login enabled
```

```
Create, Edit, Quit, Save, Fast_Save, List, or Help?
```

Setting PRIMENET-related CONFIG Directives

Each node on your PRIMENET network must include certain network-related configuration directives in its CONFIG file. Be sure that the necessary directives are included on each node that you administer.

This section summarizes the network-related CONFIG file directives. For information about using the directives, refer to the next section, Using the PRIMENET-related CONFIG Directives. For more information about these CONFIG directives and about CONFIG file in general, refer to the *System Administrator's Guide, Volume 1: System Configuration*.

Summary of the PRIMENET-related CONFIG Directives

<i>Directive</i>	<i>Function</i>
LHC	Assigns a physical device address to an LHC300 logical device number. The LHC300 logical device number is included in the PRIMENET and/or NTS configuration file.
NPUSR	Specifies the maximum number of phantom users allowed on the node at one time. Many Prime network services require phantom processes.
NRUSR	Specifies the maximum number of remote users allowed on the node at one time.
NSLUSR	Specifies the maximum number of slaves allowed on the node at one time. This is the same as the number of simultaneous remote file accesses on the node. If you want to receive messages from operators on remote nodes via RFA, you must configure at least one slave.
REMBUF	Sets terminal input/output ring buffer sizes for remote users.
SYNC CNTRLR	Assigns a physical controller address to a logical controller number and specifies the protocol of the file to be downline loaded into the controller.

Using the PRIMENET-related CONFIG Directives

This section explains how to use the network-related CONFIG directives.

LHC

LHC assigns a physical device address to an LHC300 logical device number. An LHC300 (LAN Host Controller 300) is a controller board that connects a 50 Series host to a LAN300 network. LHC300s support PRIMENET, NTS, both PRIMENET and NTS concurrently, or WSI300. PRIMENET will not start on a host unless there is an LHC directive for every LHC300 that is configured for the host in the PRIMENET configuration file. LHC has this syntax:

LHC logical-device-number device-address

where:

logical-device-number	Specifies the LHC300's logical device number. <i>logical-device-number</i> must be in the range from 0 through 7. The LHC300 logical device number is also included in the PRIMENET and/or NTS configuration file.
device-address	Specifies the LHC300's physical device address. The LHC300 physical device address is set by a dip switch on the LHC300. The valid device addresses are: 15 ₈ , 16 ₈ , 17 ₈ , 32 ₈ , 37 ₈ , and 56 ₈ . You can also use the LIST_COMM_CONTROLLERS and the STAT COMM commands to show the device addresses of the LHC300s in a system, regardless of whether or not the LHC300s are configured with LHC directives in the CONFIG file.

If you enter invalid input for the LHC directive, PRIMOS displays an error message during system cold start. For information about the LHC error messages, refer to the *System Administrator's Guide, Volume II: Communication Lines and Controllers*.

NPUSR

NPUSR specifies the maximum number of phantom users allowed on the node at one time. It has this format:

NPUSR number

where *number* is a positive octal integer that indicates the maximum number of phantom users allowed on the node. The minimum (and default) value is 4. The maximum value is the number of user processes supported by your CPU minus the number of terminal users (NTUSR), NTS

terminal users (NTSUSR), PRIMENET remote users (NRUSR), slaves (NSLUSR), assignable lines (NAMLC), and NTS assignable lines (NTSASL). The maximum number of user processes is 17000_8 (960 decimal) for the 6350™ and 6550™ and 1130_8 (600 decimal) for all other models. When setting NPUSR, ensure that there are enough phantom processes to support all the network services used on the node. The following servers are required:

- PRIMENET: NETMAN
- Route-Through (for PRIMENET gateway nodes): RT_SERVER
- File Transfer Service (FTS): YTSMAN and at least one file transfer server. There can be as many as seven file transfer servers on a node as described in Chapter 10, Configuring File Transfer Service (two to eight phantoms)
- LAN300 Network Management: NM_SERVER and four transient servers, LHC_DLL_SERVER, LHC_ULD_SERVER, LTS_DLL_SERVER, and LTS_ULD_SERVER. Since it is unlikely that more than one transient server would be required at once, you need to allow only two phantoms for LAN300 Network Management: one for NM_SERVER and one for the transient servers.
- PRIMOS TCP/IP: TCP/IP_MANAGER, MAILER_DAEMON, SMTP_SERVER nn , one FTP_SERVER nn phantom for each LHC300 dedicated to PRIMOS TCP/IP (maximum of two), one phantom for each remote FTP session (initiated by a remote FTP user). For more information, see the *PRIMOS TCP/IP Guide*.

Network-based applications on the node and spoolers may also require phantom processes.

Note

At Rev. 22.0, you no longer have to reserve phantom slots with NPUSR for LOGIN_SERVER, TIMER_PROCESS, and NTS_SERVER. They are now considered to be *system servers* rather than phantoms. System servers are assigned processes from the pool that PRIMOS reserves for itself, not from the pool of user processes. The LIST_SERVER_NAMES and STAT US commands display the system servers running on the system.

NRUSR

NRUSR specifies the number of processes to be reserved for PRIMENET remote logins. It has this format:

NRUSR number

where *number* is a positive octal integer that indicates the maximum number of remote users allowed on the node. The maximum value for *number* is 1604_8 (900 decimal), the maximum number of virtual circuits supported by PRIMENET. The default value is 0.

Note

NRUSR + NTUSR + NTSUSR + NPUSR + NSLUSR + NAMLC + NTSASL cannot exceed the maximum number of user processes supported by your CPU. The maximum number of user processes is 17000₈ (960 decimal) for the 6350™ and 6550™ and 1130₈ (600 decimal) for all other models.

NSLUSR

NSLUSR sets the maximum number of slave processes allowed on the node. Each remote user using Remote File Access (RFA) to access files on the node requires a slave process for the duration of the access. These slave processes come out of the pool of user processes. If you want to receive messages from operators on remote nodes via NPX, you must configure at least one slave. If the slave process pool is exhausted when a remote user makes an attach request, the E\$NSLA (no NPX slaves available) error code is returned. NSLUSR has this format:

NSLUSR number

where *number* sets the maximum number of simultaneous remote file accesses on the node. The default value is 0. Observe these guidelines when setting *number*:

- *number* must be less than or equal to 1440₈ (800 decimal).
- NSLUSR + NTUSR + NTSUSR + NRUSR + NPUSR + NAMLC + NTSASL cannot exceed the maximum number of user processes supported by your CPU. The maximum number of user processes is 17000₈ (960 decimal) for the 6350™ and 6550™ and 1130₈ (600 decimal) for all other models.

REMBUF

Note

On nodes running Rev. 22.0, we recommend that you use the CAB command rather than the REMBUF directive to set your remote buffer sizes. For information on the CAB command, see Chapter 9, Setting PRIMENET-related PRIMOS.COMI commands.

REMBUF sets the terminal input and output ring buffer sizes for remote users. Remote users are those logged in to the node over PRIMENET. REMBUF has this syntax:

REMBUF in-buff-size out-buff-size

where:

in-buff-size	Sets the terminal input buffer size in halfwords (two characters per halfword). The default and minimum values are both 202 ₈ halfwords (260 bytes decimal). To leave the input buffer size unchanged, enter 0.
out-buff-size	Sets the terminal output buffer size in halfwords (two characters per halfword). The default and minimum values are both 101 ₈ halfwords (130 bytes decimal). To leave the output buffer size unchanged, enter 0.

Total size of input buffers plus output buffers cannot exceed 2734000₈ (768K halfwords or 1536K bytes decimal). This includes the buffers for both local and remote users.

Setting REMBUF for RINGNET Users

To improve throughput on a system where users are logging in remotely across a ring network, increase the output buffer size to 402₈ halfwords (516 bytes decimal).

Setting REMBUF for PSDN and Non-Prime Node Users

If remote login is allowed from a PSDN or non-Prime node, set the REMBUF input and output sizes to at least the octal value of the default packet size times the default window size for those links. (The default packet and window sizes for the node's PSDN and non-Prime node links are in the PRIMENET configuration file.) For example, if the node accepts remote login calls from a non-Prime node with a default packet size of 256 and a default window size of 7, set the REMBUF input and output buffers to 7000₈ halfwords (1792 decimal bytes).

However, because window size and packet size can now be negotiated for each call, you must increase the REMBUF input and output buffer sizes if window size and packet size are ever negotiated to values higher than their defaults. On the other hand, if window and packet sizes are consistently negotiated down to smaller than their default values, you can decrease the REMBUF values to conserve memory space.

Setting the REMBUF values is essentially a tradeoff — you can increase throughput by increasing the REMBUF values, but it is at the cost of increased memory and buffer usage.

SYNC CNTRLR

Note

On nodes running Rev. 21.0 and above, we recommend that you use the `COMM_CONTROLLER` command to load your ICS controllers. (You can use `COMM_CONTROLLER` and `SYNC CNTRLR` independently or in combination.) For more information on the `COMM_CONTROLLER` command, see Chapter 9, Setting PRIMENET-related PRIMOS.COMI commands.

SYNC CNTRLR assigns a physical controller address to a logical controller number and specifies the protocol of the file to be downline loaded into the controller. You must include a SYNC CNTRLR directive for every ICS2 or ICS3 that is supporting PRIMENET synchronous lines. SYNC CNTRLR has this syntax:

SYNC CNTRLR controller-number device-address protocol

where:

controller-number	Indicates the logical controller number. The valid values for ICS2 and ICS3 controllers are 0 and 1.
device-address	Specifies the physical device address of the specified controller in octal. Usually 10 ₈ or 11 ₈ is given for an ICS2 or ICS3.
protocol	Specifies the protocol of the file to be downline loaded into the controller. For controllers supporting full-duplex lines, use the HDLC or BSCX25 protocol token, depending on how the line is configured in the PRIMENET configuration file. For ICS3 controllers supporting half-duplex lines, use the BSCX25 token.

Examples of the SYNC CNTRLR directive are as follows:

```
SYNC CNTRLR 1 10 HDLC
SYNC CNTRLR 0 11 BSCX25
```

For more information on SYNC CNTRLR, see the *System Administrator's Guide, Volume II: Communications Lines and Controllers* and the *ICS User's Guide*.

Setting PRIMENET-related PRIMOS.COMI Commands

This chapter describes the PRIMENET-related commands that you must insert in each node's PRIMOS.COMI file. The PRIMOS.COMI file is executed at cold start. You must insert the commands in the following order, which corresponds to the sections in this chapter. (There may be other commands interspersed in between.)

- START_DSM
- COMM_CONTROLLER
- START_NET
- ADDISK
- CAB

For more information on these commands, refer to the *Operator's Guide to System Commands*, the *Operator's Guide to Prime Networks*, and the *DSM User's Guide*.

START_DSM

START_DSM starts Distributed Systems Management (DSM) on the local system. In the PRIMOS.COMI file, the START_DSM command must come after the CONFIG -DATA command that reads the system configuration file and the ADDISK commands that add the *local* disks. START_DSM must come before the COMM_CONTROLLER, START_NTS, and START_NET commands to ensure that their startup messages are logged.

Insert a START_DSM command with this syntax in your PRIMOS.COMI file:

```
START_DSM
```

COMM_CONTROLLER

COMM_CONTROLLER loads the software into the ICS and LHC300 controllers in the node. You must insert the COMM_CONTROLLER command(s) in PRIMOS.COMI before the START_NTS or START_NET command. COMM_CONTROLLER can load all the controllers

of the same type in the node concurrently, provided that they all use the same software file and protocol. The `COMM_CONTROLLER` command(s) in your `PRIMOS.COMI` file should have the syntax shown below. (Many of the options shown below are abbreviations. For a complete description of `COMM_CONTROLLER`, see the *System Administrator's Guide, Volume II: Communication Lines and Controllers*.)

`COMM_CONTROLLER -LOAD -DEV device -DA device-address -PN pathname -PR token -NQ`

where:

- LOAD** Initiates a full downline load of a specified file or protocol combination to a designated controller. The controller is automatically shut down, verified, and loaded.
- DEV device** Specifies the device type. The following devices are supported: ICS1, ICS2, ICS3, LHC, and LTS.
- DA device_address** Specifies the *device_address* of the controller to be loaded, which is a two-digit octal number. You can determine this address by using either the `STATUS COMM` command or the `LIST_COMM_CONTROLLERS` command.
- PN pathname** Specifies the pathname of the object file that contains the load parameters. If you specify the filename alone, the `DOWN_LINE_LOAD*` directory is assumed.
- PR token** Specifies a communications protocol token used by the LHC300, ICS2, or ICS3 controllers. You *must* use this option when downline loading an LHC300. These tokens are available:

<i>LHC300</i>	<i>ICS2/3</i>
<i>Controller</i>	<i>Controller</i>
LLCX25	ASYNC
NTS	SDLC
TCP	HDLC
	BCSX25
	BSCRJE

Enter LLCX25 for LHC300s running only PRIMENET, NTS for LHC300s running only NTS, or LLCX25 *and* NTS for LHC300s running NTS and PRIMENET concurrently. TCP is for LHC300s running PRIMOS TCP/IP; you cannot downline load both the NTS and the TCP protocols on the same LHC300.

- NQ** Executes the command without prompting you for confirmation.

The `COMM_CONTROLLER` command allows the concurrent loading of multiple controllers of the same type, provided that they are connected to the same backplane and are using the same file and protocol combinations. To do so, use the `-ALL` option instead of the `-DEVICE_ADDRESS (-DA)` option. `COMM_CONTROLLER` loads all the controllers specified in the `-DEV` option.

START_NET

`START_NET` starts PRIMENET on a node and reads the global network configuration file to determine its position in the network topology. `START_NET` then spawns the ISC Network Server (`ISC_NETWORK_SERVER`) to support remote InterServer Communications (ISC). The ISC network server supports remote DSM. If the node is configured as a gateway node (a node that routes data between other nodes that are indirectly connected), `START_NET` automatically starts up the Route-through Server (`RT_SERVER`). `START_NET` starts LAN300 Network Management if the node is attached to a LAN300 and that service has not already been started by the `START_NTS` command. (Before starting PRIMENET on a LAN300 on which NTS is already running, `START_NET` verifies that `START_NTS` used the same system name and the same LAN300 name. If this test fails, `START_NET` does not start PRIMENET. To avoid this problem, use the same name for the LAN300 in both configuration files and always use the name given by the system's `SYSNAM CONFIG` directive for the system name.) Finally, `START_NET` opens a network event log file, or reopens it if network event logging was turned off by the last `STOP_NET` command.

WARNING

Do not attempt to use Pre-Rev. 21.0 `START_NET` or a configuration file created with Pre-Rev. 21.0 `CONFIG_NET` to start Rev. 22.0 PRIMENET.

Place `START_NET` near the beginning of `PRIMOS.COMI`, after `START_DSM` and `COMM_CONTROLLER`, but before the `ADDISK` commands that add *remote* partitions. Network initialization is completed before execution of the command that follows `START_NET`. However, even after `START_NET` has finished executing and the network is initialized, a little more time is required before the node can communicate with remote systems. Therefore, you should place `START_NET` near the beginning of your `PRIMOS.COMI` file to allow time for the network to become active before other system startup commands or users try to use the network. `START_NET` must precede any `ADDISK -ON` commands because `ADDISK` checks to see if a remote node is configured before adding the partitions for that system. If you are using FTS, `START_NET` must appear before the `CO SYSTEM>FTS.SHARE.COMI` command. You can place the `START_NET` command either before or after shared libraries.

Note

START_NET starts up PRIMENET, all ring and full-duplex connections, and LAN300 Network Management. However, it does not start up half-duplex lines. The operator must start half-duplex lines as a separate task.

The START_NET command in your PRIMOS.COM1 file must have this syntax:

START_NET [-NODE nodename] [config_pathname]

where:

-NODE nodename	Specifies the name of the system to be started. Previously this was a required option. Now, since every system is given a system name at cold start, START_NET uses the system name as the PRIMENET node name. Although you can still specify a node name, START_NET displays an error message and stops if it is inconsistent with the system name given by the SYSNAM CONFIG directive.
config_pathname	The pathname of the network configuration file. If <i>config_pathname</i> does not end with .CONFIG, START_NET appends .CONFIG (and thus searches for <i>config_pathname</i> .CONFIG). If that search is unsuccessful, START_NET searches for <i>config_path</i> next. If you omit this option, the default pathname, PRIMENET*>PRIMENET.CONFIG, is used.

ADDISK

ADDISK makes the specified disk partition or partitions available to users on the system. First, ADDISK searches the table of logical disks for available table entry locations; then, if one or more are found, ADDISK starts up the specified disk partition or partitions.

No more than 238 logical disks can be added to a system. This limit applies to both local and remote disks. Local disk partitions are those on your system; remote disk partitions are those on remote nodes in the network. Logical disk numbers range from 0₈ through 355₈. In this discussion we use the terms **disk** and **partition** interchangeably; do not confuse them with a physical disk drive.

This section describes how to use ADDISK to make remote disk partitions accessible by Remote File Access (RFA). For more complete information, refer to the *Operator's Guide to System Commands*.

Starting Up Remote Disk Partitions

Use the following ADDISK command format to make partitions on remote nodes available to users on the local node:

ADDISK diskname-1 [diskname-2 . . . diskname-9] -ON nodename

where:

diskname-n

Indicates the name of a remote partition. All disknames must be unique. You cannot add a new partition if its diskname is the same as that of a disk already added. The remote partition does not have to be started, nor does the remote system have to be running. If you attempt to add more than nine partitions in one command line, ADDISK displays this message:

Too many objects specified. "diskname-10" (addisk)

You cannot rename or protect a remote partition. The name and the write-protection status of a device are always assigned at the device's local system.

nodename

Indicates the name of the remote node on which the partition(s) reside. The local node must have RFA access rights to this remote node. For more information, see Chapter 3, PRIMENET Security.

CAB

The CAB command sets the buffer sizes for all types of asynchronous lines; for a full description, see the *System Administrator's Guide, Volume II: Communications Lines and Controllers*. For nodes running Rev. 22.0, we recommend that you use the CAB command rather than the REMBUF CONFIG directive to set the buffer sizes for remote login lines (remote buffers).

A CAB -REMBUF command in your PRIMOS.COMI file sets the buffer sizes to be allocated to all remote login lines as they become active. There is no way to preset the buffer sizes for specific remote login lines, because they are not given line numbers and allocated buffers until they become active. However, you can use CAB to change the buffer sizes for specific *active* remote login lines, provided that you have the proper privileges. (For more information, see the section below entitled *Configuring Specific Remote Login Lines With CAB*.) The CAB command in your PRIMOS.COMI file for setting the remote buffer sizes must have this syntax:

CAB -REMBUF -IBS nnn -OBS nnn

where:

- REMBUF** Instructs CAB to set the buffer sizes to be allocated to all remote login lines as they become active.
- IBS *nnn*** Sets the input buffer size for remote login lines. *nnn* is the number of eight-bit characters that can be held in the buffer. The default value used at cold start is 256 characters; the legal range is from 2 to 8190. Other than at cold start, if you omit -IBS or supply a value of 0, CAB uses the current input buffer size.
- OBS *nnn*** Sets the output buffer size for remote login lines. *nnn* is the number of eight-bit characters that can be held in the buffer. The default value used at cold start is 384 characters; the legal range is from 100 to 8190. Other than at cold start, if you omit -OBS or supply a value of 0, CAB uses the current output buffer size.

If you omit either -IBS or -OBS, CAB does not change the size of the buffer you omit. You cannot omit both options. The following example shows a CAB command used in a PRIMOS.COMI file to set the buffer sizes for remote login lines.

```
CAB -REMBUF -IBS 1792 -OBS 1792
```

Verifying the Remote Buffer Sizes

To verify that the CAB command has established the correct remote buffer sizes, enter a LAB command with the following syntax:

```
LAB -REMBUF
```

LAB presents a display similar to the following:

```
-----
|          || Initial Buffer Sizes | |
|          ||-----|
|          ||   Input   |   Output   |
|-----||-----|-----|
| REMBUF  ||    1792    |    1792    |
|-----||-----|-----|
```

Configuring Specific Remote Login Lines With CAB

Once a remote login line is active, you can enter STAT USER to display its line number, then enter a CAB command to change its input and output buffer sizes. You can use CAB from the supervisor terminal to change the buffer sizes of any remote login line. However, if the buffer sizes have been changed by an application program running on the line, your changes will not

take effect until the application terminates. The following example shows the CAB command to change the buffer sizes on line 17:

```
CAB -LINE 17 -IBS 128 -OBS 128
```

You can also use CAB from a nonsupervisor terminal to configure a line either on the local or on a remote node, provided that you have DSM privileges to use CAB on the target node. You must also include the `-ON` option in your command line, even if the target line is on the local node. (For more information on DSM, see the *DSM User's Guide*.) The following example shows the syntax to configure a remote login line on the local node from a nonsupervisor terminal:

```
CAB -LINE 27 -IBS 128 -OBS 128 -ON
```

To verify that the buffer sizes for the line are correct, enter a LAB command with the following syntax:

```
LAB -LINE 27 -ON
```

To set the buffer sizes of a line on a remote node, you must include the `-ON` option and the node name on the CAB command line. Again, you must have DSM privileges to use this command. The following example shows the syntax to configure a line on the node named Harry:

```
CAB -LINE 56 -IBS 256 -OBS 256 -ON HARRY
```

To verify that the buffer sizes for the line are correct, enter a LAB command with the following syntax:

```
LAB -LINE 56 -ON HARRY
```

Remote Buffer Sizes for RINGNET Users

To improve throughput on a system where users are logging in remotely across a ring network, increase the remote output buffer size to 516 eight-bit characters.

Setting REMBUF for PSDN and Non-Prime Node Users

If remote login is allowed from a PSDN or non-Prime node, set the remote input and output buffers to be at least equal to the default packet size times the default window size for those links. (The default packet and window sizes for the node's PSDN and non-Prime node links are in the PRIMENET configuration file.) For example, if the node accepts remote login calls from a non-Prime node with a default packet size of 7 and a default window size of 256, set the remote input and output buffers to 1792 eight-bit characters.

However, because window size and packet size can now be negotiated for each call, you must increase the remote input and output buffer sizes if window size and packet size are ever negotiated to values higher than their defaults. On the other hand, if window and packet sizes are consistently negotiated down to smaller than their default values, you can decrease the remote buffer values to conserve memory space.

Setting the remote buffer sizes is essentially a tradeoff — you can increase throughput by increasing the buffer sizes, but it is at the cost of increased memory usage. The increased memory usage is temporary, however, because buffers are used only when a line is active. As soon as a line disconnects, its buffers return to available memory.

Configuring File Transfer Service

This chapter explains how to use FTGEN to configure FTS after it has been installed on your system. It also describes how to perform the following FTS-related administrative tasks. For more information on these tasks, refer to the *Operator's Guide to Prime Networks*. For information on installing FTS and setting FTS-related ACLs, refer to Chapter 2, Installing PRIMENET Software.

- Assigning FTS-related access rights
- Allocating space in the FTSQ* directory
- Configuring and maintaining the FTS database with FTGEN
- Recovering from an invalid database
- Starting up and shutting down FTS

Introduction

FTGEN lets allows you to set up and configure these three parts of FTS:

- File transfer servers, which are phantom processes that handle file transfer requests
- File transfer queues, which hold file transfer requests
- File transfer sites, which are local or remote nodes between which files are transferred

You can configure as many as eight file transfer servers, each of which takes requests from its own queue. A server can handle up to eight requests from its queue simultaneously, whereas a queue can hold up to 9999 requests. An additional special server, YTSMAN, receives file transfer requests from remote sites and passes them to appropriate servers.

The file transfer servers and YTSMAN are started at the supervisor terminal with the FTOP command, which is described in the *Operator's Guide to Prime Networks*.

To establish FTS with a remote system, you must to obtain the following information from the remote administrator:

- Remote node name
- Remote server name
- Remote server password

Note

Refer to the file FTS>INFO>FTS.RUNO for information on FTS installation, run-time requirements, changes since FTS Rev. 1, and directory structure layouts.

FTS Access Rights

For FTS to function properly on your system, you must assign the proper access rights to both FTS servers and FTS users. These access rights are described below.

ACL Systems

If your system uses Access Control Lists (ACLs), you must assign appropriate ACL rights to the FTS servers. (The user IDs of servers are defined in the FTS configuration. Servers are started, by name, using the FTOP command.) You must also ensure that the FTSQ* directory on your master disk has the following ACL settings:

- Every server, including YTSMAN, must have ALL access rights to FTSQ*.
- The supervisor terminal process (user ID SYSTEM) must have ALL access rights to FTSQ*.
- The \$REST default access for FTSQ* must be set to DALURW, because users access FTSQ* through the FTR command. Also, users must be able to delete temporary request files with the FTR -CANCEL option.

Furthermore, you should inform users of server IDs so that they can grant the servers access to their directories. FTS server rights must be set to DALURW in both source file and destination file directories.

Users who want to keep their main directories private can create a special subdirectory for transfers. They should give the FTS server DALURW rights to this subdirectory, and a minimum of LU rights to any higher level directories in its pathname.

For example, if the FTS directory pathname is

`<MAINDISK>TOPDIR>FTSDIR`

then the FTS server needs LU rights to TOPDIR in addition to DALURW rights to FTSDIR.

Alternatively, a user can set the \$REST default access rights to all directories to DALURW, and the server uses these rights.

Systems Without ACLs

If your system does not use ACLs, inform users that they need the following access rights:

- Read access to source directories
- Write and Delete access to any directories in which they will create log files
- Read, Write, and Delete access to destination directories
- Owner status in any directories in which they will be creating new files (for example, in destination directories and in any directories where log files will be created)

The normal rules for using passwords on non-ACL systems govern the acquisition of access rights. If the pathname of a source, destination, or log file contains passwords, the user must include the passwords on the FTR command line. The entire pathname should be in single quotes. We recommend that owner passwords be used as a matter of course, particularly in view of the last point in the list above. Source and destination directories that are password-protected should be protected in such a way that the passwords confer the rights indicated above.

Users are sometimes reluctant to give their user ID and passwords to people who want to send files to them through FTS. Suggest that they create directories without passwords exclusively for FTS use, and that they have FTS users send files to those public directories.

Note

Do not assign a password to the FTSQ* directory.

FTSQ* Directory Size

The FTSQ* directory holds copies of files that are being transferred, along with the server, queue, and site log files that you configure with FTGEN. You should allocate a generous amount of space for FTSQ*.

During everyday use of FTS, the server, queue, and site log files increase in size. The only limit is the maximum disk quota of the directory or the size of the partition. If you archive these logs regularly, FTSQ* will always have adequate space. A simple way of archiving log files is to add a CPL file to the startup file. The CPL file can date-stamp the logs, then copy them to another partition for later tape backup or deletion.

FTGEN Commands

This chapter groups FTGEN commands into these four categories:

- General FTS configuration commands that apply to FTS as a whole. These commands initialize the FTS database and display the status of the current FTS configuration, which includes sites, servers, and queues. The HELP command (available inside the

FTGEN command environment) displays information about FTGEN commands. (Monitoring FTS with the FTOP command is described in the *Operator's Guide to Prime Networks*.)

- Commands that configure file transfer queues. These commands add, modify, and delete queues. They block submissions to a queue, purge all requests from a queue, set a queue's maximum size, set the default priority of requests in a queue, set up a queue log file, and list or save the queue configuration.
- Commands that configure file transfer servers. These add, modify, and delete servers. They set up server log files, server names, passwords, priority levels, timeslices, request retry intervals, maximum requests handled, and port numbers. They assign each server queue, and list or save the server configuration.
- Commands that configure local and remote sites. These add, modify, and delete FTS sites, define the site's address, set up the site's log file, and display or save the site configuration. An example of configuring an FTS site with FTGEN is provided in the section entitled FTS Configuration Session, later in this chapter.

Notes

Configure FTS servers with server passwords to guard against unauthorized file transfers from remote FTS sites. Confer with the System Administrators at the other FTS sites within your network to ensure that they use matching passwords.

Configure Rev. 1 FTS sites with the correct FTS issue number, or file transfers to these sites may fail. See the FTGEN ISSUE command in the section entitled Configuring Local and Remote Sites, later in this chapter.

FTGEN Subcommands

Certain FTGEN commands put you in a subcommand environment. When you use an FTGEN command to add or modify a queue, server, or site, the response is a subcommand prompt for the appropriate item. For example, if you give the command:

```
ftgen> ADD_SERVER NAMEONE
```

the next prompt is:

```
server:
```

This prompt accepts server subcommands to configure or modify the server NAMEONE. FTGEN repeats the server prompt until you give the subcommand FILE or QUIT, which returns you to the FTGEN command level.

Each item (queue, server, or site) has its own set of acceptable subcommands. Many of the subcommands have default values to simplify FTS configuration. Thus, certain subcommands are used only to change the default parameter value.

FTS holds templates of default configurations. These templates allow you to configure future servers, queues, or sites with the same attributes by using only the appropriate ADD command and the FILE subcommand. The appropriate ADD command includes the name of the new server, queue, or site to be added. If the new server, queue, or site differs in some way from the default template, you need to use only those subcommands that define the difference.

The use of commands and subcommands is demonstrated in FTS Configuration Session, later in this chapter.

General FTGEN Commands

The general FTGEN commands include the INITIALIZE_FTS command, which initializes the FTS subsystem database, and the STATUS command, which displays the current status of the FTS configuration. The HELP command displays information about the FTGEN command.

► INITIALIZE_FTS

Abbreviation: IFTS

The INITIALIZE_FTS command initializes the FTS subsystem database to a consistent state by creating and initializing the appropriate files if they do not already exist. INITIALIZE_FTS then displays the current state of the FTS configuration. Use this command in the following circumstances:

- After installing or reinstalling the FTS subsystem database directory and before using the FTGEN commands to configure servers, queues, and sites.
- When you are attempting to recover from an invalid database, as described in Recovering From an Invalid Database, later in this chapter.

► HELP | | |----------| | SUBJECTS | | USAGE | | subject |

The HELP command displays information about the FTGEN command. To obtain a list of subjects for which help is available, enter:

OK, *HELP SUBJECTS*

For information on FTGEN's command syntax, enter:

OK, *HELP USAGE*

► STATUS

Abbreviation: ST

The STATUS command displays the current state of the FTS configuration, the number of servers, queues, and sites that are configured, and the FTS issue number.

Note

The FTS issue number is particularly important to Rev. 2 FTS sites because it must be configured with the ISSUE issue-no. site subcommand. Do not confuse the FTS issue number with the FTS revision number. For more information, refer to the description of the ISSUE command in Configuring File Transfer Sites, later in this chapter.

The STATUS command also checks the validity of the contents of the FTS subsystem database, and displays a message if the database is invalid.

Configuring File Transfer Servers

Use the following server commands to configure the FTS phantom server processes that service the local request queues and incoming remote requests. You can configure up to eight file transfer servers, each of which handles its own queue. Each queue must have a corresponding file transfer server. One file transfer server usually is sufficient for a site with average use.

<i>Server Command</i>	<i>Function</i>
ADD_SERVER	Adds a new server.
DELETE_SERVER	Deletes a server.
LIST_SERVER	Lists a server configuration.
MODIFY_SERVER	Modifies an existing server.

The ADD_SERVER and MODIFY_SERVER commands put you in the server subcommand environment. Server subcommands are described in the next section, Server Subcommands.

► ADD_SERVER server-name

Abbreviation: AS

The ADD_SERVER command adds a new server to the FTS configuration and places you in the server subcommand environment, where you can use server subcommands to set its configuration. The server name must conform to Prime filename syntax. If you attempt to add a server that is already included in the configuration, ADD_SERVER displays an error message.

► DELETE_SERVER server-name

Abbreviation: DS

The DELETE_SERVER command deletes a server from the configuration. You cannot delete a server while it is running.

**► LIST_SERVER { -ALL
server-name }**

Abbreviation: LS

The LIST_SERVER command displays the configuration of the specified file transfer server on your screen. To display the configurations of all file transfer servers, enter -ALL instead of a server name.

► MODIFY_SERVER server-name

Abbreviation: MS

The MODIFY_SERVER command allows you to modify the configuration of an existing server by placing you in the server subcommand environment, where you can use server subcommands. If the server does not exist, MODIFY_SERVER displays an error message. You cannot modify a server while it is running.

Server Subcommands

When you enter the ADD_SERVER or MODIFY_SERVER command to configure a file transfer server, you are placed in the server subcommand environment. The server subcommand prompt indicates your location:

```
server:
```

This section describes the server subcommands, which are summarized below. In the descriptions that follow, the term **current server** refers to the server that you are currently configuring, that is, the one you specified on the ADD_SERVER or MODIFY_SERVER command line.

<i>Server Subcommand</i>	<i>Function</i>
FILE	Files (saves) the server configuration on disk, then returns you to the FTGEN command level.
HELP	Displays help information.
LINKS	Sets the maximum number of simultaneous requests the server can handle.
LIST_SERVER	Displays the server configuration on your screen.
LOG	Names the server log file.

MAX_LOCAL_REQUESTS	Sets the maximum number of local requests that the server can handle.
MAX_REQ_RETRY	Sets the maximum number of transfer retries.
MESSAGE_LEVEL	Sets the server log message level.
PASSWORD	Defines the server password.
PORT	Sets the server port number.
PRIORITY	Sets the server process priority level.
PROGRAM	Provides the server program name.
QUEUE	Specifies the queue to be serviced.
QUIT	Returns you to the FTGEN command level.
REQ_RETRY_INTERVAL	Sets the interval between request retries.
SITE_RETRY_INTERVAL	Sets the interval between retries to sites that are down.
TIMESLICE	Sets the server process timeslice.

► **FILE**

The **FILE** subcommand files (saves) the server configuration on disk, then returns you to FTGEN command level. To return to the FTGEN command level without saving the configuration, enter the **QUIT** subcommand.

► **HELP** | | |-----------------| | SUBJECTS | | USAGE | | subject |

The **HELP** subcommand displays information about the FTGEN command. To display a list of subjects for which help is available, enter:

OK, **HELP SUBJECTS**

To display information on FTGEN command syntax, enter:

OK, **HELP USAGE**

► **LINKS number-of-links**

The **LINKS** subcommand specifies the total number of requests that the server can handle simultaneously. *number-of-links* must be in the range from 1 through 8. The default number of links is 8. The number of links specified affects the value of **MAX_LOCAL_REQUESTS**, which must be set to roughly half the value of **LINKS**. If you reduce the value of **LINKS**, thereby causing **MAX_LOCAL_REQUESTS** to exceed the maximum allowed, FTGEN displays a warning message and automatically adjusts the value of **MAX_LOCAL_REQUESTS**.

The relationship between valid values for LINKS and the maximum values for MAX_LOCAL_REQUESTS is illustrated below:

LINKS:	1 2 3 4 5 6 7 8
MLR maximum:	1 2 2 2 3 3 4 4

This subcommand is provided for tuning purposes only; there is no guarantee that reducing the number of LINKS will improve performance.

► LIST_SERVER

Abbreviations: LS, L

The LIST_SERVER subcommand displays the current server configuration on your screen. This allows you to display the configuration and its initial defaults when you are adding a new server. After modifying the configuration, use LIST_SERVER to check your work before saving the configuration with the FILE subcommand.

► LOG $\left\{ \begin{array}{l} \text{filename} \\ \text{OFF} \\ \text{-OFF} \end{array} \right\}$

The LOG subcommand specifies the name of the log file to be used by the current server. The server records events such as startup and shutdown messages in this log file, which resides in the FTSQ* directory. The MESSAGE_LEVEL subcommand specifies the level of detail to be used in the log file.

To disable server event logging, enter -OFF (or OFF) instead of a filename. The default is -OFF. However, when the server is started up with its log file disabled or unspecified, a file is created in the FTSQ*>COMO.FTS directory that records the server's startup and shutdown messages. This file is given the same name as the server.

If a log file is specified, these startup and shutdown messages are recorded only in the server's log file; the FTSQ*>COMO.FTS>server-name file is not created.

► MAX_LOCAL_REQUESTS value

Abbreviation: MLR

The MAX_LOCAL_REQUESTS subcommand specifies the maximum number of local requests that can be handled simultaneously by the FTS server. This value is related to the value given in the LINKS subcommand, which sets the maximum number of requests that the server can handle simultaneously. The MLR value cannot be more than roughly half the value of LINKS, as shown below:

LINKS:	1 2 3 4 5 6 7 8
MLR maximum:	1 2 2 2 3 3 4 4

Note that the value of MLR may be automatically adjusted if the value of LINKS is reduced.

This subcommand is provided for tuning purposes only; there is no guarantee that reducing the value of MLR will improve performance. We recommend that you always use the default values for MLR.

► **MAX_REQ_RETRY** count

Abbreviation: **MRR**

The **MAX_REQ_RETRY** subcommand specifies the maximum number of times that the FTS server retries certain types of failed requests. *count* must be in the range from 0 through 255. The default value is 144. If you specify 0, the FTS server does not retry requests. When the retry limit is reached for an individual request, it is put on hold. To release it, use the **RELEASE** option to **FTR**.

This subcommand does not affect requests that are never retried.

► **MESSAGE_LEVEL** { **NORMAL** **DETAILED** **STATISTICS** **TRACE** }

Abbreviation: **MSGL**

The **MESSAGE_LEVEL** subcommand specifies the level of information to be entered in the server log file that you request with the **LOG** subcommand. Each log message includes the number of the server link to which the message relates, and a number representing the message level at which the message is logged. For example,

```
10.17.24: [1.2] Remote file is <TSTDsk>RECEIVE>FILE1
```

refers to the request that was active on server link 1, and has been logged at the **DETAILED** log level (2).

You can specify the following levels of detail:

<i>Message Level</i>	<i>Abbreviation</i>	<i>Result</i>
1 NORMAL	NRM	Enters minimum details in the log; this is the default.
2 DETAILED	DET	Logs all events.
3 STATISTICS	STAT	Shows DETAILED information and STATISTICS .
4 TRACE	TRC	Shows DETAILED , STATISTICS , information.

► PASSWORD password

The PASSWORD subcommand specifies the password for the file transfer server. The password can be as many as 32 characters long and include the following characters:

a-z, A-Z, 0-9, #, \$, %, *, &

Remote file transfer requests that are addressed to a server that has a password must include its password to be accepted.

The FTS configuration files on the other nodes must include the identical server password along with the site address. The ADDRESS site subcommand enters a site address and its password into an FTS configuration file.

Uppercase or lowercase matching of the received server password and the password contained in the FTS configuration database for the server is not required between FTS Rev. 2 sites. However, case matching is required for transfers between FTS Rev. 1 and Rev. 2 sites.

Note

By default, servers do not use passwords. However, for file security purposes, we strongly recommend that you use passwords.

► PRIORITY $\left\{ \begin{array}{c} 0 \\ 1 \\ 2 \\ 3 \end{array} \right\}$

Abbreviation: **PR**

The PRIORITY subcommand sets the PRIMOS process priority level, which ranges from 0 through 3, for the current file transfer server. When the server is started, it is automatically assigned the priority set by this subcommand. The default, 1, is the value for a normal user process.

► PORT port-number

The PORT subcommand specifies the PRIMENET port at which the current server process awaits incoming requests passed off by YTSMAN, the FTS manager process. The legal values for *port-number* are 1 through 99; the default value is 1.

Caution

The port number you specify must not be used by any other active PRIMENET application. FTGEN does not check for uniqueness of port numbers.

► **PROGRAM filename**

The PROGRAM subcommand specifies the filename of the executable file for the current server. When the server is started, the program contained in this file becomes a phantom process. You must enter the full name of the executable file, including any suffix. The file you specify must reside in the FTSQ* directory. The default filename is the Prime-supplied server called FTP.SEG.

► **QUEUE queue-name**

The QUEUE subcommand names the queue that is to be serviced by the current server. There is no server default queue name; you must supply a unique name.

You must configure this queue with the ADD_QUEUE command, as described in Configuring File Transfer Queues, later in this chapter.

► **QUIT**

Abbreviation: Q

The QUIT subcommand terminates a server configuration session and returns you to the FTGEN command level without saving any of your changes on disk. To save a configuration session on disk, use the FILE subcommand.

► **REQ_RETRY_INTERVAL minutes**

Abbreviation: RRI

The REQ_RETRY_INTERVAL subcommand specifies the interval between retries for certain types of failed requests. The legal range of values is 0 through 60 (minutes), with a default value of 30 minutes.

If you specify 0, the FTS server retries failed requests immediately.

► **SITE_RETRY_INTERVAL minutes**

Abbreviation: SRI

The SITE_RETRY_INTERVAL subcommand specifies the interval between which FTS retries sending failed requests when the failure is caused because the remote site is not available. The legal range of values is 5 through 60 (minutes), with a default value of 30 minutes. Frequent retries may result in high costs over Packet Switching Data Networks (PSDNs).

► **TIMESLICE** *time-slice*

Abbreviation: TS

The **TIMESLICE** subcommand sets the timeslice for the current server process. When the server is started up, the timeslice you specify with this command is set automatically. The default is 20 (2 seconds).

Configuring File Transfer Queues

Use the following queue commands to configure the FTS queues, which store file transfer requests before they are forwarded by the server. You can configure as many as eight file transfer queues, each of which has its own file transfer server. The **ADD_SERVER** command adds and configures file transfer servers, as described in *Configuring File Transfer Servers*, earlier in this chapter.

<i>Queue Command</i>	<i>Function</i>
ADD_QUEUE	Adds a new queue.
BLOCK_QUEUE	Blocks submissions to a queue.
DELETE_QUEUE	Deletes a queue.
LIST_QUEUE	Lists a queue configuration.
MODIFY_QUEUE	Modifies an existing queue.
PURGE_QUEUE	Deletes all requests from a queue.
UNBLOCK_QUEUE	Unblocks a queue.

The **ADD_QUEUE** and **MODIFY_QUEUE** commands put you in the **QUEUE** subcommand environment. Queue subcommands are described in the next section.

► **ADD_QUEUE** *queue-name*

Abbreviation: AQ

The **ADD_QUEUE** command adds a new queue to your FTS configuration and places you in the queue subcommand environment, where you can use queue subcommands to define its configuration.

The queue name must conform to Prime filename syntax and cannot contain any full stop characters. If you attempt to add a queue that already exists, **ADD_QUEUE** displays an error message.

Note

You must use this command to add any queues that are named in a *server configuration*. The server-queue association is unique.

► **BLOCK_QUEUE queue-name**

Abbreviation: BQ

The BLOCK_QUEUE command blocks the queue you specify, preventing users from adding file transfer requests. Use the UNBLOCK_QUEUE command to unblock the queue.

► **DELETE_QUEUE queue-name**

Abbreviation: DQ

The DELETE_QUEUE command deletes the specified queue. You can delete a queue only when it is empty.

► **LIST_QUEUE { -ALL
queue-name }**

Abbreviation: LQ

The LIST_QUEUE command displays the configuration of the specified queue on your screen. To display the characteristics of all file transfer queues, enter -ALL instead of a queue name.

► **MODIFY_QUEUE queue-name**

Abbreviation: MQ

The MODIFY_QUEUE command allows you to modify an existing queue by placing you in the queue subcommand environment, where you can use queue subcommands to modify the queue's configuration. You cannot modify a queue while its file transfer server is running. If you try to modify a queue that does not exist in the FTS configuration, MODIFY_QUEUE displays an error message.

► **PURGE_QUEUE queue-name**

Abbreviation: PQ

The PURGE_QUEUE command deletes all the requests in the queue that the file transfer server is not currently processing.

► **UNBLOCK_QUEUE queue-name**

Abbreviation: UBQ

The UNBLOCK_QUEUE command unblocks the specified queue, allowing users to enter new requests.

Queue Subcommands

The `ADD_QUEUE` and `MODIFY_QUEUE` commands place you in the `QUEUE` subcommand environment, where you can use queue subcommands to configure the queue. The queue subcommand environment prompt, shown below, indicates your location:

queue :

This section describes the queue subcommands. The term **current queue** refers to the queue that you are currently configuring; that is, the queue you specified as an argument to the `ADD_QUEUE` or `MODIFY_QUEUE` command.

<i>Queue Subcommand</i>	<i>Function</i>
<code>BLOCK_QUEUE</code>	Blocks the queue.
<code>FILE</code>	Files (saves) the queue configuration on disk, then returns you to the <code>FTGEN</code> command level.
<code>HELP</code>	Displays help information.
<code>LIST_QUEUE</code>	Displays the queue configuration.
<code>LOG</code>	Sets the queue log file.
<code>MAXIMUM_REQUESTS</code>	Sets the maximum size of the queue.
<code>MESSAGE_LEVEL</code>	Sets the queue log message level.
<code>PRIORITY</code>	Sets the default priority of requests on the queue.
<code>QUIT</code>	Returns you to the <code>FTGEN</code> command level without saving your configuration changes on disk.
<code>UNBLOCK_QUEUE</code>	Unblocks the queue.

► `BLOCK_QUEUE`

Abbreviation: `BQ`

The `BLOCK_QUEUE` subcommand blocks the current queue, preventing users from adding new requests. Use the `UNBLOCK_QUEUE` command to unblock the queue.

► `FILE`

The `FILE` subcommand files (saves) the current queue configuration on disk, then returns you to `FTGEN` command level. To return to the `FTGEN` command level without saving the configuration, enter the `QUIT` subcommand.

► **HELP** $\left[\begin{array}{l} \text{SUBJECTS} \\ \text{USAGE} \\ \text{subject} \end{array} \right]$

The **HELP** subcommand displays information about the **FTGEN** command. To display a list of subjects for which help is available, enter:

OK, **HELP SUBJECTS**

To display information on **FTGEN** command syntax, enter:

OK, **HELP USAGE**

► **LIST_QUEUE**

Abbreviations: **LS**, **L**

The **LIST** subcommand displays the current queue configuration on your screen. This allows you to display the configuration and its initial defaults when you are adding a new queue. After modifying a queue configuration, use **LIST_QUEUE** to check your work before saving the configuration with the **FILE** subcommand.

► **LOG** $\left\{ \begin{array}{l} \text{filename} \\ \text{OFF} \\ \text{-OFF} \end{array} \right\}$

The **LOG** subcommand specifies the name of the log file to be used by the current queue. The queue records events such as startup and shutdown messages in this log file, which resides in the **FTSQ*** directory. The **MESSAGE_LEVEL** subcommand specifies the level of detail to be used in the log file.

To disable queue event logging, enter **-OFF** (or **OFF**) instead of a filename. The default is **-OFF**.

► **MAXIMUM_REQUESTS** number-of-requests

Abbreviation: **MAXR**

The **MAXIMUM_REQUESTS** subcommand specifies the maximum number of requests that can be held in the current queue. This subcommand is valid only when you are adding a new queue to the configuration with the **ADD_QUEUE** command. Once the queue is configured, you cannot modify the maximum number of requests. The default number of requests in a queue is 9999.

► **MESSAGE_LEVEL** {
 NORMAL
 DETAILED
 STATISTICS
 TRACE

Abbreviation: **MSGL**

The **MESSAGE_LEVEL** subcommand specifies the level of information to be entered in the queue log file that you request with the **LOG** subcommand. Each log message includes the number of the server link to which the message relates, and a number representing the message level at which the message is logged. For example,

10.17.24: [1.2] Remote file is <TSTDSK>RECEIVE>FILE1

refers to the request that was active on server link 1, and has been logged at the **DETAILED** log level (2).

You can specify the following levels of detail:

<i>Message Level</i>	<i>Abbreviation</i>	<i>Result</i>
1 NORMAL	NRM	Enters minimum details in the log; this is the default.
2 DETAILED	DET	Logs all events.
3 STATISTICS	STAT	Shows DETAILED information and STATISTICS .
4 TRACE	TRC	Shows DETAILED , STATISTICS , and TRACE information.

► **PRIORITY** value

Abbreviation: **PRI**

The **PRIORITY** subcommand specifies the default priority for the requests in the current queue; that is, the priority assigned to a request when the **-PRIORITY** option is not given on the **FTR** command line. *value* can be in the range from 0 through 7, with a default value of 0. The highest priority is 7 and the lowest is 1.

If you specify 0, the priority mechanism is disabled, causing the file transfer server to ignore all priority settings. Instead, the server handles requests in the order of submission. While the priority mechanism is disabled, a request to which the user does not assign a priority value is assigned a priority of 5. This ensures that a request to which the user did not assign priority is given a reasonable priority if the priority mechanism is subsequently re-enabled. Remember, however, that the file transfer server ignores all priority settings while the priority mechanism is disabled; priority values are still assigned to requests in case the mechanism is subsequently re-enabled.

It is not possible to set the default priority value to 8 or 9 because only the System Administrator is allowed to use those priority values when using FTR.

► QUIT

Abbreviation: Q

The QUIT subcommand terminates a server configuration session and returns you to the FTGEN command level without saving any of your changes on disk. To save a configuration session on disk, use the FILE subcommand.

► UNBLOCK_QUEUE

Abbreviation: UBQ

The UNBLOCK_QUEUE subcommand unblocks the current queue, allowing users to submit new requests. This is the default.

Configuring Local and Remote Sites

Use the following site commands to configure FTS sites. A site's configuration includes its PRIMENET node name or X.25 address(es), server passwords, and other information. Although you must configure the local site (on your node), you should also configure the remote sites that users on your node contact regularly. This provides a convenience to users on your node: when contacting a configured site, they need only include the site name on the command line. FTS retrieves the rest of the site information from the FTS configuration file, relieving users from the cumbersome task of including it all on the command line.

<i>Site Command</i>	<i>Function</i>
ADD_SITE	Adds a new site.
DELETE_SITE	Deletes a site.
LIST_SITE	Lists a site configuration.
MODIFY_SITE	Modifies a site.

The ADD_SITE and MODIFY_SITE commands put you in the site subcommand environment, which is described in Site Subcommands, later in this chapter.

► ADD_SITE site-name

Abbreviation: ASITE

The ADD_SITE command adds a new site to the FTS configuration and places you in the site subcommand environment, where you can define the site's configuration. For *site-name*, use the

node name that is entered in the PRIMENET configuration file created with CONFIG_NET. This should be the same name given by the SYSNAM CONFIG directive in the node's CONFIG file. If you attempt to add a site that already exists, ADD_SITE displays an error message.

Note

You must add your own local site in order for FTS to work. For example, if you are working from Node A, and you want to transfer files from Node B to Node C, you must add a site on Node A to the FTS configuration. For convenience, you should also configure sites for Nodes B and C.

► DELETE_SITE site-name

Abbreviation: **DSITE**

The DELETE_SITE command deletes the specified site name from the configuration.

► LIST_SITE { -ALL site-name }

Abbreviation: **LSITE**

The LIST_SITE command displays the configuration of the specified site on your screen. To display the configurations of all sites, specify -ALL instead of a site name.

► MODIFY_SITE site-name

Abbreviation: **MSITE**

The MODIFY_SITE command allows you to modify an existing site by placing you in the site subcommand environment, where you can use site subcommands to modify the site's configuration. If you attempt to modify a site that has not been added to the configuration file, MODIFY_SITE displays an error message.

Site Subcommands

The ADD_SITE and MODIFY_SITE commands place you in the site subcommand environment, where you can use site subcommands to modify a site's configuration. The site command environment prompt indicates your location:

site:

This section describes the site subcommands, which are summarized below. The term **current site** refers to the site you are currently configuring, that is, the one you specified on the **ADD_SITE** or **MODIFY_SITE** command line.

<i>Site Subcommand</i>	<i>Function</i>
ADDRESS	Defines the address of the current site.
FILE	Files (saves) the site configuration on disk, then returns you to the FTGEN command level.
HELP	Displays help information.
ISSUE	Defines the issue number of the FTS software.
LIST_SITE	Displays the site configuration.
LOG	Sets the site log file.
MESSAGE_LEVEL	Sets the site log message level.
QUEUE	Sets the default site queue.
QUIT	Returns you to the FTGEN command level without saving your configuration on disk.

► **ADDRESS address**

Abbreviation: **ADDR**

The **ADDRESS** subcommand specifies the address of a local or remote site. Site addresses have a maximum length of 128 characters and consist of two or three parts. The first part must be either the node's X.25 standard address or its PRIMENET node name. The PRIMENET node name is entered in the PRIMENET configuration file created with **CONFIG_NET**; it should be the same name that is given by the **SYSNAM CONFIG** directive in the node's **CONFIG** file. Use the node's X.25 standard address only if the node is not configured in the PRIMENET configuration file. The second part of a site address is a plus sign (+) followed by the server name. If the server at the address has a password, you must enclose it in parentheses and append it to the end of the address.

Note

Uppercase or lowercase matching of the received server password and the password contained in the FTS configuration database for the server is not required between FTS Rev. 2 sites. It is required for transfers between FTS Rev. 1 and Rev. 2 sites.

For example, **WILLOW+WEEP** is the node name **WILLOW** with the file transfer server name **WEEP**. If **WILLOW** was not configured in the PRIMENET configuration file, you would have to use its X.25 standard address: **311020400052+WEEP**. Using the first example, if the server **WEEP** had a password of **TEARS**, its address would be **WILLOW+WEEP(TEARS)**.

In the following example, the file **BRANCH** is being transferred to the file **LEAF** on the remote node **RIVER** (identified by the Destination Site option, **-DS**).

```
FTR BRANCH <TREE>LEAF -DS RIVER
```

or

```
FTR BRANCH <TREE>LEAF -DS :311020100059+WEEP
```

In the second case, the site **311020100059+WEEP** is the destination node's X.25 address, plus the name of its file transfer server. (If the destination site is not configured in the FTS configuration file, the request requires a **-QUEUE** specification.)

► FILE

The **FILE** subcommand files (saves) the current site configuration on disk, then returns you to **FTGEN** command level. To return to the **FTGEN** command level without saving the configuration, enter the **QUIT** subcommand.

► HELP | | |----------| | SUBJECTS | | USAGE | | subject |

The **HELP** subcommand displays information about the **FTGEN** command. To display a list of subjects for which help is available, enter:

```
OK, HELP SUBJECTS
```

To display information on **FTGEN** command syntax, enter:

```
OK, HELP USAGE
```

► ISSUE issue-no

The **ISSUE** subcommand defines the issue number of the FTS software installed at your site. (Do not confuse the FTS issue number with the FTS revision number.) The issue number is displayed when you first enter **FTGEN**, or in response to the **STATUS** command. The issue number of a remote site is displayed to the operator when a transfer is initiated and the local record of the remote site is incorrect. A warning message is output indicating the correct issue number for that site. Below is a table of currently released issues of FTS. You may have any earlier PRIMOS revision or FTS revision installed on your system.

<i>FTS Rev.</i>	<i>Issue Number</i>	<i>PRIMOS Rev.</i>	<i>Will Run On</i>
1.0	14	19.0	18.2 and above
1.0	15	18.4	18.2 and above
1.1	17	19.1, 19.2	19.0 and above
2.0	20	19.3	19.0 and above
2.0	21	19.4	19.0 and above

Note

To avoid file transfer failures on Rev. 1 sites, configure each site with an issue number that reflects the FTS revision.

► LIST_SITE

Abbreviations: LS, L

The LIST subcommand displays the current queue configuration on your screen. This allows you to display the configuration and its initial defaults when you are adding a new queue. At any other time, it allows you to check that the configuration is correct before saving it with the FILE subcommand.

► LOG

The LOG subcommand specifies the name of the log file to be used by the current site. All significant site events are recorded in this log file, which resides in the FTSQ* directory. The MESSAGE_LEVEL subcommand specifies the level of detail to be used in the log file.

To disable site event logging, enter -OFF (or OFF) instead of a filename. The default is -OFF.

► MESSAGE_LEVEL {
NORMAL
DETAILED
STATISTICS
TRACE
}

Abbreviation: MSGL

The MESSAGE_LEVEL subcommand specifies the level of information to be entered in the site log file that you request with the LOG subcommand. Each log message includes the number of the server link to which the message relates, and a number representing the message level at which the message is logged. For example,

```
10.17.24: [1.2] Remote file is <TSTDsk>RECEIVE>FILE1
```

refers to the request that was active on server link 1, and has been logged at the DETAILED log level (2).

You can specify the following levels of detail:

<i>Message Level</i>	<i>Abbreviation</i>	<i>Function</i>
1 NORMAL	NRM	Enters minimum details in the log; this is the default.
2 DETAILED	DET	Logs all events.
3 STATISTICS	STAT	Shows DETAILED information and STATISTICS.
4 TRACE	TRC	Shows DETAILED, STATISTICS, and TRACE information.

► **QUEUE queue-name**

The QUEUE subcommand associates a queue with the current site. The queue, and the server assigned to it, must be already added to the FTS configuration file. (For more information, refer to the descriptions of the ADD_SERVER and ADD_QUEUE commands.)

There is no default site queue. If you do not configure one, all FTR requests to this site must name a queue using the -QUEUE option.

► **QUIT**

Abbreviation: Q

The QUIT subcommand terminates a server configuration session and returns you to the FTGEN command level without saving any of your changes on disk. To save a configuration session on disk, use the FILE subcommand.

FTS Configuration Session

To configure FTS, use FTGEN. Log in as SYSTEM at the supervisor terminal. Type the following command (FTGEN responds with an FTGEN prompt).

OK, **FTGEN**

FTGEN>

To create a record of your configuration for future use, start a command output file (COMO) before running FTGEN. The following session shows how to use FTGEN on a system that has not yet been configured.

```
OK, COMO FTGEN.LIST
OK, FTGEN
[FTGEN rev 2.0]
FTS STATUS
-----
Server directory is ftsq*.
System issue number is 20.
The FTS data base is invalid. (status)
ftgen> INITIALIZE_FTS /* Initializes FTS on your system.*/
FTS STATUS
-----
Server directory is ftsq*.
System issue number is 20.
Number of queues configured is 0.
Number of servers configured is 0.
Number of sites configured is 0.
ftgen> ADD_SERVER SRV
server: PASSWORD PUBLIC
server: QUEUE FTS$1
server: MESSAGE_LEVEL TRACE
server: PROGRAM SRV.SEG
server: L
Server          : srv
Server Status   : Running.
Password        : Public
Queue           : fts$1
Log             : srv.log
Message_level   : trace
Program         : srv.seg
Port            : 1
Run Priority     : 1
Timeslice       : 20
Max. Req. Retry : 144
Req. Retry Int. : 30
Site Retry Int. : 30
Links           : 8
Max. Local Req. : 4
server: FILE
Server added.
ftgen> ADD_QUEUE FTS$1 /* Adds a single queue. */
queue: MAXIMUM_REQUESTS 200
queue: L
Queue           : fts$1
Queue status    : unblocked.
Log             : -OFF
Message_level   : normal
```

```
Maximum_requests : 200
Priority : 5
Current number of requests queued is 0
Current associated server is srv
queue: FILE
Queue added.
ftgen> ADD_SITE OAK /* Adds the local Rev. 2.0 */
site: ADDRESS OAK+SRV(PUBLIC) /* (Issue 20) source site. */
site: QUEUE FTS$1
site: L
Site : oak
Address : oak+srv(public)
Type : prime
Issue : 20
Queue : fts$1
Log : -OFF
Message_level : normal
Site up at : 83-11-02.09:53:23
site: FILE
Site added.
ftgen> ADD_SITE LINDEN /* Adds a remote Rev. 2.0 */
site: ADDRESS 311061700567+SRV /* (Issue 20) site. */
site: QUEUE FTS$1
site: L
Site : LINDEN
Address : 311061700567+srv
Type : prime
Issue : 20
Queue : fts$1
Log : -OFF
Message_level : normal
Site up at : 83-11-02.09:54:26
site: FILE
Site added.
ftgen> QUIT /* Exits you from the FTGEN utility. */
OK, COMO -E
```

Note

If you want to configure an FTS Rev. 1.0 (Issue 14) or 1.1 (Issue 17) site, you would use the above procedure specifying the appropriate issue number.

Recovering From an Invalid Database

This section describes how to recover from an invalid FTS database. FTS validates its own database. As long as FTS sees its database as valid, the file `VALID_SUBSYSTEM.FTS` exists in the `FTSQ*` directory. The `FTSQ*` directory is the run-time FTS directory. It contains the FTS configuration database and acts as the spool directory for FTS transfer requests. If the database becomes invalid for any reason, FTS deletes `VALID_SUBSYSTEM.FTS`.

If the FTS database does become invalid, there are four recovery procedures, each more drastic than the one before. Follow these steps to perform the first, mildest, recovery procedure:

1. Log in with the `SYSTEM` user ID.
2. Enter `FTGEN` to invoke the `FTGEN` utility.
3. Enter `INITIALIZE_FTS`.

If the preceding procedure does not recover the database, try the following procedure:

1. Enter `FTOP`.
2. Enter `FTOP -STOP_SRVR` to close down the file transfer servers.
3. Enter `FTOP -STOP_MNGR` to close down the FTS Manager phantom, `YTSMAN`.

If you are still unsuccessful, initialize FTS, then follow this procedure to check the validity of the database:

1. Enter `RESUME FTSQ*>INIT -WORLD_RESET`.
2. Enter `RESUME FTSQ*>HINIT`.
3. Enter `FTGEN`.
4. Enter `INITIALIZE_FTS`.

If the database is still invalid, follow this last, most drastic procedure:

1. Enter `ATTACH FTSQ*`.
2. Enter `DELETE @@.FTS -FILE -VERIFY`. Delete only the following files:

```
PROCESS_TABLE.FTS
QUEUE_CONFIG.FTS
SITE_CONFIG.FTS
NETWORK_INFORMATION.FTS
```

3. At the supervisor terminal, reshare FTS by entering the following commands:

```
COMI SYSTEM>FTS.SHARE.COMI
```

```
RESUME FTSQ*>INIT -RESET -SUBSYSTEM FTSQ*
```

RESUME FTSQ*>HINIT

FTGEN

INITIALIZE_FTS (in response to the FTGEN> prompt)

4. Use FTGEN to recreate the FTS configuration file.

Notes

Once FTS database recovery is complete, use the FTGEN commands `LSITE -ALL`, `LS -ALL`, and `LQ -ALL` to verify that the configuration is correctly restored.

The FTS database invalid message appears if you type the `STATUS` command at the beginning of an FTGEN initialize session. This is an incidental occurrence of the message; disregard it.

Shutting Down FTS

Perform the following procedure to shut down FTS:

1. Enter the `FTOP -STOP_SRVR` command or the `FTOP -ABND_SRVR` command to stop the FTS servers.
2. Enter the `FTOP -STOP_MNGR` command to stop YTSMAN.

Configuring NETLINK

The NETLINK Configuration File

The NETLINK Configuration file allows NETLINK's initial state as seen by a user to be tailored to the requirements of a particular system. For example, NETLINK's DNIC might be set to match the PSDN connected to the system.

You can create and edit the configuration file using a text editor such as EMACS. The file contains any NETLINK command and, in that sense works like a command input file. Each time NETLINK is invoked, it reads and executes the contents of the configuration file.

Use of a NETLINK Configuration file is optional. However, if a configuration file is used, it must be placed in PRIMENET*>NETLINK and must be named NETLINK.CONFIG.

In the example below, the configuration file defines two NETLINK profiles. The LAN profile is intended for use with local area networks (Ringnet and LAN300); it sets some timers and modes to get the best possible echo response over the network. The PSDN profile is intended for use with networks where there is a per-packet cost structure; it sets timers and modes to prevent transmission (and cost) of many small packets and sets the default case for connections to be "no reverse charging", a common requirement when connecting to hosts via a PSDN.

Lines beginning with /* are comment lines, and therefore are ignored by NETLINK.

```
/* Sample NETLINK Configuration file
/* Define a profile to be used with Ringnet and LAN300
mode remote_echo
poll 1
set 4:1
profile lan -save
/* Define a profile to be used with PSDNs
mode no_remote_echo
poll 5
set 4:10
fcty no_charge
profile psdn -save
```

When NETLINK is invoked, connections will be established using the profile defined last in the configuration file, in this case, the PSDN profile. If the user wants the LAN profile, he or she must simply enter the command PROFILE LAN.

Errors in the NETLINK Configuration File

Because the NETLINK Configuration file simply contains NETLINK commands, errors in those commands are handled the same way as if they were typed by the user; i.e. NETLINK error messages will be displayed on the user's terminal. The configuration file will continue to be read even if there is an error in a command.

For example, the following configuration file contains an error:

```
SET 4:1 50:1 5:1
DNIC 1234
```

Since there is no X.3 parameter 50, when NETLINK is invoked the results are

```
[NETLINK Rev 22.1 Copyright (c) 1988, Prime Computer, Inc.]
```

```
50:UNK
```

The error in the SET command is reported as "50:UNK". Using the PAR command to look at the values of the X.3 parameters and using the PROFILE command to look at the DNIC value, it can be seen that execution of the configuration file continues even if an error is found:

```
@ PAR
```

```
2: FULL DUPLEX
3: FORWARD DATA ON:  CR  ESC  Editing  Terminators  Form  Other
Cntrl
4: IDLE TIMER = 0.0 Sec.
7: ON BREAK: Interrupt  Send indication of break  Discard output
12: X-OFF/X-ON ENABLED

1:1 2:1 3:126 4:1 5:1 6:1 7:21 8:0 9:0 10:0 11:3 12:1 13:4 14:0 15:0
16:127
17:24 18:18 19:1 20:0 21:0 22:0
```

```
@ PROFILE
```

```
Profile BASE for next Connect ; loaded from library profile <none>
```

Operational Parameters

Debug: Off
Polling time: 0.5 Secs.
Escape Character: '@' Normal
Terminal type: Unknown
Terminal speed: 1200 bps
Parity: ASCII8
Prompt: '@'
Mode: CCITT

Connect parameters

Dnic: 1234
TO address: <none>
Port: <none>
Facilities: Reverse Charging
Protocol ID: 1 0 0 0 (decimal)
User Data: <none>

Appendices

CONFIG_NET Error Messages

This appendix lists the CONFIG_NET error messages in alphabetical order, along with an explanation and suggested response. Specific access names, names, network names, node names, or protocols are replaced by *access name*, *name*, *network name*, *node name*, and *protocol name* in this appendix. Error messages that begin with one of those designations are also listed in alphabetical order. For example, if you receive the message:

`SDLC is not a valid framing type.`

look for the following message in this listing:

`protocol name is not a valid framing type.`

A non-Prime node *node name* may not be attached to an HDX or Ring network.

You attempted to add a non-Prime node to an HDX or ring subnetwork. Nodes running non-PRIMENET X.25 software can be connected only to FDX lines, LAN300s, and PSDNs.

`access name is not a valid access right.`

The access right you entered is not valid. The valid access rights are NONE, RFA, RLOG, IPCF, and ALL.

`Address format is hex-pairs separated by dashes.`

You entered a MAC (+LSAP) address that is not in the correct format. MAC addresses must contain 12 hex digits in the format *nn-nn-nn-nn-nn-nn*. The Link Service Access Point (LSAP) address is optional; if used, it must be two hex digits appended to the MAC address by a plus sign (+): *nn-nn-nn-nn-nn-nn+nn*.

`Already in use.`

CONFIG_NET expected a new name, but you entered a name that is already in use in your network.

`An address must consist of 1 to 16 digits.`

You specified an address that was longer than 16 digits or contained non-decimal characters.

At least one *PSDN name* address MUST be specified.

You did not specify any PSDN addresses for nodes on that PSDN.

At least two nodes must be configured on a LAN300.

You tried to configure only one node on a LAN300.

At least two nodes must be configured on a ring.

You tried to configure only one node on a ring.

Configuration file *filename* is formatted incorrectly.

The file you specified on the command line was not generated by a compatible version of CONFIG_NET. CONFIG_NET displays this message if you attempt use a pre-Rev. 21.0 version of CONFIG_NET to edit a configuration file created or edited by a Rev. 21.0 version of CONFIG_NET.

CONFIG_NET cannot be re-started.

You cannot issue the START command to restart CONFIG_NET.

DSS Order must be a value between 0 and 7.

You tried to specify a value outside the stated range.

DSS Pattern must be a value between 0 and 15.

You tried to specify a value outside the stated range.

Duplicate or invalid LAP(B) address *address*.

You attempted to configure an LAP(B) address that is either already in the configuration or invalid. The legal values are 1 and 3.

Duplicate or invalid MAC address.

You attempted to configure a MAC address that is either already in the configuration or invalid. MAC addresses must contain 12 hex digits in the format *nn-nn-nn-nn-nn-nn*. A Link Service Access Point (LSAP) address is optional; if used, it must be two hex digits appended to the MAC address by a plus sign (+): *nn-nn-nn-nn-nn-nn+nn*.

Enter only 256, 512, or 1024.

When using option 6 of the Ring submenu, Set maximum frame size for a node on this ring, you entered an invalid frame size. The only valid frame sizes are 256, 512, and 1024.

First item only was taken for edit.

In Edit mode, you entered more than one value in response to a prompt. CONFIG_NET accepts only value at a time in Edit mode; it has accepted your first entry and ignored the others.

Gateway node *node name* cannot be running pre-Rev.-19.3 PRIMOS.

You tried to configure a node running pre-Rev. 19.3 PRIMENET as a gateway node. Gateway nodes must have Rev. 19.3 or later software.

Illegal number *number*.

You attempted to add alphabetic characters where numeric input is required.

Internal error in CONFIG_NET.

This is not a normal user error. Contact your System Administrator or representative from your Prime Customer Support Center.

Just one LAP(B) address, please.

You entered more than one LAP(B) address for a node. Nodes can have only one LAP(B) address.

Just one MAC(+LSAP) address, please.

You entered more than one MAC(+LSAP) address for a node. Nodes can have only one MAC(+LSAP) address.

LHC logical device number LHC*n* already configured on node *node name*.

The LHC300 logical device number you entered is already being used on *node name*.

LHC number must be between 0-7.

You attempted to add an LHC logical device number outside the stated range.

Line is already in use on node *node name*.

You tried to add an already configured line to *node name*. You cannot add a line that already exists.

Line number must be between 0-7.

You tried to configure a line number outside the stated range.

Maximum logical channel number must be between 1-4095.

You entered a value outside the stated range.

name is a network name, not a node name.

You specified a network name when a node name was requested.

name is not a known network name.

You tried to add a node to a network that is not included in the configuration.

name is not a network name.

The name you specified is not the name of one of the subnetworks in the configuration.

name is not a valid node name.

You specified an invalid name for a node, such as a number.

network name is not a network of type *subnetwork type*.

You specified a subnetwork that is the wrong type; for example, a ring subnetwork when CONFIG_NET expected a LAN300 subnetwork.

network name is the name of a different type of network.

You specified the name of one type of subnetwork when CONFIG_NET expected another type.

Network address *address* is in use for another node.

You tried to enter a network address that is already specified for another node.

Network name "*name*" cannot be longer than 32 chars.

You entered a network name with more than 32 characters.

Network name *name* contains characters other than alphanumeric and ". / _ \$ - # & " .

You entered a network name containing characters other than letters, numbers, and the seven special characters listed between the double quotes in the error message.

Network name *name* must begin with a letter.

You entered a network name beginning with a character other than a letter.

No help available

The HELP file that you requested is not in the PRIMENET* directory.

node name does not have any *network name* lines configured.

You tried to edit PSDN or FDX line information for a node that is not configured on a PSDN or FDX line. Use Edit mode to add the appropriate line information.

node name is already configured on *network name*.

The node you attempted to add is already configured on the subnetwork you are currently editing.

node name is not a configured node.

The node you specified is not included in the configuration file, or not configured on the subnetwork you are currently editing.

node name is not a node on *network name*.

The node you specified is not on the subnetwork you are currently editing.

Node ID *number* is already in use. Please select another.

You tried to configure a ring node ID that is already assigned to another node.

Node name "*name*" cannot be longer than 6 chars.

You entered a node name with more than six characters.

Node name "*name*" contains characters other than alphanumeric and "./_\$-#&".

You entered a node name containing characters other than letters, numbers, and the seven special characters listed between the double quotes in the error message.

Node name "*name*" must begin with a letter.

You entered a node name beginning with a character other than a letter.

Node *node name* does not have a ring node ID to change. Return to CREATE mode to be prompted for the new ID.

After adding *node name* to a ring in Edit mode, you attempted to change its ring node ID before assigning an ID in the first place. Transfer to CREATE mode; CONFIG_NET will prompt you for *node name*'s ring node ID.

Node *node name* has been configured to the maximum limit of networks of this type. Node *node name* will not be added.

You attempted to configure *node name* on more than one ring network, more than two LAN300 networks, more than eight FDX networks, or more than eight PSDNs. You cannot exceed these configuration limits.

Only one LHC number, please.

You attempted to enter more than one LHC300 number for a node on a LAN300. Nodes can be connected to a given LAN300 by only one LHC300 running PRIMENET.

Packet size must be between 16-256.

You tried to specify a value outside the stated range.

Password cannot be longer than 32 chars.

You entered a password with more than 32 characters.

Please enter a number from the menu only.

You specified an Edit menu option number that is not on the menu.

protocol name is not a valid framing type.

The framing type you entered is not valid. The valid framing types are HDLC, BSC-ASCII, and BSC-EBCDIC.

protocol name is not a valid protocol.

The protocol you entered is not valid. The valid protocols are LAP and LAP(B).

PSDN address *address* is in use for another node.

You tried to enter a PSDN address that is already specified for another node.

RFA is not enabled between nodes *node name1* and *node name2*.

You tried to edit the node-to-node password between two nodes that do not have RFA enabled. Node-to-node passwords can only be configured between nodes that have RFA enabled.

RFA is specified over two links between nodes *name1* and *name2*. Forced User Validation must be enabled/disabled over both.

In your network configuration, you connected *node name1* and *node name2* by two different links. Over one link, you specified RFA and answered YES to the Forced User Validation? prompt. Over the other link, you specified RFA and did not choose to force user validation. You must give the same answer to the Forced User Validation? prompt for both links. (A *link* may be a ring, a LAN300, a full-duplex line, a half-duplex line, a gateway connection, or a PSDN connection.)

Ring Node ID must be between 1-247.

You tried to configure a ring node ID outside the stated range.

Select either LAP or LAPB, please.

You entered a value other than LAP or LAP(B) as the protocol for a full-duplex line. LAP and LAP(B) are the only legal values.

Synchronous line is already in use on *node name*.

You attempted to add an already existing synchronous line between *node name* and a PSDN.

Too few nodes configured on this network.

You tried to configure a RINGNET or LAN300 with only one node. Such subnetworks must contain two or more nodes.

Too many options specified.

You entered more than one value in response to the option prompt. Enter only one of these responses: CREATE, EDIT, QUIT, SAVE, FAST_SAVE, LIST, or HELP.

Two nodes must be configured on each FDX Prime-to-Prime Line.

You tried to configure a Prime-to-Prime FDX line with only one node. Such lines must be connected to two nodes.

You should not specify access from a node to itself.

You tried to assign a node access to itself. Nodes can be assigned access only to other nodes.

name cannot be used as a node name. It is already in use.

name cannot be used as a node name because it is already being used as the name of a subnetwork.

node name is not a known node name.

You entered a node name that is not part of the configuration you are editing.

name cannot be used as a gateway node name. It is already in use.

name cannot be used as a gateway node name because it is already being used as a subnetwork name.

Two nodes must be configured on each FDX Prime-to-Prime line.

You assigned only one node to a full-duplex line, or you used the Node submenu to delete a node that was on an FDX line.

Too few nodes configured on this network.

You tried to configure a RINGNET or LAN300 with only one node. Such subnetworks must contain two or more nodes.

Too many options specified.

You entered more than one value in response to the option prompt. Enter only one of these responses: CREATE, EDIT, QUIT, SAVE, FAST_SAVE, LIST, or HELP.

The Maximum number of virtual circuits must be 1-900.

You tried to specify a value outside the stated range.

The *net. name* physical network has reached its maximum of *n* nodes.

Node *node name 1* will not be added.

.
.
.

Node *node name m* will not be added.

In this message, *name* is the name of a subnetwork (a ring, a LAN300, a full-duplex line, HDX, or a PSDN). You have attempted to configure too many nodes on the subnetwork. The maximum number of nodes per subnetwork is 247 for a ring, 256 for a LAN300, 2 for a full-duplex line, 9999 for HDX, or 9999 for a PSDN. Nodes *node name 1* through *node name m* will not be added to the subnetwork.

The *net. name* physical network has exceeded its maximum of *n* nodes. You must DELETE, using Edit Mode, one or more nodes to bring the node count down to the maximum node limit before continuing. List of nodes on *network name*:

node name1

.
.
.

node namem

In this message, *network name* is the name of a subnetwork (a ring, a LAN300, a full-duplex line, HDX, or a PSDN). You have attempted to configure too many nodes on the subnetwork. The maximum number of nodes per subnetwork is 247 for a ring, 256 for a LAN300, 2 for a full-duplex line, 9999 for HDX, or 9999 for a PSDN. Enter Edit mode again and delete nodes from the subnetwork until the subnetwork contains no more than the maximum number of nodes.

The PSDN name "*name*" cannot be longer than 32 chars.

You entered a PSDN name with more than 32 characters.

The PSDN name *name* contains characters other than alphanumeric and "./_\$-#&".

You entered a PSDN name containing characters other than letters, numbers, and the seven special characters listed between the double quotes in the error message.

The PSDN name *name* must begin with a letter.

You entered a PSDN name beginning with a character other than a letter.

There is currently no access configured between *node name1* and *node name2* over HDX.

You attempted to change HDX passwords between two nodes that do not have access rights configured between them.

This line already exists.

You entered the number of an existing line when a new line number was required.

This line does not exist.

You tried to edit a line number that is not configured.

This node does not have any lines configured for HDX. This option cannot be executed at this point.

You attempted to change a half-duplex line number on a system that has no half-duplex lines.

Too few nodes configured on this network.

You tried to configure a RINGNET or LAN300 with only one node. Such subnetworks must contain two or more nodes.

Too many options specified.

You entered more than one value in response to the option prompt. Enter only one of these responses: CREATE, EDIT, QUIT, SAVE, FAST_SAVE, LIST, or HELP.

Two nodes must be configured on each FDX Prime-to-Prime Line.

You tried to configure a Prime-to-Prime FDX line with only one node. Such lines must be connected to two nodes.

Unknown PSDN: *name*

The PSDN name you entered is unknown to CONFIG_NET. Valid PSDN names are TELENET, TYMNET, UNINET, DATAPAC, PSS, and X25.

Warning: Node *node name* is not configured on any networks.

You added *node name* to the configuration, but did not define it as connected to any other nodes via a ring, a LAN300, a full-duplex line, the half-duplex subnetwork, a PSDN, or a gateway connection.

Window size must be between 1-7.

You tried to specify a value outside the stated range.

You should not specify access from a node to itself.

You tried to assign a node access to itself. Nodes can be assigned access only to other nodes.

PRIMENET Glossary

This appendix contains a glossary of PRIMENET terminology.

Access Control List (ACL)

See ACL.

access right

For local PRIMOS operation, the degree of access that a user or process has to a file or directory. For example, the Read (R) access right allows someone to view a file. *See also* ACL.

When used in a node's PRIMENET configuration file, access rights describe the types of access local users have to each node on the network. These access rights are available: NONE, IPCF, RLOG, RFA, and ALL.

ACK

The acknowledgment character.

ACK byte

A byte in the trailer portion of a RINGNET data packet that is set by the PNC of the receiving node to acknowledge a successfully received message. It can also be set to indicate whether invalid data was seen by any active PNC, as described in the definition of parity check.

ACL

A list of access pairs that specify the access rights of users. An access pair has the form

`identifier:access`

where *identifier* is an individual user ID, an access group (beginning with a period), or the identifier \$REST, and *access* is one or more of the following rights:

- | | |
|---|---|
| O | Sets all access rights (except P and ALL) |
| P | Protect a directory |
| D | Delete entries from a directory |

A	Add entries to a directory
L	Read contents of a directory
U	Attach to a directory
R	Read contents of a file
W	Change contents of a file
X	Execute an Executable Program Format (EPF)
ALL	Allows all rights described above (OPDALURWX)
NONE	Allows no access rights whatsoever

An Access Control List (ACL) protects a file system object by allowing access only to the users listed in the ACL and by allowing those users only the access rights specified. The PRIMOS SET_ACCESS (SAC) and EDIT_ACCESS (EDAC) commands create or edit the ACL for a file system object. See the *Prime User's Guide* for more information on access control lists.

ADD_REMOTE_ID

See ARID.

ARID

ADD_REMOTE_ID, a command that allows a process or user to add a *remote ID* that is valid on the target node. This ID is remote in the sense that it must be listed in the System Administrator's Directory (SAD) of the target node. The user or process must use ARID when *forced user validation* is in effect between the nodes.

asynchronous communication

A method of transmitting data in which each character is preceded by a start bit and followed by a stop bit. The time interval between the characters varies.

asynchronous line

A line that carries asynchronous communication.

Binary Synchronous Communication (BSC)

A protocol and framing method supported by PRIMENET for synchronous lines. BSC framing can use either the ASCII or the EBCDIC character set.

bit

An acronym for binary digit. Eight bits constitute a byte.

broadcast packet

A ten-byte packet, periodically sent by a RINGNET node, that contains the ring node ID. This packet is received by all active PNCs on the RINGNET.

BSC

See Binary Synchronous Communication.

byte

Eight bits of data. A character, for example, is one byte.

cable segment

A 500-meter (maximum) segment of standard IEEE 802.3 50-ohm coaxial cable. Cable segments form the physical transmission medium for most LAN300 networks. (The LAN Multiport Transceiver 300, described below, provides a cableless LAN300.)

cache file

A file optionally created by START_NET that contains the PRIMENET configuration information that is pertinent to the local node. START_NET uses the cache file on subsequent startups, greatly speeding up PRIMENET initialization.

cascade

To attach an LTS300 or LMT300 to another unit of the same type, rather than directly to the LAN300. As many as four LTS300s can be cascaded from each other; LMT300s can be cascaded two deep.

CCITT

Consultative Committee for International Telephony and Telegraphy, an advisory committee established under the auspices of the United Nations to recommend standards for telephone systems and computer networks. X.25 is an example of a CCITT standard.

communication line

See communication link.

communication link

The physical transmission medium between two nodes that allows them to transmit and receive data. PRIMENET can run on the following types of communication links: RINGNET LANs, LAN300 LANs, PSDNs, and full-duplex and half-duplex synchronous lines. Two nodes can also be linked by one or more intervening gateway nodes.

CONFIG_NET

The PRIMENET configuration program, used to create or edit PRIMENET configuration files. Also the name of the command that invokes the program.

CONFIG_NTS

The NTS configuration program, used to create or edit NTS configuration files. Also the name of the command that invokes the program.

CRC

Cyclic Redundancy Check, a error check performed by a PNC on every data packet that it transceives on the RINGNET. If a packet fails this test, the PNC sets the ACK byte accordingly.

CSMA/CD

Carrier Sense Multiple Access with Collision Detection, the access method used to decide which station on a LAN300 takes control of the communication medium and transmits the next message.

Cyclic Redundancy Check

See CRC.

data field

The portion of a data packet that contains the actual data.

data packet

A packet that contains packet protocol and actual data. It consists of a leading frame, a header, a data field, and a trailing frame. The PRIMENET configuration file sets the maximum size of data packets.

Distributed Systems Management

See DSM.

downline load

The process of writing operational software into a device that cannot load (or boot) itself, usually because it lacks permanent storage capability.

DSM

Distributed Systems Management, a set of software products and services that support the administration and day-to-day management of single and networked Prime computer systems. DSM enables systems to be administered and controlled collectively from any convenient point on the network and simplifies administrative tasks such as resource monitoring and event logging.

event

A significant system or network occurrence such as a cold start, machine check, disk error, or network link problem.

FDX

See full-duplex.

File Transfer Generation

See FTGEN.

File Transfer Manager

See YTSMAN.

File Transfer Operator

See FTOP.

File Transfer Request

See FTR.

File Transfer Service (FTS)

A program that transfers files between PRIMENET nodes. Because FTS queues the files to be transferred, the target (or source) node need not be active when the request is made. FTS is comprised of the following utilities: FTR (File Transfer Request), FTGEN (File Transfer Generation), and FTOP (File Transfer Operator).

Forced User Validation

A security feature that forces a network user or process to use the ARID (ADD_REMOTE_ID) command to add a *remote ID* before accessing the target node. This ID is remote in the sense that it must be listed in the System Administrator's Directory (SAD) of the target node.

framing

The process of prefixing and suffixing a packet with control characters before sending it over the network. Framing corresponds to Level 2 in the OSI model. HDLC and BSC framing are supported by PRIMENET.

FTGEN

File Transfer Generation, an FTS utility used to configure the FTS database. FTGEN is described in the *PRIMENET Planning and Configuration Guide*.

FTOP

File Transfer Operator, an FTS utility used to monitor and control FTS. FTOP is described in the *Operator's Guide to Prime Networks*.

FTR

File Transfer Request, an FTS utility for submitting file transfer requests.

FTS

See File Transfer Service.

full-duplex

A type of synchronous communications in which both systems can send and receive signals simultaneously. For PRIMENET, full-duplex is used over permanently configured, dedicated connections (cables or leased telephone lines). Full-duplex lines can link a Prime node to another Prime node, a non-Prime node running X.25 1984, or a PSDN.

gateway

See gateway node.

gateway access

The access rights that users on a node have to another node that is indirectly connected (through a gateway node). Access rights between nodes are specified in the PRIMENET configuration file. For example, in the configuration illustrated in Figure A-1, Nodes A and C communicate through gateway Node B. The gateway access from Node A to Node C is IPCF; the gateway access from Node C to Node A is RLOG.

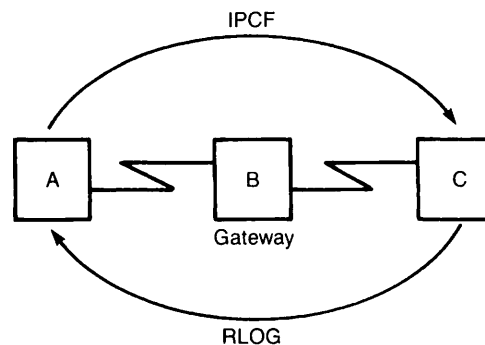


Figure G-1
Gateway Access

gateway node

A node configured to route messages between two other nodes, allowing them to communicate even though they are not directly connected. The Route-through Server phantom on the gateway node performs the routing function.

half-duplex

A type of synchronous communications in which data transfer occurs in only one direction at a time. Each system alternates between sending and receiving signals. For PRIMENET, half-duplex communication occurs over temporary connections, generally dialup telephone lines. PRIMENET supports only Prime-to-Prime half-duplex communications.

HDLC

High-level Data Link Control, a Level 2 (link level) protocol used on full-duplex lines. HDLC meets the CCITT X.25 standard and is supported and used by PRIMENET.

HDX node

A node with a half-duplex line.

header

The beginning portion of a packet that contains information such as the IDs of the source and destination nodes and the packet type.

host

A computer on a network. The word "host" is used because users connect to the system and use its resources as "guests," even though they are not directly attached.

ICS1, ICS2, ICS3

Intelligent Communications Subsystem, Model 1, 2, or 3; microprocessor-based communications controllers that manage asynchronous lines, synchronous lines, or both. The ICS1 and ICS2 support asynchronous communication lines, whereas the ICS3 supports synchronous and asynchronous lines concurrently. These lines can be configured to support a variety of protocols and electrical interfaces for communication with various terminals and controllers, other Prime computers, and computers of other manufacturers.

indirect address

The PSDN address of a node that is not directly connected to the PSDN, but instead connected to the PSDN through one or more gateway nodes.

Intelligent Communications Subsystem, Model 1, 2, 3

See ICS1, ICS2, ICS3.

International Organization for Standardization

See ISO.

Interprocess Communications Facility

See IPCF.

InterServer Communications

See ISC.

IPCF

A set of subroutines that permit applications to send and receive messages within a PRIMENET network, or to transfer messages between processes on the same system. Also, an access right (configured through CONFIG_NET) that enables systems to communicate using IPCF subroutines only.

ISC

InterServer Communications, a kernel facility that provides *sessions* through which any two PRIMOS servers can synchronize their operations and exchange messages. The servers can be on the same node or on different nodes across the network. (*See also* remote ISC.)

ISC Network Server

ISC_NETWORK_SERVER, a process that allows ISC servers to conduct sessions across a PRIMENET network.

ISO

An organization responsible for developing the Open Systems Interconnection (OSI) model, a seven-layered network architecture.

LAN

A network in which independent computer systems are physically connected and communicate at a high speed over a short distance, such as within a building. RINGNET is Prime's Local Area Network that uses a ring topology. LAN300 is Prime's IEEE 802.3 compliant LAN that uses a bus topology.

LAN Host Controller 300

See LHC300.

LAN Multiport Transceiver 300

See LMT300.

LAN Terminal Server 300

See LTS300.

LAN Transceiver 300

See LT300.

LAN300 Network Management Facility

A layer of software that provides service functions to the LAN300. These functions are LHC300 downline loading and upline dumping, LTS300 downline loading, upline dumping, error and event reporting, statistics gathering, status commands, and a diagnostic loopback capability.

LAN300

Prime's IEEE 802.3 compliant Local Area Network that uses a bus topology and the CSMA/CD access method. Most LAN300s consist of one or more 500-meter (maximum) segments of coaxial cable, joined by local or remote repeaters. (The LAN Multiport Transceiver 300, described below, provides a cableless LAN300.)

LAP

Link Access Procedure, a Level 2 (link level) protocol defined by X.25 and supported by PRIMENET.

LAPB

Link Access Procedure Balanced, a Level 2 (link level) protocol defined by X.25 and supported by PRIMENET.

LCN

The X.25 Logical Channel Number of a virtual circuit. When combined with the LCGN, forms the X.25 Virtual Circuit Number.

LCGN

The X.25 Logical Channel Group Number of a virtual circuit. When combined with the LCN, forms the X.25 Virtual Circuit Number.

leading frame

A bit pattern that indicates to the PNC that a data packet follows.

Level 1

In the OSI model, the hardware interface level. This level acts as an intermediary between the physical transmission medium and Level 2, the link level.

Level 2

The link level in the OSI model. Level 2 describes how each message should be framed before it is sent on the network.

Level 3

The packet (or network) level in the OSI model. Level 3 describes the format of packets that are sent on the network, handles error recovery, and controls the flow of data between processes on a pair of communicating nodes.

LHC300

LAN Host Controller 300, an intelligent controller that is inserted in the backplane of a 50 Series host. An LHC300 provides an interface between PRIMOS and a LAN300, thereby supporting PRIMENET, NTS, both products concurrently, or WSI300.

Link Access Procedure

See LAP.

Link Access Procedure Balanced

See LAPB.

LMT300

LAN Multiport Transceiver 300, a hardware component that provides network access for eight LHC300s or LTS300s. These devices are attached with transceiver cables. Since LMT300s can be cascaded two deep, as many as 64 nodes to be connected to the cable segment via the same MAU (64 LTS300s, cascaded four deep on each of the 16 LMT300 ports). This saves hardware costs when a large number of nodes are clustered in the same location.

LMT300s serve another purpose: they allow hosts and LTS300s to be connected into a network that does not contain a cable segment at all. Such a network is a cableless LAN300; its maximum size is also 64 LTS300s, as described above. LAN Multiport Transceiver 300s are also referred to as fanout units.

Local Area Network

See LAN.

local node

A node on a network from which a user issues commands to communicate with a remote node.

local repeater

A single microprocessor-based component that links two 500-meter (maximum) coaxial cable segments, making a LAN300 as long as 1000 meters. Local repeaters boost the signal, allowing longer LAN300s.

logical channel number

See LCN.

LT300

LAN Transceiver 300, a hardware component that provides network access for an LHC300 or an LTS300. The LT300 is attached to the cable segment by a MAU.

LTS300

LAN Terminal Server 300, a microprocessor-based terminal server that provides network access for eight asynchronous terminals or other asynchronous devices. An LTS300 can be connected to the LAN300 via a transceiver cable and a transceiver, or cascaded from another LTS300.

MAU

A small mechanism that pierces a LAN300 cable segment, creating an attachment point for a transceiver or a repeater. The MAU used by Prime is called nonintrusive because it has a piercing pin mechanism that merely pierces the cable segment rather than separating it. Also referred to as a tap.

MDLC

Multiline Data Link Controller, a communications controller that handles full-duplex and half-duplex synchronous lines.

multicast

To place a message on a LAN300 network without addressing it to a specific node. LTS300s multicast messages such as requests for downline loads of software.

Multiline Data Link Controller

See MDLC.

NAK

Negative Acknowledgment, a signal that indicates either that a RINGNET data packet failed a cyclical redundancy check (CRC), or that an ACK byte did not pass parity checking. When the node that sent the packet receives the NAK, it retransmits the data.

NETLINK

A PRIMENET utility that enables a user to gain access to another Prime node on a PRIMENET network or a non-Prime node across a PSDN. The non-Prime node must adhere to the CCITT PAD protocols (X.3/X.28/X.29).

NETMAN

The Network Manager, a process that handles PRIMENET activity. NETMAN appears on the STATUS USERS list as nsp (network server process).

Network Administrator

The person responsible for maintaining the proper and continuous operation of a network. Responsibilities include using CONFIG_NET to configure the network, ensuring that appropriate security measures are taken, and maintaining the daily network operation. Sometimes, the same person serves as Network Administrator and System Administrator. *See also* System Administrator.

Network Terminal Service

See NTS.

node

An independent computer system that is part of network.

node-to-node password

A password created with CONFIG_NET and used between two nodes communicating across PRIMENET. Once established, the node-to-node password is known only to the kernels of the communicating nodes; it is completely transparent to PRIMENET users.

NTS configuration

A description of the topology, addresses, and Network Management responsibilities in one or more LAN300 networks. This information is included in the NTS configuration file.

NTS configuration file

A segment directory that contains the NTS configuration in binary format. This file is created with CONFIG_NTS, the NTS configuration program, and loaded into an NTS host with the START_NTS command.

NTS

A software product that supports communications between 50 Series hosts and asynchronous devices (usually terminals) over a LAN300 network. The asynchronous devices are attached to LAN Terminal Server 300s instead of hosts.

packet

A sequence of data and control characters that are arranged in a specific format and sent across the network as a unit.

Packet Assembler/Disassembler

See PAD.

packet, broadcast

See broadcast packet.

packet, data

See data packet.

packet size

The number of bytes in a packet.

Packet Switching Data Network

See PSDN.

PAD

Packet Assembler/Disassembler, a hardware component that provides a number of functions for a cluster of terminals: controlling normal terminal operation, controlling normal X.25 circuit functions, passing characters from terminal to host over a virtual circuit, passing characters to terminal as they are received from host over virtual circuits, handling call clearing, and providing other functions using the X.3 recommendation. NETLINK emulates a PAD.

parity bit

A bit the value of which indicates whether an ACK is good or corrupt. On RINGNET, this bit is contained in the ACK byte that is sent by the PNC.

parity check

A check performed by a RINGNET PNC to determine whether the ACK byte for a data packet is good or corrupt. The PNC sets the parity bit in the ACK byte accordingly.

path

The sequence of intervening nodes between two nodes in a network.

PNC

PRIMENET Node Controller, hardware that controls ring protocol and the flow of data between nodes on a ring.

PNC II

PRIMENET Node Controller II, hardware that controls ring protocol and the flow of data between nodes on a ring.

PNCDIM

The PNC device interface module.

port

An address within a node to which an incoming network request can be routed. Each node in a PRIMENET network has a pool of available ports that a program running under PRIMOS can assign.

PRIMENET

Prime's X.25-based networking software that provides Remote Login service (RLOG), Remote File Access (RFA), File Transfer Service (FTS), NETLINK utility, and IPCF subroutines. PRIMENET runs on a number of physical transmission media: RINGNET LANs, LAN300 LANs, PSDNs, and synchronous lines.

PRIMENET address

A numeric address that PRIMENET uses internally to identify a node. CONFIG_NET automatically generates this address based on the name of the node.

PRIMENET Node Controller

See PNC.

PRIMENET Node Controller II

See PNC II.

protocol

A set of rules governing communication between two nodes in a network.

PSDN

Packet Switching Data Network, a wide area network in which the X.25 protocol defines communication between X.25-compatible equipment called Data Terminal Equipment (DTE) and processors called Data Circuit Termination Equipment (DCE). To transmit data, PSDNs divide long messages into shorter units with a fixed maximum length (packets). Examples of PSDNs include TELENET, UNINET, TYMNET, PSS or an equivalent private network.

PSDN address

A unique sequence of as many as 15 digits assigned by a PSDN to any node that is directly or indirectly connected. A two-digit subaddress indicates an indirect connection.

PSDN Administrator

The person employed by a PSDN to maintain the proper and continuous operation of the PSDN.

PSDN gateway

A communication link between two different PSDNs. Also referred to as an **X.25 gateway**.

Remote File Access

A PRIMENET service that enables a user to access files on a remote node as if the files were on the local node. RFA is the corresponding access right in the PRIMENET configuration file.

Remote ISC

InterServer Communications being used across a PRIMENET network, with the assistance of the ISC Network Server.

Remote Login

A PRIMENET service that enables users to log in to a remote node without first logging in to the local node. RLOG is the corresponding access right in the PRIMENET configuration file.

Remote naming

A security feature that allows the identity (user name, project, and groups) of a process running on one node to be communicated to another node. Remote naming is used by two Prime network services: Network Process Extension (NPX), which supports Remote File Access (RFA), and InterServer Communications (ISC). Both NPX and ISC use remote naming to check the identity of the user or process that is requesting their services across network.

remote node

A node that can communicate with the local node across a network.

remote repeater

Remote repeaters are used to join cable segments in a LAN300 network. A remote repeater, also called a fiber optic repeater, consists of two microprocessor-based components joined by a fiber optic cable that can be as long as 1000 meters. This fiber optic cable is also called a link segment; there can be no stations attached to it.

remote user

A user on a remote node.

RFA

See Remote File Access.

ring

See ring network.

ring network

A type of Local Area Network (LAN) where the cable is ring shaped. Prime's ring LAN, RINGNET, is a token-passing ring network.

ring node ID

A number from 1 through 247 that identifies, and is unique to, a particular node on a RINGNET network.

RINGNET

One of Prime's LANs for Prime-to-Prime communications. A RINGNET network contains Prime nodes connected by cable in a ring configuration. Each node is logically connected to all the other nodes on the ring. RINGNET uses a token-passing protocol to control communication around the ring.

RLOG

See Remote Login.

Route-through

The message routing operation performed on a gateway node that connects two nodes or networks.

Route-through Server

RT_SERVER, the server that performs route-through, enabling a node to serve as a gateway node for communication between nodes that are not directly connected.

server

A process or cooperating set of processes available to perform one or more functions. FTS servers service local request queues and incoming requests from remote systems. ISC servers exchange messages between themselves, either locally or across the network.

slave process

A process on a local node that handles a request initiated by a user on remote node to access files or to attach to a directory on the local node. A slave acts for a single remote user until the remote user releases the slave process. The number of slave processes available is set by the System Administrator in the local node's CONFIG file.

SMLCnn

The logical line number of a synchronous communication line on a Prime node.

START_DSM

Command that starts up Distributed Systems Management (DSM) on a local system without interrupting PRIMOS operation.

START_NET

Command that starts PRIMENET on a local system without interrupting PRIMOS operation.

START_NTS

Command that starts NTS on a local system without interrupting PRIMOS operation.

station

A point on a LAN300 at which a controller, transceiver, and MAU are attached to a cable segment.

STOP_DSM

Command that shuts down Distributed Systems Management (DSM) on a local system by logging out all DSM server processes. This command does not interrupt PRIMOS operation.

STOP_NET

Command that shuts down PRIMENET on a local system without interrupting PRIMOS operation.

STOP_NTS

Command that shuts down NTS on a local system without interrupting PRIMOS operation.

System Administrator

The person responsible for maintaining the proper and continuous operation of a system. The System Administrator's duties can include network-related tasks such as setting PRIMENET-related ACL rights and setting up File Transfer Service (FTS). The same person may serve as both the System Administrator and the Network Administrator. *See also* Network Administrator.

timeout

The condition that occurs when a transmitting RINGNET node sees neither a token nor the packet within a certain time period. A break in the ring or token recovery can cause a timeout. The node waits for a token and retransmits the packet. If a second timeout occurs for the same packet, no further attempt to retransmit is made.

token recovery

The mechanism PRIMENET uses to replace a lost RINGNET token.

token ring protocol

The communications protocol used by RINGNET. The token, a special bit pattern, circulates continuously around the ring. A node cannot transmit data until it detects the token.

trailer

The portion of the ring packet that contains information such as the ACK byte and the trailing frame.

trailing frame

A special bit pattern that indicates to the PRIMENET Node Controller (PNC) that the end of the data packet has been reached.

transceiver

A device that receives and transmits data simultaneously. LT300 and LMT300 transceivers provide LAN300 network access for LTS300s and LHC300s. The PRIMENET Node Controller (PNC) is a transceiver that uses a four-bit time delay between reception and transmission of data.

transceiver cable

A cable that connects an LHC300 or an LTS300 to a transceiver.

user validation

The process of checking a remote user's ID before allowing that user to access information on a node. The user must have established the remote ID with the ADD_REMOTE_ID (ARID) command.

virtual circuit

A logical network connection that enables transmission of data between two processes. IPCF subroutines are used to establish virtual circuits in PRIMENET. PRIMENET supports 900 virtual circuits.

WACK

Wait Acknowledge, a signal that indicates that a receiving RINGNET node acknowledges the packet, but does not have a buffer free to receive it. The transmitting node retransmits the packet.

window size

The maximum number of frames or packets that can be sent before an acknowledgment must be received.

X.3

A CCITT recommendation entitled "Packet Assembly/Disassembly Facility in a Public Data Network." X.3 outlines the procedures for packet assembly/disassembly for asynchronous transmissions.

X.25

A CCITT recommendation entitled "Interface Between Data Terminal Equipment (DTE) and Data Circuit Terminating Equipment (DCE) for Terminals Operating in the Packet Mode and Connected to Public Data Networks by Dedicated Circuit." The X.25 recommendation and the X.25 protocol, based on the recommendation, define communication between X.25-compatible equipment called Data Termination Equipment (DTE) and processors called Data Circuit Termination Equipment (DCE) in a PSDN.

X.28

A CCITT recommendation entitled "DTE/DCE Interface for a Start-Stop Mode Data Terminal Equipment Accessing the Packet Assembly/Disassembly Facility (PAD) in a Public Data Network Situated in the Same Country." The X.28 recommendation describes the interfacing procedures that enable an asynchronous terminal to be connected to a PAD.

X.29

A CCITT recommendation entitled "Procedures for the Exchange of Control Information and User Data Between Assembly/Disassembly Facility (PAD) and a Packet Mode DTE or Another PAD." The X.29 recommendation describes the interfacing procedures that enable a PAD to communicate with an X.25 network.

X.121

A CCITT recommendation entitled "International Numbering Plan for Public Data Networks." The X.121 recommendation describes an addressing scheme, supported by NETLINK, to uniquely identify computer systems within PSDNs.

YTSMAN

Yellowbook Transfer Server Manager. File Transfer Service (FTS) requires a minimum of two phantom processes. One phantom is for YTSMAN, the File Transfer Manager, and one phantom is for a file transfer server. YTSMAN manages requests from the file transfer server to and from PRIMENET.

Index

A

Access rights

- ALL, 3-4
- CONFIG_NET prompts, 6-17
- editing with CONFIG_NET, 6-46
- example of CONFIG_NET dialog to set, 3-6
- FTS-related, 3-3, 10-2
- gateway access editing strategy, 6-51
- IPCF, 3-3
- NETLINK-related, 3-3
- NONE, 3-3
- non-Prime nodes, 3-6
- RFA, 3-4
- RFA-related, 3-10
- RLOG, 3-4
- specifying with CONFIG_NET, 3-4
- symmetry requirements, 3-6

ACLs

- for LAN300 Network Management Facility, 2-4
- for Network Administrator, 2-3
- for RT_SERVER, 2-3
- for YTSMAN, 2-4
- FTS-related, 2-4
- ISC-related, 2-4
- PRIMENET-related, 2-2
- summarized, 2-5

Active mode, 1-10

Adding objects to a configuration, 6-43

ADDISK command, 1-3, 9-3 to 9-4

ADD_QUEUE, FTGEN subcommand, 10-13

ADD_REMOTE_ID command, 3-9, 3-11

Addresses

- compatibility, 4-12
- CONFIG_NET-generated, 4-8, 4-10
- editing with CONFIG_NET, 6-49
- FDX, 4-9, 6-23
- for mixed-Rev. networks, 4-10
- indirect FDX, 4-10
- indirect LAN300, 4-8

LAN300, 6-23

LAPB, 4-10

Level 2, 4-8, 4-10

Level 3, 4-8 to 4-9

link level, 4-8

LSAP, 4-8

MAC, 4-8

multiple, 4-11

non-Prime nodes, 4-8, 4-10, 6-24

null, 4-8, 4-10

packet level, 4-9

PRIMENET, 4-11

PSDN, 4-6, 4-11

summarized, 4-6

ADD_SERVER, FTGEN

subcommand, 10-6

ADD_SITE, FTGEN subcommand, 10-18

ALL access right, 3-4

ARID command, 3-9, 3-11

B

BLOCK_QUEUE, FTGEN

subcommand, 10-14

BSC framing protocol, 1-10

BSC-ASCII protocol, 6-13, 6-15

BSC-EBCDIC protocol, 6-13, 6-15

Buffer sizes, displaying with LAB, 9-6

Buffers

for non-Prime nodes, 8-5, 9-7

for PSDN lines, 8-5, 9-7

for RINGNET, 8-5, 9-7

remote, 6-16, 6-27, 8-4, 9-5

setting with CAB, 9-5

C

CAB command, 9-5

Cables

coaxial, 1-7

fiber optic, 1-6

twin-axial, 1-5

Call Request packets, 4-8 to 4-9

Cascade, 1-7

CCITT, 1-3

Channel number, logical, 6-15, 6-26

Checklist, configuration, 5-9

Coaxial cables, 1-7

Cold start, 9-1

COMDEV pack, 2-1

Commands

ADDISK, 1-3, 9-3 to 9-4

ADD_REMOTE_ID, 3-9, 3-11

ARID, 3-9, 3-11

CAB, 9-5

COMM_CONTROLLER, 9-1

CONFIG_NET, 6-2

CONFIG_NTS, 1-6

CONFIG_UM, 2-5

COPY, 1-4

EDIT_PROFILE, 3-2, 3-10

FTOP, 10-1 to 10-2

LAB, 9-6

LIST_COMM_CONTROLLERS, 8-2

LIST_SYSTEM_SERVERS, 8-3

LOGIN, 1-1

START_DSM, 9-1

START_NET, 9-3

START_NTS, 9-3

STAT COMM, 8-2

STAT US, 8-3

COMM_CONTROLLER command, 9-1

Communications lines, 1-4

Compatibility address, 4-12

CONFIG directives

LHC, 8-2

NPUSR, 8-2

NRUSR, 8-3

NSLUSR, 1-3, 3-10, 8-4

REMBUF, 8-4

summarized, 8-1

SYNC CNTRLR, 8-6

SYSNAM, 1-6

CONFIG file, 8-1

CONFIG_NET

access rights prompts, 6-17

adding a new node, 6-44

adding a non-Prime node, 6-44

adding a PSDN address, 6-45

adding a subnetwork, 6-45

CONFIG_NET (continued)

- adding gateway nodes or access, 6-45
- adding half-duplex line, 6-45
- adding objects, 6-43
- address generation, 4-8
- address prompts, 6-22
- addresses, 4-6
- automatic address generation, 4-10
- command format, 6-2
- contrasted with NETCFG, 4-5
- Create mode, 6-3
- CREATE selection, 6-5
- displaying a configuration, 6-54
- displaying help text, 6-2
- Edit mode, 6-3, 6-27
- EDIT selection, 6-29
- error indications, 6-4
- FAST_SAVE selection, 6-55
- forced user validation prompt, 6-18
- full-duplex prompts, 6-8, 6-12
- gateway access prompts, 6-20
- gateway prompts, 6-10
- half-duplex prompts, 6-8, 6-13
- Help facility, 6-3
- Help mode, 6-2
- invoking, 6-2
- LAN300 prompts, 6-7, 6-12
- List facility, 6-3, 6-54
- mode selection, 6-2
- modes of operation, 6-3
- node prompts, 6-11
- node prompts, universal, 6-16
- node-to-node password prompt, 6-19
- non-Prime node prompts, 6-10, 6-24
- option prompt, 6-2
- password generation, 6-14
- pre-Rev. 19.3 node prompts, 6-10, 6-24
- prompts, 6-5
- PSDN prompts, 6-9, 6-14
- QUIT selection, 6-56
- quitting, 6-56
- revision compatibility, 4-3
- RINGNET prompts, 6-7, 6-12
- SAVE selection, 6-55
- saving a configuration quickly, 6-55

- saving and validating a configuration, 6-55
- terminating, 6-56
- user validation prompts, 6-18
- validating a configuration, 6-55
- validation, 6-4, 6-55
- verification, 6-4

CONFIG_NTS program, 1-6**CONFIG_UM program, 2-5****Configuration**

- adding objects, 6-43
- checklist, 5-9
- creating, 6-5
- defined, 4-1
- deleting objects from, 6-49
- displaying with CONFIG_NET, 6-54
- editing, 6-27
- examples, 5-1, 7-2
- global, 4-2
- inconsistencies, 4-2
- indicating unknown information, 4-4
- listing examples, 7-108
- modification strategy, 6-45
- multiple, 4-2
- NTS, 1-6
- saving and validating, 6-55
- saving quickly, 6-55
- validating, 6-55

Configuration file

- changing the active file, 4-5
- described, 4-1
- guidelines for using multiple files, 4-5
- pre-Rev. 19.3 files, 4-5
- reasons for different files, 4-3
- reasons for identical files, 4-2

Configuring, PRIMENET, 4-1**Controllers**

- ICS, 9-1
- ICS2, 8-6
- ICS3, 1-11, 8-6
- LHC300, 1-7, 8-2, 9-1
- loading software into, 9-1
- maximums for a host, 1-9
- MDLC, 1-11
- PNC, 1-6

COPY command, 1-4

- CREATE, CONFIG_NET selection, 6-5

Create mode

- described, 6-3
- examples, 7-2
- explained, 6-5
- prompts, 6-5

D**Data Communications Equipment (DCE), 4-10, 6-27****Data Set Status, editing with CONFIG_NET, 6-52****Data Terminal Equipment (DTE), 4-10, 6-27****Database**

- FTS, 10-26
- PRIMENET, 4-2

DCE, 4-10, 6-27**Default packet size, 8-5, 9-7**

- non-Prime nodes, 6-26

PSDNs, 6-15**Default window size, 8-5, 9-7**

- non-Prime nodes, 6-26

PSDNs, 6-15**DELETE_QUEUE, FTGEN subcommand, 10-14****DELETE_SERVER, FTGEN subcommand, 10-7****DELETE_SITE, FTGEN subcommand, 10-19****Deleting objects from a configuration, 6-49****Dialup lines, 1-10**

- contrasted with half-duplex lines, 3-16

- security considerations, 3-14

Disks, remote, 9-3**Displaying a configuration, 6-54****Distributed Systems Management see: DSM****DLL.LOG file, 2-5****DOWN_LINE_LOAD* directory, 9-2****DP8880/2 protocol, 1-7****DSM**

- configuring for LAN300 Network Management, 2-5

- log file, 2-2

- remote, 9-3

- starting, 9-1

- Unsolicited Message facility, 2-5

DSM* directory, contents, 2-2
 DSM.SHARE.COMI command file,
 9-1
 DSS interrupts, 6-52
 DTE, 4-10, 6-27

E

EDIT, CONFIG_NET selection, 6-29

Edit mode

access rights editing, 6-46
 adding objects, 6-43
 address modification, 6-49
 deleting objects, strategy for, 6-49
 described, 6-3, 6-27
 DSS interrupts editing, 6-52
 entering, 6-29
 examples, 7-70
 full-duplex protocol editing, 6-47
 full-duplex submenu, 6-35
 gateway access editing, 6-51
 gateway nodes or access addition,
 6-45
 half-duplex editing, 6-42
 half-duplex line addition, 6-45
 half-duplex line number editing,
 6-48
 half-duplex submenu, 6-39
 help information, 6-30
 LAN300 submenu, 6-42
 LHC300 editing, 6-48
 main Edit menu, 6-29
 menus, 6-29
 node addition, 6-44
 node deletion, 6-50
 node submenu, 6-31
 non-Prime node addition, 6-44
 non-Prime node indication, 6-48
 password editing, 6-47
 PSDN address addition, 6-45
 PSDN logical line editing, 6-48
 PSDN submenu, 6-37
 RINGNET submenu, 6-33
 ring node ID editing, 6-47
 subnetwork addition, 6-45
 subnetwork deletion, 6-50
 version number considerations,
 6-29
 virtual circuit maximum editing,
 6-49

Editing a configuration
 examples, 7-70
 procedure, 6-27
 EDIT_PROFILE command, 3-2, 3-10
 Error detection, CONFIG_NET, 6-4
 Event messages, 2-5
 Examples
 Create mode, 7-2
 Edit mode, 7-70
 List mode, 7-108
 External login programs, 3-2

F

Fanout unit, 1-7
 Fast select calls, 1-13
 FAST_SAVE selection, 6-55
 FDX
 see: Full-duplex
 Fiber optic cable, 1-6
 File transfer servers
 configuration, 10-6
 described, 10-1
 IDs, 10-2
 remote server information, 10-1
 File Transfer Service
 see: FTS
 Forced User Validation
 CONFIG_NET prompt, 6-18
 described, 3-9, 3-11
 Frame size, RINGNET, 6-54
 Framing protocol prompt, 6-13
 Framing type, prompt for PSDNs,
 6-15
 FTGEN program
 command categories, 10-3
 described, 10-1
 subcommand environment, 10-4
 FTGEN subcommands
 ADD_QUEUE, 10-13
 ADD_SERVER, 10-6
 ADD_SITE, 10-18
 BLOCK_QUEUE, 10-14
 DELETE_QUEUE, 10-14
 DELETE_SERVER, 10-7
 DELETE_SITE, 10-19
 HELP, 10-5
 INITIALIZE_FTS, 10-5
 LIST_QUEUE, 10-14
 LIST_SERVER, 10-7

LIST_SITE, 10-19
 MODIFY_QUEUE, 10-14
 MODIFY_SITE, 10-19
 PURGE_QUEUE, 10-14
 STATUS, 10-6
 UNBLOCK_QUEUE, 10-14
 FTOP command, 10-1 to 10-2
 FTP program, 8-3
 FTS
 access rights required, 3-3, 10-2
 ACL settings, 2-4
 advantage over COPY command,
 1-4
 configuration session example,
 10-23
 configuring servers, 10-6
 database, 10-3, 10-26
 described, 1-4
 installation procedure, 2-1
 log files, 10-3
 phantoms required, 8-3
 queue configuration, 10-13
 recovering from an invalid
 database, 10-26
 shutting down, 10-27
 site configuration, 10-18
 terminating, 10-27
 FTS.INSTALL.COMI, 2-1
 FTSQ* directory
 access rights required, 10-2
 contents, 2-2
 installation, 2-1
 size, 10-3
 Full-duplex
 address prompts, 6-23
 addresses, 4-9
 CONFIG_NET prompts, 6-8, 6-12
 configuration checklist, 5-11
 described, 1-9
 Edit mode submenu, 6-35
 editing with CONFIG_NET, 6-47
 framing protocol prompt, 6-13
 indirect addresses, 4-10
 names, 6-8
 protocol prompt, 6-13
 synchronous line number prompt,
 6-12

G

Gateway

- access rights editing strategy, 6-51
 - access rights prompts, 6-20
 - adding gateway nodes or access, 6-45
 - CONFIG_NET prompts, 6-10
 - connection, 1-12
 - guidelines, 1-13
 - node, 1-12
 - PSDN, 4-4
 - security considerations, 3-14
- Gateway node, 9-3
- Global configuration, 4-2

H

Half-duplex

- adding a line, 6-45
- CONFIG_NET prompts, 6-8, 6-13
- configuration checklist, 5-12
- editing with CONFIG_NET, 6-48
- Edit mode submenu, 6-39
- passwords, 3-13

Half-duplex lines, described, 1-10

Half-duplex nodes, 1-10

Half-duplex subnetwork, 1-11

HDLC protocol, 1-10, 6-13, 6-15

HDX

see: Half-duplex

-HELP, CONFIG_NET option, 6-2

Help facility, CONFIG_NET, 6-3

HELP, FTGEN subcommand, 10-5

Help information

- displaying CONFIG_NET command syntax, 6-2
- displaying help text within CONFIG_NET, 6-2

I

ICS controller, 9-1

ICS1 controller, 6-13

ICS2 controller, 8-6

ICS3 controller, 1-11, 8-6

IDs

- File transfer servers, 10-2
- local, 3-9
- NPX slave, 3-10

remote, 3-9

ring node, 1-6, 6-12

IEEE 802.3 LAN, 1-6

Indirect LAN300 addresses, 4-8

INITIALIZE_FTS, FTGEN subcommand, 10-5

Installation procedures

File Transfer Service, 2-1

LAN300 Network Management

Facility, 2-1

PRIMENET, 2-1

Intelligent Communications

Subsystem 3 (ICS3), 1-11

International communications, 1-12

Interprocess Communications Facility (IPCF), 1-4

Interserver Communications

see: ISC

Invoking CONFIG_NET, 6-2

IPCF, 1-4

IPCF access right, 3-3

ISC, 3-3

ACL settings required, 2-4

remote, 3-7, 9-3

remote naming use, 3-7

servers, 9-3

ISC_NETWORK_SERVER, 2-1, 9-3

ISCNSR.CPL file, 2-1

ISO 8881 procedures, 6-27

ISO DP8880/2 protocol, 1-7

L

LAB command, 9-6

LAN Host Controller 300

see: LHC300

LAN Terminal Server 300 (LTS300), 1-7

LAN300

address prompts, 6-23

cableless, 1-7

CONFIG_NET prompts, 6-7, 6-12

configuration checklist, 5-11

configuration guidelines, 1-7

described, 1-6

Edit mode submenu, 6-42

indirect addresses, 4-8

maximum number of nodes, 6-8

multiple configurations, 1-9

names, 6-7

topology, 1-6

topology guidelines, 1-7

LAN300 Network Management Facility

ACL group, 2-4

CONFIG_UM program, 2-5

described, 1-6

directory, 2-5

DSM Configuration for, 2-5

event messages, 2-5

installation, 2-1

phantoms required, 8-3

startup, 9-3

LANs

IEEE 802.3 (LAN300), 1-6

maximums for a host, 1-8

RINGNET, 1-5

LAP protocol, 6-15

LAPB address, 4-10

LAPB protocol, 6-13, 6-15

Level 2 addresses, 4-8

Level 3 addresses, 4-8 to 4-9

LHC CONFIG directive, 8-2

LHC300

CONFIG_NET prompt, 6-12

described, 1-7

editing with CONFIG_NET, 6-48

logical device number, 6-12

maximums for a host, 1-9

WSI300 requirements, 1-9

LHC300 controller, 8-2, 9-1

LHC_DLL_SERVER phantom, 8-3

LHC_ULD_SERVER phantom, 8-3

Lines, communications, 1-4

Link Access Protocol Balanced

(LAPB), 6-13

Link Access Protocol Balanced

(LAPB) address, 4-10

Link Service Access Point (LSAP)

address, 1-7, 4-8

LIST, CONFIG_NET selection, 6-54

List facility, CONFIG_NET, 6-3, 6-54

List mode

described, 6-54

examples, 7-108

LIST_COMM_CONTROLLERS

command, 8-2

LIST_QUEUE, FTGEN

subcommand, 10-14

LIST_SERVER, FTGEN
 subcommand, 10-7
 LIST_SERVER_NAMES command,
 8-3
 LIST_SITE, FTGEN subcommand,
 10-19
 LLC2 protocol, 1-7
 LMT300 Multiport Transceiver, 1-7
 Local Area Networks (LANs)
 IEEE 802.3, 1-6
 LAN300, 1-6
 maximums for a host, 1-8
 RINGNET, 1-5
 Local disks, 9-1
 Local ID, 3-9
 Local repeater, 1-6
 Log file, 2-2
 Logical channel number, 6-15, 6-26
 LOGIN command, 1-1
 Login programs, external, 3-2
 LOGIN_SERVER, 8-3
 Logs, DSM, 2-5
 Loopback, 1-6
 LSAP address, 1-7, 4-8
 LTS300, 1-7
 LTS_DLL_SERVER phantom, 8-3
 LTS_ULD_SERVER phantom, 8-3

M

MAC address, 1-7, 4-8
 MAU, 1-7
 MDLC controller, 1-11
 Media Access Control (MAC)
 address, 1-7, 4-8
 Medium Access Unit (MAU), 1-7
 Menus, Edit mode, 6-29
 Mixed-Rev. networks
 addresses, 4-10
 with pre-Rev. 19.3 nodes, 4-3
 with pre-Rev. 21.0 nodes, 4-3
 Modems, 1-10
 Modifying objects in a configuration,
 6-45
 MODIFY_QUEUE, FTGEN
 subcommand, 10-14
 MODIFY_SITE, FTGEN
 subcommand, 10-19
 Multiline Data Link Controller
 (MDLC), 1-11

Multiple addressing, PSDN, 4-7
 Multiple configurations, 1-9
 Multiport Transceiver (LMT300), 1-7

N

Naming, remote, 3-7
 Negotiation, window and packet size,
 6-16
 NETCFG
 contrasted with CONFIG_NET,
 4-5
 example of use, 4-12
 using to find address of an old
 node, 4-10
 NETLINK utility
 access rights required, 3-3
 described, 1-3
 security considerations, 3-13
 NETMAN phantom, 2-1, 2-3, 8-3
 NETMAN.SAVE file, 2-1
 Network
 initialization, 9-3
 topology, 6-6
 Network management, LAN300
 see: LAN300 Network
 Management Facility
 Network Process Extension (NPX)
 facility, 1-3
 Network server process, 2-1, 2-3
 Network Terminal Service
 see: NTS
 NETWORK.LOG file, 2-2
 NETWORK_MGT* directory, 2-5
 NETWORK_MGT.INSTALL.CPL
 file, 2-1
 NETWORK_SERVER.COMI file,
 2-1
 New nodes, 4-11
 NM_SERVER phantom, 8-3
 NMSR.LOG file, 2-5
 Node
 adding, 6-44
 CONFIG_NET prompts, 6-11,
 6-16
 configuration checklist, 5-13
 deleting, 6-50
 Edit mode submenu, 6-31
 gateway, 1-12
 new and old, 4-11
 virtual circuit maximum, 6-49

Node-to-node access rights, 3-2
 Node-to-node password,
 CONFIG_NET prompt, 6-19
 Node-to-node passwords, described,
 3-8
 NONE access right, 3-3
 Non-Prime nodes
 access rights guidelines, 3-6
 adding to the configuration, 6-44
 address requirements, 4-8 to 4-9
 CONFIG_NET prompts, 6-10,
 6-24
 configuration checklist, 5-14
 described, 1-7
 editing with CONFIG_NET, 6-48
 FDX addresses, 4-10
 LAN300 addresses, 4-8
 REMBUF CONFIG directive
 setting for, 8-5
 -NO_WAIT, CONFIG_NET option,
 6-2
 NPUSR CONFIG directive, 8-2
 NPX
 described, 1-3, 3-10
 remote naming use, 3-7
 NRUSR CONFIG directive, 8-3
 NSLUSR CONFIG directive, 1-3,
 3-10, 8-4
 NTS
 defined, 1-6
 maximum configuration for a
 host, 1-9
 phantoms required, 8-3
 relation to PRIMENET, 1-6, 1-9
 NTS_SERVER, 8-3
 Null addresses, 4-8, 4-10
 Null passwords, 3-2

O

Old nodes, 4-11
 Option prompt, 6-2 to 6-3

P

Packet Assembler/Disassembler
 see: PAD
 Packet level addresses, 4-9
 Packet size, 8-5, 9-7
 non-Prime nodes, 6-27
 PSDNs, 6-15

Packet Switching Data Network
 see: PSDN

Packets, Call Request, 4-8 to 4-9

PADs, 1-3, 4-10, 6-11

Passive mode, 1-10

Passwords
 editing with CONFIG_NET, 6-47
 half-duplex, 3-13, 6-13
 minimum length, 3-2
 node-to-node, 3-8, 6-19
 null, 3-2
 random generation by
 CONFIG_NET, 6-14, 6-20
 Ring 0, 3-8
 user, 3-2

Phantoms
 RT_SERVER, 2-3, 9-3
 summarized, 8-3
 YTSMAN, 10-1

PNC controller, 1-6

PNC II controller, 1-6

Pre-Rev. 19.3 nodes
 CONFIG_NET prompts, 6-10, 6-24
 problems when not identified, 4-3
 protocol for full-duplex lines, 6-13
 security considerations, 3-16

Pre-Rev. 21.0 nodes, 4-3

PRIMENET
 ACL settings, 2-2
 addresses, 4-11
 configuration file location, 2-2
 database, 4-2
 installation procedure, 2-1
 line choice criteria, 1-5
 line priority order, 1-5
 line types, 1-4
 maximum configuration for a host, 1-9
 phantoms required, 8-3
 relation to NTS, 1-9
 revision compatibility, 4-4
 security considerations, 3-1
 services, 1-1
 starting, 9-3
 subnetwork types, 1-4
 transmission media, 1-4

PRIMENET* directory, contents, 2-1

PRIMENET Node Controller (PNC), 1-6, 1-9

PRIMENET* directory, described, 4-1

PRIMENET.CONFIG file, 2-2, 4-1

PRIMENET*>JOURNALS directory, 2-4

PRIMOS, security mechanisms, 3-2

PRIMOS.COMI file, 9-1

PRINET.INSTALL.COMI command file, 2-1

Private logs, 2-5

Processes
 maximum for cpu models, 8-4
 reserved for PRIMOS, 8-3
 slave, 8-4
 user, 8-3

Prompt, option (CONFIG_NET), 6-2

PSDN
 adding an address, 6-45
 addresses, 4-6, 4-11
 Administrator, 4-7
 CONFIG_NET prompts, 6-9, 6-14
 configuration checklist, 5-12
 described, 1-12
 Edit mode submenu, 6-37
 editing with CONFIG_NET, 6-48
 gateways, 4-4, 4-7
 international communications, 1-12
 multiple addressing, 4-7
 REMBUF CONFIG directive setting for, 8-5
 security considerations, 3-14
 subaddressing, 4-7
 supported by PRIMENET, 6-9

PURGE_QUEUE, FTGEN subcommand, 10-14

Q

Queue configuration, FTS, 10-13

QUIT, CONFIG_NET selection, 6-56

R

REMBUF CONFIG directive, 8-4

Remote buffers, 6-16, 6-27, 8-4

Remote disks, 9-3

Remote DSM, 9-3

Remote File Access, 1-3, 3-10, 8-4, 9-4

Remote ID, 3-9

Remote ISC, 3-7

Remote Login access right, 1-2

Remote Login lines, 9-6

Remote Login service, 1-1, 3-12, 8-3

Remote naming, 3-7

Remote repeater, 1-6

Repeaters
 local (LAN300), 1-6
 maximum distances, 1-7
 Remote (LAN300), 1-6
 RINGNET, 1-5

RFA
 see: Remote File Access

RFA access right, 3-4

Ring
 see: RINGNET

Ring 0 passwords, 3-8

Ring node ID
 configuring, 6-12
 described, 1-6
 editing with CONFIG_NET, 6-47

RINGNET
 CONFIG_NET prompts, 6-7, 6-12
 configuration checklist, 5-11
 Edit mode submenu, 6-33
 general description, 1-5
 maximum node separation, 1-5
 maximum number of nodes, 6-7
 names, 6-7
 REMBUF CONFIG directive setting for, 8-5
 ring node ID, 6-12

RINGNET repeater, 1-5

RLOG access right, 3-4

Route-through
 connection, 1-12
 phantom required, 8-3
 Server, 1-12

Route-through Server phantom, 2-3

RT.COMI file, 2-2

RT_SERVER phantom, 2-3, 8-3, 9-3

RT_SERVER.SAVE file, 2-2

S

SAVE, CONFIG_NET selection, 6-55

Saving and validating a configuration, 6-55

- Security
 - ACLs to protect files on the node, 3-2
 - Dialup line considerations, 3-14
 - EDIT_PROFILE command, 3-2
 - external login programs, 3-2
 - forced user validation, 3-11
 - gateway link considerations, 3-14
 - general rules, 3-2
 - half-duplex passwords, 3-13
 - multiple LAN300s, 1-9
 - NETLINK considerations, 3-13
 - node-to-node considerations, 3-2
 - node-to-node passwords, 3-8
 - pre-Rev. 19.3 nodes, 3-16
 - PRIMENET considerations, 3-1
 - PRIMOS mechanisms, 3-2
 - project profiles, 3-2
 - PSDN considerations, 3-14
 - Remote Login considerations, 3-12
 - remote naming, 3-7
 - RFA considerations, 3-10
 - symmetry requirements, 3-6
 - user passwords, 3-2
 - Server configuration (FTS), 10-6
 - Servers
 - file transfer, 8-3
 - ISC_NETWORK_SERVER, 9-3
 - LOGIN_SERVER, 8-3
 - NTS_SERVER, 8-3
 - TIMER_PROCESS, 8-3
 - Site configuration (FTS), 10-18
 - Slave processes, 8-4
 - SLAVE.COMII file, 2-1
 - START_DSM command, 9-1
 - START_NET
 - revision compatibility, 4-4
 - usage, 4-2
 - use of PRIMENET configuration file, 4-2
 - use on LAN300 subnetworks, 6-7
 - START_NET command, 9-3
 - START_NTS command, 9-3
 - Startup file, 9-1
 - STAT COMM, 8-2
 - STAT US command, 8-3
 - Statistics gathering, 1-6
 - Status commands, 1-6
 - STATUS, FTGEN subcommand, 10-6
 - Subaddresses, PSDN, 4-7
 - Submenu, 6-31
 - Subnetwork
 - adding to the configuration, 6-45
 - defined, 1-4
 - deleting from network, 6-50
 - Supervisor terminal, 2-3
 - SYNC CNTRLR CONFIG directive, 8-6
 - Synchronous line number
 - CONFIG_NET prompt, 6-12
 - CONFIG_NET prompt for half-duplex lines, 6-13
 - CONFIG_NET prompt for PSDNs, 6-14
 - Synchronous lines
 - full-duplex, 1-9
 - half-duplex, 1-10
 - numbers, 4-10
 - restrictions, 1-11
 - SYSNAM CONFIG directive, 1-6, 9-3
 - SYSTEM process, 2-3
 - System servers, 8-3
- T**
- Tap, 1-7
 - TCP/IP, 1-6
 - TCP/IP for PRIMOS
 - described, 1-6
 - phantoms required, 8-3
 - Terminating CONFIG_NET, 6-56
 - TIMER_PROCESS server, 8-3
 - Token, 1-5
 - Topology
 - CONFIG_NET prompts, 6-6
 - LAN300, 1-6
 - Transceiver, multiport, 1-7
 - Transmission Control Protocol/Internet Protocol (TCP/IP), 1-6
 - Transmission media, 1-4
 - Twin-axial cable, 1-5
- U**
- ULD.LOG file, 2-5
 - UNBLOCK_QUEUE, FTGEN subcommand, 10-14
 - Unknown configuration information, 4-4
 - Unsolicited Message facility (DSM), 2-5
 - User passwords, 3-2
 - User processes, 8-3
 - User validation
 - CONFIG_NET prompts, 6-18
 - described, 3-11
- V**
- Validation
 - configuration, 6-4, 6-55
 - user, 3-11
 - Verification (CONFIG_NET), 6-4
 - VERIFY_USER, EDIT_PROFILE subcommand, 3-10
 - Virtual circuits
 - logical channel numbers for, 6-15
 - maximum, editing with CONFIG_NET, 6-49
- W**
- Window size, 8-5, 9-7
 - non-Prime nodes, 6-26
 - PSDNs, 6-15
 - WSIFTP_SERVERnn phantom, 8-3
 - WSIFTP_USER phantom, 8-3
 - WSI_MANAGER phantom, 8-3
- X**
- X.25 1984, 1-7, 4-3
 - X.28, 1-3
 - X.29, 1-3
 - X.3, 1-3
- Y**
- YTSMAN phantom, 2-4, 8-3, 10-1

Surveys

Reader Response Form

PRIMENET Planning and Configuration Guide DOC7532-4LA

Your feedback will help us continue to improve the quality, accuracy, and organization of our user publications.

1. How do you rate this document for overall usefulness?

☐ *excellent* ☐ *very good* ☐ *good* ☐ *fair* ☐ *poor*

2. What features of this manual did you find most useful?

3. What faults or errors in this manual gave you problems?

4. How does this manual compare to equivalent manuals produced by other computer companies?

☐ *Much better* ☐ *Slightly better* ☐ *About the same*
☐ *Much worse* ☐ *Slightly worse* ☐ *Can't judge*

5. Which other companies' manuals have you read?

Name: _____

Position: _____

Company: _____

Address: _____

_____ Postal Code: _____



NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

First Class Permit #531 Natick, Massachusetts 01760

BUSINESS REPLY MAIL

Postage will be paid by:



PrimeTM

Attention: Technical Publications
Bldg 10
Prime Park, Natick, Ma. 01760

