



***User's Guide to Prime
Network Services***

Revision 21.0

DOC10115-1LA

User's Guide to Prime Network Services

First Edition

Bernard Gilman

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 Level 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, PRIME, 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 (DOC10115-1LA) July 1987 for Revision 21.0

Update 1 (UPD10115-11A) July 1989 for Revision 22.1

CREDITS

Design: Carol Smith

Document Preparation: Kathy Normington

Editorial: Mike McNulty, Kathe Rhoades

Illustration: Jerry Vincent

Production: Judy Gordon

Project Support: Frank Calvillo, Robert Canavello, Jacki Forbes, Scott Sminkey

Composition: Julie Cyphers, Anne Marie Fantasia

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 1-800-343-2533, 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

Contents

About This Book	vii
1 Overview	1-1
Layered Architecture	1-1
Network Types	1-2
Prime Network Services	1-4
PRIMENET Architecture	1-5
Types of Networks	1-8
2 Accessing Remote Files	2-1
Remote File Access	2-1
Remote IDs	2-3
3 Logging In to Remote Systems	3-1
Remote Login	3-1
Error Messages	3-2
4 Introduction to FTS and FTR	4-1
FTS Utilities	4-1
FTR and the COPY Command	4-1
Before You Use FTS	4-2
How FTS Works	4-6
When You Use FTS	4-8
5 Transferring Files With FTR	5-1
FTR Help Facility	5-1
Sending a File	5-2
Retrieving a File	5-3
Printing a File at a Remote Site	5-4
Checking the Status of Requests	5-4
Recording File Transfers	5-7
Canceling Requests	5-10
If a Transfer Fails	5-11
Other Options	5-11

6	An FTR Reference	6-1
	Options for Submitting Requests	6-1
	Options for Managing Requests	6-11
7	NETLINK	7-1
	Overview of NETLINK	7-1
	NETLINK's Modes of Operation	7-3
	Elementary NETLINK	7-4
	NETLINK's Help Facility	7-6
	Making a Connection	7-7
	Setting Up NETLINK Profiles	7-8
	Addressing Another System	7-14
	Multiple Connections	7-17
	Establishing a NETLINK Connection Directly from the PRIMOS Command Line	7-20
	Running NETLINK From a Command Input or CPL File	7-21
	NETLINK File Transfers	7-24
	Debugging Using NETLINK	7-27
8	A NETLINK Reference	8-1
	Command Summarized by Function	8-1
	Address Formats and Syntax Rules	8-6
	Escape Sequences	8-6
	Commands Reference Dictionary	8-7
A	FTS Error Messages	A-1
	General Error Messages	A-1
	FTR Error Messages	A-2
	Messages Sent to Server, Site, Queue, and Request Log Files	A-9
B	NETLINK Error Messages	B-1
	Error Messages Generated From Systems on PSDNs	B-1
	PRIMENET Error Messages	B-2
C	PAD Parameters Used With NETLINK	C-1
	International (X.3) Parameters	C-1
	TELENET Parameters	C-4
	DATAPAC Parameters	C-5
	Prime Network Glossary	GL-1
	Index	Index-1

About This Book

The *User's Guide To Prime Network Services* provides tutorial and reference information on

- Remote file access
- Remote login
- File Transfer Service (FTS) and the File Transfer Request utility (FTR)
- NETLINK, Prime's Packet Assembler/Disassembler (PAD) emulator

The FTS and NETLINK utilities enable users to communicate with other systems on the network and to transfer files between systems.

This book is intended for network users who are familiar with PRIMOS® commands.

This book contains eight chapters and four appendices:

- Chapter 1 provides an overview of Prime network services and software.
- Chapter 2 explains how to access files that are physically located on a partition on a remote computer.
- Chapter 3 explains how to use remote login.
- Chapter 4 introduces the File Transfer Service (FTS) and the File Transfer Request (FTR), the FTS utility that you use to submit transfer requests. This chapter explains what a System Administrator and you must do before you can use FTR.
- Chapter 5 is an FTS tutorial and describes how to use the FTR utility.
- Chapter 6 is an FTR reference and provides a detailed description of all FTR options.
- Chapter 7 is a NETLINK tutorial.
- Chapter 8 is a NETLINK reference and provides a detailed description of all NETLINK options.
- Appendix A describes FTS error messages.
- Appendix B describes NETLINK error messages.
- Appendix C lists X.3 parameters supported by NETLINK.
- Prime Network Glossary describes Prime networking terms. Networking terms are printed in boldface the first time they appear in the text.

Related Documentation

System Administrators and Network Administrators who are designing a network or want their system to become part of a network should read the *PRIMENET Planning and Configuration Guide* (DOC7532-3LA) and the *NTS Planning and Configuration Guide* (DOC10159-1LA). Operators should read the *Operator's Guide to Prime Networks* (DOC10114-1LA). Programmers should read the *Programmer's Guide to Prime Networks* (DOC10113-1LA).

Other Prime documentation that may be helpful includes the following books:

- *PRIMOS Commands Reference Guide*, (DOC3108-6LA). This book is a detailed reference of user commands.
- *NTS User's Guide* (DOC10117-1LA). This book describes how to use the Network Terminal Service (NTS) to access 50 Series™ systems on a LAN300.
- *System Administrator's Guide, Volume I: System Configuration* (DOC10131-1LA). This book describes how a System Administrator can plan and configure a Prime computer system and users' environments.
- *System Administrator's Guide, Volume II: Communication Lines and Controllers* (DOC10132-1LA). This book describes how a System Administrator can configure local and network configuration lines and provides an overview of AMLC, ICS, and LTS300 controllers.
- *System Administrator's Guide, Volume III: System Access and Security* (DOC10133-1LA). This book provides a System Administrator information to establish and maintain system access and security.

New Features At Rev. 21.0

At Rev 21.0, FTS has the following new features for users:

Assigning a Relative Priority to Transfer Requests

FTR users can set the relative priority of a transfer request within a queue with the `-PRIORITY` command option and specify a date and time when the request is to be submitted for processing. The default priority of a transfer request is set by the System Administrator, who can also disable the priority mechanism. If the mechanism is disabled, requests are processed in the order in which they are submitted.

Chapter 5 describes how to use the `-PRIORITY` option.

Deferring a Transfer Request

A new FTR command option (`-DEFER date-time`) enables a user to specify the date and time that a request is to be submitted for processing. A user can modify the date and time specified to make the request immediately available for processing.

Chapter 5 describes how to use the `-DEFER` command option.

Temporary Destination Files

When FTS transfers a file, the destination file is initially created with a temporary filename that the receiving server generates. FTS prepends the letters `T$` to the destination filename to create the temporary filename. The name may be truncated to ensure that it does not exceed 32 characters. A user can display the temporary filename by executing the `LIST_DIRECTORY` command during the transfer. Progress on creating and renaming the file is recorded in the log file. On successful completion of the transfer, FTS attaches to the destination directory, deletes any existing file with the required name, and renames the temporary file to the required destination filename.

New NETLINK Option and Command

The `HFCTY` command specifies a nondefault Facilities field in hexadecimal digits and corresponds to a new `-HFCTY` option to the `C` command. Whereas the `-HFCTY` option affects only a single connection, the `HFCTY` command establishes an environment affecting any future connections.

Chapter 8 describes the `-HFCTY` option to the `C` command and describes the `HFCTY` command.

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>	<i>Example</i>
UPPERCASE	In command formats, words in uppercase indicate the names of commands, options, statements, and keywords. Enter them in either uppercase or lowercase.	NETLINK
lowercase	In command formats, words in lowercase indicate variables for which you must substitute a suitable value.	NETLINK -TO nodename
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>DEBUG</u> { -TERMINAL_TYPE } { -TTP }
Brackets []	Brackets enclose a list of one or more optional items. Choose none, one, or more of these items.	FTR -HELP [subject USAGE]
Braces { }	Braces enclose a list of items. Choose one and only one of these items.	CLOSE { file outfile }
Parentheses ()	In command or statement formats, you must enter parentheses exactly as shown.	DIM array (row, col)
Hyphen -	Wherever a hyphen appears as the first character of an option, it is a required part of that option.	FTR -HELP
<i>Bold italics</i> in examples	In examples, user input is in bold italics but system prompts and output are not.	OK, <i>RESUME MY_PROG</i> This is the output of MY_PROG.CPL OK,
Angle brackets < >	In messages, text enclosed within angle brackets indicates a variable for which the program substitutes the appropriate value.	Disk <diskname>

1 Overview

This chapter provides an overview of Prime network services and software available at Rev. 21.0. These services enable you to access files on a remote system, log in to a remote system, transfer files between Prime systems linked in a network, and communicate over an X.25 network.

This chapter describes

- Prime network user features
- PRIMENET™ architecture
- Types of network over which you can communicate

At Rev. 21.0, Prime network services are based on the **PRIMENET** distributed network facility. PRIMENET software is supported on all 50 Series systems, and provides reliable, standardized network services over all physical media over which Prime systems operate.

PRIMENET makes accessing remote information identical to accessing local information. Because this process is transparent, you are not required to learn new commands to access partitions or files on remote systems in a network. Also, you do not need to know the details about how your system is linked to other systems or the location of remote systems.

Layered Architecture

PRIMENET uses a layered architecture (described later in this chapter) that provides several benefits. The same simplicity and structured design are present no matter how many systems are linked in a network. In addition, since PRIMENET supports internationally recognized standards such as **X.25**, **X.3**, **X.28**, and **X.29**, you can easily link to any other Prime network or **Packet Switched Data Network (PSDN)** that supports the same standards. Thus, Prime systems can be integrated easily with existing equipment.

You interact only with the top layers of PRIMENET. Because these top layers interact with the lower levels, you do not have to know anything about the physical connections between linked systems, or how data is formatted and checked during transfer.

In many cases, you do not need to be aware that network connections are being used. For example, you can access remote files in exactly the same way as local files. (See Chapters 2 and 3 of this book.)

Another advantage of PRIMENET's layered architecture is that any changes made to lower levels are transparent to you. Thus, enhancements of lower levels do not change how you invoke or use PRIMENET.

Network Types

Prime network user services enable you to log in to or access files on other systems in a PRIMENET network. You can communicate with a remote system connected to the local system through any of the following network types (described later in this chapter):

- RINGNET™ (Local Area Network in a ring configuration)
- LAN300 (Local Area Network in a bus configuration)
- Point-to-point full-duplex synchronous lines
- Point-to-point half-duplex synchronous lines
- Packet Switched Data Networks (PSDNs)

You can also use the PRIMENET Route-through facility to communicate with a remote system that is indirectly connected to the local system through a series of intervening **gateway** systems.

These links enable you to log in to remote systems or access remote files from your local system. Figure 1-1 shows typical examples of network links.

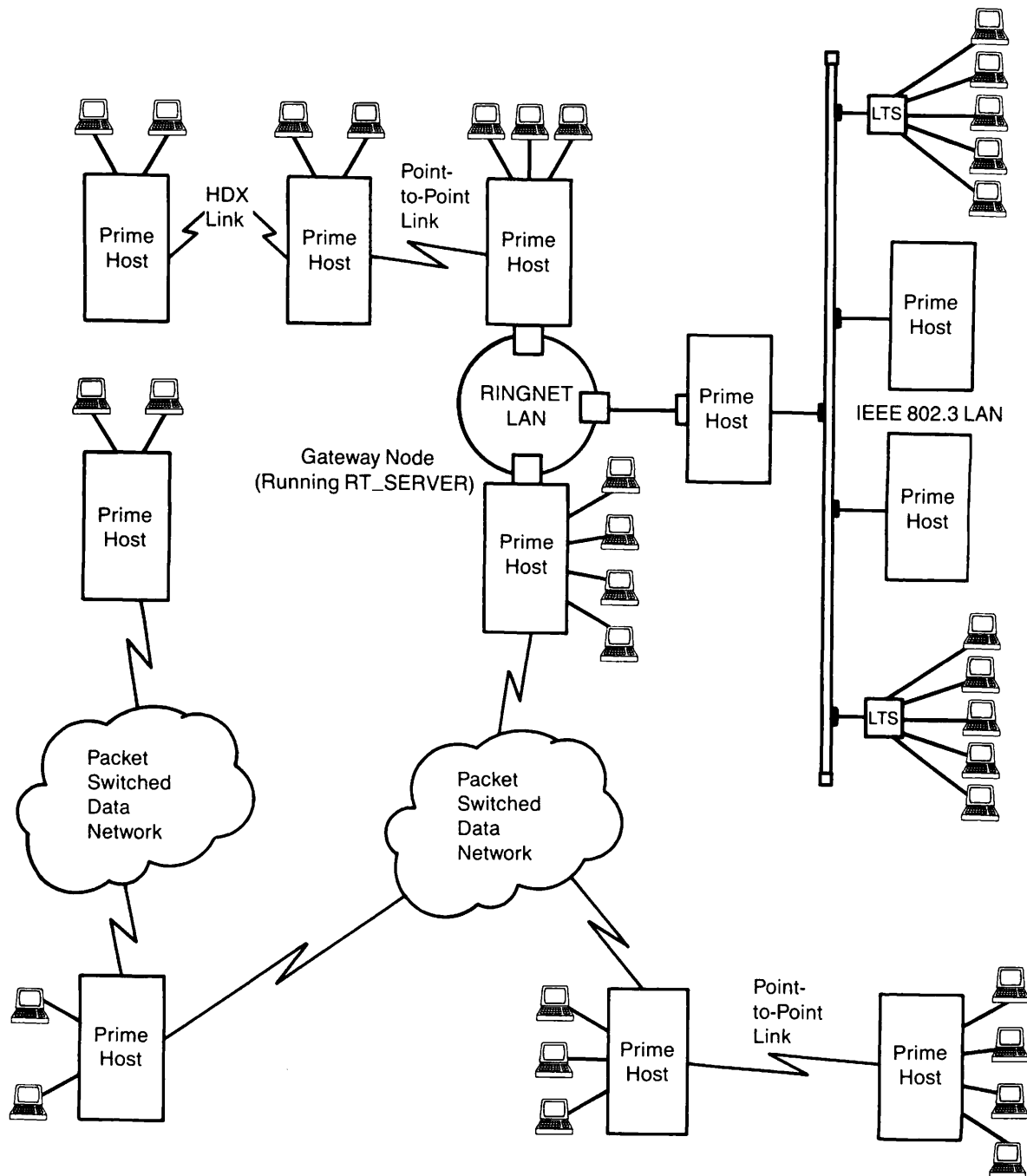


FIGURE 1-1
Examples of Network Links

Prime Network Services

Prime's network services are easy to use. You can use PRIMOS commands that you already know across networks. The next sections describe the following facilities:

- Remote file access
- Remote login
- File Transfer Service (FTS)
- The NETLINK utility

Remote File Access

Remote File Access (RFA) is a PRIMENET service that provides immediate access to any remote file within the network, even if you do not know on which system within the network the file resides. You do not have to learn any new commands to specify a remote file, because PRIMENET works with the file system to access the file transparently. In fact, you may not even know that the file is not contained within the local system. In addition, programs accessing remote files may not have to be changed or recompiled if the remote files are moved. The PRIMOS COPY command uses RFA to copy files between systems. Chapter 2 contains additional information on remote file access.

Remote Login

You can log in to any remote system on the network, as long as you have a valid user ID. Once you are logged in to a remote system, you can type commands as if you were logged in to the system locally. Chapter 3 contains additional information on remote login.

The File Transfer Service (FTS)

The **File Transfer Service (FTS)** is a separately priced product that enables you to transfer files between Prime systems in a communications network. You can send or retrieve any file in the network, as long as you have the proper access rights. If a node is currently disconnected, FTS automatically retries a transfer later.

FTS is an alternative to the COPY command and has the advantage of being able to transfer files to a disk that is not directly accessible through remote file access.

The file transfer command, FTR, includes the following options:

- Submitting, deferring, putting on hold, modifying, or canceling a transfer request
- Displaying the current status of a transfer request
- Transferring a copy of the original source file or a copy modified after you submit a transfer request
- Creating a log file to record your transfer requests

FTS has separate facilities for users, operators, and System Administrators.

- For users, the FTR command transfers files. The Network Administrator uses the FTGEN utility to install FTS on a network. See the *PRIMENET Planning and Configuration Guide* for more information on this utility.
- System operators use the FTGEN utility and the FTOP utility to monitor and expedite user requests submitted with FTR.
- FTS also includes a subroutine, FT\$SUB, that can be used in programs to perform FTR options. See the *Programmer's Guide to Prime Networks* for more information on FTS subroutines.

The NETLINK Utility

NETLINK emulates a PSDN Packet Assembler/Disassembler (PAD) and enables you to access a system over any X.25 network to which your local system is linked. NETLINK converts asynchronous terminal input into X.25-formatted packets of information that can be transmitted over an X.25 network. NETLINK works over all PRIMENET network types. PRIMENET X.25 software meets the Consultative Committee for International Telephony and Telegraphy (CCITT) 1984 X.25 communications standard for packet switched networks.

NETLINK enables you to access both Prime and non-Prime systems in an X.25 network. You need not log out of the local system to invoke NETLINK; NETLINK supports simultaneous links to a maximum of 6 remote systems and lets you move between them and the local system at will.

NETLINK can be used not only to connect to PSDNs and other Prime systems, but also for file transfer. This is described in Chapter 7.

PRIMENET Architecture

PRIMENET is made up of several layers, as shown in Figure 1-2. This layered structure is based on the **International Organization for Standardization Open Systems Interconnection (ISO OSI)** model, to make the 50 Series systems able to communicate with all other systems that support X.25 protocols. Each of the functional layers of PRIMENET has its individual functions and each interfaces with the adjacent layer or layers. Each layer is described in the next sections.

Lower Layers

Level 3, the packet interface, creates and controls virtual circuits across the network, handles error recovery, and controls the flow of information. It also keeps track of the process to which each packet is being transferred. You can write network-based programs using the **Interprocess Communications Facility (IPCF subroutines)**, which are described in the *Programmer's Guide to Prime Networks*. These routines interface directly to Level 3. Level 3's X.25 support provides a standard interface to upper-level software no matter what kinds of links make up Levels 1 and 2.

Level 2 is the link protocol level. It describes a **protocol** to which two linked nodes must adhere when they transfer information from one to the other. This protocol dictates the format of the data; how the nodes should request, transfer, receive, and acknowledge the data; and how to signal faulty transmissions, if they occur.

Level 1 is the physical layer. This layer acts as an intermediary between the physical transmission medium (twin-axial cable or transmission line) and the rest of PRIMENET and the system. Depending on the type of network, one of several controllers governs action at this level:

- PRIMENET Node Controller (PNC or PNC II)
- Multiple Data Link Controller (MDLC)
- Intelligent Communications Subsystem, Model 1, 2, or 3 (ICS1, ICS2, or ICS3, respectively)
- LAN300 Host Controller (LHC300)

These controllers, which are described in the section Types of Networks in this chapter, implement Level 1 and some Level 2 protocols.

Upper Layers

PRIMENET's upper layers provide user services. (See Figure 1-2.) These internal functions operate on the lower layers to perform actions directly specified by you or actions that facilitate completion of user tasks. These services use the same IPCF subroutines that are mentioned above.

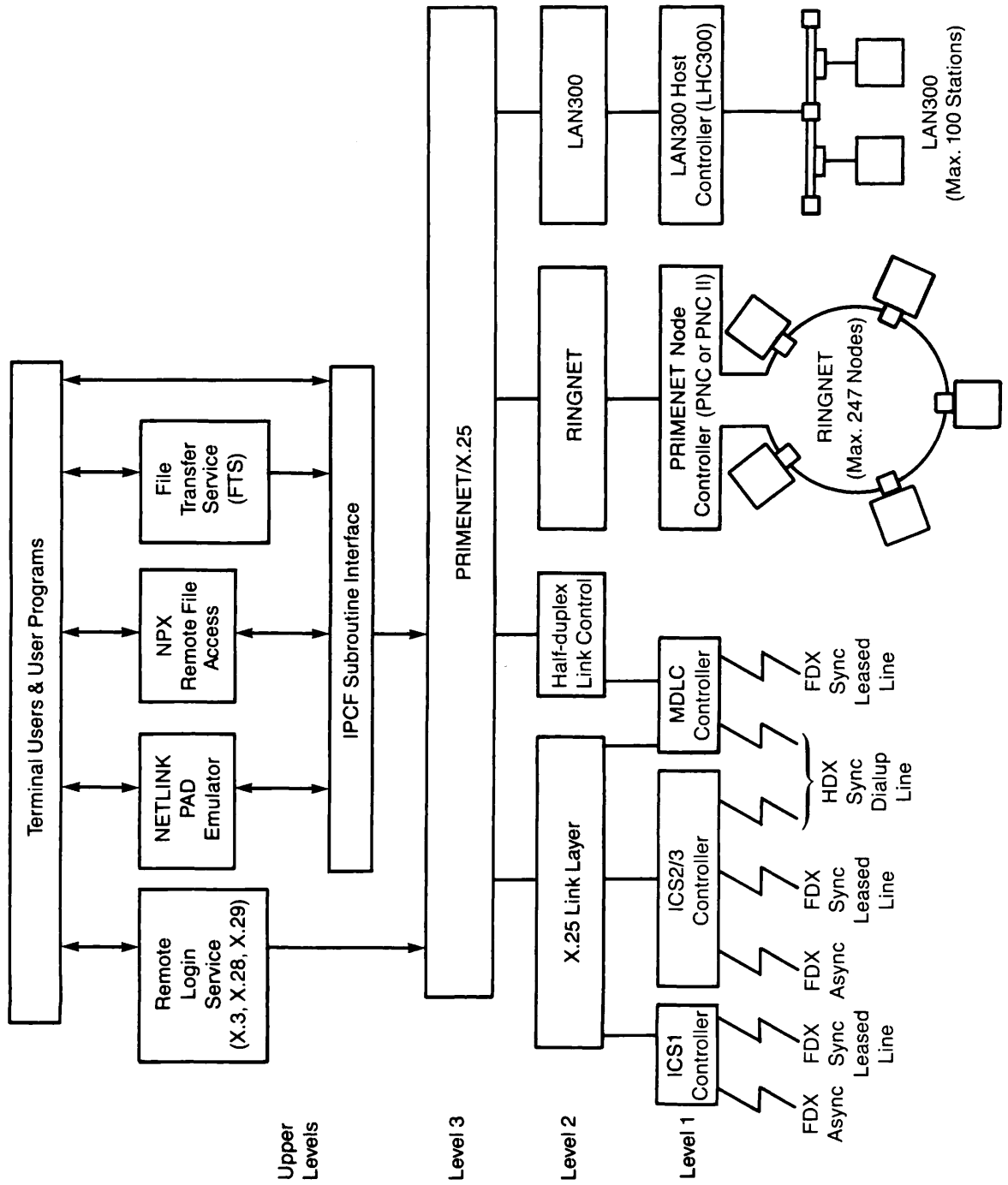


FIGURE 1-2
Layers of PRIMENET Architecture

Types of Networks

This section describes the types of networks over which PRIMENET software runs.

RINGNET

RINGNET, Prime's general purpose **Local Area Network (LAN)**, enables 247 nodes to be connected through a high-speed, one-way, serial-synchronous twin-axial cable, or a fiber optic cable. (A node is any system that is linked to other systems in a network.) See Figure 1-3.

Each node in a ring network is equipped with the following hardware:

- A **PRIMENET Node Controller (PNC)** or (**PNC II**) board, which controls the ring protocol and the flow of data between ring nodes.
- A junction box, which connects the twin-axial cable to the computer. The junction box has a passive relay that switches to "pass-through" if it detects a power failure on the PNC. This feature preserves a ring's integrity.

RINGNET uses a **token ring protocol**. A special **bit** pattern called a token circulates continuously around the **ring**. A node cannot transmit data until it grabs the token. When it can transmit, a node transmits a **packet** containing a 4-byte header and from 4 to 2044 bytes of data through its PNC.

The packet circulates around the ring to the destination node at a rate of ten megabits per second. (Data throughput may be slower; the effective data rate is approximately eight megabits per second.) The destination PNC receives the packet and sets a flag in the packet to acknowledge the receipt. The packet travels around the rest of the ring back to the source PNC, which does the following:

- Removes the packet from the ring
- Passes on the token
- Checks the acknowledgment flag
- Interrupts the source operating system to signal successful transmission

Each PNC acts as an active data **repeater** for packets between other ring nodes. As shown in Figure 1-3, Node B's PNC handles data transmitted between Node A and Node C. This repetition requires no software intervention on the part of Node B; its PNC firmware handles the data transmission.

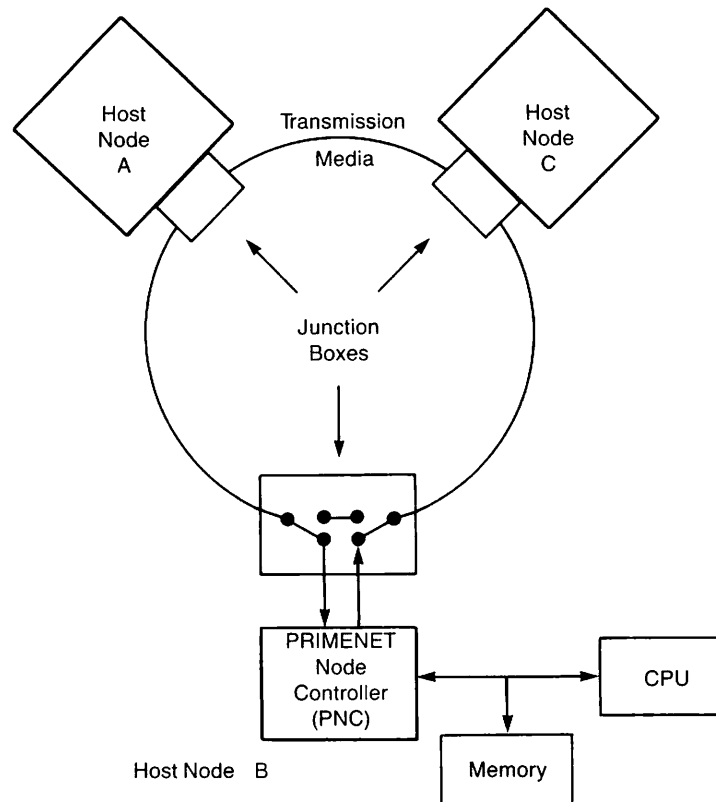


FIGURE 1-3
RINGNET Configuration

RINGNET serves all nodes in the ring equally, so that one system cannot monopolize the network. It automatically checks all packets for integrity and does not require user intervention or separate acknowledgment messages. In addition, RINGNET can be expanded into larger networks without suffering any degradation of performance.

If any of the nodes in a ring network are powered down or broken, the rest of the nodes are still able to send data around the ring. The junction box in a disconnected node allows messages to pass through without interruption to the next node in the ring.

Normally, the cable distance between adjacent active ring nodes cannot exceed 750 feet (230 meters). Each RINGNET repeater with an electrical interface allows an additional 750 feet between nodes for each repeater in the ring. RINGNET repeaters with a fiber optic interface allow distances between nodes or repeaters of 3280 feet (1 kilometer). Multiple repeaters can be used to meet the requirements of longer distances.

LAN300

LAN300, Prime's IEEE 802.3 compliant local area network, uses a bus topology. A typical standard LAN is composed of one or more bus segments, each of which can be a maximum of 500 meters long. Devices are connected to the LAN at a station. A station, also called a connection or node, is a point on the LAN at which a tap and transceiver are attached to the bus segment. A host or a server, which supports a cluster of terminals, a cluster of serial printers, or both can be connected to a station. A bus segment can have a maximum of 100 stations. A fully configured LAN can have a maximum of 1024 stations.

Figure 1-4 shows a LAN300 configuration.

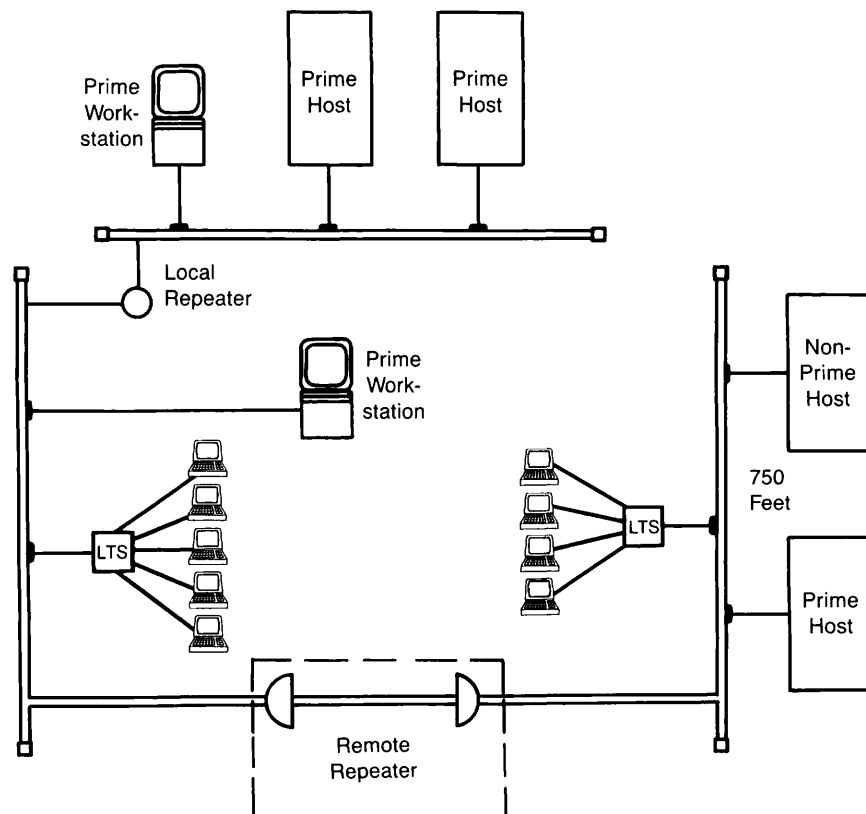


FIGURE 1-4
LAN300 Standard LAN Configuration

Point-to-Point Full-duplex Synchronous Lines

PRIMENET supports **full-duplex** synchronous communications between Prime systems over leased or dedicated telephone lines. The Network Administrator defines full-duplex during network configuration. Full-duplex lines become active when the operator starts up PRIMENET by means of the `START_NET` command, and they remain active until the operator issues the `STOP_NET` command or the system is shut down.

A full-duplex line is attached to a Prime host by means of either a **Multiple Data Link Controller (MDLC)** or an **Intelligent Communications Subsystem (ICS)** controller. The ICS1, ICS2, and ICS3 are front-end communications processors. Each has an operating system and an onboard microprocessor. The ICS controllers enable the main processor to offload communications functions, thus providing greater performance and lower overhead.

An MDLC supports a maximum of four synchronous lines. An ICS1 supports one synchronous line. An ICS2/3 controller supports a maximum of four synchronous lines for PRIMENET's use, as well as additional synchronous lines for other purposes. (The ICS1, ICS2, and ICS3 also support asynchronous lines.) PRIMENET allows a maximum of four configured synchronous lines per system, three of which may be simultaneously active.

During system configuration, the System Administrator configures controller protocols for each full-duplex synchronous line on an ICS2 or ICS3. For information on the available protocols, refer to the *ICS User's Guide* and to the description of the `SYNC_CNTRLR` (or `SMLC_CNTRLR`) directive in the *System Administrator's Guide, Volume II: Communication Lines and Controllers*.

In full-duplex communications, information travels from the processor of one node, through the MDLC, ICS1, ICS2, or ICS3, through a modem (or modem eliminator), and across the transmission lines to the modem (or modem eliminator) and controller of another node. A full-duplex line is a "two-way" connection over which both systems may send and receive signals at the same time.

For full-duplex lines, PRIMENET supports the two **X.25 High-level Data Link Control (HDLC)** protocols: **Link Access Procedure (LAP)** and **Link Access Procedure Balanced (LAPB)**. The MDLC, ICS2, and ICS3 support **Binary Synchronous Communication (BSC)** or **HDLC framing**. The ICS1 supports HDLC framing only.

Point-to-Point Half-duplex Synchronous Lines

PRIMENET's **half-duplex** synchronous lines are temporary dialup telephone connections between Prime systems. A system that has a half-duplex line can use the line to call other Prime systems, just as you can use a telephone to call different people. The Network Administrator defines PRIMENET half-duplex lines during network configuration. However, unlike full-duplex connections, PRIMENET half-duplex connections are controlled by the system operator, who establishes and breaks connections as required by users and applications.

A half-duplex line is attached to a Prime host by means of either the MDLC or ICS2/3. In half-duplex communications, information travels from the processor of one node, through the controller and a modem, and across the transmission lines to the modem and controller of another node. Data travels in only one direction at a time over a half-duplex line.

PRIMENET's half-duplex communication uses BSC-ASCII framing. Within PRIMENET, half-duplex lines can be used either between Prime systems or between a Prime system and a PSDN.

Packet Switched Data Network (PSDN) Connections

Prime systems can subscribe to Packet Switched Data Networks (PSDNs) that support the CCITT X.25 protocol standards of 1976, 1980, and 1984. Supported PSDNs include TELENET, TYMNET, and UNINET in the United States, DATAPAC in Canada, PSS in Great Britain, TRANSPAC in France, DATEX-P in Germany, and many more.

All of these networks transfer and process information in packets. PSDNs often provide service at substantial savings over methods requiring dedicated transmission lines or dialup circuits. This may be especially true in large, geographically dispersed networks.

Each Prime node can connect to a maximum of two different PSDNs. For example, a system could use one full-duplex synchronous line to connect to TELENET and another line to connect to TYMNET. A different line must be used for each PSDN connection, and only one line can be used for each PSDN connection. PRIMENET supports a maximum of three simultaneously active synchronous lines — including lines to PSDNs — per system.

The connection between a Prime system and a PSDN is either a full-duplex synchronous line or a half-duplex synchronous line. As in the case of point-to-point full-duplex lines, PSDN connections can use either HDLC or BSC framing, and either LAP or LAPB link-level protocol.

Route-through Connections

Route-through is a PRIMENET facility that allows communication between two Prime systems that are not directly connected by means of a single ring, a synchronous line, or a PSDN. The two nodes communicate through a series of intervening nodes called **gateway nodes**.

Each gateway node runs a process called the **Route-through Server**. This process routes data along the chain of gateway nodes from the original source to the final destination of the message. Route-through handles call requests and allocates the necessary virtual circuits, but remains transparent to the user. The Network Administrator sets up gateway nodes and Route-through paths.

Figure 1-5 shows a Route-through configuration in which System A communicates with System C through System B, a gateway node.

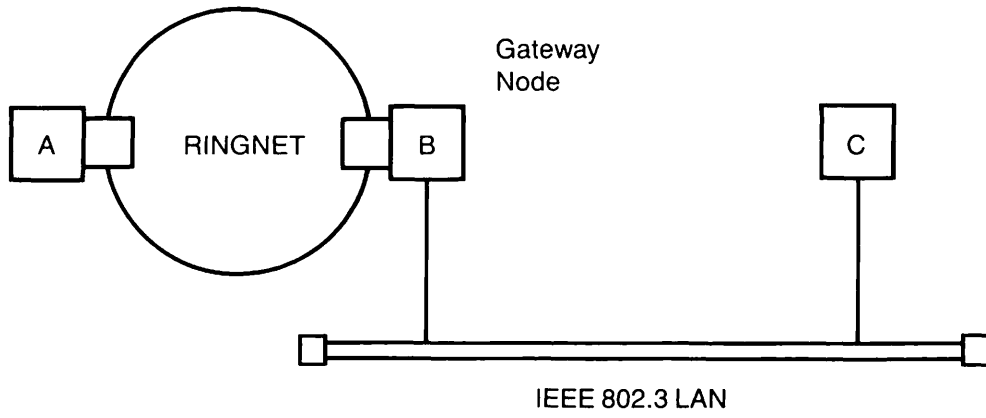


FIGURE 1-5
Route-through Configuration

2

Accessing Remote Files

This chapter explains how to use PRIMENET software to access files that are physically located on a partition on a remote computer. As part of the network configuration process, the Network Administrator decides which systems will be allowed to access one another's files. The administrator uses the CONFIG_NET utility to include this information in the network configuration file, as described in the *PRIMENET Planning and Configuration Guide*. An operator performs regular network maintenance. See the *Operator's Guide to Prime Networks* for a description of these procedures.

Remote File Access

You can access files on a Prime computer that is networked to another Prime computer the same way that you access files locally. You can copy, edit, and manipulate remote files as if they reside on the local system.

Remote File Access (RFA) is implemented internally with the **Network Process Extension (NPX)** facility and works in the following manner:

1. A **master process** requests access to a file on another system.
2. On the remote system, an **NPX slave process** receives the request. A slave is a phantom that is dedicated to receiving requests from masters on other systems. Using your user ID, the slave performs the requested operation on its system, returning data to the master. These operations are transparent to the user.

Note

The System Administrator uses the NSLUSR configuration directive to configure the number of slaves. See the *System Administrator's Guide, Volume 1: System Configuration* for a description of this directive.

Using Remote File Access

Use the STATUS DISKS command to show which local and remote partitions are available. Use commands such as ATTACH, COPY, DELETE, ED, and LD to work on remote files in exactly the same way you do on local files.

Here is an example of editing the file LOANS>UNCOLLECTED, on the partition SHARK, on the system SYSD. First check that the partition is available to you, using STATUS DISKS. The only indication that you can use remote file access is that the STATUS DISKS command shows the partition SHARK to be on system SYSD. Next invoke the EDITOR with the pathname. Note that the partition is available and you do not have to enter any special remote file access commands.

OK, **STATUS DISKS**

Disk	Ldev	Pdev	System
STATS	0	3462	
FIELDS	1	460	
MISCEL	2	71063	
FOREST	3	71061	
REEFS	4		SYSC
LAGOON	5		SYSD
SHARK	6		SYSD
SHARK2	7		SYSD
CLOUDS	10		SYSE
CLIFF1	11		SYSE
CLIFF2	12		SYSE
AERIE	13		SYSE
ROCK	14		SYSA
FALCON	15		SYSA
NEST1	16		SYSA
NEST2	17		SYSA

OK, **ED <SHARK>LOANS>UNCOLLECTED**

EDIT

L Harry

Harry W. Sloth \$38.14

C/38/18/

Harry W. Sloth \$18.14

FILE

<SHARK>LOANS>UNCOLLECTED

OK,

Note

The STATUS DISKS command displays the disks that PRIMOS searches for directories. Local disks are searched first and then remote disks. Disk names, but not directory names or filenames, must be unique. If you omit a partition name from a pathname, you could inadvertently access a file with the same name on a disk other than the one that you want to access. Therefore, it is recommended that you include the partition name in the pathname. As shown in the above example, the partition name is enclosed in angle brackets (<SHARK>).

In the following instances, however, special remote file access commands or actions are required.

- For security reasons, the remote system does not recognize your user ID as valid for file access. In this case, you must use a remote ID, as described in the next section, Remote IDs.
- The remote partition that you want to access may not be available on your system. In this case, you must either ask an operator or your System Administrator to add the partition, or use the File Transfer Service (FTS) to transfer the file to your system.

Remote IDs

The Network Administrator of a Prime computer can configure the system to "force user validation" when users on other, remote systems try to log in to it. A system that forces user validation does not automatically recognize your user ID. The slave cannot do your work on that system unless you establish a remote ID for the remote system. The slave then uses this remote ID. You must establish a remote ID to access any remote system that forces user validation.

To establish and use a remote ID, perform the following steps:

1. Ask the System Administrator on the remote system to create a user ID for you on that system. The System Administrator must do this only once.
2. Use the `ADD_REMOTE_ID` (ARID) command to add the remote ID to a list of IDs. (You can have only one remote ID on any given system. The list of remote IDs cannot exceed 16 IDs.) You must do this every time you log in and want to access the remote partition.

Note

You might want to establish remote IDs even on systems that recognize your regular user ID. For example, a remote ID may allow you certain ACL rights that your own user ID does not allow.

Example of the ARID Command

The following example illustrates a case in which you would use the `ADD_REMOTE_ID` (ARID) command. PRIMENET connects two Prime systems, SYSA and SYSB. Each system already has a number of established user IDs. However, two users, one on each system, have the same ID. For example,

<i>System</i>	<i>User ID</i>	<i>Person</i>
SYSA	RUTH	Ruth J. Morton, Payroll Department Director
SYSB	RUTH	Frank W. Ruth, Buildings and Grounds Director

Company managers want Ruth Morton to be able to access files on both SYSA and SYSB, including the directory <BURSAR>PAYROLL on SYSA. They also want Frank Ruth, who logs in on SYSB, to be able to access <BURSAR>BUDGETS>EQUIP on SYSA, but not to access the PAYROLL directory on SYSA.

Without any special protection, Frank Ruth, logged in as RUTH on SYSB, could access any files on SYSA to which RUTH (Ruth Morton) had access. To avoid this problem, the Network Administrator uses the CONFIG_NET utility to require that SYSA force user validation. This means that RUTH from SYSB is not allowed access as RUTH on SYSA. In order to access files on SYSA, the SYSB user must supply an additional user ID and password that SYSA recognizes. The System Administration Directory (SAD) of SYSA contains the user IDs and passwords that it recognizes.

For example, suppose that the SAD on SYSA lists Frank Ruth's user ID as FRANK and that the ACL for <BURSAR>BUDGETS>EQUIP provides appropriate access rights to FRANK and none for RUTH. Now, RUTH (Frank Ruth) does not have access to <BURSAR>BUDGETS>EQUIP and FRANK cannot access <BURSAR>PAYROLL.

To log in on SYSB and access the equipment budget directory (on SYSA), Frank Ruth must enter these commands:

OK, **LOGIN RUTH**

Password?

```
RUTH (user 50) logged in Friday, 7 Feb 86 9:32:02.  
Welcome to PRIMOS version 21.0  
Copyright (c) 1986, Prime Computer, Inc.  
Serial #SDIU0101200269GB (Acme Machine Co.)  
Last login Thursday, 6 Feb 86 13:21:16.
```

OK, **ARID FRANK SECRET -ON SYSA**

OK, **A <BURSAR>BUDGETS>EQUIP**

OK, **ED FIRST.QUARTER**

.
. .
. .

When Frank Ruth accesses the FIRST.QUARTER file, he does so under the ID FRANK, not RUTH.

Establishing Remote IDs

You can establish a remote ID with the `ADD_REMOTE_ID` command, which has the following format:

```
{ ADD_REMOTE_ID } remote-id [password] -ON system [-PROJECT project-id]
{ ARID           } [-PROMPT]
```

The arguments and options for this command are the same as those for the `LOGIN` command.

The *remote-id* is the user ID that the slave uses for you on the remote system, which you specify in the command line argument, *system*. The System Administrator must have defined *remote-id* as a valid user ID on the remote system.

You must also supply any *password* or *project-id* required for access to the remote system. The `-PROMPT` option sets the terminal to half-duplex and prompts you for your password, which is not echoed on the screen when you enter it. If the remote ID does not exist on the remote system, or if any required password or project ID is missing or incorrect, attempts to access the remote system fail.

You can have a maximum of 16 remote IDs, but only one for any given remote system. For example, if you add the remote ID `JINKS` on `SYSA` and then add the remote ID `LYNX` on `SYSA`, `LYNX` replaces `JINKS`. All remote IDs are removed when you log out.

Examining Your Remote IDs

With the `LIST_REMOTE_ID` (`LRID`) command, you can examine the existing remote IDs you have established. The format of this command is

```
{ LIST_REMOTE_ID } [-ON system]
{ LRID           }
```

If you use the `-ON` option, only the remote ID for *system* is listed. If you omit the `-ON` option, all of your remote IDs are displayed. Passwords are never displayed. For example,

```
OK, LIST_REMOTE_ID
```

```
System  User id                Project id
-----  -
SYSB    JIM
SYSK    JAKE                    SALES
SYSM    JODY
```

OK,

Removing Remote IDs

You can also remove remote IDs from your list, if the list gets too large. The PRIMOS command is `REMOVE_REMOTE_ID` (RRID), which has the following format:

```
{ REMOVE_REMOTE_ID }  
{ RRID } -ON nodename
```

The `REMOVE_REMOTE_ID` command enables you to remove your remote ID for a given system from your remote ID list. You may want to remove a seldom used or obsolete remote ID to add a new remote ID to your list. You may also want to access files on a remote system under a remote ID and then remove the ID to access files on the same system under your local ID. If your list has reached the 16-ID limit, you cannot add more remote IDs unless you remove at least one remote ID with the `REMOVE_REMOTE_ID` command.

If you do not have a remote ID for the system named in *nodename*, the message **Not found** appears.

3

Logging In to Remote Systems

This chapter describes remote login and lists error messages that can appear when you attempt to log in to a remote system.

Remote Login

Remote login enables you to log in to a computer that is remotely connected to the system to which your terminal is directly connected. You can use two methods to log in remotely:

- Use the LOGIN command, which is described in this chapter. You can use the LOGIN command to log in to a Prime system that is connected in a network and to which you have access rights.
- Use NETLINK, a Packet Assembler/Disassembler (PAD) emulator. NETLINK lets you connect to Prime systems over either a PRIMENET network or a Packet Switched Data Network (PSDN). It also lets you connect to non-Prime computers over a PSDN. NETLINK is described in Chapters 7 and 8.

In order to use either of these methods, you must have a valid user ID on the remote system.

Using the LOGIN Command

To log in to the remote computer named *system*, use the following LOGIN command format:

```
LOGIN user-id [password] [-PROJECT project_id] -ON system
```

Except for the -ON option, logging in remotely is identical to logging in locally.

Here is an example of a successful remote login:

```
LOGIN HANSEN -ON SYSB  
PRIMENET 21.0 SYSB  
Password? HAN
```

```
HANSEN (user 50) logged in Saturday, 25 Oct 86 10:12:12.  
Welcome to PRIMOS version 21.0  
Copyright (c) 1986, Prime Computer, Inc.  
Serial #SDIU0101200269GB (Acme Machine Co.)  
Last login Monday, 20 Oct 86 7:41:16.
```

OK,

If your terminal is already logged in, you might get an error message requesting that you log out first. To learn which remote systems are accessible from your terminal, ask your System Administrator or log in to your local system and type STATUS NETWORK. (You are not necessarily allowed to log in to all the systems that this command displays, however, since your System Administrator configures remote login and you need a valid user ID on each system.)

Error Messages

The following error messages can appear when you attempt to log in to a remote system:

CALL CLEARED

```
CLEARING CODE =:cccccc  
DIAGNOSTIC CODE =:dddddd
```

Remote login has received an unexpected clearing cause or diagnostic from the network. *cccccc* is the clearing cause in octal, and *dddddd* is the diagnostic code in octal. If this problem recurs, contact your System Administrator. For a description of these codes, see the *Programmer's Guide to Prime Networks*.

Can't connect to remote system. (RLOGIN)

Calls to the remote system are unsuccessful because the network or the remote system is down.

Can't send login line. ddddd< RCODE ddddd< ERR

Remote login could not send the login line to the remote host because of an internal error. *dddddd* are decimal numbers for the internal state variables RCODE and ERR. Refer this information to your System Administrator.

Invalid facilities. (RLOGIN)

Your system has attempted to send an illegal connect packet for the network to which it is connected. This error message indicates that an improper set of facilities is configured. Inform your System Administrator.

Invalid system name. (RLOGIN)

You have attempted to log in to a disallowed or nonexistent system, or you have spelled the system name incorrectly.

Line to remote system down. (RLOGIN)

All available links to the remote system are down.

No more remote lines available. (RLOGIN)

All of the available slots for users logging in to a remote system are in use. Only 255 users can log in to remote systems simultaneously.

No more remote lines on remote system.

The maximum number of users that the remote system allows are already logged in to the remote system. You must wait for one of these users to log out. If this problem occurs frequently, you should request that the System Administrator of the remote system configure more remote login users.

Please log out first. (RLOGIN)

You must log out of your current system before you try to log in to another system.

Remote login to that system not enabled. (RLOGIN)

Users do not have permission to attempt remote login to that system.

Remote system busy.

The remote system has all available circuits in use. Wait for one of the circuits to be freed.

Remote system down.

The remote system is not responding to messages from the network. Either the system or the network is not operating.

Remote system has too many calls in progress.

The remote system is not accepting any more remote logins since all available resources are in use. You must wait until resources are available.

Remote system not up yet.

The remote system has just been started, but users are not permitted to log in yet. Either the date and time have not been set yet or the MAXUSR command has not been issued. Wait a reasonable period and try again.

Too many network calls . (RLOGIN)

Your system is currently handling the maximum number of calls it can support. You must wait until someone finishes a call.

Too many network calls for link . (RLOGIN)

A network link is currently handling the maximum number of calls allowed. You must wait until someone finishes using the network.

4

Introduction to FTS and FTR

This chapter describes the File Transfer Service (FTS), which enables you to transfer files between 50 Series systems. FTS is a separately priced product that uses PRIMENET software. It provides a recoverable and queued file transfer mechanism that is independent of Remote File Access (RFA).

Chapter 5 contains a File Transfer Request (FTR) tutorial and Chapter 6 is a full reference for FTR options. Appendix A describes each FTS error message that might occur in any of the FTS utilities described in the next section.

FTS Utilities

The following utilities comprise FTS:

- **File Transfer Request (FTR)** — The FTS utility for submitting transfer requests.
- **File Transfer Generation (FTGEN)** — The utility that a Network Administrator uses to configure the FTS data base. FTGEN is described in the *PRIMENET Planning and Configuration Guide*.
- **File Transfer Operator (FTOP)** — The utility that an operator uses to manage the FTS system. FTOP is described in the *Operator's Guide to Prime Networks*.

Application programs can also call FTS through the FT\$SUB subroutine. A program can submit, modify, cancel, or otherwise control a request just as a user can with FTR. The *Programmer's Guide to Prime Networks* describes this subroutine.

FTR and the COPY Command

You can use either the FTR command or the COPY command to transfer files between networked Prime computers. (The NETLINK utility can be used to transfer files as well. See Chapter 7 for more information.) The two commands offer the following alternative approaches. One command may be more appropriate than the other in a given situation.

- COPY provides immediate, direct access to a remote file system. FTR provides a queued file transfer with a logging facility.

- COPY ties up your terminal while the file is being copied. FTR leaves your terminal free during a file transfer.
- COPY requires the remote site to be up and the communications link to be working at the time you request a remote file copy. Otherwise, you receive an error message and you must try again later. FTR accepts requests for file transfers at any time, regardless of the state of the remote site or the communications link. FTR queues the requests and transfers files at a time when the remote site and the communications link are functioning.
- You can use COPY and other PRIMOS commands for remote file access only when the System Administrator has enabled remote file access communications between the systems. If the communications link is expensive or scarce, FTR may be a good alternative. FTR needs to be connected only long enough to handle queued file transfer requests.
- FTS automatically overwrites a file if the file in the destination directory has the same name as the file that you are sending. COPY asks you whether you want to overwrite a file if a file in the destination directory has the same name as the copied file (unless you use the `-NO_QUERY` option).

Before You Use FTS

In order for you to use FTS, PRIMENET must be configured on your system. After FTS is installed, your System Administrator must perform certain tasks, as described next, and you should check that FTS has the correct access rights to your directory and the remote destination directory.

Administrator Tasks

Your System Administrator performs the following tasks so that you can use FTS:

- Initializes the FTS database with an FTGEN command.
- Configures one or more **file transfer servers**, which are phantom processes that handle file transfer requests. FTS requires a minimum of two phantom processes. One phantom is for a server, configured with FTGEN, which takes requests from its own queue (see below). Each file transfer server has a unique name that helps identify it. Another phantom is for YTSMAN, the **File Transfer Manager**, which receives file transfer requests from remote sites and passes them to appropriate servers. The System Administrator uses an FTOP command to start YTSMAN.

Before you submit an FTR request, use the STATUS USERS command to check that the server(s) and YTSMAN are running.

- Sets passwords on the servers with FTGEN as a security measure.

- Configures the file transfer queues. A file transfer queue holds file transfer requests that you and other FTS users make. Queues must be configured at local sites to allow local-to-local transfers. Each server process is responsible for one file transfer queue.
- Defines file transfer sites. Sites are either local or remote nodes between which files are transferred. The System Administrator at the local site must obtain the remote node name, remote server name, and remote server password from the System Administrator at the remote site and include this information in the FTS configuration.
- Before you submit a transfer request, check with your System Administrator that the site to which you want to send a file is listed as a valid destination in your system's FTS configuration file. FTS servers can be running on your system and on a destination system, but systems can send files to one another only when they are listed in each other's FTS configuration file.
- Assigns ACL rights to the following processes on your system so that PRIMENET works correctly:
 - Network Manager Process (NETMAN)
 - User ID SYSTEM
 - Route-through Server (RT_SERVER)
 - File Transfer Service

The System Administrator or an operator can start servers from the supervisor terminal with the FTOP command at system startup. Figure 4-1 illustrates the structure of FTS.

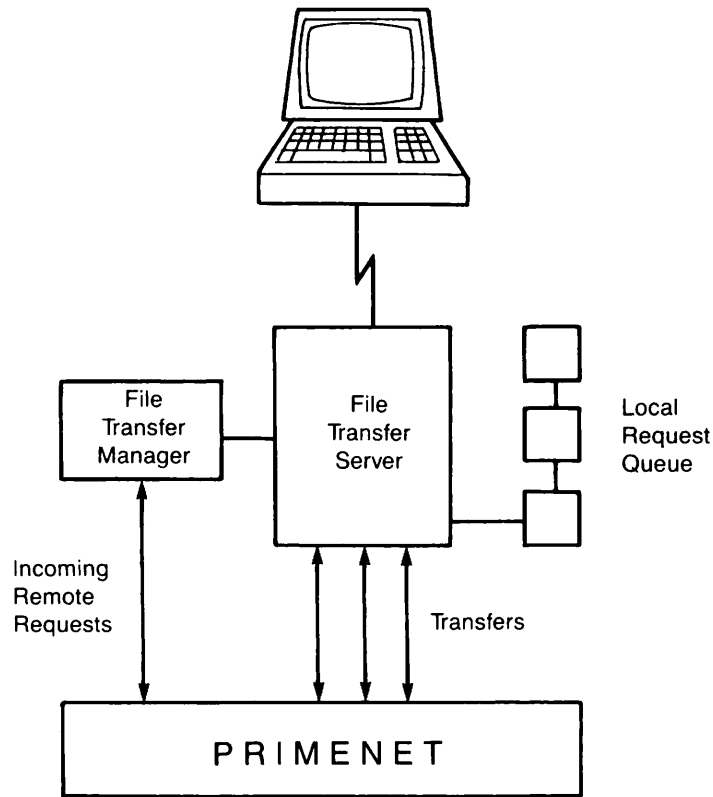


FIGURE 4-1
The File Transfer Service (FTS)

Access Rights for FTS

FTS is subject to ACL security mechanisms in the same way as other PRIMOS users and phantoms. Therefore, in order for FTS to work correctly, both you and FTS need certain file access rights. Before you run FTS, check that these rights exist as explained in the next sections.

Access rights are any combination of the following rights:

- | | |
|--------------------|--|
| Owner (O) | An owner can set all rights (except P and ALL) on files and directories. |
| Protect (P) | Access rights on directories can be changed. |
| Delete (D) | Directory entries can be deleted. |
| Add (A) | Directory entries can be added. |
| List (L) | Directory contents can be listed. |

Use (U)	A user can attach to a directory and use the directory name in a pathname.
Read (R)	A file can be read.
Write (W)	A file can be modified.
Execute (X)	An Executable Program Format (EPF) file can be executed, but cannot be copied with the standard file system utilities.

See the *Prime User's Guide* for information on setting ACLs in general.

Access Rights for the Requesting User

To send files, you need LURW access to the source directory. To retrieve files, you need ALURW access to the destination directory. If you are going to write a log file in a directory, other than the source directory, FTS needs ALURW rights to that directory. (See Chapter 6, An FTR Reference, for a description of the `-LOG` option.)

Access Rights for FTS

File transfer servers need DALURW access rights to both the directory containing the source file and to the directory receiving the file.

Setting Access Rights

Before you set or change access rights on the source directory, use the `LIST_ACCESS` command to list the access rights on that directory. Suppose a user with the ID FRED wants to transfer files from his current directory as in the following example:

OK, **LIST_ACCESS**

```
ACL protecting "<Current directory>":
    FRED:      ALL
    .WORK:    DALURW
    $REST:    LUR
```

In the example, user FRED has ALL rights to the source directory. User FRED can send files from that directory. (User FRED needs LURW access.) The FTS Server, which belongs to the \$REST access group with LUR access, needs DALURW access. FRED can use the `EDIT_ACCESS` command to add access rights for the server. To use this command, you need to know the user ID(s) of the FTS Server(s).

If you cannot determine the user ID(s) of the FTS Server(s) when you enter the STATUS USERS command, ask your System Administrator for this information. In the following example, the name of the server is FTP:

```
OK, EDIT_ACCESS <SYSS17>FRED FTP:DALURW  
OK, LIST_ACCESS
```

ACL protecting "<Current directory>":

```
FRED:          ALL  
FTP:           DALURW  
.WORK:        DALURW  
$REST:        LUR
```

Now the FTS Server can access the source directory. However, before you send a file, you must check that the server has DALURW access to the destination directory. You can use the LIST_ACCESS command if the destination directory is on your system or on a networked system that you can access remotely. (If you want to retrieve a file, you must also have ALURW access to the directory where the file resides.)

Keep the following points in mind when you create or modify access rights:

- FTR always sends a copy of a file using your ACL rights. It must have the correct ACL rights to read the file. The `-COPY` option enables you to specify that the file is to be copied when you submit the FTR request. The `-NO_COPY` option enables you to specify that the file is copied at the time it is transferred. (These options are described in Chapter 5.) If you want to delete a source file after you transfer it, the server should also have Delete (D) rights to the file. (The `-DELETE` option is described in Chapter 5.) If the transfer fails for any reason, including the lack of appropriate rights, the file is not deleted.
- You can restrict access rights to a directory and, instead, create a subdirectory with full access rights to which a remote site can transfer files. However, the remote user and the FTS Server must have at least List (L) and Use (U) access to the top-level directory. These rights enable that directory to be used in a pathname and the server to attach to and pass through that directory to access the target subdirectory.

How FTS Works

Using FTR, you can submit a request to transfer files from a local site to a remote site, or from a remote site to a local site, or between different directories on a local site. A local site is a single Prime computer from which you issue FTS commands. A remote site is another Prime computer to which or from which you want to transfer a file.

Files are transferred from a source directory at one site (called the the source site) to a destination directory at another site (called the destination site). One of these sites must be your local system; the other site is usually a remote system. (You cannot use FTR to transfer files between two remote sites.) When you retrieve a file from a remote system, the local site is the destination site and the remote site is the source site.

When you request a file transfer, FTS processes your request and passes it to PRIMENET. If the network or the remote system is down, your request waits in a queue until the communications link is active again. For example, if two systems are connected by a half-duplex PRIMENET line, file transfer requests wait in their queues until the line is started up. A file transfer request provides FTS with the following information that is needed to make a file transfer:

- Source pathname
- Destination pathname
- Destination site or source site

You can submit a file transfer request even when the communications link between two Prime computers is not operational or when the remote computer is down. File transfer requests are queued on the local (requesting) computer. Once you have submitted a file transfer request, you can display, modify, or cancel it.

File Transfer Request Names and Numbers

FTS associates each file transfer request with a name and number. The name is usually the name of the file being transferred, but it can be a name that you specify with the `-NAME` option. The length of a request name is limited to 32 characters.

The number is a sequential number that FTS assigns to the request in the order that it was submitted for transfer. Leading zeros are suppressed.

You can refer to either the name or the number in FTR command lines. The request number is handy if you have two requests with the same name. Thus, you can use a name when you have only a single request pending, or when you want information on all requests with that name. You can use a number when you want to be sure you are specifying only one request.

Temporary Destination Files

At Rev. 21.0, the FTS Server generates a temporary name for the source file and renames the file to its original name on completion of the transfer. FTS prepends the letters `T$` to the destination filename to create the temporary filename. The name may be truncated to ensure that it does not exceed 32 characters. You can enter the `LIST_DIRECTORY` command during the transfer to display the temporary filename.

The temporary filename prevents the transferred file from being accessed accidentally while the transfer is in process. The temporary filename is recorded in the network log file, which the network operator can access, to aid in identification if the transfer fails. On successful completion of the transfer, FTR performs the following tasks:

- Attaches to the destination directory
- Deletes any existing file with a name that matches the destination filename specified by the user

- Adds the destination file with its temporary name to the destination directory
- Renames the temporary file to the required destination filename

Note

When an Executable Program Format (EPF) runfile is transferred, any existing EPF will be mapped out if it is in use when FTR attempts to rename the runfile.

When You Use FTS

To use FTR, you need to know the following information:

- How to define sites
- What file types you can transfer
- How to use file transfer request names and numbers

Site Names

A unique site name and a server name identify a site. At Rev. 21.0, the site name is the system name that the System Administrator specifies in the system configuration file with the SYSNAM directive. (Pre-Rev. 21.0 sites normally use their PRIMENET system names as site names.)

File Types

Different revisions of FTS support the transfer of different types of files. This section describes what types of files FTS revisions support. Table 4-1 shows the association between FTS revisions and PRIMOS revisions.

FTS Rev. 3 supports transfers of Sequential Access Method (SAM), Direct Access (DAM), and Contiguous Access Method (CAM) files, as well as of standard SEGSAM and SEGDM segment directories.

Notes

CAM files are not supported by PRIMOS revisions prior to Rev. 20.0. FTS will not allow you to transfer a CAM file to a pre-Rev. 20.0 system. An error message is displayed if you attempt such a transfer.

If you want to transfer a CAM file from a source system whose top-level directory FTSQ* resides on a disk created by a pre-Rev. 20.0 revision of the MAKE utility, you must use FTR's `-NO_COPY` option. If you do not specify `-NO_COPY`, FTR attempts to copy the file to FTSQ* and the request fails because FTSQ* cannot contain a CAM file.

FTS Rev. 2 transfers SAM and DAM files as well as SEGSAM and SEG DAM segment directories, but does not transfer CAM files.

FTS Rev. 1 transfers SAM and DAM files only. This revision also converts transferred SAM files into DAM destination files if the files do not already exist at the remote site.

Notes

Revisions 2 and later of FTS can transfer MIDASPLUS™ files and SEG runfiles. FTS cannot transfer ROAM, DBMS, or PRISAM™ files.

FTS can transfer Prime INFORMATION™ files, subject to the above restrictions. Both parts of a Prime INFORMATION file (the data and the dictionary) must be transferred in order for the file to be useful on the destination system. A transferred Prime INFORMATION file is not known to the destination Prime INFORMATION account until a CREATE.FILE is issued with the correct filename. (The correct parameters need not be given, as they are taken from the transferred file.)

FTS and PRIMOS Revisions

Table 4-1 shows the association between FTS revisions and PRIMOS revisions:

TABLE 4-1
FTS Revisions and PRIMOS Revisions

<i>FTS Rev.</i>	<i>Released On PRIMOS Rev.</i>	<i>Will Run On PRIMOS Rev.</i>
1.0	18.4	18.2 through 19.4
1.0	19.0	18.2 through 19.4
1.1	19.1, 19.2	19.0 through 19.4
2.0	19.3	19.0 through 19.4
2.1	19.4	19.0 through 19.4
2.2	19.4	19.0 through 19.4
2.3	19.4	19.0 through 19.4
3.0	20.0	20.0 and above
3.1	20.1	20.0 and above
4.0	20.2	20.2 and above
5.0	21.0	20.2 and above

5

Transferring Files With FTR

This chapter describes the command options for submitting a file transfer request and explains how to use the FTR utility. This chapter includes the following topics:

- Using the FTR Help facility
- Sending a file
- Retrieving a file
- Printing a file
- Checking the status of a request
- Canceling a request

You should read Chapter 4, Introduction to FTS and FTR, before you use the FTR command. The next section describes the FTR Help facility.

FTR Help Facility

To obtain a list of FTR Help subjects, type one of the following commands when you are at PRIMOS command level:

FTR -HELP [subject]

or simply,

FTR -HELP

The following help text appears on the screen:

```
OK, FTR -HELP  
[FTR Rev. 5.0 Copyright (c) 1986, Prime Computer, Inc.]  
Help format :- FTR -HELP <subject>
```

E.g FTR -HELP MESSAGE_LEVEL for help on log message levels.

Sending a File

This section describes how to send a file and begins with a description of the format of the FTR command.

Format of the FTR Command

FTR transfers files between local and remote sites. You can transfer files between users on a local site, but you cannot transfer files between two remote sites. FTR considers the Prime system that you are logged in to and any remote partitions that are added to that system, to be the local site. At least one of the sites must be the local site.

The format of an FTR request is as follows:

FTR source-pathname destination-pathname -DSTN_SITE sitename [options]

The *source-pathname* is the pathname of the file that you want to send. You can give a filename if the file is in your current directory.

The *destination-pathname* specifies the name and location of the transferred file at the destination site.

The **-DSTN_SITE sitename** option specifies the name of the destination site. If you omit the **-DSTN_SITE** option, the default site is your local site. Keep in mind that the definition of local site includes added remote partitions. Therefore, you can send a file to a remote partition without using the **-DSTN_SITE** option.

FTR displays a response to your request in the following format:

Request request-name (request-number) submitted.

The *request-name* usually is the name of the file that you transfer. You can specify a different name with the **-NAME** option. The *request-number* is a unique identification number that FTR assigns.

An Example

Suppose your local site is named SYS2. The following command line shows a file transfer request to SYS4:

```
OK, FTR CENTER>REPORT EXPOST>GROUP2>TEXT -DSTN_SITE SYS4  
[FTR Rev 5.0 Copyright (c) 1986, Prime Computer, Inc.]  
Request REPORT (21) submitted.  
OK,
```

In this example, FTR queues a copy of the file REPORT from the directory CENTER to send to system SYS4 for deposit in the directory EXPOST>GROUP2 under the filename TEXT. The request name is the source filename, REPORT. The unique request number is 21.

Note

If the file is in another directory, or if the directory is passworded, you must enclose the complete pathname (including the password, if needed) in single quotation marks, as in the example, 'MARPLE CLUE>EVIDENCE'. You can type the password in either uppercase or lowercase. A password can be any length, but no more than six characters of a password are matched. If you omit a password or specify it incorrectly, you receive the following error message:

```
Passworded pathname must be fully qualified. (FTR)
```

FTR overwrites files with the same filename. In the FTR example, if a file named TEXT is in the directory EXPOST>GROUP2 before you initiate the transfer, FTR *automatically* overwrites that file with the file TEXT that you are sending. If you do not want to overwrite a file, make certain that the names of transferred files are unique.

Retrieving a File

To retrieve a file from another Prime computer, use the following command format:

```
FTR source-pathname destination-pathname -SRC_SITE sitename [options]
```

The *source-pathname* is the pathname of the file that you want to retrieve. You should give a full pathname because the file is either in another directory on your system or in a directory on another system.

The *destination-pathname* specifies the name and location of the file after it is transferred to your system: the destination site. FTR initially gives the destination file a temporary filename that, on successful completion, FTR changes to the pathname that you specified initially.

The `-SRC_SITE sitename` option specifies the name of the site where the file that you want to retrieve is stored. If you omit this option, FTR searches the local system (site) for the source file.

For example, assume you are on SYS2, and you want to retrieve a file from SYS6 to put in your directory on SYS2. You would enter the following command:

```
OK, FTR PEOPLE>LIST MYUFD>MYLIST -SRC_SITE SYS6
```

This sequence copies the file LIST in the directory PEOPLE on SYS6 into the directory MYUFD on SYS2. The request name is the source filename, LIST. Initially, FTR transfers the file from SYS6 to SYS2 with the temporary name T\$MYLIST and changes it to MYLIST on successful completion of the transfer.

Note

Keep in mind that the destination file actually arrives some time after you type in the FTR command and is transferred with a temporary filename. If you attempt to use the destination file immediately after using FTR, either you will not find the file or the file that you find will contain old data. (FTR overwrites the existing file with the same name.) Use the FTR `-STATUS` command, described below, to determine when the transfer has been completed.

Printing a File at a Remote Site

The `-DEVICE LP` option prints the specified file on the default line printer at the remote site, which is specified by `-DSTN_SITE sitename`. This option uses the PRIMOS spooler. To print a file at a remote site, use the following command format:

```
FTR source-pathname -DSTN_SITE sitename -DEVICE LP -DSTN_USER name
```

The `-DSTN_USER name` option specifies the name of the person who should receive the printout at the remote site. The file is printed with the name of the File Transfer Server (set by your System Administrator) on the first line of the banner instead of a user ID. The name specified after `-DSTN_USER` appears on the second line of the banner of the printed file. The user's name does not have to be a user ID.

For example, assume you are on a system named SYSA. The following command causes the file LETTER to be printed at the default line printer on the remote system SYSF. You cannot set any SPOOL options. FTS uses the following defaults: the first line of the banner is the user ID of the FTS Server, for example, FTP. The second line has the name of the destination user, which is, in this case, JUDY_JONES.

```
OK, FTR STUART>LETTER -DSTN_SITE SYSF -DEVICE LP -DSTN_USER JUDY_JONES
```

Checking the Status of Requests

After you submit a file transfer request, you can check its status with either the `-STATUS` or `-DISPLAY` options. They have the following formats:

```
FTR -STATUS [ request-name  
            [ request-number ]
```

```
FTR -DISPLAY [ request-name  
            [ request-number ]
```

These options display information on each of your file transfer requests and identify them by *request-name* or *request-number*. If you omit the request name, you receive a report on all your current requests.

The `-STATUS` option produces a one-line summary for each request. The `-DISPLAY` option displays complete information on each request. Both options display the status of a request, including whether the request is being processed, is still awaiting processing, or is on hold.

Using the `-STATUS` Option

The `-STATUS` option produces a one-line summary of each request which contains the following information:

- Date and time the transfer request was first submitted
- User ID of the submitting user — normally, your user ID
- Request name
- Request number
- Transfer queue name
- Priority of the request
- Status of the request

The following example illustrates the `-STATUS` option:

```
OK, FTR -STATUS
[FTR Rev 5.0 Copyright (c) 1986, Prime Computer, Inc.]
86-11-30.10:52:12 ELLEN CHAPTER (36) (FTS$5) Status - waiting(D)
OK,
```

In this example, ELLEN submitted a request named CHAPTER on November 30 at 10:52 a.m. Its request number is 36. User ELLEN deferred the request, which is now waiting with a relative priority of 5, the default priority.

The Status category can be one of the following:

<i>Status</i>	<i>Meaning</i>
Waiting	Request is in the transfer queue.
Transferring	Transfer is in progress.
Aborting	An active transfer request is aborting.
Put on hold by user	Request is being held in the transfer queue.
Put on hold by operator	Request is being held in the transfer queue.
Put on hold by FTS	Request is being held in the transfer queue.

Note

The defer symbol (D) following the status category of a request means that the request has been deferred.

Using the -DISPLAY Option

The -DISPLAY option produces a full report on the status of your requests. For example, user SMITH on the system OAK wants to transfer a file to JONES on system LINDEN. The following example shows an FTR request and the FTR -DISPLAY option:

```
OK, FTR LECTURE <LEAF>JONES>LIST -DSTN_SITE LINDEN -DSTN_USER JONES
[FTR Rev 5.0 Copyright (c) 1986, Prime Computer, Inc.]
Request LECTURE (1) Submitted.
OK, FTR -DISPLAY
[FTR Rev 5.0 Copyright (c) 1986, Prime Computer, Inc.]
Request          - LECTURE (1)
User             - SMITH
Queue            - FTSS$1
Priority          - 5
Queued           - 86-11-01.09:55:39  Status - waiting
Last attempt     - 00-00-00.00:00:00  Attempts - 0
Current time     - 86-11-01.14:03:07
Source file      - <BRANCH>SMITH>LECTURE
Source file size - 5162 bytes.
Destination file - <LEAF>JONES>LIST
Source site      - OAK
Destination site - LINDEN
Source user      - SMITH
Destination user - JONES
Source file type - SAM
Destination file type - SAM
Options -:
BINARY, COPY, NO DELETE, NO SOURCE NOTIFY, NO DESTINATION NOTIFY.
OK,
```

The display categories have the following meanings:

<i>Category</i>	<i>Meaning</i>
Request	<i>request-name (request-number)</i> . In the example, <i>request-name</i> is LECTURE and its <i>request-number</i> is 1.
User	Submitter's user ID.
Queue	Queue name where the request is queued.
Priority	Number indicating the relative priority of the request. Priority 5 is usually the default priority. The Network Administrator enables the -PRIORITY option and sets the range of permissible entries.
Queued	Date and time the request was submitted and the request status.
Last attempt	Date and time of the most recent transfer attempt and the number of transfer attempts.

Current time	Current date and time.
Source file	Pathname of the source file.
Source file size	Number of bytes. Displayed only if the source file is on the local site.
Destination file	Pathname of the destination file.
Source site	Source sitename.
Destination site	Destination sitename.
Request log file	Pathname of log file; not always displayed.
Log message level	Level of detail entered in the request log file.
Source user	A user ID (or another name) at the source site to be associated with the transferred file. Useful when notifying a user at a remote site about a transfer.
Destination user	A user ID (or another name) at the destination site to be associated with the transferred file. Useful when printing files at remote sites or when notifying a user at a remote site about a transfer.
Source file type	The type of file being sent or retrieved from the source site. The file type is not always displayed.
Destination file type	The type of file being specified for the destination file on the destination site. The file type is not always displayed.
Options	List of request options.

Recording File Transfers

It is recommended that you create an automatic log of the events related to your file transfer request or that you receive notification about the transfer request if a transfer request fails. This section describes how to use these facilities.

Logging Request Events

To create a log, include the `-LOG` option, in the form `-LOG pathname`, when you submit a request. FTR records logging information on your system — that is, the system where the request originates — in the file specified by *pathname*. Keep in mind that FTS must have ALURW access rights to the directory where you want the log file created.

If *pathname* is a simple filename, the log file is created in the directory to which you are attached when you make the request. If the file specified by *pathname* already exists, the logging information is appended to the end of that file.

For example, you might give the following command:

```
OK, FTR REMIND <LEAF>JONES>NOTE -DS OAK -DU JONES -LOG LOGFILE
```

In this case, the logging information is placed in a file called LOGFILE in your current directory.

If the file transfer is successful, the entries in LOGFILE look like the following entries:

```
11.29.14: [1.1] Request REMIND (1) started Tuesday, November 4, 1986
11.29.14: [1.1] Submitting user is SMITH
11.29.14: [1.1] Local file is <BRANCH>SMITH>REMIND
11.29.14: [1.1] Temporary file is T$REMIND
11.29.20: [1.1] RESULT: Transfer terminated: Satisfactory and Complete.
11.29.20: [1.1] File successfully renamed
11.29.21: [1.1] Request REMIND (1) finished.
```

Logging information includes progress on creating and renaming the temporary destination file and whether the transfer was completed.

The following example shows log entries when a transfer is not completed:

```
10.30.22: [1.1] Request TEST (133) started Wednesday, November 26, 1986
10.30.22: [1.1] Submitting user is SMITH
10.30.22: [1.1] Local file is <SYS12>SMITH>TEST
10.30.26: [1.1] RESULT:Transfer aborted: Remote Service is not running.
10.30.26: [1.1] The transfer will be retried later.
```

Note

If the pathname for a log file contains directory passwords, you must include the password in the pathname and put single quotation marks around the whole pathname. A password can be any length, but no more than six characters of a password are matched. An example is 'SMITH STAR>LOGFILE'.

You can increase the detail entered in your log file by specifying `-MESSAGE_LEVEL` on the FTR command line with one of the following arguments: DETAILED, STATISTICS, or TRACE. NORMAL is the default message level. The number in brackets represents the file server number and the message level, which ranges from 1 (NORMAL) to 4 (TRACE). You must also specify the `-LOG` option. For more information on the `-MESSAGE_LEVEL` option, see Chapter 6, An FTR Reference.

Requesting Notification of Transfers

You can receive notification of the progress of a submitted request through the PRIMOS MESSAGE facility. However, you may not always see all of the message notifications if you are logged out of, or are away from your terminal. To use the MESSAGE facility, specify, on the FTR command line, one of the following options:

<i>Option</i>	<i>Description</i>
<code>{ SRC_NTFY }</code> <code>{ -SN }</code>	Notifies the source users when the file transfer starts and ends. You use <code>-SRC_NTFY</code> when you transfer a file.
<code>{ -DSTN_NTFY }</code> <code>{ -DN }</code>	Notifies the destination user when the file transfer starts and ends. You use <code>-DSTN_NTFY</code> when you transfer a file.

You receive the following messages at your terminal:

```
OK, FTR NEWS IDEAS>PROJECT -DSTN_SITE SYSC -SRC_NTFY
[FTR Rev 5.0 Copyright (c) 1986, Prime Computer, Inc.]
Request NEWS (35) submitted.
```

OK,

.
.
.

```
***FTSERV (user 109 on SYSB) at 16:41
Request NEWS (35) transfer started.
```

OK,

.
.
.

```
***FTSERV (user 109 on SYSB) at 16:43
Request NEWS (35) transfer ok.
```

OK,

In this example, the first message from FTSERV indicates that the file transfer has begun. The second message indicates that the transfer was completed successfully. FTSERV is the name for the FTS Server. This name is set by the System Administrator and may be different on your system.

Note

These are deferred messages. You receive these messages only when PRIMOS displays the **OK**, prompt.

You can specify both the `-SRC_NOTIFY` and `-DSTN_NOTIFY` options together on the same command line if you want to inform a remote source user or remote recipient, as well as yourself, of the progress of the transfer. In this case, you must also identify the remote user to FTR by specifying at least one of the following options on the command line:

<i>Option</i>	<i>Description</i>
$\left\{ \begin{array}{l} \text{-DSTN_USER} \\ \text{-DU} \end{array} \right\}$ user-id	Required with <code>-DSTN_NOTIFY</code> when you are sending a file so that FTR knows whom to notify at the remote site.
$\left\{ \begin{array}{l} \text{-SRC_USER} \\ \text{-SU} \end{array} \right\}$ user-id	Required with <code>-SRC_NOTIFY</code> when you receive a file so that FTR knows whom to notify at the remote site.

For example, if the previous example had included the source notification option `-SRC_NOTIFY`, the messages listed above would be sent to both you and JOHN on SYSC.

```
OK, FTR NEWS IDEAS>PROJECT -DSTN_SITE SYSC -DSTN_USER JOHN
-DSTN_NOTIFY -SRC_NOTIFY
```

Canceling Requests

If you have submitted a request that is currently waiting in a file transfer queue, you can cancel the request with the following command:

```
FTR -CANCEL [request-name
            request-number ]
```

For example, if the request you wanted to cancel was named NEWS (12), either of the following commands would cancel the request:

```
OK, FTR -CANCEL NEWS
```

```
OK, FTR -CANCEL 12
```

You would receive the following message:

```
Request NEWS (12) canceled.
```

`-CANCEL` works only on requests waiting in the queue. To cancel requests that are in the process of being transferred, use the `-ABORT` option.

If a Transfer Fails

If a transfer fails, always check that the FTS Server has the correct access rights to the source and destination directories. Failure to give the FTS Server the correct access rights is a common error. If FTS is unable to complete your transfer request, it takes one of two actions, depending upon the reason for transfer failure.

If the Error Does Not Preclude Trying Again

If the error is not fatal — for example, the remote computer is down, but will be up later — FTS tries to transfer again. The FTS Server attempts retransmission by default every 30 minutes for 72 hours, for a total of 144 tries. The Network Administrator can set these intervals using FTGEN subsystem commands. (See the *PRIMENET Planning and Configuration Guide* for more details.)

If transmission still fails, the request is put on hold with a retry count of 143, so that one more retry is performed after an FTR `-RELEASE` command. (If the file is on hold because of an error that has not been corrected, the transfer fails again.)

If the error occurs because the temporary file that FTS created could not be renamed to the name that the user specified, a message is printed in the log file and the file retains its temporary filename. Subsequent retries use the same temporary filename, but if a user at the destination site has deleted the temporary file, the retry does not depend on the existence of that file.

If the Error Precludes Trying Again

If you enter a password incorrectly in a pathname, FTS suspends the request by putting it on hold. Either you or the system operator can perform one or more of the following steps:

- Delete the request on hold (using FTR `-CANCEL`) and then resubmit the request.
- Correct the request (using FTR `-MODIFY`) so that following a subsequent FTR `-RELEASE` command, the transfer succeeds.
- Release the request for another transfer attempt (using FTR `-RELEASE`).

Other Options

The FTR command permits other options for submitting and managing your requests. FTR options are summarized briefly in Tables 5-1 and 5-2. Chapter 6, An FTR Reference, contains full information on these options.

TABLE 5-1
FTR Submittal Options

<i>Option</i>	<i>Description</i>
-COPY	Copies a file at the time that you submit a request and transfers that copy. This is the default.
-DEFER	Specifies the date and time when the request is to be submitted for processing.
-DELETE	Deletes the local source file after it has been transferred successfully.
-DEVICE LP	Transfers a file to the default line printer.
-DSTN_FILE_TYPE	Specifies either a SAM, DAM, SEGSAM, SEGDAM, or CAM destination file type.
-DSTN_NTFY	Sends messages to the destination user when a file transfer starts and ends.
-DSTN_SITE	Specifies the site to which the file is to be transferred.
-DSTN_USER	Specifies the owner of a file that you transfer and want to print at a remote site.
-HOLD	Holds the file transfer request in the transfer queue.
-LOG	Specifies the pathname of a log file.
-MESSAGE_LEVEL	Specifies the level of detail entered in a log file.
-NAME	Specifies the name of the file transfer request.
-NO_COPY	Transfers a copy of a source file that may be modified until FTS processes the request.
-NO_DELETE	Does not delete the local source file after it has been transferred successfully. This is the default.
-NO_DSTN_NTFY	Does not send messages to the destination user when a file transfer starts and ends. This is the default.
-NO_QUERY	Does not ask you questions when you submit or modify a request.
-NO_SRC_NTFY	Does not send messages to the source user when a file transfer starts and ends. This is the default.
-QUERY	Asks you questions when you submit or modify a request. This is the default.
-QUEUE	Specifies the name of the file transfer queue in which a request is to be placed.
-PRIORITY	Specifies the relative priority of a request in the transfer queue.

TABLE 5-1
FTR Submittal Options – Continued

<i>Option</i>	<i>Description</i>
-SRC_FILE_TYPE	Specifies the source file type. Valid file types are SAM, DAM, SEGSAM, SEGDAM, and CAM.
-SRC_NTFY	Sends messages to the source user when a file transfer starts and ends.
-SRC_SITE	Specifies the site from which a file is to be transferred.
-SRC_USER	Specifies the file owner, or other user, at the source site.

TABLE 5-2
FTR Management Options

<i>Option</i>	<i>Description</i>
-ABORT	Aborts one or more file transfer requests already in progress.
-CANCEL	Cancels one or more file transfer requests sitting in the transfer queue.
-DISPLAY	Displays detailed information on an FTR request.
-HELP	Displays help information on FTR.
-HOLD	Delays one or more file transfers until a user or operator releases the request using the -RELEASE option.
-MODIFY	Modifies a submittal option of an FTR request that you submitted previously.
-RELEASE	Releases one or more held requests.
-STATUS	Displays the status of one or more requests.
-STATUS_ALL	Displays the status of all file transfer requests.

6

An FTR Reference

This chapter contains two sections, which describe all options to the FTR command. Chapter 4 contains overview information on FTR. To learn which options you need to transfer or retrieve files, see Chapter 5, Transferring Files With FTR.

You request file transfers with submittal options. Those options are described in the first section of this chapter, Options for Submitting Requests. You manage, monitor, and cancel file transfer requests with management options. Management options are described in the second section, Options for Managing Requests.

Options for Submitting Requests

This section describes in detail each option that you might use when submitting a file transfer request. The section following this one describes how you manage those requests.

► -COPY

The `-COPY` option makes a copy of the file immediately after you submit your request. (This option has no effect on files that you are retrieving from a remote source.) The FTS Server deletes the copy of the file that it sends to the destination site only after a successful transfer.

You can modify, rename, or delete the original source file after the request has been made. Changes do not affect the copy involved in the transfer. The `-NO_COPY` option (described below) causes a copy of the original file to be sent in whatever way it has been modified up until the time the FTS Server sends it to its destination.

You should be aware that selecting the `-COPY` option uses up disk space because FTS makes a copy of the source file as soon as you submit your request and saves that copy until the transfer is completed. FTS always sends a copy of the source file, but when you use the `-NO_COPY` option, FTS does not save the copy on disk but instead copies it at the time of transfer.

If the size of the local file being transferred is over 250 Kbytes, the following question appears:

```
Size of source file is xxxxxx bytes. Ok to make a copy ?
```


Type Y, YES, or OK to cause FTR to attempt to copy the file. Type N, NO, QUIT, Q, or press RETURN to transfer a copy of the original source file without storing another copy on disk. Any other response causes the original source file to be transferred. If you specified `-NO_COPY` on the command line, the above question does not appear. You can use the `-NO_QUERY` option to suppress questions of this kind.

Specifying both the `-COPY` and `-NO_COPY` options on the same command line causes an error. The default is `-COPY`.

► `-DEFER`

The `-DEFER` option enables you to specify a date and time before which the FTS Server does not process the request. You can specify the deferred time either when you submit the request or when you modify the request (if you chose to do so) before the transfer request begins. If you specify a *date-time* of 0, FTS makes the request available for processing immediately. You can also release a deferred request for immediate transfer with the `-RELEASE` option. Releasing a deferred request does not guarantee transfer at the time of release: it assures that FTR will consider the released request in the normal manner.

`-DEFER` has the following format:

`-DEFER date-time`

where *date-time* can be one of the following full formats:

<code>yy-mo-dd.hh:mm:ss</code>	<code>'dd mon yy.hh:mm:ss'</code>
<code>mo/dd/yy.hh:mm:ss</code>	<code>'dd mon yy.hh:mm:ss'</code>

The two formats in the right column must be enclosed within single quotation marks. *mon* stands for the first three characters of a month (for example, JAN, FEB, MAR) and all other symbols are one-digit or two-digit numbers that represent the following:

- yy — Year (19yy)
- mo — Month (January = 1 or 01, and so on)
- dd — Day (1 or 01 to 31)
- hh — Hour (24-hour notation)
- mm — Minute
- ss — Second

Omitted date fields are replaced by current date information; omitted time fields are replaced by zeros. (For a description of date formats, see the *PRIMOS Commands Reference Guide*.)

In the following example, the submitted request will not be processed until 3 p.m. on November 2, 1986:

```
OK, FTR FRED>TEST LTC>WORK>TEST -DS SYS16 -DEFER 86-11-02.15:00:00
```

You can also omit portions of *date-time* and PRIMOS will insert details as follows: missing date information is taken from the current date (as recorded by the system's internal clock), and missing time information is entered as 00:00 hours. PRIMOS decides what is missing based on the punctuation that you supply, using the above formats. In the following example, assuming today is November 2, 1986, the transfer request is deferred one day, from November 2 to November 3, and will be processed at 00:00 hours:

```
OK, FTR FRED>TEST LTC>WORK>TEST -DS SYS16 -DEFER 11/03
```

In the following example, again assuming the current date is November 2, 1986, the request will be deferred until 21:15 hours, November 2, 1986:

```
OK, FTR FRED>TEST LTC>WORK>TEST -DS SYS16 -DEFER 21:15
```

If you supply any other value, the following error message may be displayed:

```
Invalid defer/time supplied. (F$IDDT)
```

You can specify the `-DEFER` option with `-MODIFY`. The following example shows a request submitted on 8/20/86 with `-DEFER` and then modified by changing the date, but not the time, to 8/21/86:

```
OK, FTR FILE1 DIR>FILE2 -DS S18 -DEFER 18:00
[FTR Rev. 5.0 Copyright (c) 1986, Prime Computer, Inc.]
Request FILE1 (1) submitted.
```

```
OK, FTR -MODIFY 1 -DEFER '08/21/86 18:00'
[FTR Rev. 5.0 Copyright (c) 1986, Prime Computer, Inc.]
Request FILE1 (1) modified.
```

Note that you must respecify both the date and time after `-DEFER` even when you are modifying only the date.

The `-DISPLAY` option shows defer time if you have used the `-DEFER` command. (See Chapter 5, Transferring Files With FTR, for an example.)

► -DELETE

The `-DELETE` option specifies that the original file, which you queued for transfer from the local site to a remote site, be deleted after it has been successfully transferred. This option applies to both `-NO_COPY` and to `-COPY` on local source files. This option does not affect files being transferred from a remote site to the local site.

Specifying both the `-DELETE` and `-NO_DELETE` options on the same command line causes an error. The default is `-NO_DELETE`.

► **-DEVICE LP**

The **-DEVICE** option spools a file at the remote site's default line printer using the PRIMOS SPOOL command. You cannot specify any other line printer commands or SPOOL options with **-DEVICE**. If you do not specify LP, the following message is printed:

```
Missing command line parameter. (FTR)
```

The following command line transfers the file MEMO from the local site to a remote site called MINOS and prints it on that system's line printer:

```
OK, FTR MEMO -DEVICE LP -DS MINOS -DU CLARKE
```

The user banner is the name of the FTS Server, and the file banner is either the name FTS_SPOOL_FILE or the name of the destination user, which is CLARKE in the above example.

Only sequential, direct, and contiguous access method files (SAM, DAM, and CAM files, respectively) can be transferred with this option. Always make sure that the file you specify contains normal text and, optionally, print formatting characters.

► { -DSTN_FILE_TYPE } { SAM
DAM
SEGSAM
SEGDAM
CAM }
{-DFT }

The **-DSTN_FILE_TYPE** option specifies the file type of the destination file. Using this option, you can perform the conversion that you specify in the command line. You can convert SAM files to DAM files, and SEGSAM files to SEGDAM files (and vice versa for both pairs) between FTS Rev. 1 and FTS Rev. 2 systems. The default destination file type is the source file type when you send a file, and null when you retrieve a file from another directory or remote site.

► { -DSTN_NOTIFY }
{ -DN }

The **-DSTN_NOTIFY** option causes the FTS Server to send messages concerning the start and end of a file transfer to the logged-in destination user. Because FTS uses the PRIMOS MESSAGE facility to send these messages, the **-DSTN_NOTIFY** option cannot notify a user who is not logged in.

If you are retrieving a file, the **-LOG** option is generally preferable to **-DSTN_NOTIFY** for learning the progress and results of a file transfer because the **-LOG** option places transfer results in a file.

To send the `-DSTN_NOTIFY` message, FTS requires the name of the destination user. Use the `-DSTN_USER` option to supply this name. Omitting the destination user name causes an error, except when the destination site is the local site. In that case, the submitting user ID is used.

Specifying both the `-DSTN_NOTIFY` and `-NO_DSTN_NOTIFY` options on the same command line causes an error. The default for this option is `-NO_DSTN_NOTIFY`.

► $\left. \begin{array}{l} \text{-DSTN_SITE} \\ \text{-DS} \end{array} \right\} \text{destination-site-name}$

The `-DSTN_SITE` option specifies the name of the system to which the file is to be transferred. The length of the configured node name is limited to 32 characters. Because your System Administrator supplies the site address when configuring FTS, you only need to specify the site name in a file transfer request.

File transfers can take place between the local site and a remote site or between users at the local site. You cannot transfer files between two remote sites. Either the source site or destination site must be the local site. If no destination site is provided, the default is the local site. The definition of local site includes added remote partitions. You can send a file to a remote partition without using the `-DSTN_SITE` option.

On occasion, you may want to transfer a file to a site that is not accessed frequently enough to be configured with FTGEN. In this case, you must quote the open network address of the site in the destination site name. (See Chapter 7, NETLINK, for a description of open addressing.) If you are using open network addressing and have to specify the numeric address along with the server name, the addressing may be a maximum of 128 characters. The *destination-site-name* consists of three parts in the following format:

'address+server(password)'

The *address* can be either a site name (configured by CONFIG_NET, not by FTGEN), or a numeric address. A numeric address must begin with a colon (:). The *server* is the name of the remote file transfer server process, which name is not necessarily the same as that of your local site's server. The *password* is the remote server's password. Single quotes must surround the entire destination site name. Two examples of open network addresses are as follows:

'SYS4+FTPS (THURSDAY)'

':311081800602+FTSRV (SECRET)'

In addition, you must specify the file transfer queue using the `-QUEUE` option, and the queue must be previously configured with FTGEN. If you do not specify a queue, the default places the file transfer request on the OPEN_SYSTEM queue, if it has been configured at the submitting user's site. There is no default queue; one must be specified, such as OPEN_SYSTEM.

► $\left. \begin{array}{l} -\text{DSTN_USER} \\ -\text{DU} \end{array} \right\}$ destination-user-name

The `–DSTN_USER` option specifies the user name or owner at the destination site to which the file is to be transferred. The *destination-user-name* must conform to Prime user naming conventions and is limited to 32 characters. See Chapter 5, *Transferring Files With FTR*, for examples of this option.

The default *destination-user-name* is your user ID, if the destination site for the file is the local site. For a destination site that is a remote site, the default is null.

Use the `–DSTN_USER` option when you use the `–DSTN_NOTIFY` option or the `–DEVICE LP` option or both.

► `–HOLD`

The `–HOLD` option is both a submittal and a management option. The `–HOLD` submittal option causes the file transfer request that you submit to be held on a file transfer queue. It ensures that the request is not initiated until you say so. You free a held request for transfer with the `–RELEASE` management option, described in the section *Options for Managing Requests*.

You can modify held requests before you release them. Only you or an operator can release requests that you hold.

The `–HOLD` submittal option serves the same purpose as the `–HOLD` options described under *Options for Managing Requests*. The advantage of the `–HOLD` submittal option is that holding *on submission* ensures that the request is not initiated immediately, as it might be if there were no requests already outstanding on the request queue. The default is to initiate a request immediately.

► `–LOG pathname`

The `–LOG` option controls the automatic logging of file transfer request events, such as the start of a request submission, the name of the submitting user, the name of the file being transferred, the result of the transfer, and its termination. The `–LOG` option is recommended as preferable to the `–SRC_NOTIFY` and `–DSTN_NOTIFY` options for tracking the progress and results of a file transfer because you can specify a file that you can refer to later.

The log file specified in the *pathname* is a text file and is similar to a command output file. The `–LOG` option requires that the FTS Server have `ALURW` access to the directory where you want the log file created. Chapter 5, *Transferring Files With FTR*, has an example of log file entries. Whenever an event occurs to a file transfer request, FTS records it in this file. You can use the `–MESSAGE_LEVEL` option to specify the level of detail in the log file. (`NORMAL` is the usual detail level.)

If the specified log file already exists, new log entries are appended to it. You may want to remove periodically old entries that build up in a log file that is in continual use.

If the log file that you specify does not exist, FTR creates it. A log file that FTS creates has its read/write lock set to `UPDT` to enable FTS to update it while you are reading the file. (See the

RWLOCK command in the *Prime User's Guide*). The File Transfer Manager must have DALURW rights to your directory in order to write the results of a file transfer request to the log file.

The length of *pathname* is limited to 128 characters. If *pathname* includes a password, it must be a full pathname surrounded by single quotation marks. The default is to not generate a log file.

► { -MESSAGE_LEVEL } { -MSGL } { NORMAL
DETAILED
STATISTICS
TRACE }

The -MESSAGE_LEVEL option specifies the amount of information that is entered in the log file, which you specify with the -LOG option. In order to use -MESSAGE_LEVEL, you must also use -LOG; otherwise, an error occurs.

You can specify the following message levels:

<i>Message Level</i>	<i>Function</i>
1 <u>N</u>ORMAL	Enters a minimum of detailed information in the log including request number, requesting user ID, date of request, local filename, and result of the transfer. This is the default.
2 <u>D</u>ETAILED	Logs all information provided by the NORMAL option, plus the following: time of FTR request, remote filename, local and remote addresses.
3 <u>S</u>TATISTICS	Logs all information provided by the DETAILED option, plus the following: file size, and cpu, job, and disktime statistics.
4 <u>T</u>RACE	Logs all information provided by the STATISTICS option, plus a step-by-step listing of FTR operations.

As an example, the following command line specifies a detailed log of the transfer called MEMO to a file called RANDUM on the remote system BIRCH, in the log file RECORD at the local site:

```
OK, FTR MEMO <MEMDSK>RANDUM -DSTN_SITE BIRCH -DSTN_USER CLARKE  
-LOG RECORD -MESSAGE_LEVEL DETAILED
```

Each log message includes the number of the server link to which the message relates and the numerical value of the message level at which the message is logged. For example, the message

```
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. If you do not specify -MESSAGE_LEVEL when you submit a request, the default message level is NORMAL.

▶ **-NAME request-name**

The `-NAME` option enables you to specify the name of the request in request-name. This name uniquely identifies the request, provided that you have not submitted other requests with the same name.

The default name for a request is the name of the file being transferred. For example, the default name for a source pathname of `FRED>TEL>XYZ` would be `XYZ`. Any name that you use should conform to PRIMOS file naming standards and is limited to 32 characters.

▶ $\left\{ \begin{array}{l} \text{-NO_COPY} \\ \text{-NCPY} \end{array} \right\}$

The `-NO_COPY` option causes the current copy of a file, rather than the copy that existed when you submitted the FTR request, to be transferred.

You should be aware that any changes you make to this file between the time you make the file transfer request and the time when the file is transferred are included in the transfer.

If you use the `-COPY` option, the original file (without any subsequent changes that you might make) is copied when the FTR request is submitted and this copy is used in the file transfer. Specifying both `-NO_COPY` and `-COPY` options on the same command line causes an error. The default is `-COPY`.

▶ $\left\{ \begin{array}{l} \text{-NO_DELETE} \\ \text{-NDL} \end{array} \right\}$

The `-NO_DELETE` option specifies that the local source file, which is to be transferred from the local site to a remote site, is not to be deleted after it has been successfully transferred. This option is the default and it applies to both `-COPY` and to `-NO_COPY` transfers. Specifying both the `-NO_DELETE` and `-DELETE` options on the same command line causes an error.

▶ $\left\{ \begin{array}{l} \text{-NO_DSTN_NTFY} \\ \text{-NDN} \end{array} \right\}$

The `-NO_DSTN_NTFY` option does not notify the destination user of the start and end of a file transfer. Specifying both `-DSTN_NTFY` and `-NO_DSTN_NTFY` on the same command line causes an error. The default is `-NO_DSTN_NTFY`.

▶ $\left\{ \begin{array}{l} \text{-NO_QUERY} \\ \text{-NQ} \end{array} \right\}$

The `-NO_QUERY` option ensures that you are not queried when submitting or modifying a file transfer request. This option is particularly useful for running FTS from a CPL file. See the `-COPY` option for an example of a user query.

Specifying both `-NO_QUERY` and `-QUERY` options on the same command line causes an error. The default is `-QUERY`.

► $\left\{ \begin{array}{l} \text{-NO_SRC_NTFY} \\ \text{-NSN} \end{array} \right\}$

The `-NO_SRC_NTFY` option ensures that no messages are sent by the File Transfer Server to the source user to indicate the start and end of a file transfer.

Specifying both the `-SRC_NTFY` and `-NO_SRC_NTFY` options on the same command line causes an error. The default is `-NO_SRC_NTFY`.

► `-PRIORITY` value

You can set the relative priority for your transfer request with `-PRIORITY` or modify it (with the `-MODIFY` option) after you have submitted it, but before the transfer begins. The System Administrator sets the upper and lower limits for priorities, which normally range from 1 (lowest) through 7 (highest), inclusive. Two additional values (8 and 9) are reserved for use by the System Administrator. The default value is usually 5. If you enter an illegal value, FTR displays one of the following messages:

```
Invalid priority supplied (F$IPRI)
```

```
Privileged user only (F$PUON)
```

FTR does not process a lower priority request until it has processed requests submitted with a higher priority. It is possible for lower priority requests to remain in the queue for long periods of time if other users are continually submitting higher priority requests.

The System Administrator can disable the `-PRIORITY` option or restrict access to some priorities to allow for urgent requests. When the `-PRIORITY` option is disabled, FTS ignores priority settings and services the queue in the order in which users submitted requests. If you attempt to set or modify a priority while the facility is disabled, FTR displays the following error message:

```
Warning: priority mechanism disabled!
```

The following example shows a request submitted with the `-PRIORITY` option:

```
OK, FTR FRED>TEST LTC>WORK>TEST -DS SYS16 -PRIORITY 1
```

In this example, the user is sending the file `TEST` to the directory `LTC>WORK` on destination `SYS16` with a priority of 1, the lowest priority. If another user submits a request with a higher priority, FTR processes that request first.

▶ **-QUERY**

The **-QUERY** option ensures that you are asked to confirm a submitted or modified request. (See the description of the **-COPY** option for an example of a user query.)

The **-NO_QUERY** option suppresses such user queries for that request only. Specifying both the **-QUERY** and **-NO_QUERY** options on the same command line causes an error. The default is **-QUERY**.

▶ **-QUEUE queue-name**

The **-QUEUE** option specifies the name of the queue in which the file transfer request is to be placed. The length of the queue name is limited to 32 characters.

Normally, you use this option only when you send files to a remote site that has not been configured by FTGEN. In this case, you must use the **-QUEUE** option and you must specify a queue that has been configured with FTGEN. The default queue is **OPEN_SYSTEM**, if that queue has been configured. (See your System Administrator for a list of file transfer queues within your network.)

The **-QUEUE** option is seldom used for transfers to configured sites. These requests are automatically placed on the queue for the remote site that the System Administrator has configured. If the **-QUEUE** option is used in this situation, it overrides the default setting.

▶ $\left\{ \begin{array}{l} \text{-SRC_FILE_TYPE} \\ \text{-SFT} \end{array} \right\} \left\{ \begin{array}{l} \text{SAM} \\ \text{DAM} \\ \text{SEGSAM} \\ \text{SEGDAM} \\ \text{CAM} \end{array} \right\}$

The **-SRC_FILE_TYPE** option specifies the file type of the source file. For retrieving files, you can use this option to specify the type of a remote source file. Before transfer commences, the FTS Server determines whether the remote source file type matches the type specified. The transfer is rejected if they do not match. The default for local source files is the type of the source file; otherwise, it is null.

▶ $\left\{ \begin{array}{l} \text{-SRC_NTFY} \\ \text{-SN} \end{array} \right\}$

The **-SRC_NTFY** option causes the FTS Server to send messages to you concerning the start and end of a file transfer. Since FTS uses the PRIMOS MESSAGE facility to send these messages, this option cannot notify you when you are not logged in.

If you are retrieving a file, the **-LOG** option is generally preferable to **-SRC_NTFY** for learning the progress and results of a file transfer because **-LOG** places transfer results in a file.

To send the `-SRC_NOTIFY` message, include the `-SRC_USER` option on the command line. You do not have to specify your name because FTS uses the logged-in user ID as the default.

Specifying both the `-SRC_NOTIFY` and `-NO_SRC_NOTIFY` options on the same command line causes an error. The default is `-NO_SRC_NOTIFY`.

▶ $\left. \begin{array}{l} \text{-SRC_SITE} \\ \text{-SS} \end{array} \right\}$ `source-site-name`

The `-SRC_SITE` option specifies the name of the system from which the file is being transferred. The length of the configured node name is limited to 32 characters. When your System Administrator has configured FTS, you need only to specify the site name in a file transfer request. FTS refers to its configuration for all site addresses.

File transfers can take place between the local site and a remote site or between users at the local site, but not between two remote sites. Either the source site or destination site must be the local site. You do not have to specify the local site because FTS uses this as the default. FTS gets the required information on sites from its configuration.

On occasion, you may want to transfer a file from a site that is not accessed frequently enough to have been configured. In this case, you must quote the open network address of the site as the source site name. Open network addressing for `-SRC_SITE` is identical to that for `-DSTN_SITE`. See the description of `-DSTN_SITE` earlier in this chapter for details on the format of open network addressing.

▶ $\left. \begin{array}{l} \text{-SRC_USER} \\ \text{-SU} \end{array} \right\}$ `source-user-name`

This option identifies the user name or owner at the source site from which the file is being transferred. The *source-user-name* must conform to PRIMOS user naming conventions and is limited to 32 characters.

The default is your user ID if the source site for the file is the local site. The default is null when the source site is a remote site.

Use this option when you use the `-SRC_NOTIFY` option or the `-DEV LP` option or both.

Options for Managing Requests

Use the following options to manage file transfer requests that you have submitted. If you are logged in as SYSTEM, you gain FTS operator privileges that enable you to manage file transfer requests submitted by any user on the system.

Note

FTR commands that you use while logged in as SYSTEM affect all FTR user-submitted requests.

The options have the following format:

FTR option $\left[\begin{array}{l} \text{request-name} \\ \text{request-number} \end{array} \right]$

Descriptions of Management Options

Each FTS site has a default File Transfer Server and file transfer queue. Requests are placed on that queue until the server associated with the queue transfers the queued requests.

Usually, all sites have the same queue associated with them. However, depending on your local FTS configuration, different sites (or groups of sites) may have different queues associated with them. In such cases, the `-QUEUE` option enables you to specify to which queue you want a request to be sent. See your System Administrator for a list of file transfer sites and their associated transfer queues.

► **-ABORT** $\left[\begin{array}{l} \text{request-name} \\ \text{request-name} \end{array} \right]$ `[-QUEUE queue-name]` $\left\{ \begin{array}{l} \text{-NO_QUERY} \\ \text{-NQ} \end{array} \right\}$

The `-ABORT` management option aborts a request, even if the transfer is already in progress, and puts it on hold. See the `-HOLD` option later in this chapter for more information. FTR also enables you to abort with one command all transfer requests that you have submitted. A request that is not in an eligible state to be aborted (for example, those already aborting) does not cause an error. Instead, FTR finds and aborts eligible requests. You can use the `-QUEUE` option to abort only those requests in *queue-name*. If you specify a particular request, the aborted request name and number are displayed. If you do not specify a particular request, FTR displays the following question:

```
Ok to abort all requests?
```

You can suppress this question with the `-NO_QUERY` option. If you do not want to abort all of your requests, type N, NO, QUIT, Q, or press RETURN. To abort all requests, type Y, YES, or OK. The system interprets any other response as a negative response. Aborted request names and numbers are not displayed. Instead, the following message appears:

```
All eligible requests aborted.
```

► **-CANCEL** $\left[\begin{array}{l} \text{request-name} \\ \text{request-number} \end{array} \right]$ `[-QUEUE queue-name]` $\left\{ \begin{array}{l} \text{QUERY} \\ \text{-NO_QUERY} \\ \text{-NQ} \end{array} \right\}$

The `-CANCEL` management option deletes a request from a file transfer request queue. If the transfer is already in progress, or aborting, the request is not deleted. FTR also enables you to cancel with one command all file transfer requests that you have submitted. Requests that are not

in an eligible state to be canceled (for example, those already in progress or aborting) do not cause an error. Instead, FTR finds and cancels all eligible requests. Canceled request names are not displayed. Instead, the following message appears:

```
All eligible requests canceled.
```

If you specify a request name or a request number, that specific request is canceled on any configured file transfer queue. The request name and number are displayed. If you do not specify a request name or number, all requests that you submitted, on any configured queue, are canceled, and the message shown above is displayed. You can use the `-QUEUE` option to cancel only those requests in `queue-name`. If you specify a request, canceled request names and numbers are displayed. If you do not specify a particular request, the following question is displayed:

```
Ok to cancel all requests ?
```

You can suppress this question with the `-NO_QUERY` option. If you do not want to cancel all of your requests, type N, NO, QUIT, Q, or press RETURN. To cancel all requests, type Y, YES, or OK. The system interprets any other response as a negative response.

```
► -DISPLAY [request-name
            request-number] [-QUEUE queue-name] { -QUERY
                                                  -NO_QUERY
                                                  -NQ }
```

The `-DISPLAY` management option shows detailed information about requests. The information includes all that is given by the `-STATUS` option and all that is included in the request. For all formats of the FTR `-DISPLAY` command, passwords contained in the source file pathname, destination file pathname, or log file pathname are displayed only for requests that you own. For other requests, passwords are removed from these pathnames. The following information is displayed:

- Source and destination sites
- Whether the file is to be deleted after the transfer
- Request log file name
- Source and destination pathnames
- The queue on which the request is residing
- The relative priority of the request

If you specify a request name or a request number, that specific request, on any configured file transfer queue, is displayed. If you do not specify a request name or number, all requests that you submitted, on any configured queue, are displayed. The `-QUEUE` option can be used to restrict the requests that are displayed to only those requests found in `queue-name`. If more than one request is output, you are asked between requests if you want to continue output. To suppress the display of this prompt, use the `-NO_QUERY` option.

► **-HELP [subject]**

The **-HELP** management option displays help information. To obtain a list of subjects on which help is available, type either

OK, **FTR -HELP SUBJECTS**

or simply,

OK, **FTR -HELP**

To get help on using FTR command options, type either

OK, **FTR -HELP USAGE**

or simply,

OK, **FTR**

You can also use the following PRIMOS HELP commands to get help: HELP FTR, HELP FTS, HELP FTGEN, HELP FTOP.

► **-HOLD** $\left[\begin{array}{l} \text{request-name} \\ \text{request-number} \end{array} \right]$ **[-QUEUE queue-name]** $\left\{ \begin{array}{l} \text{-QUERY} \\ \text{-NO_QUERY} \\ \text{-NQ} \end{array} \right\}$

The **-HOLD** management option holds a specified request. The request is not initiated until it is released. (See the **-RELEASE** option.) If the request is in a state other than waiting, the command has no effect. FTR also enables you to put all requests on hold with one command. A request that is not in an eligible state to be held (such as one in progress, already held, or aborting) does not cause an error message to appear. If you specify a request name or a request number, that specific request is held in any configured file transfer queue. The request name and number are displayed. If you do not specify a request name or number, all requests you submitted, in any configured queue, are held. FTR does not display the names of requests that it is holding, but displays the following message:

All eligible requests held.

Use the **-QUEUE** option to hold only those requests in *queue-name*. When FTR displays the requests that have been held, FTR includes a **--More--** prompt, which indicates that the display is to be continued after every 23 lines. Use the **-NO_QUERY** option to suppress this prompt.

► **-MODIFY** $\left[\begin{array}{l} \text{request-name} \\ \text{request-number} \end{array} \right]$ [valid-options]

The **-MODIFY** management option modifies the characteristics of a submitted file transfer request prior to initiation. Requests that are not in an eligible state to be modified (for example, those in progress or aborting) do not cause an error message to appear. Instead, FTR modifies all eligible requests that are found. Held requests are not retried until they have been released. Once the requests have been modified, the following message appears:

```
All eligible requests modified.
```

If you specify a request name or a request number, all requests having that name or number, on any configured queue that belongs to you, are modified. The modified request names and numbers are displayed. If you do not specify a request name or number, all requests belonging to you are modified in all configured queues. The message shown above is displayed. You can modify any transfer option, with the following exceptions:

-QUEUE	-NO_COPY	-COPY
-DSTN_SITE	-SRC_SITE	-HOLD
-DSTN_FILE_TYPE	-SRC_FILE_TYPE	

Modifying the characteristics of a request is similar to canceling a request and resubmitting it. However, the **-MODIFY** option keeps the request in the same position in the queue. Therefore, modifying a request generally does not affect the time when the request is initiated unless you modify the priority or defer time of the request. However, canceling and resubmitting a request is likely to delay the initiation time of the transfer.

If you do not specify any valid options, the request will have the following items modified:

- Number of retries is set to zero
- Date and time of last retry is set to zero

If the requests are waiting, this makes them eligible for immediate retry by the File Transfer Server without waiting until the next 30-minute retry period has expired. This can be useful when a previously inoperative site becomes operational and you would like your pending request to be retried as soon as possible.

► **-RELEASE** $\left[\begin{array}{l} \text{request-name} \\ \text{request-number} \end{array} \right]$ [-QUEUE queue-name] $\left\{ \begin{array}{l} \text{-QUERY} \\ \text{-NO_QUERY} \\ \text{-NQ} \end{array} \right\}$

The **-RELEASE** management option initiates a file transfer request that was previously held by the **-HOLD** management option, the **-HOLD** submittal option, or by FTS.

Requests that are not in an eligible state to be released (such as those waiting, transferring, or aborting) do not cause an error. FTR finds and releases all eligible requests. Released request names are not displayed. Instead, the following message appears:

```
All eligible requests released.
```

If you specify a request name or a request number, that specific request is released on any configured file transfer queue. The name and number are displayed.

If you do not specify a request name or number, all the requests that you submitted, on any configured queue, are released. The message shown above is displayed.

You can use the `-QUEUE` option to release only those requests found in *queue-name*. If you specified a request, the released request names and numbers are displayed. If you did not specify a particular request, all requests are released.

When FTR displays the requests that have been released, FTR includes a `--More--` prompt, which indicates that the display is to be continued after every 23 lines. Use the `-QUERY` option to suppress this prompt.

► `-STATUS` $\left[\begin{array}{l} \text{request-name} \\ \text{request-number} \end{array} \right] `[-QUEUE queue-name]` $\left\{ \begin{array}{l} \text{-QUERY} \\ \text{-NO_QUERY} \\ \text{-NQ} \end{array} \right\}$$

The `-STATUS` management option displays information about the current status of the request. For operators logged in under the user ID `SYSTEM`, it displays information on all users. The following information is displayed for each request:

- Date and time the request was queued
- User name of the submitting user
- Name and number of the request
- The queue on which the request resides
- The relative priority of the request
- The current status of the request

If you specify a request name or a request number, that specific request, on any configured file transfer queues, is shown.

If you do not specify a request name or number, then all requests you submitted, on any configured queue, are shown.

You can use the `-QUEUE` option to show only those requests in *queue-name*. If more than a page (23 lines) is output, you are asked at the end of each page whether you want to continue or not. Use the `-NO_QUERY` option to suppress this prompt.

► `-STATUS_ALL` `[-QUEUE queue-name]` $\left\{ \begin{array}{l} \text{-QUERY} \\ \text{-NO_QUERY} \\ \text{-NQ} \end{array} \right\}$

The `-STATUS_ALL` management option returns information about all the currently queued file transfer requests on all the configured transfer queues. You can also see where your requests are in the queue.

Note

This command provides the same information as the `-STATUS` option, except that it provides information on all user requests, not just your own.

The information that `-STATUS_ALL` displays for each request is identical to that displayed in `-STATUS`.

- Date and time the request was queued
- User name of the submitting user
- Name and number of the request
- The queue on which the request resides
- The relative priority of the request
- The current status of the request

You can use the `-QUEUE` option to show only those requests in *queue-name*. If more than a page (23 lines) is output, you are asked at the end of each page whether you want to continue or not. Use the `-NO_QUERY` option to suppress this prompt.

7

NETLINK

This chapter includes the following NETLINK information:

- A description of NETLINK and Packet Switched Data Networks (PSDNs)
- NETLINK's modes of operation
- How to invoke NETLINK
- Network addresses
- NETLINK command procedures

Chapter 8, A NETLINK Reference, describes all NETLINK commands, options, and parameters. Appendix B contains NETLINK error messages.

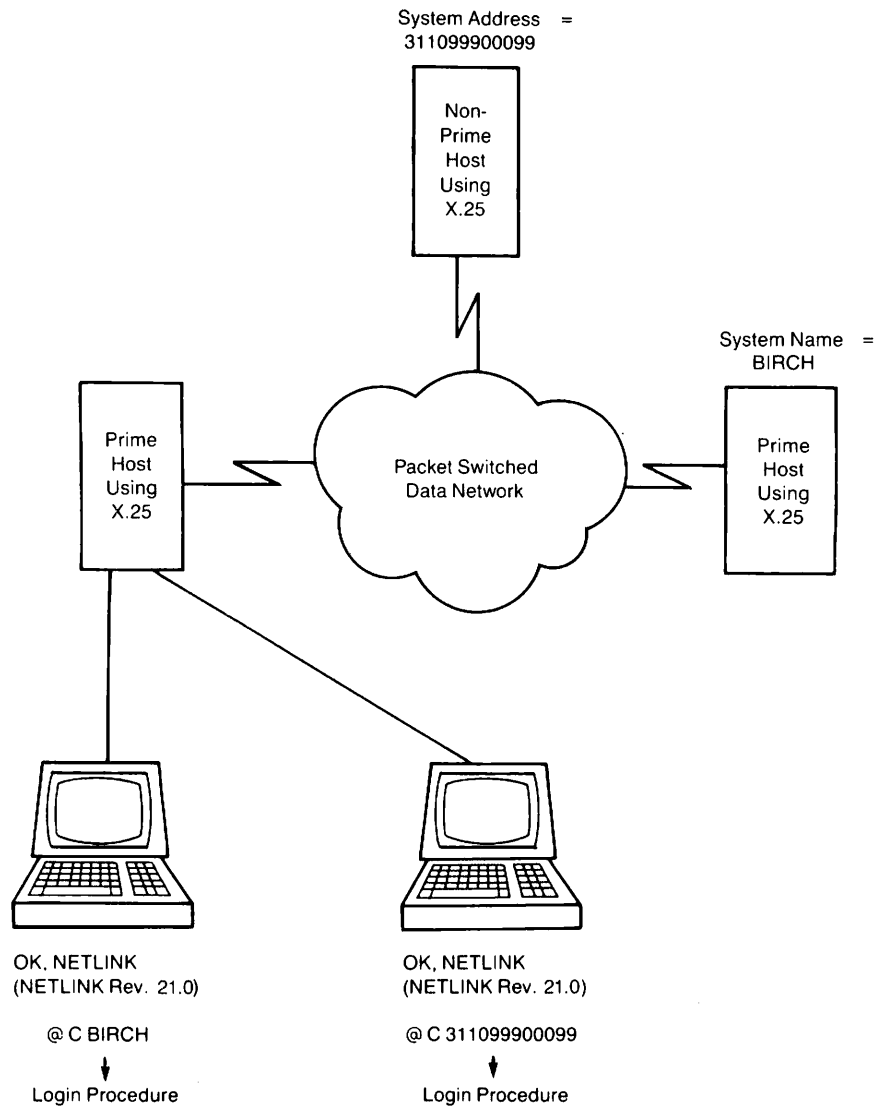
Overview of NETLINK

NETLINK is an interactive utility which enables you to maintain as many as six simultaneous remote login connections, and to switch between these connections. NETLINK provides you with alternative methods of remote login and file transfer in a PRIMENET environment and with hosts linked through PSDNs. For example, if your Prime system is connected to TELENET, you can use NETLINK to connect to other systems connected to TELENET.

50 Series systems can connect to PSDNs that support the CCITT X.25 protocol standards of 1976, 1980, and 1984. Supported PSDNs include TELENET, TYMNET, and UNINET in the United States, DATAPAC in Canada, PSS in Great Britain, TRANSPAC in France, DATEX-P in Germany, and many more.

In addition to having its own configurable features, NETLINK supports CCITT Recommendations X.3 and X.29. All of these provide flexibility in tailoring the connection characteristics to the needs of the remote system.

Figure 7-1 shows a diagram of NETLINK.



**FIGURE 7-1
NETLINK**

To use NETLINK's capabilities fully, you should have some general knowledge of X.3, X.29, and PSDN operation. For special applications, you may need to refer to documentation from the CCITT or from your PSDN. However, the only requirements for using NETLINK, which this guide assumes, are

- Knowledge of the remote node name or X.25 address
- A user ID on the remote node
- Knowledge of any other user-entry passwords or validation codes

The remainder of this chapter provides an introduction to NETLINK functionality, and discusses the major features.

NETLINK's Modes of Operation

NETLINK has two major modes of operation: Command mode and Data Transmission mode.

Command Mode

Command mode enables you to pass commands to NETLINK that perform the following tasks:

- Establish or clear connections
- Switch between open connections
- Modify NETLINK or PSDN parameters associated with a particular connection
- Change the operation of NETLINK

NETLINK displays a prompt to tell you that it is in command mode. The default prompt is '@', but you can change this for each connection using the PROMPT command, described in Chapter 8, A NETLINK Reference.

Data Transmission Mode

Data Transmission mode enables you to interact with a remote host to which you have established a NETLINK connection. NETLINK enters Data Transmission mode either when a new connection is initiated or when a suspended connection is reactivated. All characters that you type on your keyboard, except for the escape sequence, are passed directly to the remote host. This enables you to log in normally and to perform other operations.

NETLINK does not transmit the BREAK Key (CONTROL-P) to a remote host, but can use the X.29 PAD break message (controlled by X.3 parameter 7). See the descriptions of the SET and PAR commands in Chapter 8, and the X.3 parameter descriptions in Appendix C.

Switching Between Modes

Escape sequences enable you to switch between Data Transmission mode and Command mode. NETLINK's default escape character is '@', but you can change this on a per-connection basis using the ESCAPE command, described in Chapter 8. For example, pressing RETURN, typing the escape character (@), and pressing RETURN again returns you to NETLINK Command mode. To return to Data Transmission mode, use the CONTINUE command (described in Chapter 8).

Elementary NETLINK

The basic steps for using NETLINK after you log in are described below:

1. Enter NETLINK Command mode by issuing the command

OK, **NETLINK**

When you enter Command mode for the first time, the NETLINK copyright message is printed followed by the @ prompt.

2. Connect to the remote system by issuing the subcommand

@ **C address**

address is either a host address assigned by the PSDN or a system name that PRIMENET uses. For example, 9060023, :12349060023 and SYS2 are all valid addresses.

When a connection has been established, the following message appears:

address Connected

3. Log in to the system as you would normally, entering any validation codes or passwords as required.
4. Once you finish a terminal session, log out as you would normally. The following message appears:

address Disconnected

When you terminate a connection to a remote host, you re-enter Command mode and the @ prompt appears. You can now connect to another site or return to PRIMOS. Note that you may execute PRIMOS commands or re-enter the PRIMOS environment without terminating your NETLINK session by issuing the '!' or PAUSE commands, both of which are described in Chapter 8, A NETLINK Reference.

5. To end a NETLINK session and return to PRIMOS, enter the command

@ QUIT

Example of a NETLINK Session

The following example shows a basic terminal session. User responses are in bold type. The password is not echoed on the terminal.

OK, **NETLINK**

[NETLINK Rev. 22.1 Copyright (c) 1988, Prime Computer, Inc.]

@ **C SYS9**

SYS9 Connected

PRIMENET 22.1 SYS9

LOGIN HOBBITT

Password?

HOBBITT (user 28) logged in Friday, 05 Dec 88 10:45:32.

Welcome to PRIMOS version 22.1

Copyright (c) 1988, Prime Computer, Inc.

Serial #SDIU0101200269GB (Acme Book Co.)

Last login Friday, 05 Dec 88 10:38:28.

OK,

.
.
.

[Continue with session.]

OK, **LOGOUT**

HOBBITT (user 28) logged out Friday, 05 Dec 88 10:46:44.

Time used: 00h 01m connect, 00m 01s CPU, 00m 01s I/O.

Wait...

SYS9 Disconnected

@ **QUIT**

OK,

NETLINK's HELP Facility

You can get a brief summary of NETLINK subcommands and options by typing HELP in response to the @ prompt. For example,

OK, **NETLINK**

[NETLINK Rev. 22.1 Copyright (c) 1988, Prime Computer, Inc.]

@ **HELP**

Basic commands:

```
C      <address>      Connect to specified address
NC     <address>      Connect without reverse charging
CALL  <address>      Connect and remain in command mode
Quit                               Exit to PRIMOS
PAuse                               Exit to PRIMOS, allow 'S' to continue
COntinue  [<n>]      Continue a currently active circuit
D or CLEAR [<n>]    Disconnect a currently active circuit
! <primos_cmd>      Execute a PRIMOS command from within Netlink
```

Address format summary:

```
<sysname>    <1-10 digits>    <dnic>:<1-10 digits>
:<12-15 digit address>
```

Escape sequences while connected:

```
<CR> <CR>          Escape to command mode
cntrl^P          Send a control^P in the data stream
```

--More--

Profile Parameter Commands:

```
PROMPT <text>          ESCape {<char> | NORMal | ENable}
TO [<address>]         DNIC <dnic>          PORT <n>
TTP {<id> | <name>}    SPEED <bps>          BPS <bps>    POLL <n>
MODE {Remote_ECHO | No_Remote_ECHO | CCITT | TELENET}
PRID [<bytes>]         HPRID <hex_string>
FCTY [{CHarGe | No_CHarGe}] [<bytes>]    HFCTY <hex_string>
DATA [<text>]          MDATA <text>        LDATA <text>    LMDATA <text>  HDATA <hex_string>
Debug {ON | OFF | DUMP | HEX}
PARITY {ASCII8 | ECS | MARK | SPACE | ODD | EVEN}
```

Other commands:

```
STATus          Switch {<n> | BASE}          RESET [<n>]
Profile [{<n> | <name> [{-SAve | -DeLete}] | BASE | -List}]
SET {<parameter>:<value> ... | <name>}    PAR [ <parameter> ...]
```

```

FILE <treename> [ -NTTY -LINE -PAD -CPS <n> -No_SIGnal ]
OUTfile <treename> [ -NTTY -TimeOUT <n> -Continue -No_SIGnal ]
CLOSE { FILE | OUTfile }

```

--More--

Address formats and syntax rules:

```

<system name>                The name of the remote system
or
For Mode CCITT:  p    +    dnic  +    ntn
                  (1 digit) (4 digits) (up to 10 digits)
                  p    +    dcc   +    nn
                  (1 digit) (3 digits) (up to 11 digits)

<pdnic>:<ntn>, <pdcc>:<nn>    Full address which NETLINK interprets
<ntn>, <nn>                  NETLINK will prefix with default DNIC or DCC
:<up to 15 digits>          Literal address, not interpreted by NETLINK
or

For Mode TELENET: p    +    dnic  +    area  +    number  +    ss
                   (1 digit) (4 digits) (3 digits) (2-5 digits) (2 digits)

<p dnic>:<area number>.<ss>   Full address which NETLINK interprets
<area number>.<ss>          NETLINK will prefix with default DNIC
:<area number>.<ss>          NETLINK will not prefix with DNIC

```

@

After the HELP display appears, you receive another @ prompt and can continue with your NETLINK session.

You can also type NETLINK -HELP to see the same HELP message. In this case, you are returned to your system after the HELP message is displayed.

Making a Connection

Use the C or NC command to connect to a remote host. The commands have the following format:

C address [options]

NC address [options]

Use the C command for most connections. For a reverse charge or a collect call (C), any network communications charges are billed to the remote host, which, presumably, passes those charges on to the logged-in user.

Many hosts, especially hosts connected to PSDNs, do not allow collect calls. Use the NC command to hosts that do not permit collect calls. For an NC call, any charges are billed to the originating site.

To connect to a remote host computer, you must know its name or its numeric address. Machines can have many addresses, but only one name. The address is either a name (such as BEECH) or a set of numbers (such as 1234413788). The PRIMOS STATUS NETWORK command lists the names of network nodes (full-duplex, ring, LAN300, or Packet Switched Data Network) that your node can access. There may be additional nodes, not listed, that your node can address by number. Ask your System Administrator for the numeric addresses of computers that you can access.

Since NETLINK can operate over any PRIMENET connection, you can use it to access any system in your network which is connected to PRIMENET. In addition, you can use NETLINK to access both PRIME and non-PRIME systems connected to your PSDN.

Setting Up NETLINK Profiles

Definition and Background

A NETLINK circuit has many attributes which depend on variables associated with your terminal, the target X.25 host, the PAD¹, and the X.25 services. Many of these circuit attributes may be configured by you, the target host and the PAD. Some of the attributes may be adjusted per circuit, while others are global, i.e., affect all circuits, to the NETLINK session. These attributes include

- The X.3/Telenet² parameters, which define characteristics specific to the terminal, i.e. actions that the PAD is to take on receipt of particular input from the terminal, such as a 'break'.
- The 'Connect' parameters, defined as the X.25 aspects of the circuit, such as facilities, which NETLINK uses while establishing a connection.
- The 'Operational' parameters, which define how NETLINK is to control the circuit and present things to the user, i.e., NETLINK's basic operational environment.

It is likely that when connections are repeatedly made to the same host, certain combinations of these parameter settings will be used repeatedly or vary only slightly. For example, one combination of settings might always be used for connections over PSDN's, while another combination might always be used for connections to a particular non-PRIME site.

¹The PAD (Packet Assembler-Disassembler) is a device, usually part of a network node and normally implemented in software, which provides support for start-stop asynchronous terminals over the network by "packetizing" the asynchronous character stream from the terminal before sending the data into the network, and conversely translating packets from the network into character streams before sending them to the terminal.

²Telenet parameters apply only when Mode TELENET has been selected. For more information on this, refer to the MODE command described in Chapter 8, A NETLINK Reference, and the section later in this chapter, Addressing Another System.

For these situations, NETLINK provides the capability to create 'snapshots' of such combinations of parameter settings which would be available on demand during your NETLINK sessions. This capability is known as NETLINK Profiles. It is also sometimes referred to as library profiles.

NETLINK Profiles may be created, modified, retrieved and deleted by name. A library of up to 10 named Profiles may exist during your NETLINK session.

Commonly used profiles may be pre-defined by your System Administrator and made available to all users on your system through the NETLINK Configuration file, which is described in the *Primenet Planning and Configuration Guide*. To find out which profiles, if any, have been defined in the NETLINK Configuration file, type PROFILE -LIST after you have entered NETLINK Command Mode. This displays a list of the names of the pre-defined NETLINK profiles. To display the parameter settings in a particular Profile, first type PROFILE <profile_name> where <profile_name> is one of the names on the list, then type PROFILE.

You may also pre-define your own NETLINK profiles in a PRIMOS Command Input or CPL file, which you would then save and use with future NETLINK sessions. This functionality is illustrated later in this section.

Operation

NETLINK Profiles work as follows:

When NETLINK establishes a circuit, it must set each of the Operational, Connect, and X.3/TELENET parameters to a particular value. It does this by loading the parameters with their current values. These values may

- Be the default values assigned when NETLINK is first invoked.
- Be the result of selecting a library Profile.
- Include changes to particular values made by typing any of several NETLINK Profile Parameter commands.

The current settings (those which are displayed by typing the PROFILE and PAR commands) are the ones used for the next new circuit. These parameter settings are referred to as the Base Profile.

The Base Profile can be selected from among any of the available library profiles or it can be built as any other NETLINK profile would be, by using NETLINK commands to set parameters to specific values. Note that the word 'Base' is not the name of a library profile for new circuits; it is a term given to the collection of parameter settings which will be used at a given point in time for the next new circuit.

A library profile can only be applied to a circuit by loading it into the Base Profile before establishing the circuit. For example, if library profiles 'RING', 'TELENET', and 'LOCAL' have been defined, and you want to use the profile 'RING' for your next new circuit, you must type PROFILE RING. When the connect is made, the parameter settings defined in the library profile 'RING' will be used.

Summary

NETLINK Profiles are designated combinations of parameter settings which may be created and retrieved by name within the NETLINK environment. The name of a NETLINK Profile may be up to 32 characters in length. A maximum of 10 named Profiles may exist in your NETLINK Profile library at a given time. Your NETLINK Profile library exists only for the duration of the NETLINK session in which it was created, and is therefore not saved after the NETLINK session is terminated. Commonly used NETLINK profiles may be created and stored in the NETLINK Configuration file by your System Administrator (described in the *Primenet Planning and Configuration Guide*), or you may create and store them in your own directory through the use of CPL or Command Input files (illustrated in the examples later in this chapter).

A NETLINK profile consists of

- X.3/Telenet PAD parameters: these parameters control characteristics specific to the terminal session and are defined in Appendix C. They are modified with the SET command.
- 'Connect' parameters: DNIC, destination address, PRIMENET port number, facilities, protocol ID, and user data, which are modified with the DNIC, TO, PORT, FCTY, PRID and DATA commands respectively.
- 'Operational' parameters: circuit debugging capability, polling time, escape character, terminal type, terminal speed, parity, command mode prompt, and mode, which are modified with the DEBUG, POLL, ESCAPE, TTP, SPEED, PARITY, PROMPT and MODE commands respectively.

To create a NETLINK Profile:

- Use the NETLINK commands mentioned just above to change the various parameter settings. These commands are described in Chapter 8, a NETLINK Reference.
- Save the parameter settings by typing PROFILE <profile_name> -SAVE, where <profile_name> consists of up to 32 alphanumeric characters.

To use the parameter settings from a particular NETLINK Profile with a new connection, first load them into the Base Profile by typing PROFILE <profile_name> before establishing the connection.

The complete syntax for usage of the PROFILE command and its options, as well as a concise summary of all the NETLINK commands associated with the control of NETLINK Profiles and parameters is included in Chapter 8, A NETLINK Reference.

The following two sections contain examples of the creation and usage of NETLINK Profiles.

Pre-defining a NETLINK Profile Using a Command Input File

Command input files are a way to set up pre-defined NETLINK profiles for your own use. The following example is one such command input file which defines a NETLINK profile 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.

```
OK, slist lan_profile.comi
```

```
/* sample command input file which defines
/* a profile to be used with Ringnet and LAN300
/*
mode remote_echo
poll 1
set 4:1
profile lan -save
! co -end
```

Command input files can be invoked and executed during your NETLINK session by using the ! command. The following example invokes the command input file shown in the preceding example, then makes the LAN profile the Base profile to be used for the next new connection and displays it:

```
OK, netlink
[NETLINK Rev 22.1 Copyright (c) 1988, Prime Computer, Inc.]

@ ! cominput lan_profile.comi

@ /* sample command input file which defines

@ /* a profile to be used with Ringnet and LAN300

@ /*

@ mode remote_echo

@ poll 1

@ set 4:1

@ profile lan -save

@ ! co -end

@ profile -list
Profiles available are:
  LAN

@ profile lan

@ profile
Profile BASE for next Connect ; loaded from library profile LAN

Operational Parameters

Debug:           Off
Polling time:    0.1 Secs.
Escape Character: '@' Normal
```

```
Terminal type:   Unknown
Terminal speed: 1200 bps
Parity:         ASCII8
Prompt:        '@'
Mode:          CCITT with Remote Echo
```

Connect parameters

```
Dnic:          <none>
TO address:    <none>
Port:         <none>
Facilities:   Reverse Charging
Protocol ID:   1 0 0 0 (decimal)
User Data:    <none>
```

@ par

```
2: FULL DUPLEX
3: FORWARD DATA ON: CR ESC Editing Terminators Form Other Cntrl
4: IDLE TIMER = 0.0 Secs.
7: ON BREAK: Discard output
12: X-OFF/X-ON ENABLED
```

```
1:1 2:1 3:126 4:1 5:1 6:1 7:16 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
```

@

Pre-defining a NETLINK Profile in a CPL File

The following example shows a CPL file from which you can run NETLINK and also set up a pre-defined profile named PSDN:

```
OK, slist psdn_profile.cpl

/* sample CPL file which defines
/* a profile to be used with PSDN's
/*
&data netlink
    mode no_remote_echo
    poll 5
    set 4:10
    fcty no_charge
    profile psdn -save
&tty_continue
&end
&return
```

The following example executes the CPL file, then makes the PSDN profile the Base profile to be used for the next new connection and displays it:

```
OK, r psdn_profile.cpl
[NETLINK Rev 22.1 Copyright (c) 1988, Prime Computer, Inc.]

@ mode no_remote_echo

@ poll 5

@ set 4:10

@ fcty no_charge

@ profile psdn -save

@ profile l-list
Profiles available are:
  PSDN

@ profile psdn

@ profile
Profile BASE for next Connect ; loaded from library profile PSDN

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:            <none>
TO address:      <none>
Port:           <none>
Facilities:     No Reverse Charging
Protocol ID:    1 0 0 0 (decimal)
User Data:      <none>

@ par

2: FULL DUPLEX
3: FORWARD DATA ON: CR ESC Editing Terminators Form Other Cntrl
4: IDLE TIMER = 0.5 Secs.
```

7: ON BREAK: Discard output
12: X-OFF/X-ON ENABLED

1:1 2:1 3:126 4:10 5:1 6:1 7:16 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

@

Addressing Another System

The examples in this section describe two methods of addressing another system through NETLINK. The first method uses PRIMENET system names. In this case, an address is a node name consisting of up to six characters. Your System Administrator can tell you the names of the nodes in your network. The second method, used for systems that do not have Prime network node names, uses the systems' PSDN addresses.

Prime System Name Addressing

System name addressing uses the configured name of a remote system. NETLINK automatically looks up and uses the correct address. For example,

@ **C MKTG. 5**

establishes a connection to the remote computer MKTG.5. Configured systems do not have to be Prime systems. Your Network Administrator could configure other machines as PSDN hosts. In this case, users would only need to specify C OTHER, for example, to connect to a remote non-Prime system called OTHER.

PSDN (Packet Switched Data Network) Addressing

When your system is directly connected to a PSDN, you can use open, or PSDN addressing. NETLINK provides two types of open addressing templates which may be selected with the MODE command as options CCITT or TELENET. The use of the MODE command and its options is described in Chapter 8, A NETLINK Reference. The address format definitions and syntax for Modes CCITT and TELENET are described below.

Mode CCITT

Mode CCITT supports X.121 addressing rules which take the following formats:

p + dnic + ntn
(1 digit) (4 digits) (up to 10 digits)

p + dcc + nn
(1 digit) (3 digits) (up to 11 digits)

p	International prefix. This is optional and may take the value 0 or 1.
dnic	Data Network Identification Code.
dcc	Data Country Code.
ntn	Network Terminal Number; the full address that identifies the remote site from within its serving public data network.
nn	National Number; the full address that identifies the remote site from within the national integrated numbering scheme.

For additional information on X.121 addressing formats, refer to CCITT Recommendation X.121.

X.121 addresses may be specified within NETLINK using any of the following syntax formulas:

CCITT Formula 1: full address which NETLINK interprets.

pdnic:ntn	pdcc:nn
dnic:ntn	dcc:nn

A colon must be entered after the dnic or dcc. The colon tells NETLINK to use the digits to the right of the colon as the remote site address, and to concatenate those digits to the dnic or dcc specified. For example, an address entered as 03110:11700074 will become 0311011700074 when transmitted to the network.

CCITT Formula 2: NETLINK will prefix with default dnic or dcc.

ntn (up to 10 digits)
nn (up to 11 digits)

In the case where only the remote site identification number is entered, NETLINK will prefix its default dnic or dcc, if you have previously specified one with the **DNIC** command. (The **DNIC** command is described in Chapter 8, A NETLINK Reference). Note that by selecting Mode **CCITT**, NETLINK's default dnic is automatically set to null. It will assume a value only after one has been specified with the **DNIC** command. For example, if NETLINK's default dnic has been set to 3106, an address entered as 11700074 will become 310611700074 when transmitted to the network. If no dnic or dcc has been previously specified with the **DNIC** command, the address entered as 11700074 will be transmitted to the network as 11700074 - i.e., nothing is prefixed to the address which was entered.

CCITT Formula 3: literal address, not interpreted by NETLINK.

:address (up to 15 digits)

The above formula allows a literal address of up to 15 digits to be specified. A colon must be entered preceding the address. For example, an address entered as :455660500073 will become 455660500073 when transmitted to the network. If a dnic or dcc was previously entered with the **DNIC** command, it is ignored here.

Mode TELENET

Mode TELENET supports TELENET addressing rules and takes the following format:

p + dnic + area + number + ss
(1 digit) (4 digits) (3 digits) (2-5 digits) (2 digits)

- p** International prefix. This is optional and may take the value 0 or 1.
- dnic** Data Network Identification Code. See the **DNIC** command in Chapter 8.
- area** A three-digit code used in identifying the remote site, assigned by the PSDN.
- number** The address identifying the remote site, assigned by the PSDN.
- ss** Optional two-digit subaddress.

TELENET-style addresses may be specified within NETLINK using any of the following 3 syntax formulas:

TELENET Formula 1: full address which NETLINK interprets.

p dnic:area number.ss
p dnic:area number
dnic:area number.ss
dnic:area number

Spaces are ignored by NETLINK, so if a prefix is specified, the dnic will be concatenated to it. A colon must be entered after the dnic. This tells NETLINK to use the digits to the right of the colon as the area, number, and subaddress fields, and also to concatenate those digits to the dnic specified. The first 3 digits to the right of the colon are used as the area. If there are less than 5 digits remaining following the area, NETLINK adds enough leading zeroes to make a total of eight digits in the combined area and number fields. For example, 0 3110:117 74 will become 0311011700074. If a subaddress is specified, it must be preceded by a period (.) in order for NETLINK to interpret it correctly. As with the number field, if only 1 digit is specified for the subaddress, NETLINK adds a leading zero. For example, 3110:117 74.2 will become 31101170007402.

TELENET Formula 2: NETLINK will prefix with default dnic.

area number.ss
area number

In this case, the prefix, dnic, and colon are omitted. This tells NETLINK to concatenate the specified address to NETLINK's default dnic. This dnic may have been specified with the **DNIC** command, described in Chapter 8, A NETLINK Reference, or it may be the default dnic set by selecting Mode TELENET (3110). The area, number, and subaddress fields are handled the same way as in Formula 1, above.

For example, if the default DNIC is 3110, an address entered as 117 74 will become 311011700074 when transmitted to the network. If there is no default dnic, i.e., it was cleared using the **DNIC** command, then nothing is prefixed to the specified address.

TELENET Formula 3: NETLINK will not prefix with dnic.

:area number.ss

:area number

In this case, the presence of the colon without a DNIC and prefix tells NETLINK *not* to concatenate a DNIC to the address. The colon is stripped from the address, while the area, number, and subaddress fields are interpreted the same way as in Formulas 1 and 2.

Connections to Non-PRIME Hosts or Through International Gateways

You can use NETLINK to connect your PRIME computer with any X.25-compatible host computer. For connections to non-PRIME hosts or connections through international gateways, you may need to reset some of the NETLINK profile parameters. These are described in Chapter 8, A NETLINK Reference.

Multiple Connections

NETLINK allows you to establish and maintain as many as six simultaneous connections and to switch your terminal among these connections. After you have made your first connection you may make subsequent connections by returning to Command mode (type the escape character and press RETURN) and then issuing another C or NC command.

You can switch between active circuits by ESCAPE-ing to NETLINK Command Mode and then typing the SWITCH (SW) command or the CONTINUE (CO) command. The SWITCH command leaves you in NETLINK Command Mode and changes the designated active circuit, whereas the CONTINUE command returns you to your login session on the designated circuit (however, no prompt is displayed in this case). Use the D (disconnect) command to disconnect circuits. You remain in NETLINK Command mode and the other active circuits are intact. The following example shows a system-to-system connection, and the SWITCH command:

OK, **NETLINK**

[NETLINK Rev. 22.1 Copyright (c) 1988, Prime Computer, Inc.]

@ **C ELM**

ELM Connected

PRIMENET 22.1 ELM

LOGIN SMITH

Password?

OK, **STATUS NETWORK**

```

      Node      State
    ELM        ****
    PINE        Up
    BEECH       Up
    CHERRY      Up
    BIRCH       Down
    MAPLE       Up
  
```

```

    LINDEN     Down
    ASH        Up
    LAUREL     Up
  
```

OK, @

@ **C ASH**

```

ASH Connected
PRIMENET 22.1 ASH
LOGIN SMITH
Password?
  
```

OK, @

@ **STATUS**

Circuit #	Address	Time	Pkt in	Pkt out
1	ELM	0:00	2	1
-> 2	ASH	0:00	4	3

@ **SW 1**

@ **STATUS**

Circuit #	Address	Time	Pkt in	Pkt out
-> 1	ELM	0:00	2	1
2	ASH	0:00	4	3

@ **QUIT**

```

ELM Disconnected
ASH Disconnected
OK, LO
  
```

Using Different Prompts with Multiple Connections

Specifying a different prompt for each connection can make multiple connections much easier to work with. Initially, all prompts default to '@'. You can specify a different prompt for each connection using the PROMPT command. In the following example, the user changes the prompt to LINDEN> with the PROMPT command, makes a connection from system LINDEN to ELM, then returns to LINDEN:

OK, **NETLINK**

[NETLINK Rev. 22.1 Copyright (c) 1988, Prime Computer, Inc.]

@ **PROMPT LINDEN>**

LINDEN> **C ELM**

ELM Connected

PRIMENET 22.1 ELM

LOGIN SMITH

Password?

SMITH (user 56) login in Wednesday, 06 Aug 88 00:41:32.

Welcome to PRIMOS version 22.1

Copyright (c) 1988, Prime Computer, Inc.

Serial #SDIU010200269GB (Acme Accounting Co.)

Last login Wednesday, 06 Aug 88 00:40:24.

OK, **NETLINK**

[NETLINK Rev. 22.1 Copyright (c) 1988, Prime Computer, Inc.]

@ **PROMPT ELM>**

ELM> @

LINDEN> **QUIT**

ELM Disconnected

OK,

The PROMPT, CONTINUE, SWITCH and DISCONNECT commands are described more fully in Chapter 8, A NETLINK Reference.

Establishing a NETLINK Connection Directly from the PRIMOS Command Line

Through the use of command line options, NETLINK enables you to establish a connection directly from the PRIMOS command line without entering the NETLINK environment.

Use the `-TO` option on the NETLINK command line to connect directly to a remote system. Other options to further customize your connection may be used on the command line as well. These command line options are also NETLINK commands. They are identified in the NETLINK command syntax and are described in the commands reference, both of which are in Chapter 8, A NETLINK Reference.

When using the `-TO` command option (with or without any other additional options), NETLINK connects you directly to the designated address. You can then log in, do your work, and log out. After logging out, you are returned directly to your original system, without getting the NETLINK prompt or needing the QUIT reply.

For example,

```
OK, NETLINK -TO SYS9
[NETLINK Rev. 22.1 Copyright (c) 1988, Prime Computer, Inc.]
```

```
SYS9 Connected
PRIMENET 22.1 SYS9
LOGIN HOBBITT
Password?
```

```
HOBBITT (user 28) logged in Friday, 05 Dec 88 10:57:56.
Welcome to PRIMOS version 22.1
Copyright (c) 1988, Prime Computer, Inc.
Serial #SDIU0101200269GB (Acme Book Co.)
Last login Friday, 05 Dec 88 10:55:36.
```

OK,

```
.
.
.
[Continue with session.]
```

LOGOUT

```
HOBBITT (user 28) logged out Friday, 05 Dec 88 10:58:08.

Time used: 00h 00m connect, 00m 01s CPU, 00m 00s I/O.
```

Wait...

SYS9 Disconnected

OK,

Note

The `-TO` option is especially useful in abbreviations that you create with the `ABBREV` command of `PRIMOS`. For an example of this, refer to the entry for the `TO` command in Chapter 8.

Running NETLINK From a Command Input or CPL File

You can run NETLINK from a command input (COMI) or Command Procedure Language (CPL) file.

Command Input File

If you want to use NETLINK from a command input (COMI) file to log in to a remote system, you need to create two files. One file should contain the `LOGIN` command. The other file is a command input file containing NETLINK commands that make the connection, open the file containing login information, and terminate the connection at the end of a session. The following are examples of the two files. The first example shows a file containing login information.

OK, *SLIST BIRCH.LOGIN*

```
LOGIN SMITH          /* Your user ID
```

OK, *SLIST BIRCH.COMI*

```
NETLINK             /* Invoke NETLINK.
CALL BIRCH           /* Connect to system BIRCH.
                    /* Treat input from terminal or file
                    /* as NETLINK commands.
```

```
FILE SMITH>BIRCH.LOGIN -LINE -NTTY -NO_SIGNAL
```

```
                    /* Read login information from file
                    /* BIRCH.LOGIN; -LINE option sends
                    /* one-line text packets.
                    /* -NTTY option suppresses
                    /* output of file to the screen.
                    /* -NO_SIGNAL option suppresses
                    /* end-of-file message.
```

```
CONTINUE          /* Complete connection to BIRCH;
                  /* leave NETLINK Command mode.
QUIT              /* Disconnect from BIRCH when user
                  /* types @.
CO -E            /* End COMI file.
```

Note

To insure security, login passwords should never be placed in files, such as the login file in the above example.

The following example shows the execution of the COMI file, BIRCH.COMI. You would type in only the first command line and then enter your login password at the prompt; the COMI file does the rest of the work.

```
OK, COMI BIRCH.COMI
[NETLINK Rev. 22.1 Copyright (c) 1988, Prime Computer, Inc.]
```

```
@ CALL BIRCH
```

```
@ FILE BIRCH.LOGIN -LINE -NTTY -NO_SIGNAL
```

```
@ CONTINUE
```

```
BIRCH Connected
PRIMENET 22.1
```

```
Password? YOUR_PASSWORD
```

```
SMITH (user 64) logged in Tuesday, 05 Aug 88 13:33:12.
Welcome to PRIMOS version 22.1
Serial #SDIU0101200269GB (Acme Accounting Co.)
Copyright (c) 1988, Prime Computer, Inc.
Last login Monday, 04 Aug 88 08:45:20.
```

```
OK, ED
```

```
...
...
```

```
OK, @
```

```
@ QUIT
BIRCH Disconnected
OK, CO -E
OK,
```

CPL File

The following example shows a CPL file from which you can run NETLINK.

```

OK, SLIST BIRCH.LOGIN          /* List contents of BIRCH.LOGIN
LOGIN SMITH
OK, SLIST BIRCH.CPL          /* List contents of BIRCH.CPL NETLINK file
&SET_VAR FILE := SMITH>BIRCH.LOGIN /* Set variable for the file
                                   /* (named BIRCH>LOGIN that
                                   /* contains login information.
&DATA NETLINK                    /* Invoke NETLINK.
  CALL BIRCH                      /* Connect to system BIRCH.
  FILE %FILE% -LINE -NO_SIGNAL -NTTY /* Supply login information
                                   /* from the BIRCH.LOGIN file.

CONTINUE                          /* Complete connection to BIRCH and
                                   /* leave NETLINK Command mode.
QUIT                              /* Leave NETLINK. Supply QUIT
                                   /* response when user types @
                                   /* or uses LOGOUT command, thus
                                   /* returning user to home system.
&END                              /* End of &DATA NETLINK statement.

&RETURN                          /* End BIRCH.CPL program and
                                   /* return to PRIMOS command level.

```

The following example shows the execution of the CPL file.

```

OK, RESUME BIRCH          /* Execute BIRCH to netlink to system BIRCH
[NETLINK Rev. 22.1 Copyright (c) 1988, Prime Computer, Inc.]

@  CALL BIRCH

@  FILE SMITH>BIRCH.LOGIN -LINE -NO_SIGNAL -NTTY

@  CONTINUE

```

```

BIRCH Connected
PRIMENET 22.1 BIRCH
Password? YOUR_PASSWORD
SMITH (user 17) logged in Friday, 08 Aug 88 09:50:20.
Welcome to PRIMOS version 22.1
Copyright (c) 1988, Prime Computer, Inc.
Serial #SDIU0101200269GB (Acme Tree Co.)
Last login Friday, 08 Aug 88 09:47:40.

```

```
OK, ED /* Continue with BIRCH session  
...  
...  
...
```

```
OK, @
```

```
@ QUIT
```

```
BIRCH Disconnected  
OK,
```

NETLINK File Transfers

You can use NETLINK's FILE and OUTFILE commands to copy text files either from a local to a remote host or from a remote host to a local host.

NETLINK can copy files between Prime and non-Prime systems. In fact, in some cases NETLINK may be the only way for Prime and non-Prime systems to exchange files over an X.25 network. However, NETLINK does not provide for data transparency. Thus, text is the only form of data that can be copied.

If you are copying files between two Prime systems, it is recommended that you use the File Transfer Service (FTS) or the PRIMOS COPY command instead of NETLINK. See Chapter 4, Introduction to FTS and FTR, for a comparison of FTS and COPY.

Examples of the FILE and OUTFILE Commands

The examples in the next sections show you how to use the FILE and OUTFILE commands to transfer a file to a remote system.

File Transfer Capabilities

You can successfully transfer files consisting of printing characters (including end-of-line RETURN or LF characters). Files can be transferred from any site that can display a file to the terminal user as is done by the PRIMOS SLIST command. You can transfer files to any site that can accept typed input into a file as is done by the PRIMOS ED editor.

Note

Most sites allow a single character or line to be deleted by typing certain characters. PRIMOS has erase and kill characters defined which default to the double quotation mark (") and the question mark (?), respectively. (These are configured at PRIMOS cold start.) The

file specified in NETLINK's FILE command must not contain these characters. NETLINK's OUTFILE command, used to receive files, does not process erase and kill characters.

If the site transmitting the file inserts padding characters, such as NULs or DELs after RETURN, the characters appear in the received file.

Local-to-remote File Transfers

The FILE command transfers a text file to a remote system as if you had typed the text at your terminal. Perform the following steps to send text files to a connected remote host:

1. Make a connection to the remote host and log in.
2. Start up the file editor or utility that will be used to receive the file. If you are connected to a PRIME 50-Series system, start ED and go into Input mode. If you are using ED and the file to be transferred contains semicolons or data, first get into Edit mode and type the MODE NOSEMI command before getting into Input mode. If this is not done, ED will interpret a semicolon as a RETURN.
3. Escape from the remote host by typing @ and pressing RETURN. NETLINK returns to Command mode and displays the @ prompt.
4. Enter the FILE command, the pathname of a file on a disk partition of your local system, and any options. (Refer to the FILE command in Chapter 8, A NETLINK Reference.)
5. Use the CONTINUE command to return to Data Transmission mode. The text of the transferred file appears on your screen (unless you specified the -NTTY option at step 4), and the transfer begins.
6. When the transfer is complete, the message **End of file. filename** appears on your terminal (unless you used the -NO_SIGNAL option at step 4). When the transfer is completed, you need to save the file. If you are using ED, you will be in Input mode. Press RETURN once to enter Edit mode and save the file, then exit ED.
7. Return to NETLINK Command mode and enter a CLOSE FILE command.

The following example illustrates a local-to-remote file transfer between Prime 50-Series systems. The user has already logged in to the remote host.

```
OK, ED
INPUT

@

@ FILE PINE.TRL -PAD

@ CONTINUE
```

This is a test of the NETLINK file transfer facility.

```
/* The above is text in PINE.TRL
/* that is displayed.
```

```
End of File. PINE.TRL      /* Press RETURN here.
```

EDIT

FILE PINE.TRL

OK, @

@ **CLOSE FILE**

Remote-to-local File Transfers

The **OUTFILE** command copies output from a connected remote host to a disk on your local host. Use it in the following manner to transfer files:

1. Make a connection to the remote host and log in.
2. Escape to the local host by entering @ and pressing RETURN. NETLINK returns to Command mode and displays the @ prompt.
3. Enter an **OUTFILE** command with the pathname of the filename you wish to create and any options. The pathname should indicate a partition on the local system. If you supply only a simple filename, the file will be written in the directory to which you were attached when you issued the **NETLINK** command.

Note

If a file of that name already exists, that file is overwritten, so make sure that the filename you enter with the **OUTFILE** command is unique.

4. Use the **CONTINUE** command to return to the remote host. You are at **PRIMOS** command level even though no prompt appears.
5. Issue an **SLIST** (or equivalent) command on the remote host to list the file.
6. Escape to the local host and enter a **CLOSE OUTFILE** command.

The following example illustrates a remote-to-local file transfer between Prime 50-Series systems. In this example, the user has logged in to the remote host and has entered @ RETURN to return to Command mode.

@ **OUTFILE PINE.TRL**

@ **CONTINUE**

SLIST PINE.TRL

/ Text of PINE.TRL appears
/* on your terminal.*

OK, @

@ **CLOSE OUTFILE**

@ **QUIT**

Debugging Using NETLINK

NETLINK's **DEBUG** command enables you to debug many common X.25 circuit connection problems without the need for other diagnostic line monitors. The debugging facilities enable you to see exactly what messages are sent between you and any remote host, Prime or non-Prime. For more information, see the **DEBUG** command in Chapter 8, A NETLINK Reference.

8

A NETLINK Reference

This chapter contains information on NETLINK commands and error messages. It includes the following sections:

- A summary of NETLINK commands, organized by function
- An alphabetical dictionary of NETLINK commands

To understand some NETLINK command descriptions, it is useful to have some knowledge of the CCITT Recommendations X.3 and X.25, as well as some knowledge of how to use Packet Switched Data Networks (PSDNs). For special networking applications, you may need to refer to other CCITT standards and to PSDN literature.

Appendix B, NETLINK Error Messages, lists and describes error messages that NETLINK displays as a result of network errors. Appendix C contains a reference for X.3 and TELENET parameters and their allowable values. For an introduction to NETLINK, refer to Chapter 7.

Commands Summarized by Function

This section contains brief descriptions of NETLINK commands, grouped by function. For full descriptions, see the alphabetical list in the Commands Reference Dictionary section, later in the chapter.

Some of the NETLINK commands can be used as command options to either the PRIMOS-level NETLINK command or to the C, NC, or CALL commands in NETLINK.

The following basic commands, address formats, profile commands, and other commands appear on the screen when you type HELP at the NETLINK command prompt (@). (The usual NETLINK prompt is an at sign (@), but you can change it with the PROMPT command.)

Basic Commands

You can use the following basic commands to make connections to remote hosts, to switch between active connections, to return to NETLINK Command mode, and to return to PRIMOS.

<i>NETLINK Command</i>	<i>Purpose</i>
C address	Connect to specified address
NC address	Connect without reverse charging
CALL address	Connect but remain in Command mode
<u>QUIT</u>	Exit to PRIMOS
<u>CONTINUE</u> [n]	Continue a currently active circuit
D [n/ALL]	Disconnect a currently active circuit
CLEAR [n/ALL]	Synonym for the D command
!primos_command_line	Execute a PRIMOS command from within NETLINK

Profile Parameter Commands

NETLINK profile parameter commands are used for setting the values for the three types of NETLINK profile parameters which together comprise a NETLINK profile. The three types of profile parameters are

- X.3/TELENET PAD parameters, which define characteristics specific to the terminal session.
- Connect parameters, which NETLINK uses while establishing a connection. These are the X.25 aspects of the circuit.
- Operational parameters, which define NETLINK's basic operational environment, i.e., how NETLINK is to control the circuit and present things to the user.

Table 8-1 lists the commands used for setting operational parameters. Table 8-2 lists the commands used for setting connect parameters. X.3/TELENET PAD parameters are specified with the SET command. The X.3/TELENET PAD parameters themselves are described in Appendix C.

TABLE 8-1
Commands Used for Modifying Operational Parameters

<i>Command</i>	<i>Purpose</i>
<u>DEBUG</u> { ON OFF DUMP HEX	Controls the debugging information display.
<u>ESCAPE</u> { escape-character ENABLE NORMAL	Changes NETLINK escape prompt (to a character other than @). ENABLE overrides the disabling of escape by the host. NORMAL allows the host to disable escape.
PROMPT text	Changes NETLINK command mode prompt (to something other than @). The text of the prompt may be a maximum of 31 characters in length.
MODE { REMOTE_ECHO NO_REMOTE_ECHO CCITT TELENET	Selects remote echoing or no remote echoing, and CCITT or TELENET addressing mode.
POLL n	Selects user terminal poll time interval (tenths of a second).
SPEED bps	Supplies a terminal line speed for hosts that ask for one.
BPS bps	Synonym for the SPEED command.
TO address	Selects a destination address.
TTP { id-number name	Selects the terminal type TELENET parameter for certain TELENET hosts. Only used in Mode TELENET.
PARITY { MARK SPACE ODD EVEN ASCII8 ECS	Changes the way NETLINK is to use and interpret the high bit of each byte of data sent to or received from the network.

TABLE 8-2
Commands Used for Modifying Connect Parameters

<i>Command</i>	<i>Purpose</i>
DATA text	Sets the User-data field, zero (stripped) parity.
HDATA hex_bytes	Sets the User-data field.
DNIC dnic	Sets the 4-digit data network identification code in decimal notation.
FCTY $\left[\begin{array}{c} \{ \text{CHARGE} \\ \text{NO_CHARGE} \} \\ \text{bytes} \end{array} \right]$	Specifies a maximum of 109 decimal numbers for the Facilities field. CHARGE sets reverse charging. NO_CHARGE sets no reverse charging.
HFCTY hex_bytes	Specifies a maximum of 218 hex digits for the Facilities field.
LDATA text	Sets the user data field with zero parity, overlaying the Protocol ID (PRID) field.
LMDATA text	Sets the user data field with mark parity, overlaying the Protocol ID (PRID) field.
MDATA text	Sets the User-data field, mark parity.
PORT n	Specifies a two-digit remote PRIMENET port number.
PRID bytes	Specifies the 4-byte Protocol ID (PRID) field in decimal notation.
HPRID hex_bytes	Specifies the 4-byte Protocol ID (PRID) field in hexadecimal notation.

Profile parameter commands can be used in any of the following ways:

- As options to the NETLINK command at PRIMOS level, where they establish a default profile for all connections of the NETLINK session. For example,

```
OK, NETLINK -DNIC 2342
```

- As NETLINK commands, where they modify both the operational and connect parameters of the current circuit or the base profile for subsequent connections. (They do not affect connections already established in this NETLINK session.) For example,

```
OK, NETLINK
[NETLINK Rev. 22.1 Copyright (c) 1988, Prime Computer, Inc.]
@ FCTY 1 1
@ POLL 1
```

- As options to the C, NC, or CALL commands in NETLINK, where they modify only the profile of the connection about to be made, as in the following example:

```
OK, NETLINK
[NETLINK Rev. 22.1 Copyright (c) 1988, Prime Computer, Inc.]
@ C 405 99 -FCTY 1 1 -POLL 1
```

To be used as an option on the PRIMOS command line, a profile command must be preceded by a hyphen.

Other Commands

Table 8-3 lists miscellaneous NETLINK commands.

TABLE 8-3
Miscellaneous NETLINK Commands

<i>Command</i>	<i>Purpose</i>
STATUS	Shows active circuits.
SWITCH { n BASE }	n switches the current circuit to circuit n . BASE switches the current circuit to the Base Profile.
RESET [n]	Sends an X.25 packet-level RESET.
PROFILE { profile_name [-SAVE -DELETE] -BASE -LIST }	Switches to and displays the profile for circuit n . Loads a named profile for new connections or SAVES/DELETES a named profile. Displays the profile to be used for new connections. Lists the names of predefined profiles.
SET parameter:value...	Sets X.3/TELENET terminal parameters.
PAR [parameter...]	Displays X.3/TELENET terminal parameters.
FILE pathname [-NTTY -LINE -PAD -CPS n]	Prepares a local file transfer to a remote system.
OUTFILE pathname [-NTTY -CONTIN -TIMEOUT n]	Copies remote host output to a local file.
CLOSE { FILE OUTFILE }	Ends a file transfer.

Address Formats and Syntax Rules

Addresses may be specified in any of the following ways:

system name	The name of the remote system
or	
For Mode CCITT:	p + dnic + ntn (1 digit) (4 digits) (up to 10 digits)
	p + dcc + nn (1 digit) (3 digits) (up to 11 digits)
pdnic:ntn	Full address which NETLINK interprets
pdcc:nn	
ntn	NETLINK will prefix with default DNIC or DCC
nn	
:up to 15 digits	Literal address, not interpreted by NETLINK
or	
For Mode TELENET:	p + dnic + area + number + ss (1 digit) (4 digits) (3 digits) (2-5 digits) (2 digits)
p dnic:area number.ss	Full address which NETLINK interprets
area number.ss	NETLINK will prefix with default DNIC
:area number.ss	NETLINK will not prefix with DNIC

Escape Sequences

There are two types of escape sequences:

(CR) escape_char (CR)	Escape to Command Mode
CTRL-P	Send a CTRL-P in the data stream

Commands Reference Dictionary

This section describes NETLINK commands in alphabetical order.

► BPS bits-per-second

The BPS command is a synonym for the SPEED command, which is described later in this chapter.

► C address [options]

The C command connects to the remote system that you specify in *address*. You can append an option list to the C command or to the other connection commands, CALL and NC. The options can be any of the profile parameter commands (except for PARITY), although only the connect profile options are described here. Connect profile options and their arguments are listed below:

<i>Option</i>	<i>Description</i>
-DATA text -MDATA text -HDATA hex_bytes -LDATA text -LMDATA text	The -DATA text and -MDATA text options allow a maximum of 12 characters of text for the User-data field. -DATA inserts the characters with parity bits stripped; -MDATA inserts the characters with parity bits marked as received from PRIMOS. -HDATA is the same as -MDATA except that the data is entered in hexadecimal notation. For example, -HDATA C1C2C3C4 would be the same as entering -MDATA ABCD. -LDATA is the same as -DATA except that the user data starts at and overlays the Protocol Identification Field (PRID). -LMDATA is the same as -MDATA except that user data starts at and overlays the Protocol Identification Field (PRID).
-FCTY $\left[\begin{array}{c} \{ \text{CHARGE} \\ \text{NO_CHARGE} \} \\ \text{bytes} \end{array} \right]$	The -FCTY option specifies a non-default Facilities field. For connections to X.25 1984 PSDNs and Prime hosts running PRIMOS Rev. 21.0 and beyond, the legal range for <i>bytes</i> is 0 to 109 decimal numbers that you enter into the Facilities field. For connections to X.25 1980 PSDNs and pre-Rev. 21.0 Prime hosts, <i>bytes</i> can be a maximum of 63 decimal numbers, the values of which can be 0 through 255. If you specify this option without arguments, a zero-length Facilities field results. CHARGE sets reverse charging. NO_CHARGE sets no reverse charging.
-HFCTY bytes	The -HFCTY option specifies a non-default Facilities field in hexadecimal digits. For connections to X.25 1984 PSDNs and Prime hosts running PRIMOS Rev.

21.0 and beyond, the valid range of bytes is 0 to 109 (218 characters, two characters per byte, in pairs, no separators). For connections to both X.25 1980 PSDNs and pre-Rev. 21.0 Prime hosts, the maximum is 63 bytes, the values of which can be 00 through FF. If you specify the option without arguments, a zero-length Facilities field results.

-PORT n

The **-PORT** option specifies a PRIMENET style port, *n*, between 0 and 99. This option is required when the destination of the connection is a program on PRIMOS, rather than the Remote Login service running on a Prime host. PORT 0 is the default and the destination of the Remote Login service.

-PRID { bytes
 text }

The **-PRID** option specifies either the 4 decimal bytes of the Protocol ID field or a quoted string of 4 characters. The bytes must be between 0 and 255; the string must be enclosed in single quotation marks ('). Characters are inserted into the Protocol ID field with stripped parity. The data replaces the default Protocol ID field. For Mode CCITT, it is 1 0 0 0; for Mode TELENET it is 1 0 3 0. Do not use this option with the **-PORT** option because the **-PORT** option uses this field to pass a port number. If you do not specify any arguments, the Protocol ID field is not included in the call request packet.

-HPRID hex_bytes

-HPRID allows you to enter the Protocol identification Field in hexadecimal notation. For example, **-HPRID 0A0B0C0D** would be the same as **-PRID 10 11 12 13**.

-DNIC dnic

The **-DNIC** option sets the 4 digit data network identification code in decimal notation. The information entered will replace NETLINK's default DNIC, which is null for Mode CCITT and 3110 for Mode TELENET.

► **CALL address [options]**

The **CALL** command functions exactly like the **C** command, except that after the connection is made, NETLINK remains in Command mode. Therefore, characters are sent to NETLINK rather than to the remote host. The **CONTINUE** command, described below, is required to complete the connection. The *address* and *options* are identical to those described for the **C** command.

► **CLEAR** $\left\{ \begin{array}{l} n \\ \text{ALL} \end{array} \right\}$

The CLEAR command is a synonym for the D command, described below.

► **CLOSE** $\left\{ \begin{array}{l} \text{FILE} \\ \text{OUTFILE} \end{array} \right\}$

The CLOSE command ends the transfer of a file through NETLINK. The CLOSE command either closes a remote file after you have issued the FILE command or closes a local file after you have issued the OUTFILE command. Only one local or one remote file can be active at any one time.

► **CONTINUE** [*n*]

The CONTINUE command returns you to a previously connected circuit. Use it when you switch between multiple connections and when you return to a connection after you have issued a NETLINK command. The connection number, *n* (value 1 through 6), is not needed for single connections. If you do not specify *n* in multiple connections, NETLINK reconnects the most recently active circuit.

► **D** $\left\{ \begin{array}{l} n \\ \text{ALL} \end{array} \right\}$

The D command disconnects a circuit. Either a specific circuit (given as *n*) or all circuits (given as ALL) can be disconnected. If you do not specify *n*, NETLINK disconnects the most recently active circuit.

► **DATA** *text*
MDATA *text*
HDATA *hex_bytes*
LDATA *text*
LMDATA *text*

The DATA, MDATA, HDATA, LDATA and LMDATA commands correspond to the -DATA, -MDATA, -HDATA, -LDATA and -LMDATA options of the C command. Whereas the options affect only a single connection, the commands establish an environment affecting any future connections.

The DATA and MDATA commands allow a maximum of 12 characters of *text* for the User-data field. DATA inserts the characters with parity bits stripped; MDATA inserts the characters with parity bits marked as received from PRIMOS. HDATA inserts hex bytes equivalent to MDATA. LDATA and LMDATA are the same as DATA and MDATA respectively, except that the user data starts at and overlays the Protocol Identification Field (PRID).

▶ DEBUG {
 ON
 OFF
 DUMP
 HEX
 }

The **DEBUG** option displays control and data message interchanges. **DEBUG ON** displays transmitted or received messages and other events useful for the identification of bugs or network problems. **DEBUG OFF** is the default condition, which does not display debugging data. **DEBUG DUMP** displays the contents (in octal notation) of every packet moved over the virtual circuit being debugged. **DEBUG HEX** displays the contents of every packet moved over the virtual circuit in both ASCII text and hexadecimal notation.

▶ **DNIC number**

The **DNIC** command specifies the Data Network Identification Code for addressing.

The information entered will replace **NETLINK**'s default **DNIC**, which is null for Mode **CCITT**, and 3110 for Mode **TELENET**.

▶ ESCAPE {
 escape-character
 ENABLE
 NORMAL
 }

NETLINK's default escape character is '@'. The **ESCAPE** command allows you to change the escape character. The escape character must be a single character. Changing the escape character is useful when you are already connected to one remote system through **NETLINK** and you want to connect to another. For example, you can be linked to **SYS3** through **SYS1** and **SYS2**, and use *escape-character* to return to **SYS1**, not **SYS2**.

ESCAPE ENABLE allows you to override X.3 parameter 1, i.e. it allows the user to escape to Command Mode in cases where a host system has chosen not to allow this. **ESCAPE NORMAL** allows the host to inhibit escape to Command Mode by setting X.3 parameter 1 to zero.

ESCAPE *escape-character* is applied on a per-circuit basis, whereas **ESCAPE ENABLE/NORMAL** is applied globally to all circuits.

▶ **FCTY** [{
 CHARGE
 NO_CHARGE
 }
 bytes]

The **FCTY** command specifies a non-default Facilities field in decimal notation and corresponds to the **-FCTY** option of the **C** command. Whereas that option affects only a single connection, the **FCTY** command establishes an environment affecting any future connections.

At Rev. 21.0 and beyond, the valid range of the *bytes* parameter can be 0 to 109 decimal numbers, the values of which may be 0 through 255, that you enter into the Facilities field. They replace the default facilities values of 1127. If you specify the option without arguments, a zero-length Facilities field results.

Note

For connections to X.25 1980 PSDNs and pre-Rev. 21.0 Prime hosts, the valid range is 0 through 63 decimal numbers, the values of which may be between 0 and 255.

In addition, the FCTY command can have ASCII mnemonics for specific facility parameter/value byte pairs. The following mnemonics are available:

CHARGE	Sets reverse charging
NO_CHARGE	Sets no reverse charging

An NC command to NETLINK is the same as specifying *C address* -FCTY NO_CHARGE.

► FILE pathname [options]

The FILE command transfers a text file to a remote system. The text must be input to a program such as an editor or a command line on the remote host.

Input is taken from the specified file. Forwarding begins only after you issue the CONTINUE command to continue the connection with the remote system. See Chapter 7, NETLINK, for an example of how to use the FILE command to run NETLINK from a command input file.

The following options are available:

<i>Option</i>	<i>Description</i>
-CPS n	Delays each packet so that the average data rate does not exceed <i>n</i> characters per second. You can use this option with the -LINE option to overcome problems associated with X.25 equipment that does not properly flow control the Packet Assembler/Disassembler (PAD). Remote system parameters or X.25 equipment can sometimes cause too high a data rate, which, in turn, can cause remote system character loss.
-LINE	Sends to the remote host data packets consisting of only one line of text per packet. Some non-Prime hosts accept only one line of text per packet. (Prime hosts normally fill each packet with as many lines of text as it will hold.) Such a remote host will not properly reassemble a file transmitted with filled packets. This option forwards data a line at a time to avoid problems with such hosts.
-NO_SIGNAL	Inhibits the End of file. message that usually appears in NETLINK.
-NTTY	Inhibits displaying a file that is being transferred on the terminal. Information typed at the keyboard is still printed.

-PAD Inserts, or pads, a space at the beginning of each null line. This option prevents the PRIMOS ED editor on a remote system from switching from Input mode to Edit mode when a null line is encountered.

▶ **HDATA hex_bytes**

HDATA is the same as MDATA, except that the data is entered in hexadecimal notation. For example, HDATA C1C2C3C4 would be the same as MDATA ABCD. See the DATA and MDATA commands for more information.

▶ **HELP**

The HELP command displays NETLINK commands and a brief description of each one.

▶ **HFCTY hex_bytes**

The HFCTY command specifies a non-default Facilities field in hexadecimal digits and corresponds to the -HFCTY option of the C command. Whereas that option affects only a single connection, the HFCTY command establishes an environment affecting any future connections.

The *bytes* parameter can be a maximum of 109 bytes (218 characters) in length, the values of which may be 00 through FF.

Note

For connections to X.25 1980 PSDNs and pre-Rev. 21.0 Prime hosts, the valid range is 0 through 63 bytes, the values of which may be 00 through FF.

The hex digits replace the default facilities of 01 01. The bytes are in pairs, which conforms to CCITT standards X.3 and X.29 (see Appendix C, NETLINK Parameters). If you specify the option without arguments, a zero-length Facilities field results.

▶ **HPRID hex_bytes**

HPRID allows you to enter the Protocol Identification field in hexadecimal notation. For example, HPRID 0A0B0C0D would be the same as PRID 10 11 12 13. See the PRID command for more information.

▶ **LDATA text**

The LDATA command is the same as the DATA command, except that the user data starts at and overlays the Protocol Identification field (PRID).

► **LMDATA text**

The LMDATA command is the same as the MDATA command, except that user data starts at and overlays the Protocol Identification field (PRID).

► **MDATA text**

The MDATA command is the marked-parity version of the DATA command. See the DATA command for a description of the MDATA command.

► **MODE** $\left\{ \begin{array}{l} \text{REMOTE_ECHO} \\ \text{NO_REMOTE_ECHO} \\ \text{CCITT} \\ \text{TELENET} \end{array} \right\}$

The MODE command turns remote echoing on or off and selects the addressing mode template. REMOTE_ECHO turns on echoing and sets your terminal to half-duplex, which improves the performance of applications such as EMACS across a high-speed network such as a ring or LAN300. With these options, NETLINK uses different packet-forwarding criteria to improve performance.

Caution

Remote Echo mode can drastically increase costs over Packet Switched Data Networks.

NO_REMOTE_ECHO, which is the default, turns remote echoing off and sets your terminal to full-duplex. NETLINK observes normal forwarding characteristics.

MODE CCITT, which is the default, tells NETLINK to expect X.121 addressing. MODE TELENET tells NETLINK to expect TELENET style addressing, and causes NETLINK to display and utilize TELENET parameters.

► **NC address [options]**

The NC command connects to *address*. Use the NC command when collect calls (reverse charge) are not permitted, such as on international or on internetwork connections. The *address* and *options* are identical to those of the C command.

► **OUTFILE** *pathname* [*options*]

The **OUTFILE** command writes output from a remote host into a file (specified by *pathname*) located on the local host. Enter an **SLIST** (or equivalent) command on the remote host. The following options are available:

<i>Option</i>	<i>Description</i>
-CONTIN	Appends the data to the end of the specified file without overwriting it.
-NO_SIGNAL	Inhibits the End of outfile message that normally appears on a timeout.
-NTTY	Inhibits the printing of output information on the terminal. Input information is still printed.
-TIMEOUT <i>n</i>	Causes NETLINK to close the outfile automatically if data has not been received for <i>n</i> seconds. Timeout counting does not start until after NETLINK has received some data. This means that if you delay entering the SLIST (or equivalent) command, there is not a timeout.

Because **NETLINK** may be talking to a non-Prime host, no protocol can be used. Therefore, data transparency cannot be provided; text files only can be transferred.

► **PAR** [*parameters*]

The **PAR** command displays the **PAD** parameter settings which characterize the terminal session for the current circuit. If no current circuit exists, then the **PAD** parameter settings for the Base profile are displayed. If parameters are specified with the **PAR** command, only the specified parameters and their values are displayed. If no parameters are specified with the **PAR** command, all parameters and their values are displayed. **TELENET** parameters and their values are displayed only when the circuit for which the parameters are being displayed is in Mode **TELENET**.

Parameters are specified by typing the **PAD** parameter ID numbers, separated by spaces. Lists of the **CCITT X.3** and **TELENET** parameters with their ID numbers appear in Appendix C. When parameters are specified with the **PAR** command, **NETLINK**'s display will be in the following format:

parameter:value parameter:value

Both parameter ID numbers and values are printed in decimal notation. An unsupported parameter has **UNK** in the Value field.

A request to read national parameters (such as **TELENET**'s) must have the National Options Marker (**NOM**) preceding the parameters. Because the **NOM** specifying **TELENET** is 0:33, you would enter the following **PAR** command to read international parameters 3 and 4 and **TELENET** parameter 18:

@ **PAR 3 4 0:33 18**

The **PAD** parameters used with **NETLINK** are described in Appendix C.

► **PARITY** {
 MARK
 SPACE
 ODD
 EVEN
 ASCII8
 ECS

The **PARITY** command sets the parity treatment used by NETLINK when transmitting to and receiving from the network. If you are transmitting/receiving characters from the ASCII-7 character set, the high bit may be used for parity, and thus you may select from options MARK, SPACE, ODD, or EVEN using the **PARITY** command. If you are transmitting/receiving characters from the ASCII-8 character set (where no bit is available for parity), you should select the ASCII8 option, which is the default setting. It is used by PRIME and most other remote hosts. PRIME ECS format is the same as ASCII-8, except that the most significant bit is inverted (flipped). PRIME 50-Series systems store their characters internally in PRIME ECS format, although PRIMENET automatically transmits all characters in ASCII-8 format if **PARITY ASCII8** is selected. If there is need to transmit/receive characters in PRIME ECS format, the ECS option to the **PARITY** command is available.

The following settings for the **PARITY** command are recommended for NETLINK operation with remote PRIME hosts:

- When the remote PRIME host is running PRIMOS Rev. 20.2 and earlier revisions, **PARITY SPACE** is recommended. (**PARITY MARK**, **ODD** or **EVEN** will also work, because the remote system will ignore the high bit of each character). If **PARITY ASCII8** is used, characters stored in the upper half of the ASCII-8 character set will be seen as their lower half equivalents by the remote system.
- When the remote PRIME host is running PRIMOS Rev. 21.0 and later revisions, **PARITY ASCII8** is recommended. Using **PARITY SPACE**, **MARK**, **ODD**, or **EVEN** will cause certain characters to be interpreted as their "opposite half" of the character set equivalents. **PARITY SPACE** will work for the "usual" alphanumeric characters, but will jumble many special characters.

Note

Do not confuse the **PARITY** command with X.3 parameter 21, which tells NETLINK how to set and interpret parity of characters sent to and received from the terminal.

► PAUSE

The **PAUSE** command returns your terminal to PRIMOS without altering the circuit state. Use the **PRIMOS START** command to reenter NETLINK Command mode after a **PAUSE**, and use NETLINK's **CONTINUE** command to resume the connection.

The **PAUSE** command is one way to execute PRIMOS commands without altering circuit status. However, the preferred way is to use the **!** command from within NETLINK. As a result of NETLINK being converted to an EPF, potential complications can occur when the **PAUSE**

command is used without a heightened sense of awareness. Because NETLINK is an EPF, you must have a basic understanding of the PRIMOS command environment before using the PAUSE command. Following are some guidelines to be observed:

- Do not RLS the command level at which NETLINK is running, or all of your circuits will be cleared.
- If you invoke a static-mode program after issuing the PAUSE command, RLS that level before typing START, so that the START command will return you to NETLINK rather than the static-mode program.
- Do not invoke NETLINK again while PAUSEing, or you may cause an internal EPF error, and all of your circuits will be cleared.

► POLL *n*

The POLL command sets the polling time interval. The value *n* specifies the tenths of a second between polls of the terminal. NETLINK checks your input buffer for new characters every 0.*n* seconds. The default value for *n* is 5, or a polling rate of twice a second. Frequent polling (a low value of *n*) speeds up terminal response, but requires more packets. Infrequent polling (a high value of *n*) reduces the number of packets transmitted; this lowers the cost of the connection, but slows down terminal response.

► PORT *n*

The PORT command specifies a PRIMENET port, setting the profile so that subsequent connections are addressed to an application program waiting on the specified port. The default value is PORT 0, which is the destination of the remote Login Server. The value of *n* must be from 0 through 99.

► PRID $\left\{ \begin{array}{l} n \\ \text{text} \end{array} \right\}$

The PRID command establishes the Protocol Identification (PRID) field data for future connections. It specifies either the 4 decimal bytes of the Protocol Identification field, or a string of 4 ASCII characters. You must assign the bytes a value of 0 through 255. You must enclose a text string in single quotation marks ('). Text characters are inserted into the PRID field with stripped parity.

The specified PRID replaces the default PRID field of 1 0 0 0 for Mode CCITT, and 1 0 3 0 for Mode TELENET. Note that you can use this command together with the DATA command and its variations to set the user data field to a maximum size of 16 bytes.

Do not use this command if you issue the `-PORT` option or `PORT` command because `-PORT` uses the `PRID` to pass the port number. If you do not give any arguments, the `PRID` field is not included in the call request packet.

Note

In earlier versions of NETLINK, `PRID` bytes were specified in octal. All of NETLINK's numeric parameters are now specified in decimal notation, and some may also be entered as a hexadecimal string.

► **PROFILE** { ⁿ
 profile_name [-SAVE
-DELETE]
 BASE
-LIST }

The `PROFILE` command allows the creation, modification, display, and usage of NETLINK profiles. Setting the values for the individual parameters which comprise a NETLINK Profile is summarized in the Profile Parameter Commands section earlier in this chapter. A definition of NETLINK Profiles and an explanation of their usage and operation is found in Chapter 7, in the section entitled, "Setting Up NETLINK Profiles".

The syntax and explanation of the `PROFILE` command in its various forms is listed below.

PROFILE

Displays the NETLINK Profile Parameters and their settings for the current circuit. (The current circuit is indicated by `"->"` when you issue a `STATUS` command). If there is no current circuit, then the parameter settings for the Base Profile are displayed.

PROFILE n

Switches to and displays the NETLINK Profile Parameters and their settings for circuit `n`.

PROFILE profile_name

Loads the NETLINK Profile Parameter settings from `profile_name` into the Base Profile.

PROFILE profile_name -SAVE

Saves the Base Profile to `profile_name`. Profile names may be up to 32 characters long.

PROFILE profile_name -DELETE

Deletes `profile_name` from the list of available NETLINK profiles.

PROFILE BASE

De-selects the current circuit, if any, and displays the NETLINK Profile Parameters and their settings for the Base Profile. Any subsequent Profile Parameter modifications you now make will be done to the Base Profile (the Base Profile is the profile used for all new circuits).

PROFILE -LIST

Displays the names of the pre-defined NETLINK profiles available for new connections. Up to 10 named profiles may be stored by NETLINK at any given point in time during your NETLINK session.

▶ PROMPT text

The PROMPT command changes NETLINK'S Command Mode prompt. The text can be a maximum of 31 characters in length, and is displayed with a trailing space. If there are spaces in the text, then the text must be enclosed in single quotes. The text entered with the PROMPT command replaces the current prompt. A different prompt may be used for each circuit. Changing the prompt is useful when you have logged in to a remote host which displays the same prompt as NETLINK'S default prompt (@) or when trying to keep track of your active circuits in cases where you have established multiple connections.

▶ QUIT

The QUIT command returns you to PRIMOS from NETLINK. All active connections are disconnected.

▶ RESET [n]

The RESET command with no argument specified sends an X.25 packet level RESET on the current circuit. If n is specified, the RESET is sent on circuit n.

▶ SET { parameter:value parameter:value... } { profile_name }

The SET command sets the X.3 parameters that control terminal characteristics. You specify individual parameters and their values in decimal notation. NETLINK supports X.3 parameters for international and PSDN connections. A complete description of X.3 parameters can be found in the CCITT X.3 documentation. Appendix C contains a list of the X.3 parameters.

To set national parameters such as TELENET's, you must specify the National Options Marker preceding the parameter. For example, the National Options Marker for TELENET is 0:33, so you would enter the SET command as follows to set TELENET parameter 18 to the value 2:

```
@SET 0:33 18:2
```

SET <profile_name> loads the PAD parameter settings from profile <profile_name> into the current circuit. If there is no current circuit, then they are loaded into the Base profile.

► SPEED bits-per-second

The SPEED command (for which BPS is a synonym) tells NETLINK how to respond to terminal speed inquiries from the remote host. It does this by setting the values of X.3 parameter 11 and TELENET parameter 26 to correspond to the speed given in **bits-per-second**.

► STATUS

The STATUS command either displays the status of all active circuits or displays the message **No Active Circuits**. The displayed information includes NETLINK circuit number, address, time (in hours and minutes) that the circuit has been open, and traffic information (number of packets sent and received). An arrow indicates the currently active circuit when there are multiple connections. For example,

```
@ STATUS
```

Circuit #	Address	Time	Pkt in	Pkt out
-----	-----	----	-----	-----
1	BIRCH	6:11	425	233
-> 2	ASH	3:32	13	6
3	LINDEN	2:01	337	158
4	311061700702	1:20	18	6

► SW {ⁿBASE}

The SWITCH command is used in multiconnection operations. It enables you to switch the current circuit to circuit *n*. Your terminal remains in Command mode. You must issue a CONTINUE command to connect to the specified circuit. The CONTINUE *n* command is identical in results to entering SW *n* followed by CONTINUE.

SWITCH BASE selects the Base profile as the 'current circuit'. Any subsequent Profile Parameter modifications you make will now be done to the Base profile.

► **TO address**

The TO command establishes a destination address. As an example, C SYS9 and C -TO SYS9 are the same command. If you enter either as a command to NETLINK, a subsequent C command, without an address, connects to the default address.

TO is most useful when it is entered as -TO on the PRIMOS command line invoking NETLINK, because it allows you to bypass Command mode entirely. This enables you to construct abbreviations (using the PRIMOS ABBREV command), such as

OK, **ABBREV -ADD_COMMAND DENVER NETLINK -TO DENVER**

When you use -TO this way, NETLINK performs an implied QUIT if the connection is broken. For example,

OK, **DENVER**

[NETLINK Rev. 22.1 Copyright (c) 1988, Prime Computer, Inc.]

DENVER Connected

/ user session with remote system
/* user logs out*

DENVER Disconnected

OK, */* you are now on your local system*

You can use additional options with -TO as required. The following example is the equivalent of using the NC command and creates an abbreviation (FARGO) for an otherwise lengthy command:

OK, **ABBREV -ADD_COMMAND FARGO NETLINK -TO 701884 -FCTY NO_CHARGE**

► **TTP** $\left\{ \begin{array}{l} \text{id-number} \\ \text{name} \end{array} \right\}$

The TTP command tells NETLINK the terminal type. This command affects only TELENET and a few types of hosts. Those hosts "read the terminal type" and perform special character handling for different terminal types. Allowed terminal names are: UNKNOWN, BEEHIVE, FOX, OWL, PRINT, PT45, VT50, VT100, PST100, PT200, and PT250.

Names are translated into the appropriate value for TELENET parameter 23. If you specify a number, this number is used as the value for TELENET parameter 23.

► !primos_command_line

The ! command allows a PRIMOS command line to be typed and executed from within NETLINK. Active PRIMOS abbreviations are expanded. Since NETLINK is an EPF, there are no limitations on the programs which may be run. At the end of execution, control is returned to NETLINK Command Mode.

Note

Do not invoke NETLINK using the ! command. This may cause an internal EPF error and all your circuits will be cleared.

Appendices

A

FTS Error Messages

This appendix lists and explains the error messages produced by FTS. The messages are divided into the following sections:

- General error messages that any FTS utility may produce.
- Messages produced by the FTR utility, which enables you to submit and manage file transfer requests.
- Messages sent to the server, site, queue, and request log files. The System Administrator configures server, site, and queue log files with the FTGEN utility, as described in the *PRIMENET Planning and Configuration Guide*. These logs normally reside in the FTSQ* directory.

A request log file is associated with a particular file transfer request. The user who submits the request creates the request log file by including the `-LOG` option on the FTR command line. The messages in this section generally indicate the progress of FTR requests and the nature of any errors encountered while requests are processed.

Some messages appear in more than one section. Many messages also occur in applications that use the FT\$SUB subroutine, which is described in the *Programmer's Guide to Prime Networks*.

General Error Messages

The following errors can occur in any of the FTS utilities.

Argument too long. (F\$ARTL)

You specified an argument that was longer than the maximum allowed argument length.

Argument too short. (F\$ARTS)

You specified an argument that was shorter than the minimum allowed argument length.

FTS not ready for use. (Q\$QNRD)

The FTS database has not been initialized with the FTGEN INITIALIZE_FTS command.

No help is available on the subject xxxxxx

You have requested help regarding a topic for which online documentation is unavailable.

The FTS database is invalid. (Q\$NVDB)

The FTS database has been corrupted, or an FTGEN INITIALIZE_FTS command has not been performed after FTS installation.

FTR Error Messages

The following messages may occur when you are using FTR.

Bad command line format. (F\$BDCL)

The format of the command line is incorrect. You should type FTR LETTER -CANCEL instead of FTR -CANCEL LETTER.

Bad device name. (F\$BDDN)

You typed an invalid device name. LP is the only correct device name.

Bad site name format. (F\$BDSN)

You type an invalid site name. The site name must be a valid one and adhere to the PRIMOS filename standard. See the *Prime User's Guide* for more information on naming standards.

CAM files not supported on the remote system. (F\$PCNT)

You are trying to transfer a CAM file to a site that is not capable of handling such files (that is, a pre-Rev. 20.0 site or a Rev. 20.0 site with disks created by a pre-Rev. 20.0 revision of the MAKE utility).

Command lines must be null. (F\$CLMN)

You specified an FTR management option and included extraneous items on the command line. Reissue the command, ensuring that the command line contains only the items specifically documented for the management option you are using.

Conflicting options. (F\$CNOP)

The options that you specified conflict. For example, you specified a request with both -COPY and -NO_COPY when you must specify either one option or the other.

Copy flag may not be modified. (F\$CPMD)

You tried to modify the copy flag. This is not allowed. For example, the following command would generate this error:

```
OK, -MODIFY 2 -COPY
```

Copy option only applies to local source file. (F\$CPLS)

You specified this option when you were retrieving a file from a remote site. This is not allowed. The -COPY option applies only when you are sending local files.

Delete option only applies to local source file. (F\$DLLS)

You specified the -DELETE option when you were retrieving a file from a remote site. This is not allowed. The -DELETE option applies only when you are sending local files.

Destination file access mode invalid. (F\$DFAC)

The destination file type is not one that FTS supports. Only SAM, DAM, SEGSAM, SEGDM, and CAM files are supported.

Destination file has not been specified. (F\$DFNS)

You did not specify a destination pathname. See Chapter 5, Transferring Files With FTR, for the format of an FTR command line.

Destination file may not be modified. (F\$DFMD)

You tried to modify the destination file option. This is not allowed.

Destination site is not configured. (F\$DSNC)

The destination site has not been configured in the FTS configuration for your site.

Destination site may not be modified. (F\$DSMD)

You tried to modify the destination site name. This is not allowed.

Destination user name invalid. (F\$DUIN)

You used an invalid destination user ID. The user ID must conform to the PRIMOS standard for user IDs. See the *Prime User's Guide* for more information.

Destination user not specified when destination notify requested. (F\$DUNS)

You did not specify a destination user (with -DSTN_USER) with your request to send a file. You must specify a destination user if you use the FTR -DSTN_NOTIFY option.

Device transfer from remote site not allowed. (F\$DRNA)

You attempted to retrieve a file from a remote site and send it a local device. This is not allowed.

Duplicate option. (F\$DUOP)

You duplicated one or more options on a command line. The following example duplicates the -SRC_NOTIFY option. This is not allowed:

```
OK, FTR <ASH>TREE <ELM>BRANCH -SRC_NOTIFY -DSTN_USER CLARKE -SRC_NOTIFY
```

Full pathname too long. (F\$FPTL)

You exceeded the maximum pathname length of 128 characters.

Hold flag may not be modified. (F\$HDMD)

You tried to modify the hold flag. This is not allowed. For example, the following command would produce this error:

```
OK, FTR -MODIFY 3 -HOLD
```

Illegal file or directory conversion. (F\$IFDC)

You used the `-SRC_FILE_TYPE` or `-DSTN_FILE_TYPE` options in an invalid combination. See Chapter 6, An FTR Reference, for more information on these options.

Invalid defer date/time supplied. (F\$IDDT)

You specified a date or time with the `-DEFER` option in an invalid format. See Chapter 6, An FTR Reference, for a description of this option.

Invalid destination file type. (F\$IDFT)

You did not specify a correct destination file type. See the `-DSTN_FILE_TYPE` option description in Chapter 6, An FTR Reference, for a description of this option.

Invalid source file type. (F\$ISFT)

You specified an incorrect source file type. See Chapter 6, An FTR Reference, for more information on the `-SRC_FILE_TYPE` option.

Message level specified but request log treename omitted. (F\$MBNL)

You specified the `-MSGL_LEVEL` option with a specific level, for example, `DETAILED`, but you did not specify a log filename with the `-LOG` option.

Missing command line parameter. (F\$MCLP)

The command line has a required parameter missing. The following example omits a destination user ID with the `-DSTN_USER` option:

```
OK, FTR <ELM>TREE <ASH>BURN -SRC_NTFY -DSTN_USER
```

Networks unavailable. (F\$NUNA)

You tried to use FTR to submit a request, but the network has been shut down or is not configured.

No Copy flag may not be modified. (F\$NCMD)

You tried to modify the `NO_COPY` flag. This is not allowed. For example, the following command would cause this error:

```
OK, FTR -MODIFY 2 -NO_COPY
```

No copy option only applies to local source file. (F\$NCLS)

You specified the NO_COPY option when you were retrieving a file from a remote site. This is not allowed. The NO_COPY option is allowed only when you send files from your system to another system.

No delete option only applies to local source file. (F\$NDLS)

You specified the -NO_DELETE option when you were retrieving a file from a remote site. This is not allowed. The -NO_DELETE option is allowed only when you are sending local files.

No eligible request of this name found. (F\$NERF)

You attempted to modify, abort, release, hold, or cancel requests with the specified name without success because either they do not exist or they are in an ineligible state. For example, you would receive this error if you tried to hold a request that was already held.

No request of this name found. (F\$NRFD)

You specified a nonexistent request name when you used a -DISPLAY or -STATUS option to check the status of a particular request. Check that you specified the right name, or use the request number in the command.

No requests queued. (F\$NRQD)

You tried to list the contents of a queue that is empty.

Not configured. (F\$NTCF)

You specified a site, server, or queue that had not been configured with FTGEN.

Only one management option allowed. (F\$OMOP)

You specified more than one management option. This is not allowed. For example, FTR -ABORT LETTER -CANCEL is not allowed.

Passworded pathname must be fully qualified. (F\$PSFQ)

Either you did not specify a passworded pathname from the directory down to the filename or you did not enclose the complete pathname, including the password, in single quotation marks, or both.

Priority x for administrator only

You specified a priority value that is reserved for the System or Network Administrator's use only. You must specify a value in the range 1 through 7.

Privileged user only (F\$PUON)

You either specified a priority that is not allowed or the Network Administrator has disabled the -PRIORITY option. See Chapter 6, An FTR Reference, for a description of this option.

Queue blocked. (Q\$QBLK)

You tried to submit a request to a queue that has been blocked with the FTGEN BLOCK_QUEUE command. The queue must be unblocked with the FTGEN UNBLOCK_QUEUE command so that requests can be accepted.

Queue does not exist. (Q\$QNEX)

You tried to submit a request to a request queue that has not been configured with FTGEN.

Queue full. (Q\$FULL)

The request queue is full.

Queue name may not be modified. (F\$QNMD)

You tried to modify the -QUEUE option. This is not allowed.

Remote treename incorrectly specified. (F\$RTIS)

You specified a pathname for the destination site that was incomplete. You must specify the entire pathname in the command line.

Request already aborting. (F\$RQAB)

You tried to use an FTR management option (except -STATUS or -DISPLAY) on an aborting request. This is not allowed.

Request already put on hold by FTS. (F\$RQHF)

You tried to hold or abort a request that FTS is holding. This is not allowed.

Request already put on hold by operator. (F\$RQHO)

You tried to hold or abort a request that has already been held by an operator. This is not allowed.

Request already put on hold by user. (F\$RQHU)

You tried to hold or abort a request that has been put on hold already.

Request held by operator. (F\$RHPR)

You tried to release an operator-held request.

Request log treename same as source or target treename. (F\$RLST)

You specified a log filename that is not different from the source or destination pathname.

Request waiting. (F\$RQWT)

You tried to release a waiting request. This is not allowed.

Segment dir. transfer to/from a Rev 1 site is not supported. (F\$PINS)

You tried to transfer a SEG file to or from a Rev. 1 FTS site. This is not allowed.

Source file access mode invalid. (F\$SFAC)

The source file type that you specified is not one that FTS supports. Only SAM, DAM, SEGSAM, SEGDM, and CAM files are supported.

Source file does not exist. (F\$SFNE)

You tried to transfer a nonexistent file. Check to see that you specified an existing file for the transfer request.

Source file has not been specified. (F\$SFNS)

You did not specify a file to be sent or retrieved in the transfer request.

Source file type may not be modified. (F\$SFMD)

You tried to modify the source file type. This is not allowed.

Source or destination site must be local. (F\$SDSL)

You cannot make file transfers between two remote sites. You can transfer requests either in loopback on a local site, or between local and remote sites only.

Source site is not configured. (F\$SSNC)

You specified a source site that has not been configured with FTGEN.

Source site may not be modified. (F\$SSMD)

You tried to modify the source site. This is not allowed.

Source user name invalid. (F\$SUIN)

You specified an incorrect source user ID. User IDs must conform to the PRIMOS naming standard. See the *Prime User's Guide* for more information.

Source user not specified when source notify requested. (F\$SUNS)

You did not specify the source user (with `-SRC_USER`). You must specify a source user if you use the `-SRC_NOTIFY` option in the command line when you retrieve a file.

Specified and actual source file types differ. (F\$SFTD)

You used the `-SRC_FILE_TYPE` option, but the file type that you specified differs from the actual source file type.

Transfer in progress. (F\$TRPR)

You tried to release, cancel, modify, or hold a transferring request. This is not allowed.

Transfer rejected: Problem with remote file.

The file could not be opened for transfer. Check to be sure you have spelled the filename correctly. Also, check with the remote site to be sure that the partition has sufficient space for the file you are transferring, and that the remote server has access to the destination directory.

Transfer rejected: Will not retry.

This message, which usually appears along with other messages, indicates that an error has occurred and that retrying the transfer will not help until the error is corrected. The request is put on hold.

Transfer to a device as well as a file is not allowed. (F\$TDFN)

You specified both a destination file and a destination device (-DEVICE LP) in one transfer request. This is not allowed.

Transferring a file to itself is not possible. (F\$TFNP)

You used only one filename for two files in a transfer request. The source and destination file cannot be the same.

Transferring a SEG directory to a DEVICE is not supported. (F\$TDNS)

You tried to print a SEG file type on a remote line printer. This is not allowed.

Unable to create temporary file. (Q\$UCTF)

The number of temporary files in the FTSQ* directory may have reached the maximum number as a result of queued requests. The operator should do the following:

- Investigate the possibility of canceling old requests.
- Check that correct FTS-related access rights are assigned.
- Check that the partition containing FTSQ* is not full and that quotas on FTSQ* and its partition are set to appropriate values.

Unknown keyword. (F\$BDKW)

You specified an argument in the command line that FTS does not recognize. For example, the following command line contains an unknown keyword, -FRED:

OK, **FTR<ASH>TREE<ELM>BRANCH -FRED**

The command line should also include -DSTN_USER (abbreviation is -DS) for the user ID FRED.

Unknown option. (F\$UNOP)

You specified an option in the command line that FTS does not recognize. For example, the following command line specifies an invalid option, `-EXTRA`:

```
OK, FTR <ELM>TEST <ASH>ANSWERS -DSTN_USER JONES -SRC_NOTIFY -EXTRA
```

Warning: Priority mechanism disabled!

The Network Administrator has disabled the `-PRIORITY` option.

Messages Sent to Server, Site, Queue, and Request Log Files

The following messages are sent to the server log file and also to the relevant queue, site, and request logs if they exist. Many of these messages indicate the progress of FTR requests and the nature of any errors encountered while requests are processed. Requests are often retried after these messages appear.

Except where otherwise noted, a variety of file system problems can cause each of these messages. Each message is usually accompanied by one or more PRIMOS messages indicating the specific file system problem. If the problem recurs and the accompanying messages do not provide enough explanation, contact your System Administrator.

Can't create subsystem from remote node.

Refer to the general comments at the beginning of this section.

Can't submit to queue.

Refer to the general comments at the beginning of this section.

Database locking mechanism error.

Refer to the general comments at the beginning of this section.

Dynamic memory allocation error.

Refer to the general comments at the beginning of this section.

Error modifying server entry

Refer to the general comments at the beginning of this section.

Error reading server entry

Refer to the general comments at the beginning of this section.

Error reading server queue

Refer to the general comments at the beginning of this section.

Error when positioning to end of queue log file

Check to be sure the correct FTS-related access rights are assigned. Also check to be sure that the partition containing FTSQ* is not full, and that the quotas on FTSQ* and its partition are set to appropriate values.

Failed to initialize the lock/status file

Refer to the general comments at the beginning of this section.

Failed to open the queue log file

Check to be sure the correct FTS-related access rights are assigned. Also check to be sure that the partition containing FTSQ* is not full, and that the quotas on FTSQ* and its partition are set to appropriate values.

Failed to open the server lock file

Check to be sure the correct FTS-related access rights are assigned. Also check to be sure that the partition containing FTSQ* is not full, and that the quotas on FTSQ* and its partition are set to appropriate values.

Failed to open the server log file

Check to be sure the correct FTS-related access rights are assigned. Also check to be sure that the partition containing FTSQ* is not full, and that the quotas on FTSQ* and its partition are set to appropriate values.

Failure attaching home:

FTS could not attach to its normal attach point to change the temporary name given to the transferred file. The transferred file may have retained its temporary filename in the destination directory. (FTS prepends T\$ to the destination filename to create the temporary file.)

Failure attaching to destination directory

FTS could not attach to the destination directory to change the temporary name given to the transferred file. The transferred file may have retained its temporary filename.

Failure deleting existing file:

FTS could not delete a file with the same name as the destination file. The transferred file may have retained its temporary filename in the destination directory.

Failure renaming temporary file:

FTS could not attach to the destination directory to restore the original name given to the destination file. The transferred file may have retained its temporary filename in the destination directory.

File successfully renamed

FTS transferred the destination file with a temporary name and restored its original filename upon successful completion of the transfer.

FTS not ready for use .

The FTS database has not been initialized with the FTGEN INITIALIZE_FTS command.

Home ufd required .

Refer to the general comments at the beginning of this section.

Illegal address .

Refer to the general comments at the beginning of this section.

Item already modified by another user .

Refer to the general comments at the beginning of this section.

Item not found .

Refer to the general comments at the beginning of this section.

Item not modified .

Refer to the general comments at the beginning of this section.

Item not queued .

Refer to the general comments at the beginning of this section.

Item status not changed .

Refer to the general comments at the beginning of this section.

Local procedure error .

Refer to the general comments at the beginning of this section.

Message deleted, please rescan .

Refer to the general comments at the beginning of this section.

NETMAN server is not running (locally or remotely) .

Use the STATUS USERS command to check whether NETMAN is running on the local system. If NETMAN is not running locally, ask your System Administrator or operator to issue the STOP_NET command and then restart the network using the START_NET command, as described in the *Operator's Guide to Prime Networks*. If NETMAN is running on the local system, the problem is probably on the remote system. FTS should retry the request until the remote system is available.

Network error - <error code>

A network error has occurred. The error code is returned by one of the IPCF subroutines. The *Programmer's Guide to Prime Networks* describes the IPCF subroutines and lists the error codes that they return.

No more messages .

Refer to the general comments at the beginning of this section.

No queue available for item.

Refer to the general comments at the beginning of this section.

No queues configured.

You attempted to list all the queues, but none were configured. Ask your System Administrator about your system's current FTS configuration.

Parameter out of range.

Refer to the general comments at the beginning of this section.

Parameter required.

Refer to the general comments at the beginning of this section.

Parameter restricted.

Refer to the general comments at the beginning of this section.

Problem assigning server port

Refer to the general comments at the beginning of this section.

Problem modifying server configuration.

Refer to the general comments at the beginning of this section.

Problem reading server configuration.

Refer to the general comments at the beginning of this section.

Problem with Route-through call request .

Refer to the general comments at the beginning of this section.

Queue blocked.

You tried to submit a request to a queue that has been blocked with the FTGEN BLOCK_QUEUE command. The queue must be unblocked with the FTGEN UNBLOCK_QUEUE command so that requests can be accepted.

Queue does not exist.

The specified queue has not been configured with FTGEN.

Queue full.

The request queue is full.

Queue recently compressed.

Refer to the general comments at the beginning of this section.

Queue status not changed.

Refer to the general comments at the beginning of this section.

Remote Service is not running.

FTS will retry the request until remote service is available.

Remote system has no free users.

FTS will retry the request until remote service is available.

Remote system is busy.

FTS will retry the request until remote service is available.

Remote system is down.

FTS will retry the request until the remote system is available.

Remote system is not fully up.

FTS will retry the request until the remote system is available.

Request not applicable.

Refer to the general comments at the beginning of this section.

Route-through circuit timeout.

Refer to the general comments at the beginning of this section.

Route-through node has insufficient system memory.

Refer to the general comments at the beginning of this section.

Route-through protocol error.

Refer to the general comments at the beginning of this section.

Route-through server is not running.

The Route-through Server, RT_SERVER, is not running.

Server queue not configured

The specified server queue is not configured. Use the FTGEN ADD_QUEUE command to add the queue to the configuration.

Shared memory is full.

Refer to the *System Administrator's Guide, Volume I: System Configuration* for information on managing shared memory.

Temporary File is <full pathname>

This is the temporary filename that FTS at the destination site has assigned to the destination file.

The FTS database is invalid.

Either the FTS database has been corrupted, or an FTGEN INITIALIZE_FTS command has not been performed after FTS installation.

Timeout on call request to remote system.

This message indicates a network error. FTS may retry the request successfully.

Timeout on clear request to remote system.

This message indicates a network error. FTS may retry the request successfully.

Timeout on reset request to remote system.

This message indicates a network error. FTS may retry the request successfully.

Transfer failure: <text>

The transfer failed for the reason specified. The cause of the failure is usually a communications failure.

Unable to create temporary file.

The number of temporary files in the FTSQ* directory may have reached the maximum number as a result of queued requests. If possible, the operator should cancel old requests. In addition, check to be sure the correct FTS-related access rights are assigned.

B

NETLINK Error Messages

Any of several error conditions can occur while you are making or using a NETLINK connection. For example, the remote host or the data connection can fail. Error messages displayed by PSDNs and by PRIMENET software through NETLINK are listed below.

Error Messages Generated From Systems on PSDNs

The following error messages may appear when you try to connect to a system on a PSDN.

<address> Access Barred

Access is not allowed from your *address*.

<address> Busy

All available circuits to the remote host named *address* are busy. Try again later.

<address> Invalid Call

There is an error in the call request packet, or the host PSDN does not accept calls of this type.

<address> Local Procedure Error

A network protocol error has been encountered. Try again later. If the problem persists, inform your System Administrator.

<address> Network Congestion

Temporary network problems exist. Try again later. If the problem persists, inform your System Administrator. This message indicates problems with the local network or with a Packet Switched Data Network (PSDN).

<address> Not Obtainable

No path is available to the remote host. This message may indicate an incorrect host *address*.

<address> Out of Order

The remote host is currently not available to network users.

<address> Refusing Collect Call

You cannot make collect calls to *address*. Use the NC command.

<address> Remote Procedure Error

A network protocol error has been encountered. Try again later. If the problem persists, inform your System Administrator.

PRIMENET Error Messages

The following messages may appear either when you are connecting to a PRIMENET node or during the life of a connection.

<address> Disconnected <number> (Network Server logged out)

The networks have been shut down on your local system with the STOP_NET command. NETLINK logs you out of the remote system to which you are connected.

Host down

The line to the remote host is down.

Illegal address

The address that you specified is not a legal network address. Type STATUS NETWORK at PRIMOS level to see a list of correct network names and/or addresses.

Network Server logged out

NETMAN, the network server, stopped. It logs out, shutting off network services and loopback services. This message also appears if the operator stops NETMAN.

No remote users

Remote users are not allowed to log in to the system that you specified in your address. Usually this message that the maximum number have already logged in and there is no room for another user.

Port not assigned

The port that you specified has no process waiting to receive calls.

Rejecting

For PRIMENET nodes, this message means that the remote node is not in your system's address tables. See your System Administrator to find out if that node has been configured.

For non-PRIMENET hosts or user ports (port IDs between 1 and 99), this message indicates that the receiving process or machine rejected the user's request. For example, a non-Prime host might reject your remote login call request because the facilities are unacceptable.

System busy

Usually, this message indicates a lack of resources that are required for the establishment of the virtual circuit. Try again later.

System not up

The remote system is down. Try again later.

Timeout on call request

Your call request to the remote node was timed out. This indicates that the other node or the network (especially if it is a PSDN) is congested or down. Try again later.

Timeout on clear request

Your call request to the remote node was timed out when you tried to clear the circuit. Generally, this is not something you should worry about. You may leave a virtual circuit established, but when you log out, your end of the virtual circuit is guaranteed to disappear.

Timeout on reset request

This message appears if PRIMENET tried to reset the virtual circuit in response to a network event and the network failed to respond to two reset requests issued in succession. The virtual circuit is cleared, but you must reconnect and send data again.

Route-through Error Messages

The following section describes each message that may occur from Route-through errors.

Routed-Thru call request looping

A Route-through call request is looping because of a mismatch in network configurations over a network. Route-through operates by establishing a series of virtual circuits between intermediate nodes along its path, and partially because these paths are statically determined at PRIMENET configuration, it is possible that a path between two nodes could contain a loop. This loop can be detected, but not avoided or removed. Ask your System Administrator to resolve the problem.

Routed-Thru circuit timeout

An acknowledgment to a call request (circuit establishment) over a Route-through path (involving one or more gateway nodes) has not been received in a short enough period of time. This indicates that one or more of the intermediate gateway nodes or networks is badly congested or has gone down. It can also indicate that the Route-through path is extremely long. Try again later. If this message is repeated, call your System Administrator.

Route-Thru: Not enough memory

The buffer area allocated by the Route-through Server to perform the exchange of messages over the pair of virtual circuits that make up each Route-through virtual circuit was either exhausted or the Route-through Server was congested. Try again later.

Route-Thru protocol error

Some intermediate gateway is either down, or has violated the intergateway protocol during the establishment of the end-to-end virtual circuit, which is cleared. Try again later.

Route-Thru server down

In the circuit establishment or traffic phases, this message indicates that every path to the remote node is down. Specifically, at some intermediate node, the Route-through Server (as distinct from the Network Server) has logged out. This can also happen in the middle of the virtual circuit traffic. In either case, the Route-through Server may have been logged out by the operator. Try again later, or contact the local or remote System Administrators to resolve the problem.

C

PAD Parameters Used With NETLINK

This appendix presents the X.3 terminal characteristics parameters supported by NETLINK. These parameters are decimal values that are set with NETLINK's SET command and displayed with NETLINK's PAR command.

NETLINK supports only the TELENET and DATAPAC national options. Supported TELENET and DATAPAC parameters are also shown here. See appropriate TELENET literature for additional information about use of the TELENET parameters. See DATAPAC literature for more information on the DATAPAC parameters. Refer to CCITT Recommendation X.3 for additional information on the use of X.3 parameters.

International (X.3) Parameters

The following CCITT parameters are supported:

- 0 - National options marker. Including this causes subsequent parameters in the SET command to be interpreted as national (PSDN-specific) parameters.
 - 0 - Datapac (Canada)
 - 33 - Telenet (USA)
- 1 - PAD recall using a character. This determines whether or not the user can return to command mode.
 - 0 - not possible
 - 1 - possible
- 2 - Echo. The TERM or SET_ASYNC commands cause this parameter to be changed.
 - 0 - no echo
 - 1 - echo
- 3 - Data forwarding.
 - 0 - no data forwarding character
 - 1 - alphanumeric characters (A-Z, a-z, 0-9)
 - 2 - carriage return
 - 4 - ESC, BEL, ENQ, ACK
 - 8 - DEL, CAN, DC2

- 16 - ETX, EOT
- 32 - HT, LF, VT, FF
- 64 - All other control characters

The only valid combinations are
0,2 6(2+4), 18(2+16), 126(2+4+8+16+32+64)

- 4 - Idle timer delay. This timer determines how often NETLINK forwards characters to the remote host when there is no other reason to do so.
 - 0 - no idle timer-based forwarding
 - 1 through 255 - timer value in 50 msec (1/20 sec) intervals
- 5 - Ancillary device control. This determines flow control of the terminal by the PAD, or "reverse flow control". This parameter is *not* set by the TERM or SET_ASYNC commands.
 - 0 - disabled
 - 1 - enabled
- 6 - Control of PAD service signals. This determines whether or not NETLINK outputs certain messages to the terminal.
 - 0 - do not output certain messages
 - 1 - output all messages
- 7 - Break handling. This determines the action NETLINK takes when a "break" or control-P is typed by the user.
 - 0 - nothing
 - 1 - interrupt
 - 2 - reset
 - 4 - send indication of break
 - 8 - escape to command mode
 - 16 - discard output

The only valid combinations are 0, 1, 2, 8, 21(1+4+16)
For proper operation with a remote Primenet system, parameter 7 must be set to the value 21.
- 8 - Discard output.

Used when parameter 7 is 21. 0 indicates normal data transmission, 1 indicates output is to be flushed. Not set by the user.
- 9 - Padding after Carriage Return.
 - 0 - no padding after CR
 - 1 through 255 - number of padding characters
- 10 - Line folding.
 - 0 - no line folding
 - 1 through 255 - enable line folding, value = length of line in characters
- 11 - Speed of terminal line (This parameter is read-only; it cannot be set by the user.) See CCITT Recommendation X.3 for a list of encodings representing line speeds.

- 12 - Flow control of the PAD. This determines whether or not XOFF and XON characters typed by the user will flow control output from Netlink. The TERM -XOFF or SET_ASYNC commands cause this parameter to be changed.
- 13 - Linefeed insertion after Carriage Return. This determines if and when a LF is to be inserted into the data stream to and/or from a terminal when a CR is seen. The -LF and -NOLF options to the TERM command cause the values 4 or zero respectively to be set.
 - 0 - insert LF after CR when sending CR to the terminal
 - 1 - insert LF after CR when a CR is echoed to the terminal
 - 4 - insert LF after CR when sending CR to the terminal and when a CR is echoed to the terminal
 - 5 - insert LF after CR when sending CR to the terminal and when a CR is echoed to the terminal
 - 6 - insert LF after CR when a CR is sent from the terminal and when a CR is echoed to the terminal
 - 7 - insert LF after CR when sending CR to the terminal, when a CR is sent from the terminal, and when a CR is echoed to the terminal
- 14 - Padding after linefeed.
 - 0 - no padding after LF
 - 1 through 255 - number of padding characters
- 15 - Editing. This determines whether or not NETLINK itself will perform erase and kill processing (in addition to Primos).
 - 0 - disabled (PRIMOS only)
 - 1 - enabled (NETLINK and PRIMOS)
- 16 - Character Delete. This is the erase character used with parameter 15.
 - 0 through 126 - the decimal equivalent of the erase character in ASCII format, e.g., A = 65
- 17 - Line delete. This is the kill character used with parameter 15.
 - 0 through 126 - the decimal equivalent of the kill character in ASCII format, e.g., A = 65
- 18 - Line display. This is the character which will cause the line to be redisplayed; used with parameter 15.
 - 0 through 126 - the decimal equivalent of the line display character in ASCII format, e.g., A = 65
- 19 - Editing PAD service signals. These are the characters returned to the user to indicate characters that have been erased; used with parameters 15, 16, 17.
 - 0 - do not display any indication
 - 1 - use a format suitable for printing (paper) terminals
 - 2 - use a format suitable for display (video) terminals

- 20 - Echo mask. This determines how characters are to be echoed.
 - 0 - echo all characters with no special rules (use normal Primos rules)No other values are supported by NETLINK.
- 21 - Parity treatment. This determines parity interpretation rules for use with the terminal line (*not* the network).
 - 0 - no parity checking or generationNo other values are supported by NETLINK.
- 22 - Page wait. This determines if output is to be paused after a "page" is output to the terminal.
 - 0 - disabledNo other values are supported by NETLINK.

TELENET Parameters

The following TELENET (national options 33) parameters are supported:

- 1 Linefeed insertion
- 2 Network message delay
- 3 Enable local (network) echo
- 5 Data forwarding characters
- 9 CR padding
- 10 LF padding
- 12 Line width
- 13 Page length
- 14 Line folding
- 16 Interrupt on BREAK (TELENET discontinued)
- 17 Break code (TELENET discontinued)
- 18 NVT options
- 23 Terminal type
- 26 Terminal speed
- 27 Delete character
- 28 Cancel character
- 29 (Line Re-)Display character
- 30 Abort output character (TELENET discontinued)
- 34 Transmit on timers
- 35 Idle timer
- 36 Interval timer
- 40 Insert code on BREAK (TELENET discontinued)
- 45 Send APP on BREAK (TELENET discontinued)
- 54 DTE-to-DCE flow control (TELENET discontinued)
- 58 Connection escape enable
- 59 Flush on BREAK (TELENET discontinued)

DATAPAC Parameters

The following DATAPAC (national options 0) parameters are supported:

126 Linefeed insertion

Prime Network Glossary

This chapter contains a glossary of terms that refer to Prime networks or data communications in general. Terms that are in italics in definitions are defined elsewhere in the glossary.

Access Control List (ACL)

A list of access pairs used to specify the *access rights* of users. An access pair is a pair of 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	Protects a directory
D	Deletes entries from a directory
A	Adds entries to a directory
L	Reads contents of a directory
U	Attaches to a directory
R	Reads contents of a file
W	Changes contents of a file
X	Executes 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 in the ACL. You associate an ACL with a file system object using the PRIMOS SET_ACCESS (SAC) command or the PRIMOS EDIT_ACCESS (EDAC) command. See the *Prime User's Guide* for more information on access control lists.

access right

Generally, the degree of access to information that a user or process has on a system or *network*. For example, the Read (R) access right allows someone to view a file.

When used in reference to *PRIMENET configuration*, access right describes the type of service enabled between systems. With *CONFIG_NET* (the network configuration utility), the Network Administrator sets up access rights between pairs of systems in the network. For example, *CONFIG_NET* permits granting of *remote login* privileges between systems. Thus, remote login is an access right. You can configure the following access rights for a network: NONE, IPCF, RLOG, RFA, and ALL.

ACK

The acknowledge character.

ACK byte

This *byte* is in the trailer portion of a *RINGNET data packet* and is set by the *PRIMENET Node Controller* (PNC) of the receiving node to indicate whether or not that the message was successfully received (ACK = Acknowledge). 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

See Access Control List.

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 may vary.

asynchronous line

A line that carries *asynchronous communication*.

Binary Synchronous Communication (BSC)

A *protocol* and *framing* method supported by *PRIMENET*. BSC framing can use either the ASCII or the EBCDIC character set.

bit

An acronym for binary digit. Eight bits constitute a *byte*.

boot server

A *server* that is responsible for either initiating or receiving a request to *downline load* executable code to a *LAN300 Terminal Server* (LTS300).

broadcast packet

See packet, broadcast.

BSC

See Binary Synchronous Communication.

byte

Eight *bits* of data. A character, for example, is one byte.

cache file

In the context of *START_NET*, an optionally created file containing the latest *network configuration* information relevant to the local *node*. A cache file speeds up network initialization when restarting the network with the same configuration.

Carrier Sense Multiple Access with Collision Detection (CSMA/CD) access method

The access method used to decide which *station* on a *LAN300* takes control of the communication medium and transmits the next message.

CCITT

See Consultative Committee for International Telephony and Telegraphy.

communication line

See communication link.

communication link

The connecting medium between two systems that allows them to transmit and/or receive data. At Rev. 21.0, types of communication links include *LAN300*, *RINGNET*, *synchronous lines* (*full-duplex* and *half-duplex*), and *Packet Switched Data Network* (PSDNs). Two systems can also be linked by one or more intervening *gateway nodes*.

CONFIG_NET

PRIMENET's global *network configuration* utility (or configurator). Also, the command used to invoke the configurator.

CONFIG_NTS

A menu-driven and prompt-driven program for configuring *Network Terminal Service* (NTS) networks.

Consultative Committee for International Telephony and Telegraphy (CCITT).

An advisory committee established under the auspices of the United Nations to recommend worldwide standards.

CRC

See cyclic redundancy check.

CSMA/CD

See Carrier Sense Multiple Access with Collision Detection access method.

cyclic redundancy check (CRC)

A check performed by a *PRIMENET Node Controller (PNC)* on every *data packet* that it *transceives*. If a packet fails this test, the *PRIMENET Node Controller (PNC)* sets the *ACK byte* accordingly.

data field

The portion of the *data packet* that contains the actual data in *protocol* format.

data packet

See packet, data.

Distributed System Management (DSM)

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.

downline load

The process of reading software and load parameters into a controller that cannot self-boot.

downline load host

The system on a *Network Terminal Service (NTS)* network responsible for loading software into *LAN300 Terminal Servers (LTS300s)* and *LAN300 Host Controllers (LHC300s)* on the network. Normally, both a primary and secondary downline load host are configured to reduce network traffic if the primary host goes down.

DSM

See Distributed System Management.

dump server

A *server* that is responsible for either initiating or receiving an upline dump (memory image) from a *LAN300 Terminal Server (LTS300)*.

event

A significant system or *network* occurrence such as a cold start, machine check, disk error, or network link problem.

event reporting host

The host on a *LAN300* network responsible for receiving event reports from *LAN300 Host Controllers* (LHC300s) and *LAN300 Terminal Servers* (LTS300s). Event reports include notices of *downline loads* and upline dumps, along with any kind of error reports. Normally, both primary and secondary event reporting hosts are configured to reduce needless network traffic in case the primary host goes down.

FDX

See full-duplex.

File Transfer Generation (FTGEN)

The *File Transfer Service* (FTS) utility that a *System Administrator* or *Network Administrator* uses to configure the FTS database. FTGEN is described in the *PRIMENET Planning and Configuration Guide*.

File Transfer Manager

See YTSMAN.

File Transfer Operator (FTOP)

The *File Transfer Service* (FTS) utility that an operator uses to manage the FTS system. FTOP is described in the *Operator's Guide to Prime Networks*.

File Transfer Request (FTR)

The *File Transfer Service* (FTS) utility for submitting transfer requests.

File Transfer Service (FTS)

A queued file transfer program that enables files to be transferred between Prime systems in a *network*. FTS comprises the following utilities: *File Transfer Request* (FTR), *File Transfer Generation* (FTGEN), and *File Transfer Operator* (FTOP).

framing

The process of prefixing and suffixing a message with control characters before sending it over a *communication link*. The control characters are said to frame the message. *HDLC* and *BSC* are types of framing.

FTOP

See File Transfer Operator.

FTR

See File Transfer Request.

FTS

See File Transfer Service.

full-duplex

A communication mode in which both systems can send and receive signals at the same time. In a *PRIMENET* environment, full-duplex communication occurs over a permanently configured, dedicated connection (cables or leased telephone lines). Full-duplex lines can link a Prime system to a PSDN or to another Prime system.

gateway

See gateway node.

gateway access

The *access rights* between two systems that communicate through a *gateway node*. For example, consider the configuration shown in Figure GL-1. Systems 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. Gateway access is defined during *network* configuration.

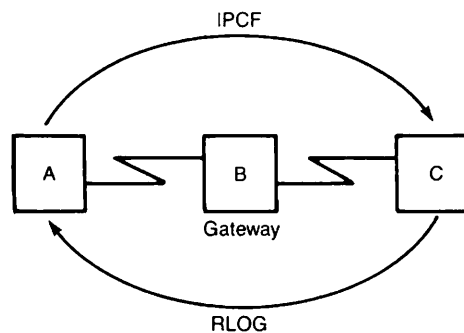


FIGURE G-1
Gateway Access

gateway node

A system on which the *Route-through Server* is configured. A gateway node can route messages between two other systems. Two systems may communicate via a gateway node even if they are not directly connected.

half-duplex

A communication mode in which data transmission occurs in only one direction at a time. Each system alternates between sending and receiving signals. In a *PRIMENET* environment, half-duplex communication occurs over temporary connections (generally, dialup telephone lines). Half-duplex *PRIMENET* lines may link two Prime systems, but may not link a Prime system to a non-Prime system or to a *Packet Switched Data Network* (PSDN).

HDLC

High-level Data Link Control; a *full-duplex* link *protocol* and a type of *framing* that meets the *CCITT X.25* standard. HDLC is supported and used by *PRIMENET*.

HDX

See half-duplex.

HDX network/HDX subnetwork

The set of all *half-duplex* (HDX) *nodes* and lines in a *network*.

HDX node

A node that has a *half-duplex* line attached to it.

header

The beginning portion of a *packet* that contains information such as the IDs of the target and sending *node* or packet type.

ICS1, ICS2, ICS3

See Intelligent Communications Subsystem, Model 1, 2 or 3.

indirect address

The *Packet Switched Data Network* (PSDN) address of a *node* that is not directly connected to the PSDN, but instead is connected to the PSDN through one or more *gateway nodes*.

Intelligent Communications Subsystem, Model 1, 2 or 3

Microprocessor-based communications controllers that manage *asynchronous lines* or *synchronous lines* or both. The ICS1 and ICS2 support asynchronous serial communication lines. The ICS3 can support synchronous and asynchronous serial *communication lines* concurrently. These lines can be configured to support a variety of *protocols* and electrical interfaces for communication with various terminal devices and controllers, other Prime computers, and the computers of other manufacturers.

Interprocess Communications Facility (IPCF)

A set of subroutines that permit applications to send and receive messages within a Prime *network*, or to transfer messages between processes on the same system. Also, an *access right* (selected through *CONFIG_NET*) that enables systems to communicate using IPCF subroutines only. IPCF access is the minimum access that you can configure between systems.

International Organization for Standardization (ISO)

Organization responsible for developing Open Systems Interconnection (OSI) model, a 7-layered network architecture.

IPCF

See Interprocess Communications Facility.

ISO

See International Organization for Standardization.

LAN

See Local Area Network.

LAN300

Prime's IEEE 802.3 compliant *Local Area Network* that uses a bus topology. A standard LAN300 is composed of bus segments, each of which can be a maximum of 500 meters in length. Devices are connected to a LAN300 at a *station*, where a controller, *transceiver*, and tap are attached to the bus segment. A station supports a host or a cluster of terminal or serial printers or both. The LAN300 uses the *Carrier Sense Multiple Access with Collision Detection (CSMA/CD) access method*.

LAN300 Host Controller (LHC300)

An intelligent controller that is plugged into the backplane of a 50 Series host and provides the interface between PRIMOS and a LAN300. The code on the LHC300 is a combination of Prime written software and the microprocessor. This controller transmits and receives data on a LAN300.

LAN300 Network Management Facility

LAN300 network management software. This facility supports services such as *LAN300 Host Controller (LHC300)* and *LAN300 Terminal Server (LTS300) downline loading*, LHC300 and LTS300 upline dumping, LHC300 and LTS300 name and address translation, and network event reporting and monitoring. The LAN300 Network Management Facility also provides a user interface that consists of loopback and status commands.

LAN300 Terminal Server (LTS300)

A remote microprocessor-based asynchronous communications server that provides the *LAN300* interface for a maximum of eight asynchronous devices.

LAP

See Link Access Procedure.

LAPB

See Link Access Procedure Balanced.

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 tells the *PRIMENET Node Controller* that a *data packet* follows.

Level 1

PRIMENET's hardware interface. This level (or layer) acts as an intermediary between the physical transmission medium (twin-axial cable or transmission line) and *Level 2*.

Level 2

PRIMENET's link level. It describes a *protocol* for transferring data between two directly connected systems.

Level 3

PRIMENET's packet level. It creates and controls connections across the *network*, handles error recovery, and controls the flow of data between processes on a pair of communicating systems.

LHC300

See LAN300 Host Controller.

Link Access Procedure (LAP)

A type of link-level *protocol* defined by X.25 and supported by Prime.

Link Access Procedure Balanced (LAPB)

A type of link-level *protocol* defined by X.25 and supported by Prime.

Local Area Network (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 or building complex. *RINGNET* is Prime's Local Area Network that uses a ring configuration. *LAN300* is Prime's IEEE 802.3 compliant LAN that uses a bus configuration.

local system

A system on a *network* from which a user issues commands to communicate with another *remote* system.

LTS Command mode

An LTS300 input mode. An LTS300 accepts commands from terminal users to establish connections, change line parameters, and perform related tasks. See also Data Transfer mode.

LTS Data Transfer mode

An LTS300 input mode that establishes a connection and transfers data to the remote host. *See also* Command mode.

LTS300

See LAN300 Terminal Server.

MDLC

See Multiple Data Link Controller.

Multiple Data Link Controller (MDLC)

A communications controller that handles *full-duplex* and *half-duplex synchronous lines*.

NAK

Negative acknowledgment. A NAK indicates that either a *RINGNET data packet* failed a *cyclical redundancy check (CRC)*, or 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 networked Prime system or a non-Prime system across a *Packet Switched Data Network (PSDN)* if that non-Prime system adheres to the *CCITT PAD protocols (X.3/X.28/X.29)*.

NETMAN

See Network Manager Process.

network

A group of independent computer systems that are connected by communication media such as PSDNs, LANs, and *synchronous lines* and that communicate and share resources. A network can consist of systems that are all physically connected and communicate over short distances, as in a LAN, or of systems that use different communication media to communicate over long distances.

The term network is sometimes used synonymously with *subnetwork*; for example, *ring network* or *HDX network* can refer to subsets of a larger network.

Network Administrator

The person responsible for maintaining the proper and continuous operation of a *network*. Tasks 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 configuration

A description of the systems, services, and communication media that make up a *network*.

network configuration file

The file that contains the network configuration in binary format. The *Network Administrator* creates this file through *CONFIG_NET*. At network startup time, this file is loaded into *PRIMENET* by the *START_NET* command (unless a *cache file* is used).

Network Manager Process (NETMAN)

A process that handles network activity. NETMAN is X.25 Level 2 and Level 3 PRIMENET. NETMAN appears on the STATUS USERS list as nsp (network server process).

Network Process Extension (NPX) facility

An internal PRIMOS facility that provides a remote procedure call mechanism between any two *PRIMENET* systems. *Remote File Access* (RFA) uses NPX.

network protocol

See protocol.

node

An independent computer system that is part of a *PRIMENET network*.

Network Terminal Service (NTS)

A collection of software designed to support communications between terminals and hosts over a *LAN300 network*.

NPX

See Network Process Extension Facility.

NTS

See Network Terminal Service.

packet

A sequence of data and control characters that are arranged in a specific format and transmitted as a unit.

Packet Assembler/Disassembler (PAD)

Provides a number of functions: 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.

packet, broadcast

A 10-byte packet, periodically sent by a *node*, that contains the *ring node ID*. This packet is received by all active *PRIMENET Node Controllers* (PNCs).

packet, data

A package that contains *packet protocol* and data. It consists of a leading frame, header, a data field, and a trailing frame. The maximum size of the *data packet* can be set by the *Network Administrator* through *CONFIG_NET*.

Packet Switched Data Network (PSDN)

A *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.

packet size

The number of *bytes* in a *packet*.

PAD

See Packet Assembler/Disassembler.

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* and is set by the *PRIMENET Node Controller (PNC)*.

parity check

A check performed by a *RINGNET PRIMENET Node Controller (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 systems between two given systems in a *network*.

PNC

See *PRIMENET Node Controller*.

PNC II

See *PRIMENET Node Controller II*.

PNCDIM

The *PRIMENET Node Controller Interface (software) 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 distributed networking software that offers local and wide-area networking facilities.

PRIMENET address

A numeric address that *PRIMENET* uses internally to identify a *node*. *CONFIG_NET* generates this address based on the name of the node.

PRIMENET Node Controller (PNC)

PRIMENET hardware that controls ring *protocol* and the flow of data between *nodes* on a ring.

PRIMENET Node Controller II (PNC II)

PRIMENET hardware that controls ring *protocol* and the flow of data between *nodes* on a ring.

protocol

A set of rules governing communication between two systems in a *network*.

PSDN

See Packet Switched Data Network.

PSDN address

A unique sequence of as many as 15 digits assigned by a PSDN to any *node* connected directly or indirectly to the PSDN. An indirect connection is indicated when a 2-digit subaddress is used.

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. Can be referred to as an *X.25 gateway*.

Remote File Access

See RFA.

remote login

See RLOG.

remote system

A system that can communicate with the *local system* through a *network*.

remote user

A user on a *remote system*.

repeater

A device that amplifies a signal. For example, a *RINGNET* electrical repeater enables two hosts that are more than 750 feet apart to communicate. A fiber optic repeater can increase the maximum distance between adjacent *nodes* by 3280 feet (one kilometer). A fiber optic repeater can join systems in different buildings on a ring. Both kinds of repeaters can operate on a LAN together. A *RINGNET* repeater does not affect the performance of a LAN.

RFA

Remote File Access. A *PRIMENET* intersystem service or *access right* (selected through *CONFIG_NET*) that enables a user to access files on a *remote system* as though the files were on the *local system*.

ring

See ring network.

ring network

A type of *Local Area Network (LAN)*. Prime's ring LAN, *RINGNET*, is a token-passing ring network.

RINGNET

One of Prime's LANs for Prime-to-Prime communications. A *RINGNET network* is composed of Prime systems that are connected by cable in a ring configuration. Each system is logically connected to all other systems on the ring. *RINGNET* uses a token-passing *protocol* to control communication around the ring.

ring node ID

A number from 1 through 247 that identifies, and is unique to, a particular *node* on a *RINGNET network*.

RLOG

Remote login. A *PRIMENET* service that enables users to log in to a *remote system* from a local terminal without logging in to the *local system* first. The local and remote systems must be connected directly or connected through one or more *gateway nodes*. The *Network Administrator* must assign remote login access rights (selected through *CONFIG_NET*) during network configuration. These access rights are checked only on the remote system.

Route-through

The message-routing operation performed on a *gateway node* that connects two systems or *networks*.

Route-through Server (RT_SERVER)

The *server* that performs *Route-through* and enables a system to act as a *gateway node* for communication between *nodes* not directly connected through a ring, *PDSN*, or *synchronous line*.

server

A cooperating set of processes available to perform one or more functions. FTS servers service local request queues and incoming requests from *remote systems*.

slave process

A process on a *local system* that handles a request that a user on another system makes to access files or to attach to a directory on the local system. A slave acts for a single *remote user* until the remote user releases the slave process. The number of slave processes available (configured by the *System Administrator*) depends on whether the local system is using the *Route-through Server* or the *File Transfer Service (FTS)* or both.

SMLCnn

The logical line number of a *synchronous communication* line on a Prime system.

START_DSM

Command that brings up *Distributed System Management (DSM)* on the system.

START_NET

Command that starts up *PRIMENET* on a *local system*. This command works without interrupting local PRIMOS operation.

START_NTS

Command that starts up the *Network Terminal Service (NTS)*.

station

A point on a *LAN300* at which a controller, *transceiver*, and tap are attached to a bus segment.

STOP_DSM

Command that shuts down *Distributed System Management (DSM)* by logging out all DSM server processes.

STOP_NET

Command that shuts down *PRIMENET* on a *local system*. This command works without interrupting local PRIMOS operation.

subnetwork

The *nodes* in a *network* directly connected to a particular medium, such as a *full-duplex* line, or the set of all *half-duplex* lines in the larger network.

synchronous communication

Transmission in which data, characters, and *bits* are transmitted at a fixed rate. The transmitting and receiving systems are synchronized, thus eliminating the need for start and stop bits.

Generally, synchronous communication offers more efficient line usage, better error checking, and higher speeds of transmission than *asynchronous communication*.

synchronous line

A line that carries *synchronous communication*.

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 the *File Transfer Service (FTS)*. At times, the same person serves as System Administrator and *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 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.

token recovery

The mechanism *PRIMENET* uses to replace a lost *RINGNET* 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 tells the *PRIMENET Node Controller (PNC)* that the end of the *data packet* has been reached.

transceiver

A device that receives and transmits data simultaneously. The *PRIMENET Node Controller (PNC)* is a transceiver that uses a 4-bit time delay between reception and transmission of data.

upline dump host

A Prime host on an *Network Terminal Service* (NTS) *network* responsible for receiving upline dumps from *LAN300 Host Controllers* (LHC300s) and *LAN300 Terminal Servers* (LTS300s) on the network. Upline dumps are used to diagnose software failures. Normally, both a primary and secondary upline dump host are configured to reduce network traffic if the primary host goes down.

user validation

The process of checking a *remote user's* ID before allowing that user to access information on a system. 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 255 virtual circuits.

WACK

Wait acknowledge. 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. Window size is configurable only for *Packet Switched Data Network* (PSDN) links.

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 Terminal 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 Transport Service Manager. The *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

Index

Index

A

- Access rights, 4-4, 5-11
- Accessing remote files, 1-4, 2-1
- Adding remote IDs, 2-3
- ADD_REMOTE_ID (ARID) command, 2-3 to 2-4
- Address formats of NETLINK, 7-14
- Addresses
 - Prime system name, 7-14
 - PSDN, 7-14
- Architecture of PRIMENET, 1-1, 1-5
- ARID command (PRIMOS), 2-3
- Asynchronous lines, 1-2

B

- Binary Synchronous Communication (BSC) protocol, 1-11
- BSC protocol
 - see*: Binary Synchronous Communication protocol

C

- C command (NETLINK), 7-4 to 7-5, 7-17, 7-20, 8-7
- CALL command (NETLINK), 8-8
- CAM files, 4-8, 6-4, 6-10
- Canceling file transfer requests (FTR), 5-10
- CCITT, 1-5
- CLEAR command (NETLINK), 8-9
- CLOSE command (NETLINK), 7-25 to 7-26, 8-5, 8-9
- Command format, FTR, 5-2
- Command input files, 7-21
- Command input files, example of, 7-21
- Command mode of NETLINK, 7-3
- Command summary of NETLINK, 8-1
- CONFIG_NET, 2-1
- Connect profile commands, 8-4
- CONTINUE command (NETLINK), 7-17, 7-25, 8-2, 8-9, 8-19
- COPY command (PRIMOS), 1-4, 4-1
- CPL files, 6-8, 7-21, 7-23
- CPL files, examples of, 7-23

D

- D command (NETLINK), 8-2, 8-9
- DAM files, 4-8, 6-4, 6-10

- DATA command (NETLINK), 8-4, 8-9
- Data format of -DEFER option, 6-2
- Data Network Identification Code (DNIC), 7-15
- Data Transmission mode of NETLINK, 7-3, 7-25
- DBMS files, 4-9
- DEBUG command (NETLINK), 8-3, 8-10
- Debugging with NETLINK, 7-27, 8-10
- Deferred requests, 5-5, 6-2
- Destination pathnames, 5-2 to 5-3
- Destination site names, 6-5
- Destination sites (FTS), 4-7, 5-7
- Destination users, 5-7
- DNIC command (NETLINK), 8-4, 8-10

E

- EDIT_ACCESS command (PRIMOS), 4-5
- Erase character, 7-24
- Error messages
 - FTR, A-2 to A-9
 - FTS, A-1
 - NETLINK, B-1 to B-4
 - remote login, 3-2 to 3-3, B-1 to B-4
- ESCAPE command (NETLINK), 8-3, 8-10
- Establishing remote IDs, 2-5
- Examining remote IDs, 2-5
- Executable Program Format (EPF), 4-8

F

- Failed FTR transfers, 5-11
- FCTY command (NETLINK), 8-4, 8-10
- FILE command (NETLINK), 7-24 to 7-25, 8-11
- File transfer queues, 4-3
- File transfer requests (FTR)
 - canceling, 5-10
 - printing, 5-4
 - retrieving, 5-3
 - sending, 5-2
 - status of, 5-4
- File transfer servers, 4-2
- File Transfer Service (FTS), 1-4
- File transfer utilities, 4-1
- File transfers, NETLINK, 7-24
- File types of FTR, 4-8
- FTGEN utility, 1-5, 4-1, 6-10
- FTOP utility, 1-5, 4-1
- FTR
 - access rights, 4-4
 - canceling requests, 5-10

- command format, 5-2
- destination pathnames, 5-2 to 5-3
- destination sites, 4-6, 5-7
- destination users, 5-7
- error messages, A-2 to A-9
- failed transfers, 5-11
- file transfer queues, 4-3
- file transfer servers, 4-2
- file types, 4-8
- full descriptions of management options, 6-11
- full descriptions of submittal options, 6-1
- help facility, 5-1
- logging requests, 5-7
- logging requests, examples of, 5-8
- management options, 5-13, 6-11
- printing a file, 5-4
- request name, 5-2, 5-4, 6-12 to 6-13, 6-15 to 6-16
- request number, 5-2, 5-4, 6-12 to 6-13, 6-15 to 6-16
- requesting transfer notification, 5-9
- retrieving a file, 5-3
- sending a file, 5-2
- site names, 4-8
- source pathname, 5-2
- source site, 4-6
- submittal options, 5-12
- summary of management options, 5-13
- summary of submittal options, 5-11
- FTR management options
 - ABORT, 5-10, 5-13, 6-12
 - CANCEL, 5-10, 5-13, 6-12
 - DISPLAY, 5-4, 5-13, 6-3, 6-13
 - HELP, 5-13, 6-14
 - HOLD, 5-13, 6-14
 - MODIFY, 5-13, 6-3, 6-14 to 6-15
 - RELEASE, 5-13, 6-2, 6-6, 6-15
 - STATUS, 5-4, 5-13, 6-16
 - STATUS_ALL, 5-13, 6-16
- FTR submittal options
 - COPY, 5-12, 6-1 to 6-2, 6-15
 - DEFER, 5-12, 6-2
 - DELETE, 5-12, 6-3
 - DEVICE LP, 6-4
 - DSTN_FILE_TYPE, 5-12, 6-4, 6-15
 - DSTN_NTFY, 5-9, 5-12, 6-4
 - DSTN_SITE, 5-12, 6-5, 6-15
 - DSTN_USER, 5-10, 5-12, 6-6
 - HOLD, 5-12, 6-6, 6-15
 - LOG, 5-7 to 5-8, 5-12, 6-4, 6-6, 6-10

FTR submittal options (continued)

- MESSAGE_LEVEL, 5-8, 5-12, 6-7
- NAME, 5-12, 6-8
- NO_COPY, 5-12, 6-2, 6-8, 6-15
- NO_DELETE, 5-12, 6-8
- NO_DSTN_NTFY, 5-12, 6-8
- NO_QUERY, 5-12, 6-8, 6-12 to 6-13, 6-15 to 6-17
- NO_SRC_NTFY, 5-12, 6-9
- PRIORITY, 5-12, 6-9
- QUERY, 5-12, 6-10, 6-12 to 6-14, 6-16 to 6-17
- QUEUE, 5-12, 6-10, 6-15
- SRC_FILE_TYPE, 5-13, 6-10
- SRC_NTFY, 5-9, 5-13, 6-10 to 6-11
- SRC_SITE, 5-13, 6-11
- SRC_USER, 5-10, 5-13, 6-11
- DEVICE LP, 5-12

FTS

- destination sites, 4-6, 5-7
- error messages, A-1
- FTR error messages, A-2 to A-9
- local site, 4-3
- log file messages, A-9 to A-14
- new features at Rev. 21.0, viii to ix
- remote site, 4-3
- site, defined, 4-3
- source site, 5-7, 6-11

FTSQ* directory, 4-8

FTSSUB subroutine, 1-5

Full-duplex lines, 1-2, 1-11

G

Gateway nodes, 1-12

H

Half-duplex lines, 1-2, 1-11, 4-7

HDLC protocol, 1-11

HELP command (NETLINK), 8-12

Help facility

FTR, 5-1

NETLINK, 7-6

HFCTY command (NETLINK), 8-12

High-level Data Link Control protocol (HDLC), 1-11

I

ICS1

see: Intelligent Communications Subsystem

ICS2

see: Intelligent Communications Subsystem

Index-2

ICS3

see: Intelligent Communications Subsystem

Intelligent Communications Subsystem

Model 1, 1-6, 1-11

Model 2, 1-6, 1-11

Model 3, 1-6, 1-11

International Organization for Standardization (ISO), 1-5

IPCF subroutines, 1-5

ISQ, 1-5

K

Kill character, 7-25

L

LAN300, 1-2

configuration, 1-10

server, 1-10

station, 1-10

transceiver, 1-10

LAN300 Host Controller (LHC300), 1-6

LAP

see: Link Access Procedure

LAPB

see: Link Access Procedure Balanced

LDATA command, 8-4, 8-12

Level 1, 1-6

Level 2, 1-6

Level 3, 1-5

Link Access Procedure, 1-11 to 1-12

Link Access Procedure Balanced, 1-11 to 1-12

Link level, 1-6

LIST_ACCESS command (PRIMOS), 4-6

LIST_REMOTE_ID command (PRIMOS), 2-5

LMDATA command (NETLINK), 8-4, 8-13

Local-to-remote file transfers, NETLINK, 7-24

Log file, 6-7

Log file error messages, A-9 to A-14

Log message level, 5-7

Logging FTR requests, 5-7

Logging in to remote systems, 3-1

LOGIN command (PRIMOS), 3-1

M

MAKE utility, 4-8

Making a connection with NETLINK, 7-7

Management options of FTR, 5-13, 6-11

Master process, 2-1

MDATA command (NETLINK), 8-4, 8-9, 8-13

MDLC

see: Multiple Data Link Controller

MDLC protocol, 1-11

MIDASPLUS files, 4-9

MODE command (NETLINK), 8-3, 8-13

Multiple Data Link Controller (MDLC), 1-6, 1-11

Multiple NETLINK connections, 7-17, 8-19

Multiple NETLINK connections, example of, 7-18

N

NC command, 7-7, 7-17, 8-13

NETLINK

address formats, 7-14

basic commands, 8-2

Command mode, 7-3

command summary, 8-1

Data Transmission mode, 7-3, 7-25

debugging, 7-27, 8-10

error messages, B-1 to B-4

escape character, 7-3

file transfers, 7-24

Help facility, 7-6

introduction to, 7-1

invoking, 7-4

kill character, 7-24

local-to-remote file transfers, 7-24

making a connection, 7-7

multiple connections, 7-17, 8-19

multiple connections, example of, 7-18

new features at Rev. 21.0, viii to ix

parameters, C-1

PRIMENET-configured name addressing, 7-14

PSDN addressing, 7-14

remote echo, 8-13

remote-to-local file transfers, 7-26

running from a command input file, 7-21

running from a CPL file, 7-23

terminal types, 8-20

NETLINK commands

C, 7-4, 7-7, 7-17, 8-7

CALL, 8-8

CLEAR, 8-9

CLOSE, 7-25 to 7-26, 8-5, 8-9

CONTINUE, 7-17, 7-25, 8-2, 8-9, 8-19

D, 8-2, 8-9

DATA, 8-4, 8-9

DEBUG, 8-3, 8-10

DNIC, 8-4, 8-10

NETLINK commands (continued)

ESCAPE, 8-3, 8-10
 FCTY, 8-4, 8-10
 FILE, 7-24 to 7-25, 8-11
 HELP, 8-12
 HFCTY, 8-12
 LDATA, 8-4, 8-12
 LMDATA, 8-4, 8-13
 MDATA, 8-4, 8-9, 8-13
 MODE, 8-3, 8-13
 NC, 7-7, 7-17, 8-13
 OUTFILE, 7-24 to 7-25, 8-5, 8-14
 PAUSE, 8-2
 POLL, 8-3, 8-16
 PORT, 8-4, 8-16
 PRID, 8-4, 8-16
 PROMPT, 8-5
 QUIT, 7-4, 8-2, 8-18
 RESET, 8-5
 SET, 8-5, 8-18
 SPEED, 8-3, 8-19
 STATUS, 8-5, 8-19
 SW, 7-17, 8-9
 TQ, 8-3, 8-20
 TTP, 8-3, 8-20
NETMAN, 4-3
 Network Process Extension (NPX) facility,
 2-1
 Network types, 1-2, 1-8
 New features at Rev. 21.0, viii to ix
NPX
 see: Network Process Extension facility
NSLUSR directive, 2-1

O

Open network address, 6-5
 Open Systems Interconnection model, 1-5
OPEN_SYSTEMS queue, 6-10
OUTFILE command (NETLINK), 7-24 to
 7-25, 8-5, 8-14

P

Packet, 1-8
Packet Assembler/Disassembler (PAD),
 3-1
Packet Switched Data Network
 NETLINK, 3-1, 7-1, 7-14
 standards, 1-2
PAD
 see: Packet Assembler/Disassembler
 Parameters, NETLINK, C-1
 Passwords, 5-8, 5-11, 6-5
PNC
 see: PRIMENET Node Controller

PNC II

see: PRIMENET Node Controller II
 Point-to-point connections, 1-11
POLL command (NETLINK), 8-3, 8-16
PORT command (NETLINK), 8-4, 8-16
PRID command (NETLINK), 8-4, 8-16
 Prime INFORMATION files, 4-9
PRIMENET
 architecture, 1-1, 1-5
 full-duplex connections, 1-2, 1-10
 half-duplex connections, 1-2, 1-11
 LAN300 Host Controller, 1-6
 Level 1, 1-6
 Level 2, 1-6
 Level 3, 1-5
 Multiple Data Link Controller, 1-6,
 1-11
 network types, 1-2, 1-8
 Node Controller, 1-6, 1-8
 Node Controller II, 1-6, 1-8
 PSDNs, 1-2
 remote file access, 1-4, 2-1
 remote login, 1-4, 3-1
 RINGNET, 1-2, 1-8
 Route-through connections, 1-12
PRIMENET-configured name addressing,
 7-14
 Printing files remotely (FTR), 5-4
 Priority of FTR requests, 5-5, 6-9
PRISAM files, 4-9
PROMPT command (NETLINK), 8-5
PSDN
 see: Packet Switched Data Network
PSDN addressing, 7-14

Q

Queue
 file transfer, 4-3, 6-10
 OPEN_SYSTEMS, 6-10, 6-13 to 6-14,
 6-16
QUIT command, 7-4
QUIT command (NETLINK), 8-2, 8-18

R

Remote echo (NETLINK), 8-13
 Remote file access, 1-4, 2-1
 Remote IDs, 2-3
 establishing, 2-4
 examining, 2-5
 removing, 2-5
 Remote login, 1-4, 3-1
 Remote login error messages, 3-2 to 3-3,
 B-1 to B-4
 Remote-to-local file transfers, 7-26

REMOVE_REMOTE_ID command
(PRIMOS), 2-6

Repeater, 1-8
 electrical, 1-9
 fiber optic, 1-9
 Request names, 5-2, 5-4 to 5-5, 6-12 to
 6-13, 6-15 to 6-16
 Request numbers, 5-2, 5-4 to 5-5, 6-12 to
 6-13, 6-15 to 6-16
 Requesting transfer notification, 5-9
RESET command (NETLINK), 8-5
 Retransmission of file transfers, 5-11
 Retrieving files with FTR, 5-3
RINGNET, 1-2, 1-8
 repeater, 1-8 to 1-9
 token ring protocol, 1-8
RLOG
 see: Remote Login
ROAM files, 4-9
 Route-through connections, 1-12
 Route-through Server, 1-12, 4-3
 Running NETLINK from a command
 input file, 7-21
 Running NETLINK from a CPL file, 7-23
RWLOCK command (PRIMOS), 6-7

S

SAM files, 4-9, 6-4, 6-10
SEG DAM files, 4-9, 6-4, 6-10
 Segment directories, 4-9
SEGSAM files, 4-9, 6-4, 6-10
 Sending files with FTR, 5-2
 Server processes (FTS), 4-2
SET command (NETLINK), 8-5, 8-18
Site (FTS)
 defined, 4-3
 destination, 5-7
 local, 4-3
 remote, 4-3
 source, 5-7, 6-11
 Site names, 4-8, 5-2 to 5-3
 Slave processes, 2-1
SMLC CNTRLR directive, 1-11
 Source pathnames, 5-2 to 5-3
 Source sites, 5-7, 6-11
 Source users, 5-7, 6-11
SPEED command (NETLINK), 8-3, 8-19
SPOOL command (PRIMOS), 6-4
Station, 1-10
STATUS command (NETLINK), 8-5,
 8-19
STATUS DISKS command (PRIMOS),
 2-1
 Status of FTR requests, 5-5

STATUS USERS command (PRIMOS),
4-2

Submittal options of FTR, 5-11, 6-1

SW command (NETLINK), 7-17, 8-19

Synchronous lines, 1-2, 1-11

SYSNAM directive, 4-8

T

Temporary destination files, 4-7, 5-3, 5-11

Terminal types, NETLINK, 8-20

TO command (NETLINK), 8-3, 8-20

Token ring protocol, 1-8

Transceiver, 1-10

Transferring files

with FTR, 5-2

with NETLINK, 7-24

TTP command (NETLINK), 8-3, 8-20

X

X.25, 1-1, 1-5, 7-2

X.28, 1-1

X.29, 1-1, 7-2

X.3, 1-1, 7-2, 8-18, C-1

Y

YTSMAN, 4-2

Surveys

READER RESPONSE FORM

**User's Guide to Prime Network Services
DOC10115-1LA**

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: _____

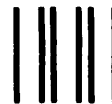
First Class Permit #531 Natick, Massachusetts 01760

BUSINESS REPLY MAIL

Postage will be paid by:



Attention: Technical Publications
Bldg 10
Prime Park, Natick, Ma. 01760



NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

