Prime®

Operator's System Overview

Revision 22.0

DOC9298-3LA

OPERATOR'S SYSTEM OVERVIEW

Third Edition

Sonya Zegarra

This guide documents the software operation of the Prime Computer and its supporting systems and utilities as implemented at Master Disk Revision Level 22.0 (Rev. 22.0).

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

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.

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

ORACLE is a registered trademark of Oracle Corp.

SyncSort is a trademark of Syncsort, Inc.

Printing History

First Edition (DOC9298-1LA) December 1984
Update 1 (UPD9298-11A) August 1985
Second Edition (DOC9298-2LA) July 1987
Third Edition (DOC9298-3LA) October 1988

Credits

Editorial: Barbara Bailey, Joyce Haines, Roberta King
Illustration: Doug Gilbert, Elizabeth Wahle
Document Preparation: Jeff Cohen
Production: Paula Brown

How to Order Technical Documents

To order copies of documents, or to obtain a catalog and price list:

United States Customers

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

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

1-800-322-2838 (Massachusetts)
1-800-541-8888 (Alaska and Hawaii)
1-800-343-2320 (within other states)

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

APPENDICES

ABOUT THIS SERIES

The Operator's Guide series is designed to help you, as a system operator or a System Administrator of a Prime® computer, do your job. This preface describes the eight Operator's Guides, together with other Prime documentation that is particularly useful for system operators and System Administrators. To display an online list of all Prime documentation, use the HELP DOCUMENTS command.

FOR THE SYSTEM OPERATOR

Before reading this book, you should have some familiarity with Prime systems. A good way to begin is to read the *PRIMOS User's Guide* (DOC4130-5LA), which explains the PRIMOS® file management system and provides introductory and tutorial information about essential commands and utilities. When you read any Prime documentation, be sure to consult the section entitled Prime Documentation Conventions, which follows the preface; this section is essential to understanding how information is presented.

After you are familiar with Prime systems, read the *Operator's System Overview*, which outlines the material in the Operator's Guide series. Then select the other books in the series as they apply to the tasks you must perform.

As you learn more about system operations, you will use the *Operator's Guide to System Commands*, as a reference for many of the special system commands and arguments that you, as an operator, will need to perform your job. The *Operator's Guide to System Commands* documents most of the commands described in the Operator's Guide series.

The Operator's Guide Series

The following books contain detailed information for the system operator.

- *Operator's System Overview* (DOC9298-3LA) introduces the series and describes computer-room operation of Prime systems.
- *Operator's Guide to System Monitoring* (DOC9299-3LA) describes how to monitor system usage, activity, and messages.

- *Operator's Guide to File System Maintenance* (DOC9300-4LA) describes the PRIMOS file system and explains how to format disk partitions, run the disk partition maintenance program, determine physical device numbers, and interpret disk-error messages.
- *Operator's Guide to the Batch Subsystem* (DOC9302-3LA) describes how to set up, monitor, and control the Batch subsystem.
- *Operator's Guide to the Spooler Subsystem* (DOC9303-3LA) describes how to set up, monitor, and control the Spooler subsystem.
- *Operator's Guide to System Commands* (DOC9304-4LA) serves as a reference guide for most of the commands described in the other books in the series.
- *Data Backup and Recovery Guide* (DOC10129-1LA) and its update package (UPD10129-11A) describe how to save information on disk or tape and how to restore that information when it is needed.
- *Operator's Guide to Prime Networks* (DOC10114-1LA) and its update package (UPD10114-11A) provide reference information about running network-related programs and monitoring network events.

Other Books for the Operator

- *Operator's Master Index* (DOC10110-4LA) indexes all the Operator and System Administrator Guides. Consulting this index is often the quickest way to find which manual has the information you need.
- The computer handbook for your particular CPU explains such topics as booting the system, shutting down PRIMOS, handling halts and hangs (including warm starts), performing tape dumps, and using the Virtual Control Panel (VCP).
- The *Using Your CPU* guide (available only for office CPUs) is intended for nontechnical users who are acting as system operators, and covers system startup and shutdown, system backups, troubleshooting, and other day-to-day system management issues.
- *MAGNET User's Guide* (DOC10156-1LA) and its update package (UPD10156-11A) describe the MAGNET utility, used to transfer data by magnetic tape from other operating systems to PRIMOS and vice versa.

FOR THE SYSTEM ADMINISTRATOR

In addition to the documentation in the Operator's Guide series, be sure to read the System Administrator's Guide series, which describes how to set up, configure, and maintain PRIMOS:

- *System Administrator's Guide, Volume I: System Configuration* (DOC10131-2LA) explains how to set up a system and allocate resources.

- *System Administrator's Guide, Volume II: Communication Lines and Controllers* (DOC10132-2LA) explains how to configure communication lines.
- *System Administrator's Guide, Volume III: System Access and Security* (DOC10133-2LA) explains PRIMOS security features and how to prevent unauthorized use of your system.
- *DSM User's Guide* (DOC10061-2LA) explains how to use the Distributed Systems Management (DSM) subsystem, including how to configure and operate DSM.

The System Administrator's Guides also provide information about most of the commands necessary to operate your Prime system.

OTHER RECOMMENDED READING

In addition to the books listed above, you may find the following books useful:

- *New User's Guide to EDITOR and RUNOFF* (FDR3104-101B) is a basic reference for any user of a Prime system and provides information about the Prime text editor and formatter.
- *PRIMOS Commands Reference Guide* (DOC3108-7LA) provides detailed information about user commands.
- *PRIMENET Planning and Configuration Guide* (DOC7532-4LA) describes how to plan, configure, and maintain PRIMENET™ software for a system.
- *User's Guide to Prime Network Services* (DOC10115-1LA) describes networking services that enable users to access files remotely, transfer files, and log in to other 50 Series™ systems on a network.
- *NTS User's Guide* (DOC10117-2LA) explains the Network Terminal Service (NTS).
- *50 Series Technical Summary* (DOC6904-2LA) describes the features of the 50 Series systems, including advanced architecture concepts and the software and hardware products the concepts support.

ABOUT THIS BOOK

The *Operator's System Overview* provides general introductory information about Prime systems for use by the operator. It describes the PRIMOS operating system, the PRIMOS file system, system resources, and system monitoring tools. You should have some familiarity with Prime systems before reading this book. If you are not familiar with PRIMOS, see the previous section, For the System Operator.

If you are a system operator, this book is intended to help you become familiar with the operations required to keep the system operating efficiently. If you are a System Administrator, this book is intended to help you gain insight into some of the tasks required of the operator to keep the system running smoothly.

HOW THIS BOOK IS STRUCTURED

This book is divided into seven chapters and two appendices:

- Chapter 1, The Role of the Operator, introduces the specific assignments and responsibilities of a system operator: system startup and shutdown, disk preparation and repair, file system maintenance, system monitoring, and backups.
- Chapter 2, The System Hardware, introduces the hardware components of a Prime system, the importance of keeping a system logbook, and the duties of the system operator for monitoring the computer room environment.
- Chapter 3, The System Software, explains how the system makes memory available to the user and the concept of paging. In addition, this chapter discusses the types of processes that use the system: interactive users, phantom processes, server phantoms, and slaves.
- Chapter 4, The File System, describes the PRIMOS file system, including directories and files, partitions, and file system maintenance (both online and offline).
- Chapter 5, The User Community, describes the organization of the user community, how to respond to user requests, and how to monitor the status of users on the system.
- Chapter 6, System Resources, describes the subsystems that make up a typical Prime computer system.

- Chapter 7, Monitoring Your System, describes methods for monitoring your system. They include performance measurement, event logging, supervisor terminal messages, system auditing, crash tape dumps, system metering, and controlling your system from a user terminal.
- Appendix A, PRIMOS Commands, lists system attributes and components alphabetically and the PRIMOS commands that you enter to display information about or change the status of those attributes and components. The 15 DSM System Information and Metering commands are also included in this appendix.
- Appendix B, Glossary, contains a glossary of terms used in this book.

NEW FEATURES AT PRIMOS REV. 22.0

This section summarizes the new features and changes at Rev. 22.0 that are discussed in this book. For more information on Rev. 22.0 changes, refer to the individual books in the Operator's Guide series.

Dual-ported Disks: A dual-ported disk is a disk drive that is connected to two systems. The function of a dual-ported disk is to allow the disk drive to be switched over to a secondary system if the primary system that is running the disk drive stops. A new option, -PRIORITY_SELECT, has been added to the following commands: ADDISK, ASSIGN DISK, and MIRROR_ON. This option specifies that the system take control of a dual-ported disk, whether or not that disk is currently being controlled from its alternate port.

Robust Partitions: Robust partitions are PRIMOS file system partitions that are error resistant. They are designed primarily for systems that use large databases, but can be used in any installation. In 25% of the cases, a robust partition will survive a halt; therefore, you do not have to run FIX_DISK on a robust partition after some halts. Robust partitions are discussed in the *Operator's Guide to File System Maintenance.*

User Processes: As many as 960 processes can be managed at one time by PRIMOS. Prior to Rev. 22.0, a maximum of 255 processes could run at the same time. Information on configuring the number of users is contained in the *System Administrator's Guide, Volume I: System Configuration.*

User Terminal Lines: With the installation of the Network Terminal Service (NTS), a system may have as many as 1024 asynchronous communication lines configured for user terminals. Detailed information on configuring asynchronous communication lines is outlined in the *System Administrator's Guide, Volume II: Communication Lines and Controllers.*

The online Rev. 22.0 INFO files reside in the INFO22.0 directory. These files contain new information about PRIMOS and other Prime software.

PRIME DOCUMENTATION CONVENTIONS

The following conventions are used throughout this document. The examples in the table illustrate the uses of these conventions.

Convention	*Explanation*	*Example*
UPPERCASE	In command formats, words in uppercase bold indicate the names of commands, options, statements, and keywords. Enter them in either uppercase or lowercase.	**SLIST**
italic	In command formats, words in lowercase bold italic indicate variables for which you must substitute a suitable value. In text and in messages, variables are in non-bold lowercase italic.	**LOGIN *user-id*** Supply a value for *x* between 1 and 10.
Abbreviations in format statements	If a command or option has an abbreviation, the abbreviation is placed immediately below the full form.	**SET_QUOTA** **SQ**
Brackets [ ]	Brackets enclose a list of one or more optional items. Choose none, one, or several of these items.	$\textbf{LD} \begin{bmatrix} \textbf{-BRIEF} \\ \textbf{-SIZE} \end{bmatrix}$
Braces { }	Braces enclose a list of items. Choose one and only one of these items.	$\textbf{CLOSE} \begin{Bmatrix} \textbf{\textit{filename}} \\ \textbf{-ALL} \end{Bmatrix}$
Braces within brackets [{ }]	Braces within brackets enclose a list of items. Choose either none or only one of these items; do not choose more than one.	$\textbf{BIND} \left[\begin{Bmatrix} \textbf{\textit{pathname}} \\ \textbf{\textit{options}} \end{Bmatrix} \right]$
Vertical bars ‖ ‖	Vertical bars enclose a list of items. Choose one or more of these items.	$\textbf{OUTPUT} \begin{Vmatrix} \textbf{\textit{filename}} \\ \textbf{TTY} \end{Vmatrix}$
Parentheses ( )	In command or statement formats, you must enter parentheses exactly as shown.	**DIM *array* (*row, col*)**
Underscore in optional phrases	In command formats, underscores indicate required portions of optional phrases.	**[OF THE FILE *pathname*]**

Underscore in examples	In examples, user input is underscored but system prompts and output are not.	`OK, RESUME MY_PROG`
		`This is the output`
		`of MY_PROG.CPL`
		`OK,`

Convention	*Explanation*	*Example*
Ellipsis ...	An ellipsis indicates that you have the option of entering several items of the same kind on the command line.	**SHUTDN** ***pdev-1*** [***...pdev-n***]
Hyphen -	Wherever a hyphen appears as the first character of an option, it is a required part of that option.	**SPOOL -LIST**
Default indicator ●	In a list of options, a bullet indicates the default choice, if one exists. If you do not select an option, the system chooses the default option.	$\begin{bmatrix} \textbf{A} \bullet \\ \textbf{O} \\ \textbf{D} \end{bmatrix}$
Subscript	A subscript after a number indicates that the number is not in base 10. For example, a subscript 8 is used for octal numbers.	200_8
Key symbol	In examples and text, the name of a key enclosed by a rectangle indicates that you press that key.	Press `Return`

1

THE ROLE OF THE OPERATOR

The system operator has the crucial role of ensuring the smooth operation of a Prime system. The specific assignments and responsibilities of an operator are defined by System Administrators, and may vary from one computer installation to another. Nevertheless, certain tasks are normally the operator's responsibility.

The functions the operator performs fall within these task groups:

- Keeping the System Logbook
- Starting up and shutting down the system
- Monitoring hardware and computer room conditions
- Maintaining the files and system
- Working with system software
- Working with users
- Monitoring system activity
- Performing tape backups
- Managing network activity

The following sections briefly explain each of these duties and responsibilities. Later chapters give more details about the commands, software, and hardware that enable you to perform these duties.

KEEPING THE SYSTEM LOGBOOK

It is essential that you maintain a system logbook to record all events affecting system operation. Record information about

- The software currently installed, such as a listing of the PRIMOS.COMI file and the system configuration file
- The hardware configuration, such as the model numbers and serial numbers of each disk drive attached to the system
- The environment, such as the temperature and humidity of the room in which the system is located
- Security issues, such as any unauthorized access to the computer room or loss or damage to equipment
- Operations, such as subsystem startups, use of the FIX_DISK utility, and any system shutdowns that occur
- Halts, such as the message given when a system halts and the address where PRIMOS halted

These logbook categories are discussed in greater detail in Chapter 2 in the section, Keeping the Logbook.

STARTING UP AND SHUTTING DOWN THE SYSTEM

Your duties as computer operator require that you know

- How to boot the system
- The contents of the startup and configuration files
- How to handle halts and hangs
- The sequence for shutting down the system smoothly

The following sections outline your tasks in each of these areas.

Booting the System

One of your basic duties as a system operator is to start up the system. Starting up the system is called **bootstrapping**, or **booting** the system. When the system is booted, the operating system is loaded into memory, either from disk or magnetic tape.

On some systems, booting occurs automatically when you first turn on the CPU. For other systems, you must manually boot the system using the BOOT, BOOTP, or BOOTT commands. These commands boot the system from Control Panel (CP) mode. The `CP1>` or `CP>` prompt is displayed.

Refer to the following chart to determine which boot command to use:

BOOT Used with the boot switch option word, which determines the device from which the bootstrap program is to be run as well as the pathname of the PRIMOS runfile. The most commonly used form of the BOOT command is BOOT 14114, which directs the CPU bootstrap program to boot PRIMOS from the default boot runfile. BOOT 10114 boots PRIMOS but prompts you for the PRIMOS runfile pathname. Unlike the following boot commands, BOOT does not perform CPU verification.

BOOTP Boots the system from CP mode. Similar to BOOT 14114 above, but automatically verifies the CPU.

BOOTT Boots the system from CP mode. Identical to BOOT 10114 above, but performs the same loading and initialization procedure as the BOOTP command.

Startup and Configuration Files

After the system has been booted, it executes the following PRIMOS startup files, which initialize and configure the system:

- PRIMOS.COMI (or C_PRMO)
- CONFIG

The PRIMOS.COMI file contains a list of the commands that start up the system software. The first command is always the CONFIG command, which reads the configuration (CONFIG) file. The startup file usually contains commands that start up subsystems such as Batch and the File Transfer Service. Other commands that are usually found in the PRIMOS.COMI file include SET_ASYNC, which specifies the asynchronous lines on the system, and SET_TIME_INFO, which establishes the local time zone and the daylight saving time setback. A listing of a PRIMOS.COMI file is shown in the handbook for your CPU and in the *Software Installation Guide, Rev. 22.0.*

The configuration file typically is named CONFIG or *sysname*.CONFIG, where *sysname* is the name of the system. This file contains **configuration directives** that set a number of global parameters for the system, such as the number of terminal users, and the name of the command device. This process is called **system configuration.** An example of a typical CONFIG file is shown in the handbook for your CPU.

After the system configuration is completed, the system loads programs provided by Prime and installs application programs. This procedure is called **system initialization.** See the *Software Installation Guide, Rev. 22.0* for examples.

Handling Halts and Hangs

A halt or hang of the system can occur after certain hardware or software failures. To recover from a halt or hang, follow this basic procedure:

- Take a **tape dump** to preserve a record of the state of the system at the time of the halt. A tape dump (also referred to as a crash dump) is the writing of the contents of memory to tape after a system halt. Tape dumps, which can be either complete or partial, are discussed more fully in Chapter 7, Monitoring Your System.
- Perform a cold start or a warm start to restart the system.

You must perform a **cold start** after certain types of halts, as listed in the handbook for your CPU. You invoke the BOOTP command, which performs the same initialization and configuration sequence as a bootstrap procedure. After cold starting the system, you should run FIX_DISK on all partitions to ensure the integrity of the file system.

A **warm start** restarts PRIMOS without having to go through the entire initialization and configuration procedure. You may perform a warm start only after certain types of halts occur. Refer to the handbook for your CPU for a listing of these halts and the sequence of steps to warm start PRIMOS.

You should refer to your CPU handbook for detailed information on recognizing halts and hangs and the correct recovery procedure to use.

System Shutdown

System shutdown involves the following steps:

1. Shutting down PRIMOS
2. Removing system power

Shutting down PRIMOS involves these general steps:

1. Limit logins.
2. Warn users that the system is coming down.
3. Force logouts and shut down subsystems.
4. Use the SHUTDN ALL command.

Refer to your CPU handbook for details on both the startup and shutdown procedures.

MONITORING THE HARDWARE AND THE COMPUTER ROOM

This task may be divided into two areas:

- The machines
- The room where the machines are located

One of your basic duties as system operator is to see that all the hardware components and devices are working well. The scope of your duties depends on the size of the installation. If your system is small, for example an office system, the hardware may consist of a cabinet, a terminal or two, and a printer, all located in an office along with desks, file cabinets, and so on. Your duties will be limited to the system equipment itself.

If your installation is a large one, with many user terminals, printers, and other devices, the CPU is likely to be located in a computer room. In this case, you will be responsible for a greater variety of devices, such as printers and plotters. You will also be responsible for monitoring the environment of the computer room.

For example, the CPU and its peripheral devices are designed to work at optimum efficiency when the temperature and humidity of the computer room are kept within the range specified by your Customer Support representative. If the temperature exceeds this range and cannot be brought under control, you should notify users and shut down the system until the problem can be identified and resolved.

These hardware components and your responsibilities for maintaining them are described in greater detail in Chapter 2, The System Hardware. Later chapters describe tasks you perform on the hardware using PRIMOS software. Refer also to your CPU handbook for details on the system configuration at your installation.

MAINTAINING THE FILE SYSTEM

Your responsibilities for maintaining the file system involve the following tasks:

- Using the MAKE utility to prepare partitions for system use
- Using the FIX_DISK utility to maintain and repair disk partitions
- Maintaining system files and directories

Preparing Partitions for System Use

The most basic component of the PRIMOS file system is the file itself. Files are listed in directories, which in turn are stored on **partitions**. A partition is a single section of the total storage area of your disks. Partitions are also sometimes referred to as disks. When trying to envision these two elements, think of a disk as a physical platter and a partition as a logical collection of one or more surfaces of those platters. Refer to Figure 4-1 in Chapter 4, The File System.

Partitions are specific, named areas of disks where portions of data are kept in storage. For example, all data relating to payroll may be kept on the partition named <PAYROL>. (Legal partition names may not be longer than six characters.)

One of your tasks as operator is to create partitions on the system, using the MAKE command. This command and other terms you need to create partitions are explained in Chapter 4, The File System. More details are available in the *Operator's Guide to File System Maintenance.*

Repairing Disk Partitions

The task of repairing disk partitions has two parts: checking the file system for inconsistencies and repairing those inconsistencies. The PRIMOS utility for repairing disk partitions is called FIX_DISK.

Use the FIX_DISK utility in the following situations:

- Routinely during every system backup
- When you suspect that the file structure has been damaged
- When you suspect that the quota system has been damaged
- If users have problems attaching to a directory or using a file
- If COPY_DISK or PHYRST report the creation of an equivalence block
- After a power failure
- When a message from the ADDISK command directs you to do so
- When selecting either Dynamic Badspot Handling (-IC) mode or Nondynamic Badspot Handling (-AC) mode
- When changing the maximum or minimum extent sizes for Contiguous Access Method (CAM) files

Some of these situations require only that you invoke FIX_DISK to check for errors (after a power failure, for example). In other situations, you should run FIX_DISK with the appropriate option to correct or modify the file system.

Chapter 4, The File System, and the *Operator's Guide to File System Maintenance* discuss the circumstances under which you use FIX_DISK and the options you use for each situation.

Maintaining System Files and Directories

PRIMOS uses special system files and directories to perform its job. They are located in three places:

- On the command device (COMDEV)
- In the Master File Directory (MFD)
- In the directory CMDNC0

The **command device**, often referred to as **COMDEV** after the directive that sets it, is the first partition (logical device zero) on disk drive 0. It is established by the COMDEV directive in the system configuration file.

The directory **CMDNC0** is always located on the command device. It holds external commands, that is, commands that are not embedded in the operating system. These commands are used by the system to perform such tasks as magnetic tape backups (MAGSAV) and listing files in a directory (LD.RUN). The system startup file (PRIMOS.COMI) and the CONFIG file are also contained in the directory CMDNC0.

The **Master File Directory (MFD)** is a special directory that contains the names of all the top-level directories and system files on a partition. Each partition has its own MFD, and each partition may have either a badspot file (BADSPT) or a dynamic badspot file (DYNBSP) in its MFD if it has physical defects, or badspots. The FIX_DISK command checks these files for a list of all records that contain badspots.

You should be familiar with the special directories located on the command device and in the directory CMDNC0, as well as with the files and subdirectories listed in the Master File Directory of each partition. These partitions and directories are discussed further in Chapter 4, The File System.

WORKING WITH SYSTEM SOFTWARE

You should be familiar with PRIMOS software, including these elements:

- PRIMOS processes, such as a Batch job, and servers, such as BATCH_SERVICE
- Subsystems, such as EMACS, SPOOLER, and DSM

PRIMOS Processes and Servers

PRIMOS uses many **processes** to get its work done. A process can be thought of as a system user. In some cases, a process is started by an interactive user from a terminal, for example, by issuing the COPY command. Another type of process is the **server**, which PRIMOS uses to put a subsystem into operation. An example is the Login server, which is the process that enables users to log in. A third type of process is started by a subsystem.

For example, when you send a job to the Batch queue, the BATCH_SERVICE server passes the job to the Batch subsystem; the Batch subsystem then starts another process to complete the job.

Your responsibilities for processes and servers are discussed in more detail in Chapter 2, The System Hardware, and Chapter 5, The User Community.

Subsystems

The software that makes up the system is unique to each Prime installation. In addition to the PRIMOS operating system, your system may have the following:

- Prime-installed programs and subsystems
- Applications programs that have been written specifically for your installation

A **subsystem** includes the programs, directories, and files that make up a utility. To activate a subsystem, you issue the appropriate subsystem command. For example, the PROP command starts the Spooler subsystem.

Although PRIMOS can work without subsystems, subsystems add to the system's usefulness by

- Helping users do certain tasks. For example, the Spooler subsystem allows you to print files.
- Helping PRIMOS administer the system. For example, the Distributed Systems Management (DSM) subsystem enables the system and network logging mechanism.
- Providing applications programs (such as Prime INFORMATION™ or ORACLE®) through which a user can perform specific jobs. For example, Prime INFORMATION provides a database management program.

Some of the Prime subsystems you are responsible for are

- The Spooler subsystem
- The Batch subsystem
- Distributed Systems Management (DSM)
- Editors (such as EMACS or ED)
- Separately priced software such as NTS, SyncSort™, or Prime INFORMATION

Your responsibilities for Prime subsystems are discussed in Chapter 6, System Resources, and Chapter 7, Monitoring Your System.

WORKING WITH USERS

To assist the users of your system in getting their work done, your responsibilities include these tasks:

- Communicating with users
- Managing user activity

Communicating With Users

In addition to using the supervisor terminal to issue commands, monitor the system, and start up subsystems and processes, you can also

- Send messages to users
- Receive messages from users
- Receive messages from the system

The system reports some messages automatically to the supervisor terminal. In most cases these are for information only and need not be acted upon. In other situations, you must take action when a message is displayed.

Other users can send requests to you, as operator, at the supervisor terminal. A typical message might request exclusive use of a tape drive. User processes also send messages to the supervisor terminal when the process finishes or halts.

You can respond to user messages by issuing the MESSAGE command. Similarly, you can use this command to send a broadcast message to all users on your system. For example, use MESSAGE to announce a system shutdown to all users currently logged in, so that they can log out.

The procedure for sending messages to users is discussed further in Chapter 5, The User Community.

Managing User Activity

The Prime system is a shared system, that is, as many as 960 processes can be running at one time, and as many as 1024 asynchronous terminal lines can be configured for a system. To avoid unnecessary competition among users and processes, it is therefore vital that the system resources be used efficiently and equitably. Your roles in managing user activity include

- Setting up new users on the system
- Configuring the system correctly
- Monitoring user status

- Managing the disk space and a user priority system

As system operator, you may have to set up user profiles in addition to monitoring the use of system resources. User profiles establish the priority each user has for sharing the system. You may also need to establish quotas on directories. These functions are discussed in Chapter 5, The User Community.

Your System Administrator may also ask you to set up security mechanisms, both for the system and for individual users. This task involves

- Using Access Control Lists (ACLs)
- Assigning users to ACL groups and projects
- Setting up ACLs on peripheral devices, such as tape drives
- Reviewing the security logs

These security functions are explained in Chapter 5, The User Community, and Chapter 7, Monitoring Your System.

MONITORING SYSTEM ACTIVITY

You can use a variety of methods to monitor system activity. They include

- Using the PRIMOS monitoring commands
- Using System Information and Metering (SIM) commands
- Reviewing system log files
- Observing supervisor terminal messages
- Reviewing security log files

These methods differ from each other primarily in the way in which you obtain the data and the purpose for which the information is used. For example, supervisor terminal messages report system events to the supervisor terminal automatically; by contrast, you must enter the PRIMOS monitoring commands from the supervisor terminal to display a report on a specific activity. Similarly, you must display a log file, or write the contents out to a file and make a hard copy, to interpret the activities you want to monitor.

The different approaches to monitoring system activity are discussed in the following sections.

Using PRIMOS Monitoring Commands

Issue a PRIMOS monitoring command either to look at a particular activity or to check the status of the system. The commands that enable you to view activity on the system are

- STATUS
- USAGE
- PRIMON
- PRIMAN

The STATUS command has several options, each of which enables you to look at a portion of system activity. For example, issuing the STATUS USERS command produces a report of user activity on the system. The USAGE command displays a report on system performance, based on data about the CPU, the disks, and memory.

PRIMON, which stands for PRIMOS Monitor, provides an on-screen dynamic display of system activity. PRIMAN™ (PRIMOS Analysis) is a usage analysis and report generating tool. These two commands can be used only at a supervisor terminal that is a video display terminal. Both PRIMON and PRIMAN are separately priced products that may be installed on your system.

PRIMOS monitoring utilities are discussed in Chapter 7, Monitoring Your System. Refer also to the *Operator's Guide to System Monitoring*, the *PRIMAN User's Guide*, and the *Operator's Guide to System Commands.*

Using System Information and Metering Commands

When Distributed Systems Management (DSM) is running on your system, the System Information and Metering (SIM) commands are available to monitor specific PRIMOS activities on your system. Many of these commands provide information similar to that obtained from the STATUS and USAGE commands. For example, both the STATUS USERS command and the SIM command LIST_PROCESS display information concerning the number of users logged in to a system, but in different formats.

SIM commands are explained in Chapter 7, Monitoring Your System. Refer also to the *DSM User's Guide*, the *Operator's Guide to System Monitoring*, and the *Operator's Guide to System Commands.*

Reviewing System and Network Log Files

The system and network log files are created by a DSM logging mechanism that is set up by your System Administrator. These messages are not displayed on the supervisor terminal when they are being written to the system log file; however, you can see them by displaying the log file.

Chapter 7, Monitoring Your System, describes how to create and display log files. The procedure for setting up the logging mechanism is discussed in the *DSM User's Guide.*

Observing Supervisor Terminal Messages

The supervisor terminal messages are also automatic in that some system messages are always displayed at the supervisor terminal. Other messages are displayed only if your System Administrator has set up the DSM logging mechanism to report certain types of messages.

Supervisor terminal messages are discussed in Chapter 7, Monitoring Your System.

Maintaining Security Log Files

The C2 Security Audit facility provides for a security logging mechanism that is completely separate from system logging. **Security logging** refers to the writing of security events (such as unauthorized attempted logins or attaches to directories) to a file. It is activated by the SECURITY_MONITOR command, which the System Administrator uses to specify the events and/or users to be monitored. The Security Audit facility is discussed in Chapter 7, Monitoring Your System, and in the *System Administrator's Guide, Volume III: System Access and Security.*

PERFORMING TAPE BACKUPS

A **tape backup** is a copy of a file or program on a tape. You may do a tape backup for one of the following reasons:

- To save data periodically to prevent loss in case of a system crash or other error
- To transfer data to another system that is not on the network
- To transfer large data files
- To free disk space
- To archive seldom-used files and directories

It is a good idea to do periodic backups of data files. These files can then be restored from tape if they are lost because of a system error or because a user mistakenly overwrote or deleted a file. In this situation, only modifications that were made after the last backup are unrecoverable. The frequency with which you do tape backups depends on such factors as how often a file is modified and how much tape storage space you have. For example, a database that is rarely modified needs to be backed up less frequently than the data files relating to payroll or inventory, which may need to be modified daily.

Sometimes you need to transmit data files to another site whose system is not on your network. Or perhaps a database is so large, it is easier to copy it to tape rather than copying it to another disk over a network.

When a partition begins to get full, you can copy some of the data files to tape. Usually, this is done to data files that have not been used recently. (For example, you may want to copy to tape a database that is used only for quarterly reports.)

The tasks involved in doing tape copies and backups are described in more detail in the *Data Backup and Recovery Guide.*

Restoring Files and Directories From Backup Copies

After you have done a tape backup of a file, directory, or partition, you may be asked to restore it. **Restoring** a file, directory, or partition refers to the transfer of the data from tape to disk. This occurs most frequently when a system crash has occurred and the data must be restored from a tape backup copy. You may also be asked to restore a file, directory, or partition that has been copied to tape onto or from another system. For information on restoring files, directories, and partitions see the *Data Backup and Recovery Guide.*

Helping Users With Magnetic Tape Requests

Users may request the exclusive use of a tape drive so that they can back up their own files onto tape. To do this, use the ASSIGN command to assign a tape drive and the REPLY command to respond to the user. This procedure is discussed in Chapter 6, System Resources, and in the *Data Backup and Recovery Guide.*

MANAGING NETWORK ACTIVITY

A **network** consists of two or more CPUs linked together electronically. An example is the PRIMENET networking software. Whether your installation is a small office installation or a large, complex installation, it may be part of a larger network of systems.

As a system operator, you may be responsible for some of the following network duties:

- Starting up and shutting down the network
- Performing file transfers
- Adding disks to remote systems on the network
- Communicating with other system operators

- Managing a local area network (LAN)
- Monitoring network activity

Chapter 6, System Resources, discusses the network resources used to accomplish these tasks. Chapter 7, Monitoring Your System, presents information on monitoring network resources. Refer also to the *User's Guide to Prime Network Services*, the *Operator's Guide to Prime Networks*, and the *NTS User's Guide* for detailed information on specific types of networks.

2

THE SYSTEM HARDWARE

To perform the tasks described in Chapter 1, you must be familiar with both the hardware and the software components of your installation. This chapter describes the hardware components of a system and covers these related topics:

- The logbook for recording system events
- The computer room and rules for monitoring the environment for your system

PRIME HARDWARE CONFIGURATION

The configuration of system hardware varies from installation to installation, but Prime systems conform to one of these two categories:

- A single-node system (not networked to other systems)
- A node on a network of systems

A single-node system usually operates with one Central Processing Unit (CPU), although some single-node systems may have two CPUs. A single-node system may be a small office system or a larger computer room system. It may have a few user terminals or many. It may have a small number of peripheral devices, or it may have a diverse configuration of devices. The significant difference between a single-node system and a networked installation is that a single-node system does not *talk* to another system by means of any network interface.

Networked installations can include small office systems as well as larger computer room systems. Essentially, they can consist of any Prime system that is part of a network. The types of network interface devices that can make up a networked system are discussed later in this chapter.

SINGLE-NODE SYSTEMS

A single-node system includes these hardware components:

- Supervisor terminal
- CPU cabinet
- Disk drive and tape drive
- User terminals
- Peripheral devices (printers, plotters, and so on)

Figure 2-1 illustrates the relationship of the hardware components to the CPU cabinet.

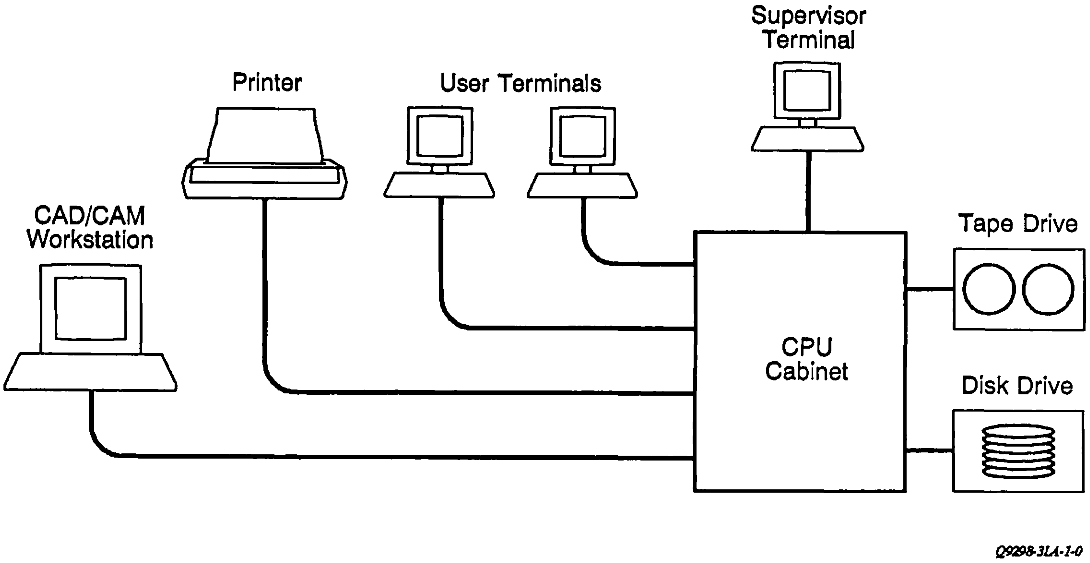


FIGURE 2-1. Single-node Prime Hardware Configuration

The components of a single-node system are discussed in the following sections. Refer to the handbook for your Prime CPU for a full discussion of that CPU's hardware. Refer also to the operating manual that accompanies each of the peripheral devices on your system.

Supervisor Terminal

In most installations, the **supervisor terminal** is a standard user terminal with a video display screen, such as a PT200™ terminal. In some cases the supervisor terminal can be a hard-copy terminal. The supervisor terminal is usually located in the computer room close to the CPU.

While a supervisor terminal can function as a regular user terminal, its most important function is to control the entire system. For example, only from the supervisor terminal can you issue commands to start up or shut down the system. In addition, some other commands work only when issued from the supervisor terminal. Using the supervisor terminal also gives you access to files and directories that are not available to the regular user. Because the supervisor terminal controls the system, it is essential to maintain security in the computer room so that the supervisor terminal is not available to unauthorized personnel.

CPU Cabinet

The CPU cabinet contains the components that control all processes connected with the system:

- One or two CPUs, which control all activity of the computer
- Memory boards, which store information temporarily before it is transferred to permanent storage elsewhere
- Power supplies, which provide the proper amount of electricity to the various parts of the computer
- Controller boards, which manage the system components that enter and retrieve data

In some systems, the disk drive and tape drive are also contained in the CPU cabinet. For clarity, these components are considered separate elements of the hardware portion of the system in this chapter, and are discussed below.

Disk Drive

The **disk drive** may be installed in your system in one of two locations:

- As a component in the CPU cabinet
- As a component of a separate peripheral cabinet

In all cases, the disk drive provides storage for volumes of data that are too large for main memory. This information is retained on the disks whether the power is on or off. When the CPU executes a program, the PRIMOS operating system reads the program and the data into main memory from the disk. Main memory and virtual memory are discussed later in this chapter.

A system can have more than one disk drive from which it can retrieve data. The disk drive in Figure 2-1 is shown as a separate element. In some cases, the disk drive and the tape drive occupy the same peripheral cabinet.

Dual-ported Disk Drive

A **dual-ported disk** is a disk drive that is physically connected to two separate systems. The function of a dual-ported disk is to allow the disk drive to be switched over to a secondary system if the primary system that is running the disk drive stops.

For example, a large database can be stored on a partition located on a dual-ported disk. If the primary system that is connected to the dual-ported disk stops running, the disk can be switched over to the secondary system. Users still have access to the database even though the primary system is shut down.

Note

Although the dual-ported disk is physically connected to two systems, the disk can be started locally on only one system.

Tape Drive

A **tape drive** may be installed in one of two locations:

- As a component in the CPU cabinet
- As a component of a separate peripheral cabinet

A tape drive enables you to copy data to or from magnetic tape. You can transfer data to another system or back up or archive data to tape on your own system. When you want to restore the data to disk, you can use the tape drive to retrieve the data. The tape drive in Figure 2-1 is shown as a separate element. In some cases, the disk drive and the tape drive occupy the same peripheral cabinet.

User Terminals

Standard **user terminals** are video display terminals that are physically attached to the host CPU. The hardware configuration shown in Figure 2-1 has two user terminals. The actual number of user terminals on a system is determined by the value of the NTUSR configuration directive specified by the System Administrator in the configuration file.

Peripheral Devices

Some of the peripheral devices that may be installed on your system include

- Printers
- CAD/CAM workstations

- Plotters
- Paper tape reader/punches
- Card reader/punches

Most installations have at least one printer. Printers can be any of the following types:

- Letter-quality printers
- Laser printers
- Parallel printers
- Serial line printers

Figure 2-1 shows a CAD/CAM workstation and one printer. The actual number of peripheral devices that are installed on a system is limited by the number of lines specified by the System Administrator in the PRIMOS.COMI file.

NETWORK INTERFACE DEVICES

A typical network configuration is shown in Figure 2-2. If your installation is part of a network, you may have one or more of the following network, or external, interface devices:

- PRIMENET Node Controller (PNC)
- LAN300 line
- LAN Host Controller (LHC)
- LAN Terminal Server (LTS)
- Modems
- Packet Switching Data Network (PSDN)

Figure 2-2 shows a PNC and an LHC attached to the host CPU. The PNC is a circuit board inside the system cabinet that connects the CPU to the PRIMENET network (known as RINGNET™).

The LHC is a circuit board inside the CPU cabinet. In Figure 2-2 the LHC connects the host CPU to the LAN300 line. This line, in turn, is connected to another CPU and to an LTS, through which other NTS user terminals and printers are attached to the LAN300 line. These components are all part of the Network Terminal Service, which is discussed in Chapter 6, System Resources. Refer also to the *NTS User's Guide* and the *NTS Planning and Configuration Guide.*

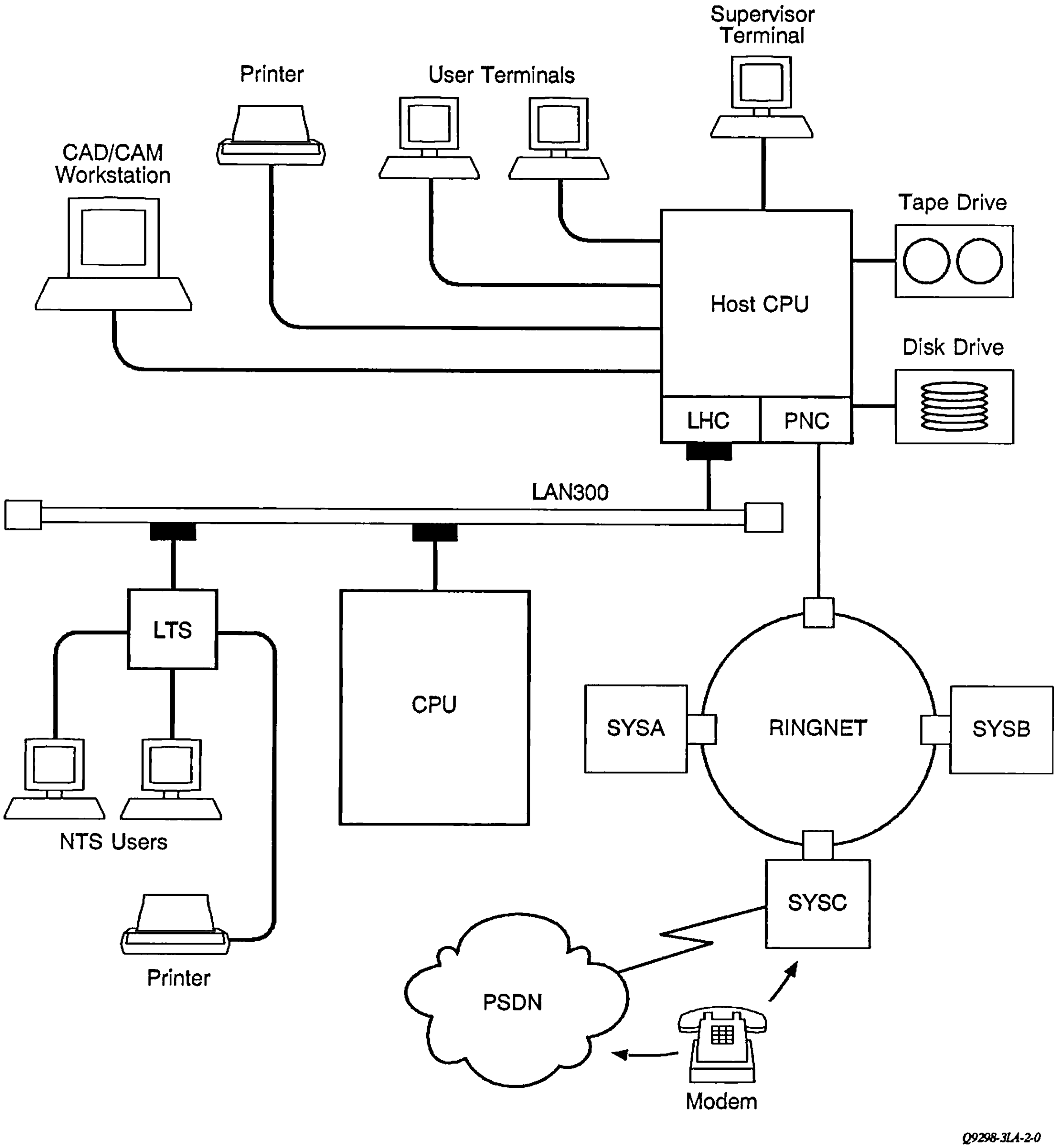


FIGURE 2-2. Typical System Configuration With Networks

Figure 2-2 shows three systems attached to the RINGNET (SYSA, SYSB, and SYSC). SYSC is also connected to a Packet Switching Data Network (PSDN). PSDN is a type of Public Data Network. Any user terminal that is attached to a system that is part of a Public Data Network can connect to the PSDN through the use of the NETLINK utility.

Modems are used to connect a user terminal to either a CPU or a PSDN by telephone lines. An example of a modem hookup would be a user who has a terminal at home and who communicates with the CPU at work by connecting his phone to the modem and dialing the correct telephone number.

THE SYSTEM LOGBOOK

Whether your system is running smoothly or having problems, it is useful to know how it is running. Two methods are used to track system events:

- Logbooks, the contents and format of which are defined by the System Administrator and entered by the operators
- Software event loggers, which are kept by the system, with some parameters supplied by the operator on the command line

The next section of this chapter discusses the purposes of logbooks and suggests some of the items that should be entered into them. Software event loggers are discussed in Chapter 6, System Resources.

The Purpose of the System Logbook

Every system should have a logbook for recording information about system status and operation. The System Administrator decides what information is entered in the logbook. The system operators enter the required information. All operators must know what information to enter into the logbook and how to enter the information.

A system logbook is used primarily to document events on the system in case a problem occurs later. Many problems give unrecognized warnings before they occur. If you enter all system events into the logbook, your Customer Support representative can find (and resolve) the problem faster than if you fail to keep careful records.

Whenever you make changes to the system startup files (PRIMOS.COMI and CONFIG), you should make an entry in the logbook in case something goes wrong and someone else has to figure out the problem.

Logbook Formats

The following list contains standards and procedures that will help you maintain an efficient logbook.

- Logbooks should be numbered and dated with the dates of the first and final entries on the spine or the cover of the book.
- Each entry in the logbook should be labeled with the date and time. This historical record is useful in reconstructing a system crash or other unexpected event and also makes it possible to correlate with external events, such as power failures.
- Each entry should be signed or initialed by the person who makes the entry. Your Customer Support representative will then know whom to ask for further information about a specific event.
- All entries should be made in indelible ink, not in pencil or erasable ink. Any incorrect entry should be neatly crossed out and initialed by the person deleting it.
- Logbooks should be bound. Loose-leaf pages are easily detached and lost, particularly if they are used often.
- The page size should allow printouts and listings to be pasted in. The exact page size is not important.
- Logbooks should always stay flat when open. This makes it easier to write in them.

Logbook Contents

Your System Administrator knows the needs of your system and therefore determines the contents of your logbook. The following lists show types of information and events that you should record in any system logbook.

Information on Halts: Record in the logbook the following information concerning halts. This information is the minimum that you should record during or after a halt.

- The status of the system when it halted. The status is provided by a halt message, which includes the segment number at which the system halted, the reason for the halt, and the contents of the status words (DSWSTAT, DSWRMA, DSWPB and, for some systems, DSWPARITY or DSWPARITY2).
- In some cases, two halt messages may appear: one indicates the address where the CPU halted and the other indicates the address where PRIMOS halted. A message that shows where PRIMOS halted indicates an abnormal halt. Record this address so that you can see exactly where the halt occurred.
- If the system halted on an uncorrected parity error, record the contents of the X, A, and B registers.
- The type of start required after the halt — that is, was a warm start or a cold start required?
- After the restart, note the behavior of the machine at various times. For instance, did the system function correctly immediately after the restart? Did it continue to function correctly after a half hour?

In addition, you may want to do a crash dump onto tape. Information on dumps, as on other procedures for handling halts, is given in the handbook for your machine.

Hardware Information: Enter the following information concerning the hardware in the logbook:

- The physical system configuration, including the model number and serial number of every piece of equipment. It may be helpful to group each type of equipment — that is, list all disk drives in a group, all terminals in another group, and so on.
- Changes to the original configuration — that is, any addition, deletion, alteration, or substitution of any piece of equipment.
- Any change in the operating status of any component, such as component failure or unexpected occurrences (even if not fatal).
- The physical device numbers (pdevs) of all partitions.

Environmental Information: Enter in the logbook the following information concerning the environment of the computer room or any breach of security:

- Any abnormal temperature or humidity conditions. Include the date, time, and duration of the conditions, if possible.
- Any other unusual conditions, such as smoke, dust, or chemical spillage. Note the date, time, and duration of the conditions.
- Any unauthorized access to the computer room, together with the date and time that the unauthorized access was discovered and the name of the person who discovered it.
- Any loss of equipment or damage to equipment, together with the date, time, and cause, if known.
- Any unauthorized use of the computer, including attempts at remote login.
- Any other unusual or unexpected events or results.
- Any action taken to correct an environmental problem.

Software Information: Enter in the logbook the following information concerning the software installed on your system:

- The listing of the system startup file PRIMOS.COMI. If you have several alternative configurations, include listings of all the alternative startup command files.
- A listing of the system configuration file (usually CONFIG).
- A listing of the contents of all the system search rule files in the directory SEARCH_RULES*.
- A list showing the segment numbers of all shared memory segments. Note that these numbers are octal representations.
- A list of the contents of the command directory, CMDNC0, and the library directories, LIB and LIBRARIES*.

- A listing of the memory loadmaps RING0.MAP and RING3.MAP for the version of PRIMOS used by the system.
- A listing of the network configuration as produced by the CONFIG_NET command.
- Any addition, deletion, alteration, or replacement to the above software information.

Operations Information: Enter in the logbook any of the following operations information:

- Every system startup. Also note any special conditions (such as the omission of the Batch or FTS system startup).
- Any use of the FIX_DISK utility, together with the name and physical device number of the partition being processed and the result of the operation.
- Any disk formatting performed, together with the name and physical and logical device numbers of the partition created and the disk drive used. Information about any backups performed, including the name of the partition copied, the date of the copy, the type of copy (for example, incremental, total, COPY_DISK, BACKUP), the type of media used (disk or tape), the media statistics (such as tape speed and density), and the number of recoverable and nonrecoverable errors (if any).
- The name of any file or directory restored to the system, together with the date, time, and reason for the restoration.
- The name of any file or directory that is archived (removed from the active disks to storage for possible later use), together with information about the type of media to which it is archived, the date and time of the archiving, and the place in which the archive is to be kept.
- The date, time, and place of storage of any event-logger printout. (The event loggers are described in Chapter 7.)
- The addition, deletion, alteration, or replacement of any commands in CMDNC0 or libraries in LIB or LIBRARIES*, together with the date, time, and reason for the action.
- Any changes to the files in SEARCH_RULES*>ENTRY$.SR.
- Any shutdowns that occur, together with information about their extent (partial or complete), date and time, and cause (such as environmental factors, plant shutdown, configuration change, or system update).
- Any top-level directories that are added to or deleted from the system.
- Any changes in the user community, including new users, deletion of existing users, modifications of users' command environment limits, and changes in users' ACLs.

THE COMPUTER ROOM

Your computer room should contain various devices that are designed to keep your computer system at the right temperature and humidity and to exclude most environmental contaminants. These devices include heating systems, air conditioners, air filters, sealed windows, and anti-static mats. Environmental problems occur if operators or users circumvent these devices. Therefore, it is important to have rules that maintain the necessary environment.

General Rules

There are two rules to which there are no exceptions:

Rule 1. *No smoking* in the computer room.

Rule 2. *No food or beverages* in the computer room.

You should enforce three additional rules as closely as possible:

Rule 3. Keep the computer room free of dust and other contaminants.

Rule 4. Monitor the computer room environment within the temperature and humidity limits specified by your Customer Support Center.

Rule 5. Keep the computer room closed to unauthorized personnel.

These rules, and the reasons behind them, are discussed in the remaining sections of this chapter.

Installation-specific Rules

The System Administrator knows the special requirements of your installation and should decide exactly what rules, in addition to those listed above, are necessary.

Most installation-specific rules deal with how authorized personnel use the computer room and its equipment, and determine such things as who performs what functions and how magnetic media (tapes and disk packs) are moved and stored

Smoking, Food, and Beverages

In a computer-room environment, smoke, food, and beverages are potential contaminants, particularly to disk and tape storage media and their attendant drives. A head crash occurs when the head comes into contact with foreign matter on the spinning platter, or disk. This contact can cause serious damage to the head and to the disk. A head crash can be caused by the careless handling of a disk or by the intake of smoke through the drive. Even a smoke particle or a fingerprint is larger than the distance between a disk's surface and the moving read/write head above it.

In addition to not eating or drinking in the computer room, all personnel should wash their hands before handling magnetic media. A doughnut eaten at coffee break can leave a residue on the fingers that may cause major problems. This is particularly true of reel-type tapes, where the recording surfaces are always handled during a load. If the surface of the tape becomes sticky, the contaminant can be transferred to the read/write heads during normal operation.

Dust and Dirt

Dust can be a major problem. A speck of dust on one of your disks can cause a head crash and the loss of many days' work. Paper dust from a printer can be a major source of airborne dust. Make sure that the printer is vacuumed regularly, for example three times a week.

If your computer room has filters on the air intakes to trap airborne dust, do not leave the doors and/or windows open. Doing so makes the air filtering system ineffective. If your computer room does not have filtered air, keep the windows sealed and the doors closed as much as possible to reduce the amount of airborne dust entering the area.

Cleaning

All computer rooms should be cleaned regularly, for example three times a week. Use vacuum cleaners; do not use brooms or dry mops because they throw dust into the air.

The air filters on machines such as disk drives and the read/write heads on tape machines should be cleaned regularly. There are several cleaning operations that you can do; others are done by your Customer Support representative. Your System Administrator schedules these tasks.

Environmental Controls

Your computers are designed to give optimum performance only within the range of operating environments specified by your system installer. Moreover, if your installation does not conform to the environmental specifications, your sales or support contracts may be invalidated. Most Prime computer systems are designed to operate at temperatures between 68 and 78 degrees Fahrenheit (20 to 26 degrees Celsius) and at humidities between 40% and 60%.

If your computer room regularly exceeds the maximum temperature or humidity requirements, shut down the system until the problem can be resolved. Do not try to solve the problem by opening the doors or windows. If you do so, you will probably let in dust and cause even more problems. The best way to resolve this problem is to consult your manager and your System Administrator.

Often, cables and boxes of supplies (such as printer forms) are brought into the computer room and occupy space that is supposed to be clear. Do not allow anything to encroach on the clear space around your machines. If you do, you may have problems with accidents and obstructed exit routes. Obstructions can also impede the airflow around your machine, causing it to overheat, even if you have reliable air-conditioning.

Unauthorized Personnel

Unauthorized personnel in the computer room can cause two kinds of problems: misuse of the supervisor terminal and mishandling of equipment. People trying to do such things as load a tape on a tape drive or load a new box of paper onto a printer can damage your equipment if they do not know the correct methods.

Keeping the computer room doors locked helps to keep unauthorized people out of the computer room. If you cannot or do not lock the computer room, you should ensure that every person allowed in the computer room is adequately trained to use the machines.

3

THE SYSTEM SOFTWARE

Chapter 2 reviewed the hardware components of a Prime system. It also outlined your responsibilities for keeping the logbook and your tasks in the computer room itself. This chapter presents those concepts that you, as an operator, need to know in order to use the PRIMOS operating system. It describes

- PRIMOS software
- PRIMOS processes
- PRIMOS security

THE PRIMOS OPERATING SYSTEM

PRIMOS is the time-sharing operating system used by all Prime systems. It allows each user to work independently of other users and their activities. It provides

- Time-shared access for as many as 960 user processes per CPU
- Segmented virtual address space for programs that use as much as 64 megabytes per user
- Access to programming languages
- Input/output control
- A file system
- Interactive and noninteractive (phantom) user jobs
- Communications systems

- System utilities
- Database management

All of the operator's and users' work is performed under control of PRIMOS. The Operator's Guide set of documents concentrates both on the software supplied by Prime for computer operations and on your interactions with the user community.

How PRIMOS Uses Memory

To make a larger amount of memory available to each user, Prime systems use a virtual memory system. This system increases the amount of memory available to users without having to increase the amount of physical memory.

Physical Memory: This includes all the hardware components of the system used to manipulate large blocks of information. As shown in Figure 3-1, these are

- Cache memory
- Main memory
- Disk storage

Physical memory is, strictly speaking, limited to cache memory and main memory. As Figure 3-1 shows, these parts of physical memory are constantly swapped with data that must be retrieved from disk storage. The page-swapping mechanism makes physical memory seem as large as all three components combined. See the discussion of virtual memory below.

- **Cache memory** is a data buffer located on the CPU board, from which data is processed by the CPU. Cache stores copies of the information contained in the most recently referenced memory locations, in units of 32 bits. The size of cache memory varies depending on the design of the CPU, and ranges from 16 kilobytes to 128 kilobytes. During program execution, memory references are faster in cache than in main memory. The CPU does not have to bring the most frequently referenced pages of data into main memory from disk storage each time they are referenced.

- **Main memory** is located on circuit boards in units of either 2, 4, 8, or 32 megabytes. The amount of main memory available on a system differs; a large system can have as much as 128 megabytes of main memory.

  Main memory is divided into units called **pages**, each page being 2048 bytes (2 kilobytes) in size. Pages serve to subdivide main memory into pieces that PRIMOS can conveniently and efficiently manage. When pages of data are needed for a process, they are read into main memory from disk storage in page units.

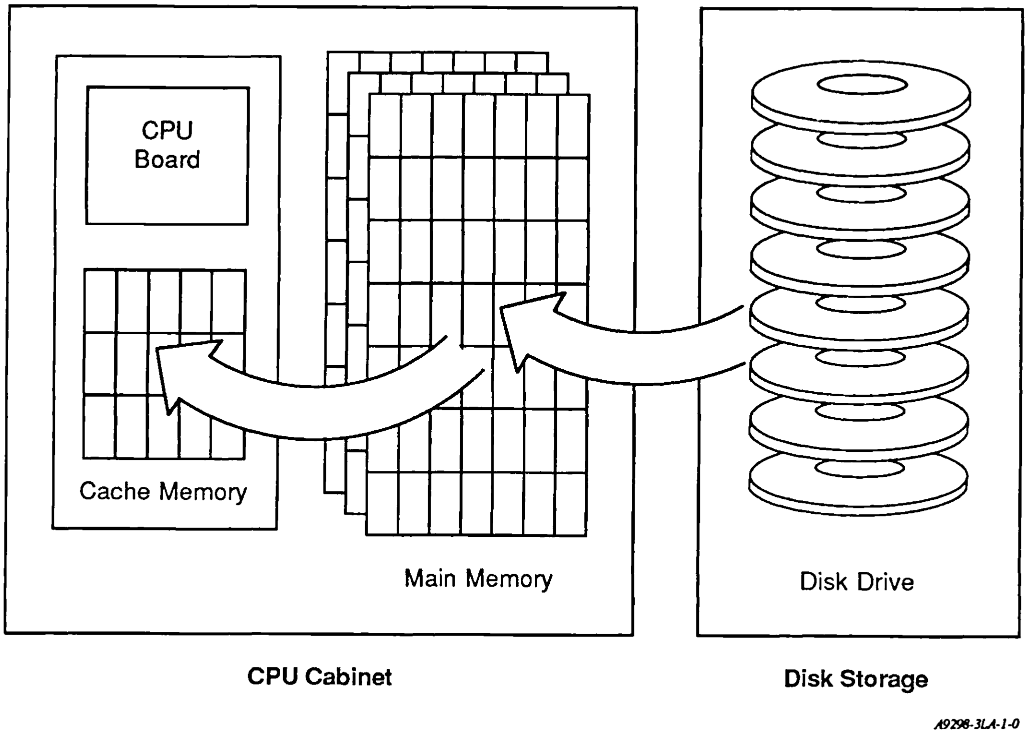


FIGURE 3-1. Physical Memory

- **Disk storage** differs from main memory and cache memory in that it consists of data not currently being used by PRIMOS. Disk storage is made up of two types of partitions:
  - o File system partitions
  - o Paging partitions

A **partition** is a grouping of part of a surface, one surface, or several surfaces of a disk or platter. Each disk storage device (disk drive) can have one or several partitions, some of which can be paging partitions. File system partitions are discussed in more detail in Chapter 4, The File System.

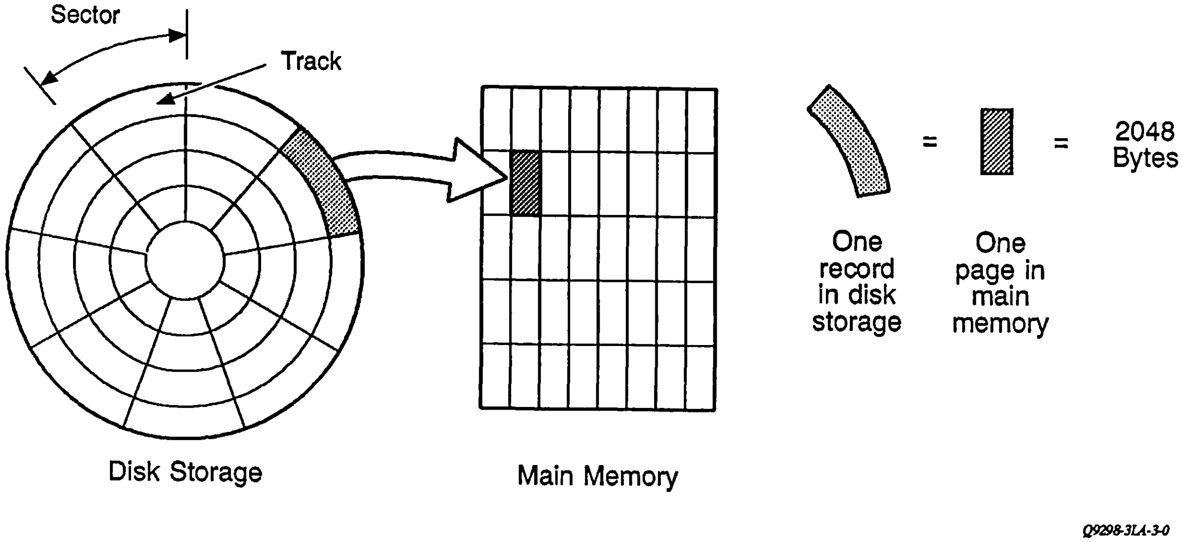


FIGURE 3-2. Storage on Disk and in Main Memory

The surface of the individual platter shown in Figure 3-2 is divided into nine **sectors** and four **tracks.** Data is organized in units called **records.** Records are equal to 2048 bytes of user data. A record also equals one **page.** When PRIMOS brings a program into main memory to process, it reads that data one page at a time. The process of transferring data between disks and memory is called **paging.**

Virtual Memory: **Virtual memory** allows a user to address more memory than actually exists in either main memory or cache memory. By using the paging mechanism, PRIMOS can run a program that is larger than main memory by moving portions of the program back and forth between main memory and disk storage.

Figures 3-3, 3-4, 3-5, and 3-6 illustrate the sequence of steps taken by PRIMOS to transfer program data between file system partitions and paging partitions in disk storage to a location in main memory to await processing.

1. When the CPU begins a process, it checks cache memory first to see if the data needed is located there. (See Figure 3-3.) If the data is found in cache memory, this is referred to as a **cache hit**.

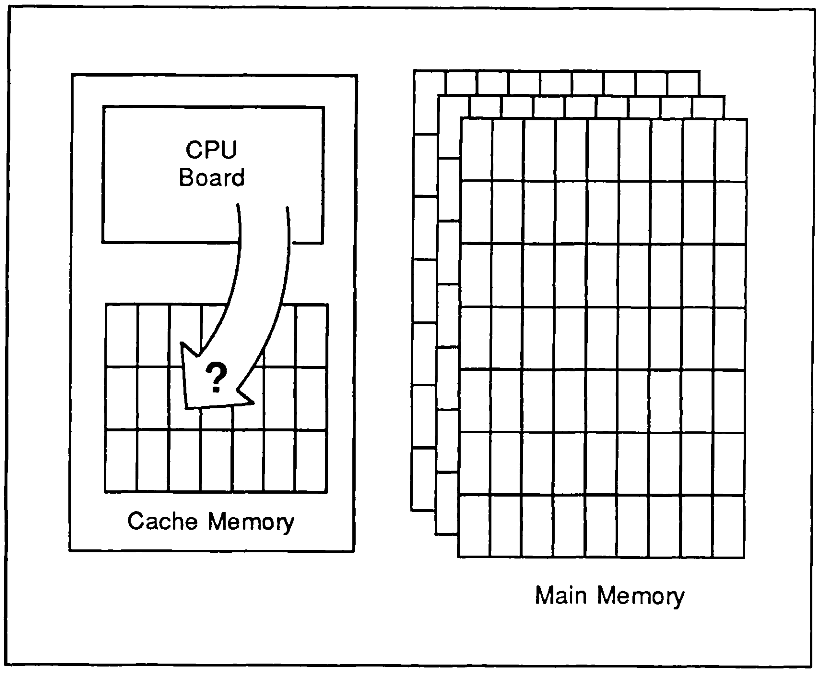


FIGURE 3-3. Checking Cache Memory

2. If the data is not located in cache memory (a **cache miss**), the CPU checks main memory for the data. If the data is in main memory, the CPU brings the data into cache memory, 64 bits at a time, for processing. (Refer to Figure 3-4.)

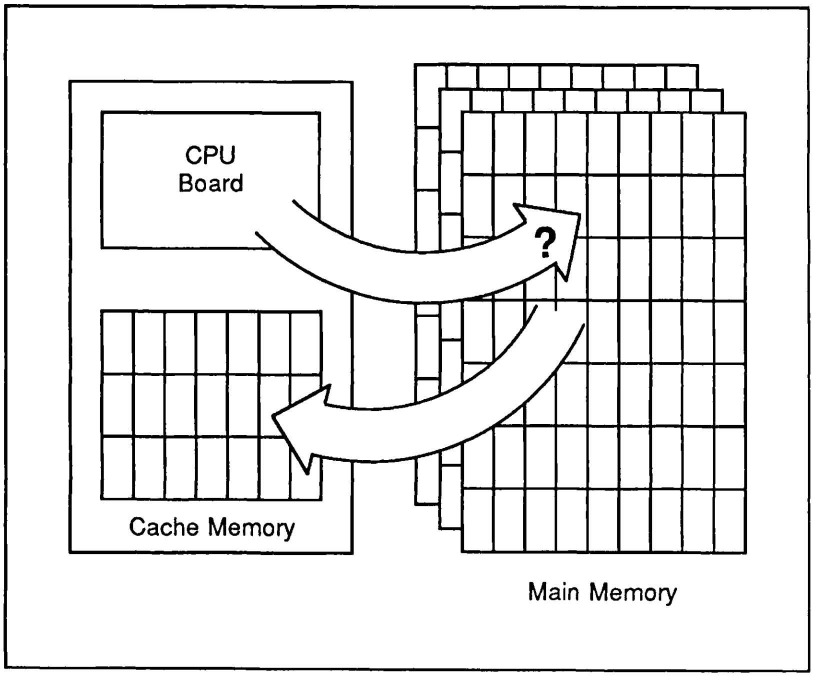


FIGURE 3-4. Checking Main Memory

3. If the data is not in main memory, a **page fault** occurs. PRIMOS then reads the data from the file system partition into the first free location it finds in main memory, as shown in Figure 3-5, and then into cache memory.

4. If all pages in main memory are in use and another process calls for pages of data to be brought into main memory (new page in Figure 3-6), some data can be paged (written) out to a special temporary storage disk called a **paging partition** (old page in Figure 3-6). PRIMOS chooses the least recently used page to move out of main memory to the paging partition.

Paging and processing continue in this manner until all the data that is needed by a program is read into main memory from paging partitions and is processed in cache memory.

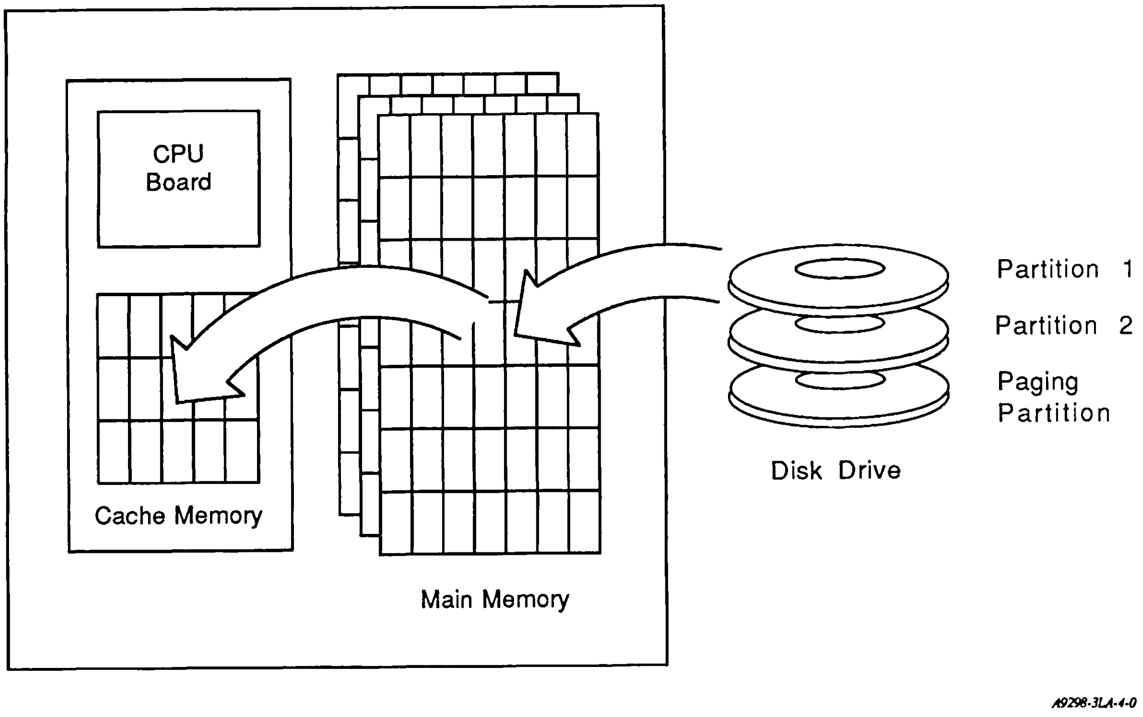


FIGURE 3-5. Reading Data From File System Partitions

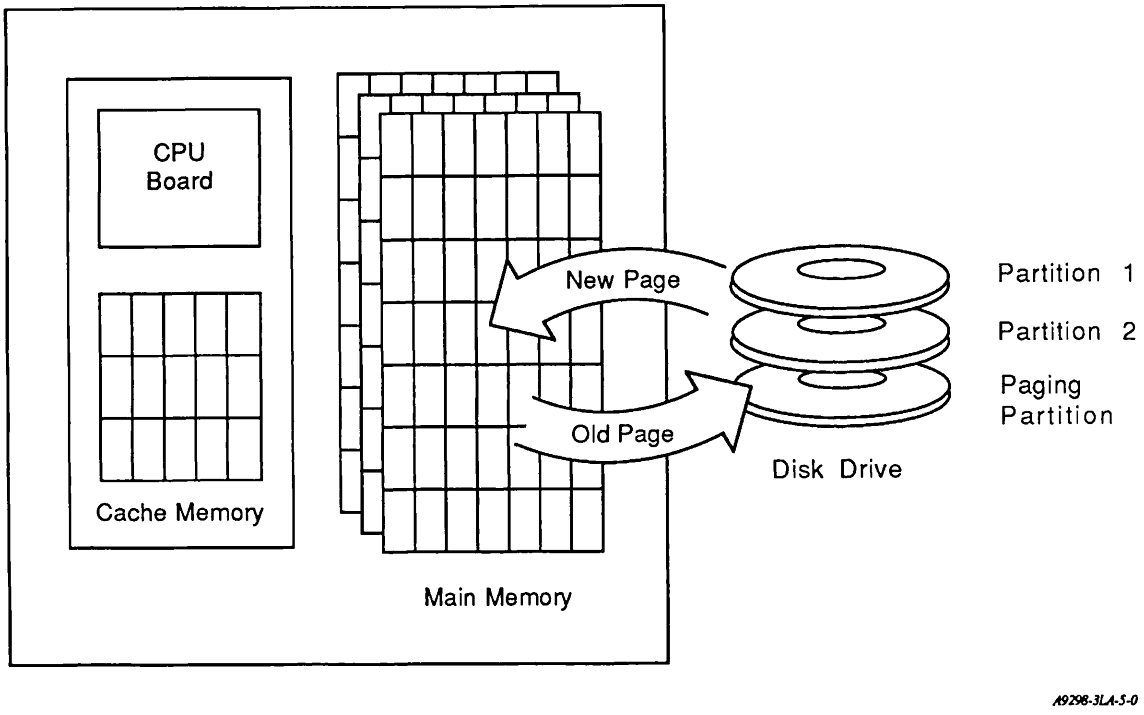


FIGURE 3-6. Swapping Data to a Paging Partition

PRIMOS locks certain critical pages against being paged out. Such pages, which usually contain system data, always remain in main memory so that the system always has access to them. Pages that are locked against being paged out are called **wired** pages.

PRIMOS allows up to eight paging partitions to a system. Paging allows for faster access to the data than would be possible if the data had to be read from permanent storage on the main file system partition each time the processing time was finished.

Time sharing systems such as PRIMOS allow processes to take turns using the CPU, with each process having a priority on the waiting list. The default priority is 1 (the lowest being 0 and the highest 3). Each process also has a set amount of time (its **timeslice**) for processing by the CPU, measured in tenths of a second. The default timeslice for a particular machine depends on that machine's model number. You can change these attributes by using the CHAP command, which is discussed in Chapter 5, The User Community.

The CPU processes the data for the timeslice allowed each process. If the timeslice ends before a process is completed, the next process on the waiting list can request that bits of data be brought into cache memory from main memory. Sometimes this results in data being overwritten in cache memory. When the first process begins another timeslice, the CPU may have to reread the data into main memory from a paging partition.

When you issue the USAGE command, as described in Chapter 7, Monitoring Your System, you can review the paging activity on your system. If your system performance seems slower than normal, this tool enables you to identify specific symptoms that will help you to diagnose the trouble.

Tape Dumps

When you experience a system halt, you want a copy of the data in memory for analysis to determine the cause of the halt. In order to do this, you take a tape dump. This is the process of dumping (writing) memory onto tape. As this procedure can take a considerable amount of time, depending on the amount of memory your system has, you may prefer to do a partial tape dump.

If, for example, you suspect that a program, subroutine, or subsystem may cause a system halt, you should define the segments addressed by the program or subsystem so that they can be dumped at the next system halt. The segments must be defined, while PRIMOS is still running, *before* a partial tape dump is done.

Use the DUMP_SEGMENT command to define the range of segments you want to dump and/or use the DUMP_USER command to specify the user whose total number of segments you want to dump, at the next halt. You can then use the data collected to pinpoint a cause of the system halt. These commands are discussed further in Chapter 7, Monitoring Your System, in the section Tape Dumps.

To use these commands effectively, you need to understand how virtual memory is organized.

Organization of Virtual Memory

Virtual memory is divided into units called **segments.** Each segment contains up to 128 kilobytes, or 64 virtual pages of 2 kilobytes each. Segments are virtual units, not physical ones, that aid both the user and the system in organizing virtual address spaces and the information contained there. For example, users can organize program code in one segment and program data in a second one. Segments also allow a user to build modular programs, one module to a segment. PRIMOS uses segments in a similar way to organize its own code into modules.

The maximum virtual address space of each user is 4096 segments; thus, each user has a virtual address space of up to 512 megabytes. These 4096 segments are subdivided into four groups called DTARs, each of which has 1024 segments. The acronym DTAR stands for Descriptor Table Address Register and is a reference that PRIMOS uses to position data in memory.

In the Prime virtual memory scheme, each user address space of 4096 segments is divided into **shared** segments and **unshared** segments, as shown in Figure 3-7.

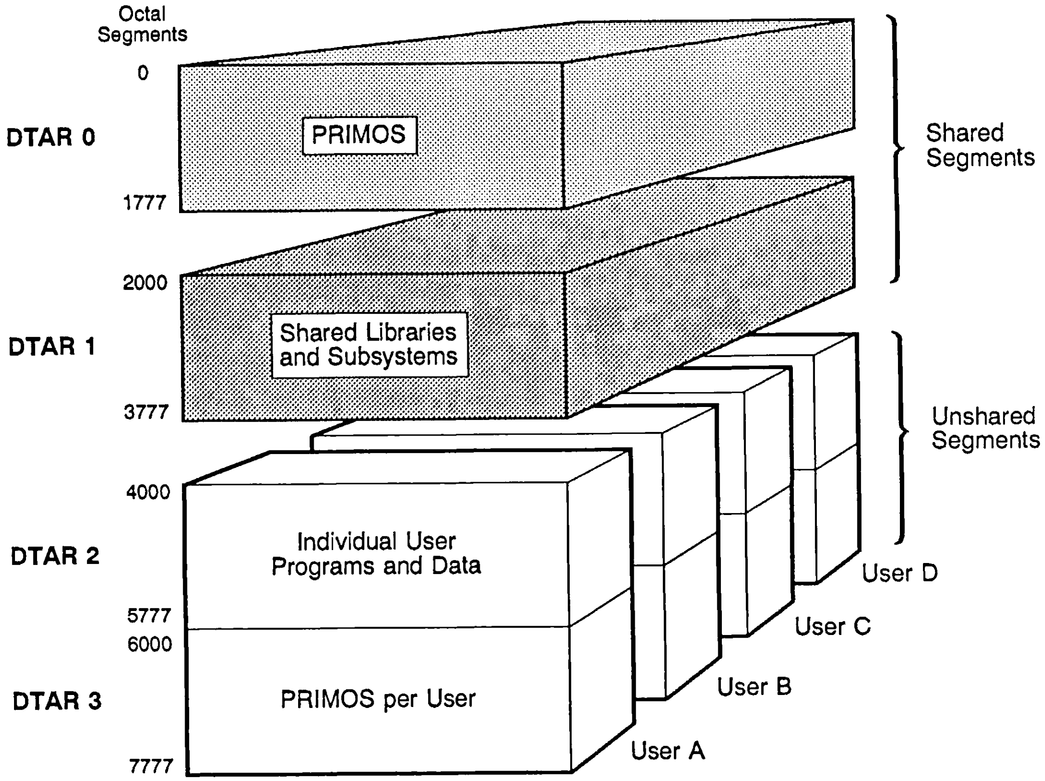
Shared Segments: The first 1024 (2000 octal) segments, shown in Figure 3-7 and numbered from 0_8 through 1777_8, are reserved for PRIMOS and shared with all users. Only a portion of this total is currently used, although all of the segments are available. The location of this group of segments is referred to as DTAR 0.

Shared libraries and application programs and shared subsystems use the next 1024 segments, 2000_8 through 3777_8. This portion of shared memory is located in DTAR 1.

Each user has access to all the virtual memory address segments in DTAR 0 and DTAR 1. It is as if a *copy* of these segments were in each user's individual memory space; whereas in fact, the segments are *shared* among all users. The PRIMOS and shared library segments that are shared by all users are represented by the two shaded areas in Figure 3-7.

Unshared (Private) Segments: In addition to those segments reserved for PRIMOS and shared libraries, 2048 unshared segments are reserved for each user. These private unshared segments are represented in Figure 3-7 by the individual DTAR 2 and DTAR 3 for each user, and are unique to each user. For example, user A can access his private segment 4007_8; it is completely different from user B's private segment 4007_8.

In actual practice, the number of private DTAR2 segments for each user is usually limited to 128 by default, although the System Administrator can alter this number when setting up the user's profile with the EDIT_PROFILE command. Refer to the *System Administrator's Guide, Volume III: System Access and Security* for information on the allocation of private user segments.



Q9298-3LA-4-0

FIGURE 3-7. Virtual Memory

The remaining private segments are in DTAR 3. These are per user segments managed by PRIMOS and are invisible to the user. They hold information for each user, such as the login name, abbreviation file, global variables, EPFs, and so on. The number of segments in DTAR 3 in actual use is very small.

PRIMOS Command Syntax

As a computer operator, you are concerned with two types of PRIMOS commands: **user commands** and **operator commands.**

User commands are available to any user from any terminal. For example, the SPOOL command enables a user to send a print request to a printer.

Operator commands are restricted to privileged users, usually the System Administrator or the system operator. In addition, some commands may have options that work only when issued from the supervisor terminal or by a privileged user.

The general format of the PRIMOS command line is as follows:

COMMAND [*names*][-OPTION *argument* [...-OPTION *argument*]]

COMMAND specifies one of the PRIMOS commands. The command must be the first word on the command line. *names* specifies the argument (or arguments) to the command. The command arguments are generally pathnames of directories or files, or an identifying name such as a user ID or a job name. -OPTION specifies a command option. Some commands do not have options.

This example of the LD command illustrates the correct command-line syntax:

```
OK, LD <system>jones>project -dtm -size
```

System Name

Every PRIMOS system requires a system name, which is defined by the System Administrator and set during cold start. You can set the system name automatically by using the configuration directive SYSNAM; otherwise, PRIMOS prompts for the system name at each cold start. Cold start does not complete until you set the system name. When PRIMENET is started on a system, it adopts the system name as its local node name.

The syntax for the system name is the same as the syntax for PRIMENET node names: the first character must be a letter; there can be up to six characters; and the characters can be only the letters A through Z, the numbers 0 through 9, and the special characters ampersand (&), hyphen (-), period (.), dollar sign ($), underscore (_), forward slash (/), or pound sign (#).

A user can obtain the system name using the STATUS SYSTEM command, as shown in this example:

```
OK, STATUS SYSTEM

System ACCTNG is currently running PRIMOS rev. 22.0
Copyright (c) Prime Computer, Inc. 1987
OK,
```

PRIMOS PROCESSES

The PRIMOS operating system is a time-shared operating system, which allows many users to use the system at once. To do this, PRIMOS manages **processes.** At Rev. 22.0, as many as 960 processes may use the system at one time. Each user of the system owns at least one process. Often, the term *user* is used synonymously with the term *process.* The exceptions are processes that do not represent specific users, such as **phantoms.**

The **phantom process** is not connected to a user terminal. It runs programs automatically, without user intervention. Its sequence of actions comes from a **command input (COMI) file** or from a **CPL file.** After creating this file, the user can start up a phantom to run the file. The phantom executes the commands in the file just as if the user had invoked the file at his or her terminal. Figure 3-8 illustrates two user processes, represented by User A and User B, and one phantom process, depicted as User C. When the phantom has executed all the commands in the file, it logs out. The phantom also logs out if it encounters an error requiring user intervention. See the *PRIMOS User's Guide* for more information on phantoms and command files. See the *CPL User's Guide* for information on CPL programs.

In this book, the term *user* refers to any user process, including either phantoms started by users or people actually logged in at user terminals. Sometimes, a distinction is made between the two user types by referring to *user phantoms* (or just *phantoms*) and *interactive users* (for users logged in at user terminals).

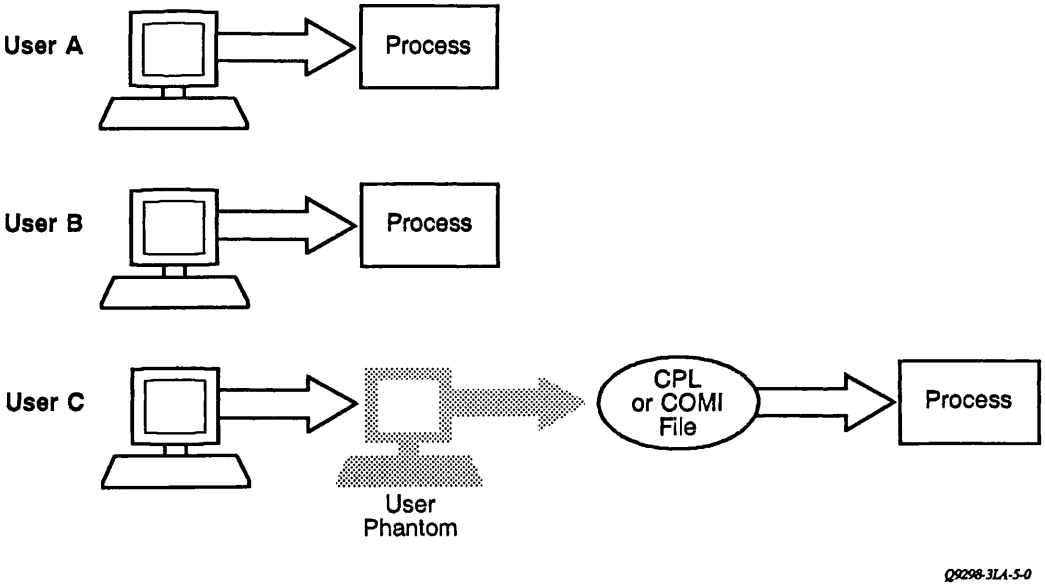


FIGURE 3-8. User and Phantom Processes

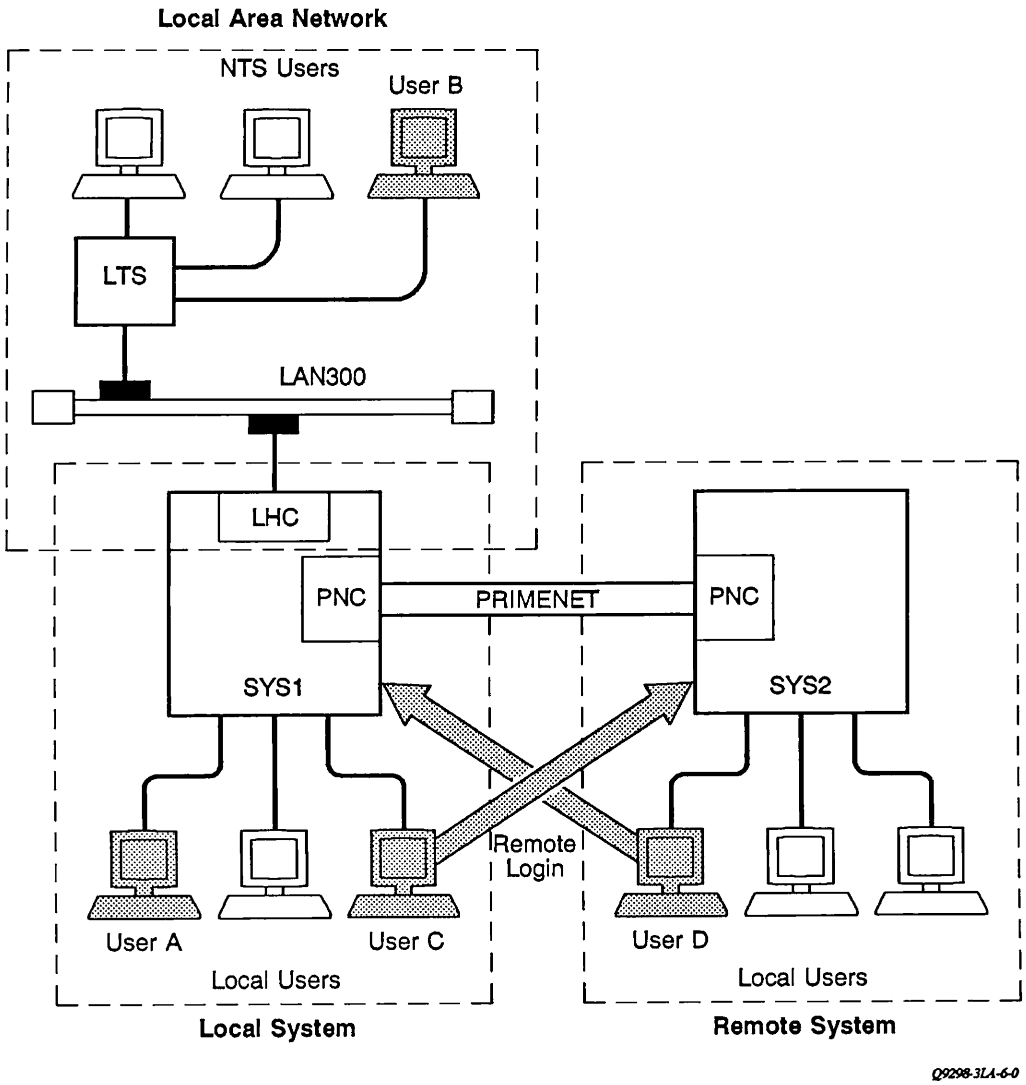


FIGURE 3-9. Four Kinds of Interactive Users

Interactive Users

A networked system can have four kinds of interactive users, as shown in Figure 3-9:

- User A is logged in at a terminal that is physically attached to the local system (SYS1) and is listed as a *local user* to SYS1.
- User B is an NTS user connected to the local system (SYS1) from a user terminal attached to a Network Terminal Server (NTS). When connected to any system on the LAN300 line, with the CONNECT command, the NTS user is considered to be a *local user* to that system.

- User C is physically attached to the local system (SYS1), but has logged in remotely to another system (SYS2) on the network. User C is listed as a *local user* to SYS1 and as a *remote user* to SYS2.
- User D is physically attached to another system on the network (SYS2), but has logged in remotely on the local system (SYS1). User D is listed as a *remote user* to SYS1 and a *local user* to SYS2.

Phantoms

Several types of phantoms run under PRIMOS. They are illustrated in Figure 3-10 and discussed in the sections below. To display the phantom processes running on your system, issue the STATUS USERS command, as shown in the example at the end of this section.

- User phantoms
- Server processes
- Phantoms started by subsystems
- Slaves

User Phantoms: The most common type of phantom is a **user phantom**, shown in Figure 3-10. It is started when an interactive user issues the PHANTOM command, followed by the name of a CPL or COMI file. The phantom runs the program in the CPL or COMI file, thus allowing the user to issue other commands or execute other programs while the phantom is running.

When a user phantom requires user input, a message is sent to the supervisor terminal as follows:

```
User nnn: Phantom requested terminal input.
```

Usually, you can ignore this message because the user who started the phantom receives a message indicating that the phantom terminated abnormally. The message is sent to the supervisor terminal to provide a record of the aborted phantom, even if the user who started the phantom logs out before the phantom aborts.

If you issue the STATUS USERS command while a user phantom is running a program, the user is listed as a phantom in addition to being listed as a user attached to a line. (See the example at the end of this section.)

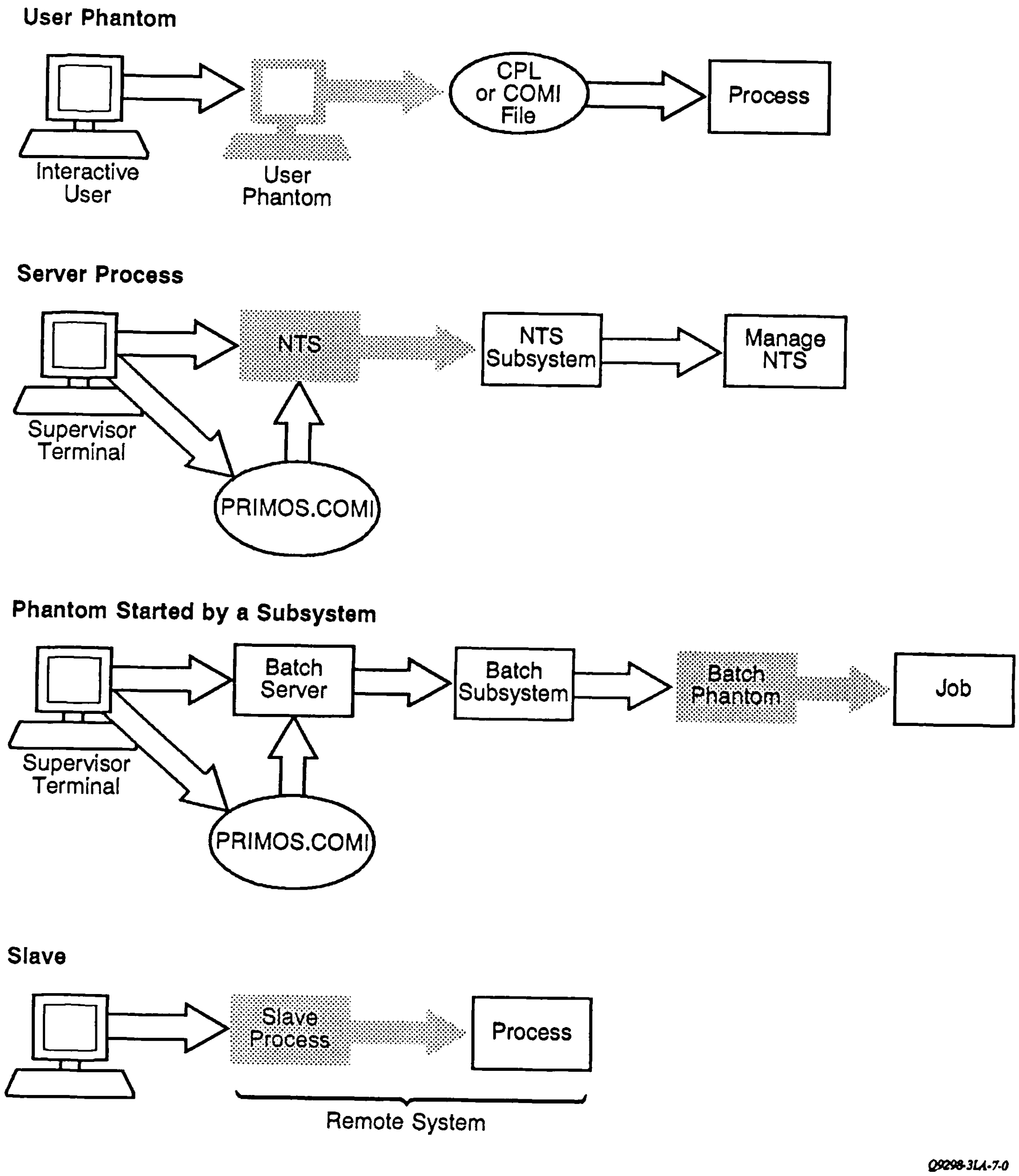


FIGURE 3-10. Types of Phantom Processes

Server Processes: Some subsystems, such as Batch, DSM, the Spooler, Network Terminal Service (NTs), and the File Transfer Service (FTS) require programs to run constantly. Usually these programs check for new items in a request queue.

A program that must be run at all times to service a subsystem is usually started as a phantom. These phantoms are called **server processes, subsystem phantoms**, or **servers.**

Server processes are started either by the system startup file when the system is booted or when you issue a command from the supervisor terminal. They are shown in Figure 3-10. Examples of server processes are

- **Network Terminal Server:** This server process facilitates remote attachment of user terminals to systems. The users at these terminals appear as local users. Network Terminal Service (NTS) provides connection management as well as PRIMOS asynchronous services. When NTS is configured on your system, the Network Terminal Server (NTS_SERVER) is displayed as a special phantom type, ncm. NTS is described in the *NTS User's Guide.*

- **Login Server:** This server process handles all terminal login attempts for local and remote users. The Login server is started when the system is booted; however, all libraries in ADMIN$.SR and LOGIN_SERVER.ENTRY$.SR must be on the command device in order for the Login server to start automatically. In addition, if you shut down the command device, for example, to run FIX_DISK, you must start the Login server when FIX_DISK finishes.

  To see if the Login server is running, use the STATUS USERS command or the LIST_PROCESS command. The Login server runs under the name LOGIN_SERVER and its process type is LSr. If, for some reason, the Login server either does not start or stops after it is started, enter the START_LSR command at the supervisor terminal.

- **Timer Process Server:** The **Timer Process server** coordinates the timing of processes running on the system. A Timer Process Server runs continuously as a phantom under the name TIMER_PROCESS, as shown by the STATUS USERS command (Figure 3-11). Its process type is **kernel** because it is part of the operating system. This phantom starts when the time is set either by the CPU's battery clock or by the SETIME command.

  The SET_TIME_INFO command allows you to specify the time zone that you are in and that is offset from Universal time (formerly Greenwich mean time). It also allows you to have your system time automatically adjusted for daylight saving time. See the *Operator's Guide to System Commands* for a discussion of the SET_TIME_INFO command.

- **Network Server:** On systems that support PRIMENET, the **Network server** or **network server process (nsp)** phantom services the network. The network server is always logged in, under the name NETMAN, and need not be monitored. The NETMAN process is shown in Figure 3-11 as User 113. The NETMAN process may be terminated by the STOP_NET command. (See the *Operator's Guide to Prime Networks.*)

Although servers are similar to user phantoms in many ways, you must often handle them differently. For instance, if a server process terminates abnormally, you must take action to get the process back in operation. In addition, you can request that a subsystem phantom log itself out at a convenient time, when it is not performing any task, so that you can make changes to the subsystem. When you shut the system down, you may warn users to stop their own phantoms, but you are responsible for the orderly shutdown of server processes.

Phantoms Started by Subsystems: Some subsystems, such as Batch and FTS, operate with two phantoms: one to service any requests to the subsystem, as discussed in the preceding paragraphs, and another to run the job once a request is received. Figure 3-10 shows how the Batch subsystem combines a server process with a user phantom. The difference between user phantoms and phantoms started by subsystems is that it is the subsystem, not an interactive user, that starts up the second phantom, although it runs under the user's name.

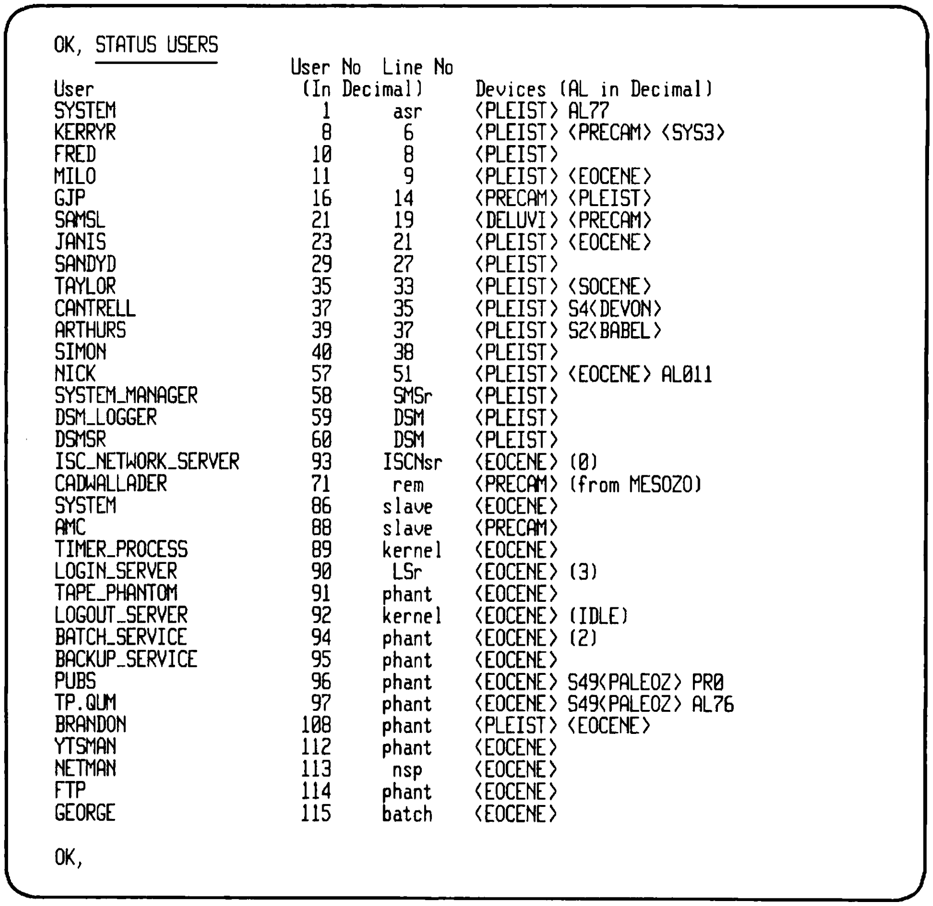
Slaves: Slaves are phantoms in that they are processes that perform operations on a system at the request of a user logged in to another node on the network. (See Figure 3-10.) Users 86 and 88 in Figure 3-11 are slave users. These processes are called slaves because they serve users on remote nodes.

A slave process represents a remote user using some resource on the local system. Usually, this resource is one of the disks that resides on the local system. For example, when a user on system A accesses a file on system B, a slave process is created on system B to perform the actual operations. This activity is usually transparent to the user on system A, but the slave process is visible to the operator and users on system B.

Slaves resemble user phantoms only in that they are not connected to terminals. Unlike user phantoms, they generate error messages at the supervisor terminal only if the error condition indicates something seriously wrong with the system.

Generally, you should be concerned with slave processes only when the system is about to be shut down. The presence of slave processes on the system at that time warns of users on other nodes who should be notified of the coming shutdown.

When you issue the STATUS USERS command, the phantoms discussed in the above paragraphs are displayed in a format similar to the following one.



```
OK, STATUS USERS
                            User No  Line No
User                        (In Decimal)     Devices (AL in Decimal)
SYSTEM                         1      asr    <PLEIST> AL77
KERRYR                         8       6     <PLEIST> <PRECAM> <SYS3>
FRED                          10       8     <PLEIST>
MILO                          11       9     <PLEIST> <EOCENE>
GJP                           16      14     <PRECAM> <PLEIST>
SAMSL                         21      19     <DELUVI> <PRECAM>
JANIS                         23      21     <PLEIST> <EOCENE>
SANDYD                        29      27     <PLEIST>
TAYLOR                        35      33     <PLEIST> <SOCENE>
CANTRELL                      37      35     <PLEIST> S4<DEVON>
ARTHURS                       39      37     <PLEIST> S2<BABEL>
SIMON                         40      38     <PLEIST>
NICK                          57      51     <PLEIST> <EOCENE> AL011
SYSTEM_MANAGER                58     SMSr    <PLEIST>
DSM_LOGGER                    59      DSM    <PLEIST>
DSMSR                         60      DSM    <PLEIST>
ISC_NETWORK_SERVER            93    ISCNsr   <EOCENE> (0)
CADWALLADER                   71      rem    <PRECAM> (from MESOZO)
SYSTEM                        86     slave   <EOCENE>
AMC                           88     slave   <PRECAM>
TIMER_PROCESS                 89    kernel   <EOCENE>
LOGIN_SERVER                  90      LSr    <EOCENE> (3)
TAPE_PHANTOM                  91     phant   <EOCENE>
LOGOUT_SERVER                 92    kernel   <EOCENE> (IDLE)
BATCH_SERVICE                 94     phant   <EOCENE> (2)
BACKUP_SERVICE                95     phant   <EOCENE>
PUBS                          96     phant   <EOCENE> S49<PALEOZ> PR0
TP.QUM                        97     phant   <EOCENE> S49<PALEOZ> AL76
BRANDON                      108     phant   <PLEIST> <EOCENE>
YTSMAN                       112     phant   <EOCENE>
NETMAN                       113      nsp    <EOCENE>
FTP                          114     phant   <EOCENE>
GEORGE                       115     batch   <EOCENE>

OK,
```

FIGURE 3-11. STATUS USERS Display

PRIMOS SECURITY

The PRIMOS operating system has security features that are necessary to meet the requirements of C2 certification specified by the U.S. Department of Defense's Trusted Computer System Evaluation Criteria. Chapter 5 of this book, The User Community, provides an overview of some of the new security features. The new Security Audit facility for recording security-related events is discussed in Chapter 7, Monitoring Your System. For complete details on all the security features available on PRIMOS, see the *System Administrator's Guide, Volume III: System Access and Security.*

4

THE FILE SYSTEM

A file system functions to organize data on disks and to provide the means to store that data and retrieve it when it is needed. This chapter introduces the elements and concepts of the PRIMOS file system, including

- Disk partitions
- Master File Directories
- Top-level directories
- Files

In addition, this chapter introduces and explains two categories of files and directories that you, as a system operator, have to monitor and use:

- System directories
- System files

If you are a new operator, you should read Chapters 1 and 2 of the *PRIMOS User's Guide*, which describe the PRIMOS file system from the user's point of view. You should also read Chapter 1 of the *Operator's Guide to File System Maintenance*, which provides a more complete explanation of files and directories from the operator's point of view.

Finally, this chapter discusses the operator's role in

- Online file system maintenance
- File system integrity

HOW THE PRIMOS FILE SYSTEM ORGANIZES DATA

Chapter 3 discussed the mechanism of bringing data into main memory from partitions. Recall that the data, in units called **records** of 2048 bytes each, is stored on disk partitions (see Figure 3-2) and is brought into memory in units called **pages.** These are the basic units by which data is moved into memory.

The user deals with this data in much larger units, called **files.** For example, a chapter in a book can be a file, as can a letter or memo. The file is the basic unit upon which most file systems are based.

Because there are many different kinds of data, used for different purposes, it is more efficient to access this information if it is organized into groups of similar types. For example, a university might want to organize its student database by class. Each student's file would be grouped with other students' files of the same class into another kind of object: a listing or catalog of all the files in the group. This listing serves as a **directory** to all the files contained in it. For more information on directories, see the section, Directories, below.

To further organize the files and directories in this example, you might group them together to form the student database. This database would probably be stored on a **partition** separate from that of the accounts payable database, for example.

Since the PRIMOS file system is central to the operation of your computer system, as a system operator you must ensure the integrity of the file system. This task includes periodic checks of certain system files and directories, as well as online and offline maintenance of partitions.

The following sections discuss the file system structure, beginning with the largest unit of organization, the partition, and continuing to the individual files.

PARTITIONS

Sometimes the terms **disk** and **partitions** are used interchangeably to refer to a sequence of surfaces (also called platters) that result from the subdivision of physical disks for the storage of specific data. In turn, the term disk is also used to refer to the disk (for example, the Winchester disk) that consists of a number of disk surfaces. For purposes of this discussion, the term **partition** or **disk partition** refers to the partitioned storage areas. **Disk** refers to the physical disk itself.

Think of the PRIMOS file system as an inverted tree, the base of which is the trunk (the partition), from which extend the branches (the directories), in which are listed other directories and files (twigs). The files are the ultimate target of most work with the file system. (See Figure 4-4.)

Most users identify disk partitions by partition names. For example, in the pathname <BEECH>BRANCH>TWIG, the name BEECH identifies a specific partition. Partition names are always preceded by a left angle-bracket. Each element of the parthname is separated by a right angle-bracket. Thus, BRANCH is the name of a directory, followed by the file, TWIG.

PRIMOS automatically determines which physical disk drive unit is being referenced by looking up the partition name in a list of partitions. For each partition, this list defines the actual physical disk on which the partition resides and the location of the partition on the physical disk. Figure 4-1 illustrates a partition (<BEECH>) that is made up of surfaces 2, 3, 4, and 5 on disk drive 0 and another partition (<POPLAR>) made up of surfaces 0 through 7 on disk drive 1.

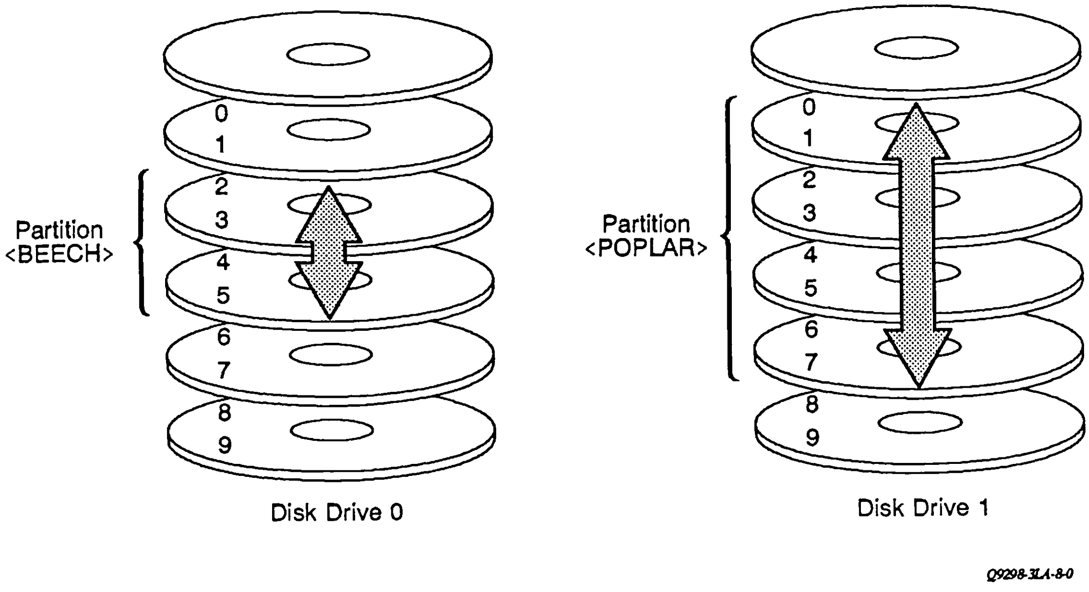


FIGURE 4-1. Disk Partition Locations

The creation and formatting of disk partitions is discussed in a later section, Creating Logical Partitions.

Identifying Partitions

Although most users identify disk partitions by their partition names, operators often perform functions when the relationship between a disk partition and its physical disk drive has not been defined. Such functions require the specification of a disk partition that is not defined to the system. In these cases, **physical device numbers** are used.

Each disk partition has a physical device number (pdev) that identifies the controller address, the drive unit on which it is mounted, the number of surfaces on the partition, and the beginning surface number on the physical disk. If there are any changes to the partition's location, its pdev must change. For example, if a partition has been associated with a particular disk drive, and the disk pack containing that partition is then placed in a different drive, or the original drive's designation is changed, the partition's address changes; therefore, its pdev must be changed.

The two partitions shown in Figure 4-1 have different pdev numbers, since they are on different disk drives (and perhaps different disk controllers), they start and end on different surfaces, and they have different numbers of surfaces.

Note

The construction of pdevs is explained in detail in the *Operator's Guide to File System Maintenance.*

Operator Commands That Affect Partitions

The physical device number of a partition is required in the following commands. Enter the pdev after the command; for example:

ADDISK *pdev*

Command	*Function*
ADDISK	Defines the relationship between a partition name and a physical partition to PRIMOS, so that users can access the partition.
ASSIGN DISK	Gives you exclusive access to a partition, so that special operator commands (such as MAKE, COPY_DISK, and PHYSAV) can be performed on that disk.
COPY_DISK	Physically copies the contents of a partition to another partition.
DISKS	Allows or disallows use of the ASSIGN DISK command for a partition. The partition is placed in the Assignable Disks Table, and from there it can be assigned.
DISKS NOT	Removes the partition from the Assignable Disks Table so that it may be added to the system for use by the user community.

FIX_DISK Determines the integrity of the file system structure of a partition; can also make repairs to the file system.

FIXRAT An obsolete version of FIX_DISK. Do not use this command on a Rev. 19.0 or later partition.

MAKE Performs the initialization, partitioning, and formatting on a physical partition so that the partition can be used. Initialization is the point at which the partition name is first assigned.

PHYRST Physically restores the contents of a physical partition from a tape created by PHYSAV.

PHYSAV Physically saves the contents of a physical partition onto magnetic tape.

SHUTDN Reverses the effect of an ADDISK command by removing a partition name from the list of partitions, and thereby prevents users from further access to the partition.

WARNING

Never use the ALL option with the SHUTDN command, unless you intend to shut down the entire system.

UNASSIGN DISK
Reverses the effect of an ASSIGN DISK command, releasing the operator's exclusive access to a partition. No other users can access the partition before or after an UNASSIGN DISKS command, until it is unassigned, removed from the Assignable Disks Table (DISKS NOT), and added to the file system (ADDISK).

Gaining Exclusive Access to Partitions

You must always assign partitions (with the ASSIGN DISK command) prior to such operations as MAKE, FIX_DISK, or COPY_DISK, unless you are running the operation as part of the system boot. You should unassign partitions (using the UNASSIGN DISK command) after you complete the operation.

Before you assign a partition, you must add its physical device number to the Assignable Disks Table, using the DISKS command. You can then assign the disk with the ASSIGN DISK command, which gives you exclusive access to the partition.

Figure 4-2 shows the order in which you must enter the specific commands when you want to shut down and start up a partition.

Shutting Down a Partition: Perform these steps in sequence to shut down a partition.

1. Use the SHUTDN command with the pdev of the partition. This ensures that no other user has access to the partition during the offline operation (step 1 in Figure 4-2).
2. Issue the DISKS command to place the partition on the Assignable Disks Table (step 2 in Figure 4-2).
3. Issue the ASSIGN DISK command to gain exclusive access to the partition (step 3 in Figure 4-2).

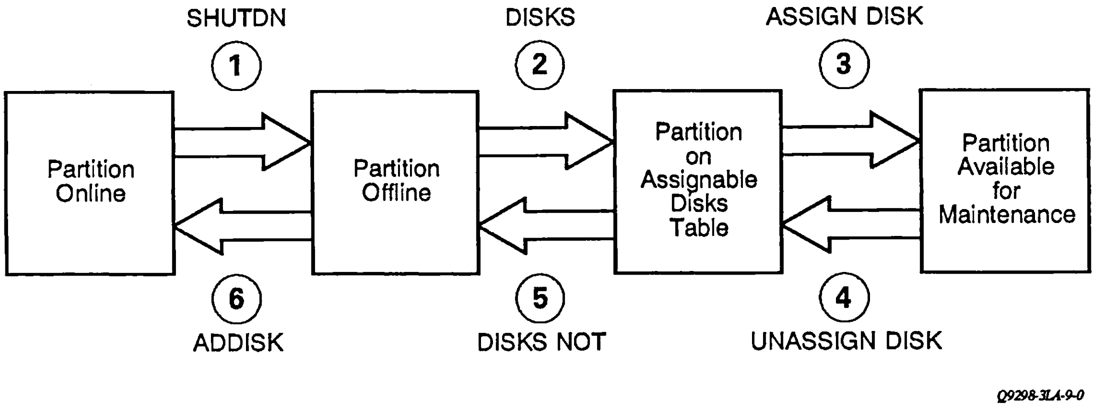


FIGURE 4-2. Steps to Shut Down and Start Up Partitions

Starting Up a Partition: Perform the following steps in sequence to start up a partition.

1. Issue the UNASSIGN DISK command to return the partition to the Assignable Disks Table (step 4 in Figure 4-2).
2. Issue the DISKS NOT command. This removes the partition from the Assignable Disks Table (step 5 in Figure 4-2).
3. Use the ADDISK command to start up the partition. This places the partition on line and makes it available to all users on the system (arrow 6 in Figure 4-2).

Note

The Assignable Disks Table has space for a maximum of 10 assignable partitions. If you attempt to add more than 10, the system responds with the error message

```
DISKS TABLE FULL
```

Partitions can be removed from the table by using the DISKS NOT command. It is more fully described in the *Operator's Guide to File System Maintenance.*

Creating Logical Partitions

Before a physical disk can be used on the system, a logical partition must be created from it and given a name by using the MAKE utility. Before you invoke MAKE, however, you must add the pdev of the logical partition you are creating to the Assignable Disks Table, by using the DISKS command. Then the logical partition can be assigned with the ASSIGN command and created with the MAKE utility. The procedure for creating a logical partition is discussed in detail in the *Operator's Guide to File System Maintenance.*

Keep in mind that after creating a partition with the MAKE command, you must then complete steps 4, 5, and 6, as shown in Figure 4-2 before PRIMOS can acknowledge the partition and it can be used by other users.

Adding Partitions to the System

Until you add a partition, the operating system does not acknowledge its existence and it cannot be accessed by other users. When you use the ADDISK command, you associate a partition name with its physical device number. This command defines the physical characteristics of a partition to PRIMOS. PRIMOS then reads information from the specified partition to determine its name, and adds the name and corresponding information to a list of partitions known to PRIMOS. (You can display this list with the STATUS DISKS command.) At this point, users can access the partition.

Rev. 21.0 and later systems can have a total of 238 added file system partitions (local and remote), plus a maximum of eight paging partitions. In addition, there can be a maximum of 10 assignable partitions in the Assignable Disks Table, giving a total of 256 possible partitions.

When a partition is to be shut down, you use the SHUTDN command to terminate file system activity on the partition and to delete the partition name from the list of known partitions. Notify users well in advance that the partition is to be shut down.

Robust Partitions

Robust partitions, available at Rev. 22.0, are PRIMOS file system partitions that are error resistant. They are designed primarily for systems that use large databases, but can be used in any installation.

Because of its error resistance, you do not have to run FIX_DISK on a robust partition after some system halts. In 25% of the cases, a robust partition will survive a halt without corruption of the file system; however, if you must run FIX_DISK on a robust partition, you can run it with the -FAST option. This reduces the time required to repair robust partitions. This procedure is generally much faster than running FIX_DISK on a standard partition.

Three commands have new options at Rev. 22.0 that you can use with robust partitions. They are listed in Table 4-1.

TABLE 4-1. Commands and Options for Use With Robust Partitions

Command	*Option*	*Purpose*
MAKE	-ROBUST	Builds a robust partition
MAKE	-MIN_EXTENT_SIZE	Sets a minimum extent size for a partition. The default is 64 blocks.
MAKE	-MAX_EXTENT_SIZE	Sets a maximum extent size for a partition. The default is 256 blocks.
FIX_DISK	-MIN_EXTENT_SIZE	Resets the minimum extent size during a partition repair. See the description above.
FIX_DISK	-MAX_EXTENT_SIZE	Resets the maximum extent size during a partition repair. See the description above.
ADDISK	-FORCE	Forces the addition of a robust partition even though the partition is no longer consistent. The added partition will be write-protected. Consequently, this option should be used only if immediate read access to the partition is required. FIX_DISK -FAST must be run on the partition before the disk can be added normally. This option should be used *only in extreme cases.*

Refer to the *Operator's Guide to File System Maintenance* for detailed information on the installation and repair of robust partitions.

Disk Mirroring

The purpose of **disk mirroring** is to increase system availability by making it possible to process with pairs of partitions. These partitions are identical; if one fails, the other is an exact duplicate and is available for use. The transition to the use of the duplicate is automatic.

Mirroring means that all records that are written to a partition, called the **primary partition** are also written to a **secondary partition**. You specify which is the primary and which is the secondary partition at the time you create the mirrored pair.

Reading of the records, however, is split between the two mirrored partitions. This reduces the average time it takes to read a record. Figure 4-3 illustrates a mirrored pair of partitions.

Mirrored partitions must be exactly alike in size and position on a disk. Robust partitions may be mirrored; however, once mirrored, both partitions will be robust.

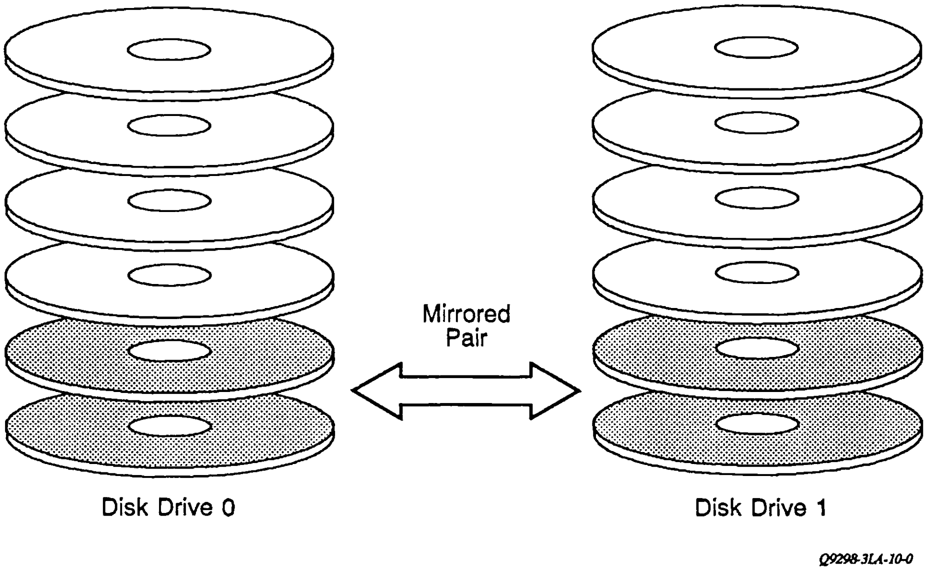


FIGURE 4-3. A Mirrored Pair of Partitions

The MIRROR_ON command allows you to start a mirror. This command can be issued only from the supervisor terminal. In addition, one of the mirroring configuration directives must be in the configuration file for this command to be valid.

The MIRROR_OFF command allows you to remove a partition from a mirrored pair. Either the primary or secondary partition may be shut down with this command, which must be issued from the supervisor terminal.

Refer to the *Operator's Guide to File System Maintenance* for more information on mirrored partitions.

Dual-ported Disks

A **dual-ported disk** is a disk drive that is physically connected to two systems. The function of a dual-ported disk is to allow the disk drive to be switched over to a secondary system if the primary system that is running the disk drive halts.

For example, a large database can be stored on a partition located on a dual-ported disk. If the primary system that is connected to the dual-ported disk stops running, the disk can be switched over to the secondary system. This enables the users to maintain access to the database even though the primary system is shut down.

Using the -PRIORITY_SELECT Option: Three commands at Rev. 22.0 have the new -PRIORITY_SELECT option that enables a system to take over control of a dual-ported disk. These are

- ADDISK
- ASSIGN DISK
- MIRROR_ON

The use of these commands and cautions on the use of the -PRIORITY_SELECT option are discussed in the *Operator's Guide to System Commands.*

WARNING

Do not switch a dual-ported disk unless you are sure that the other system is not running or does not have the disk added locally. If you do, you may corrupt the data on the disk. Dual-ported disks, like standard disks, can be added locally (with the ADDISK command) to only one system.

DIRECTORIES

Directories are a special type of file. A **directory** contains a list of subdirectories and files and information regarding each file.

There are three general categories of directories: the Master File Directory (MFD), the top-level directory, and the subdirectory, as shown in Figure 4-4.

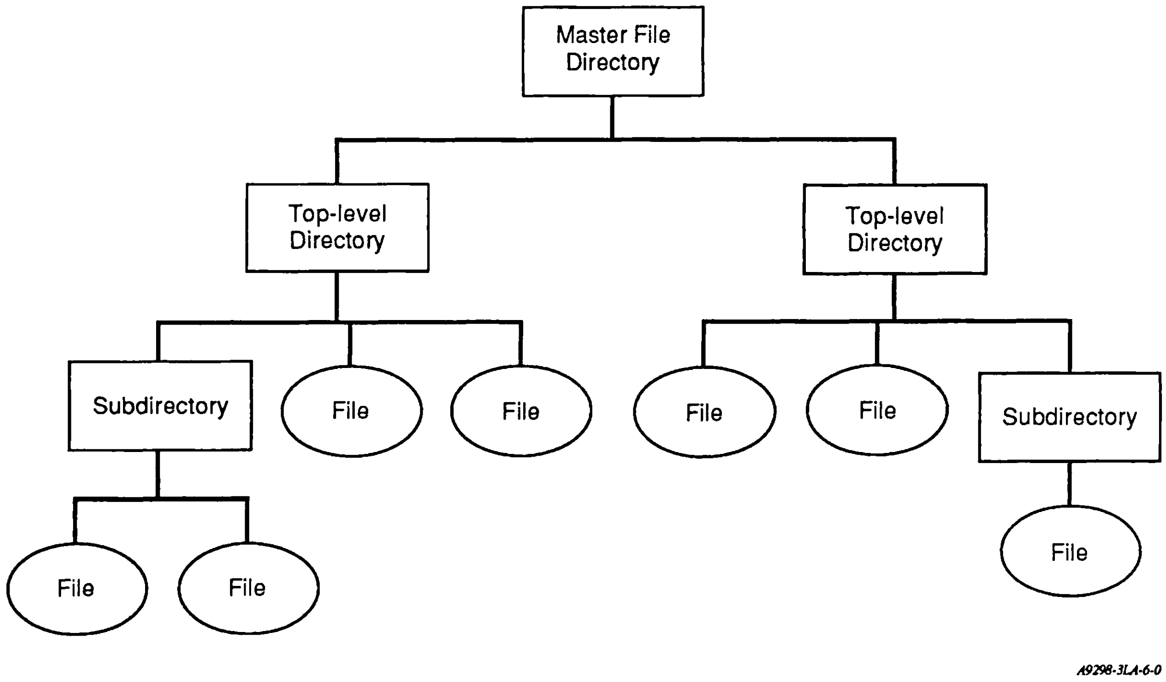


FIGURE 4-4. PRIMOS File System

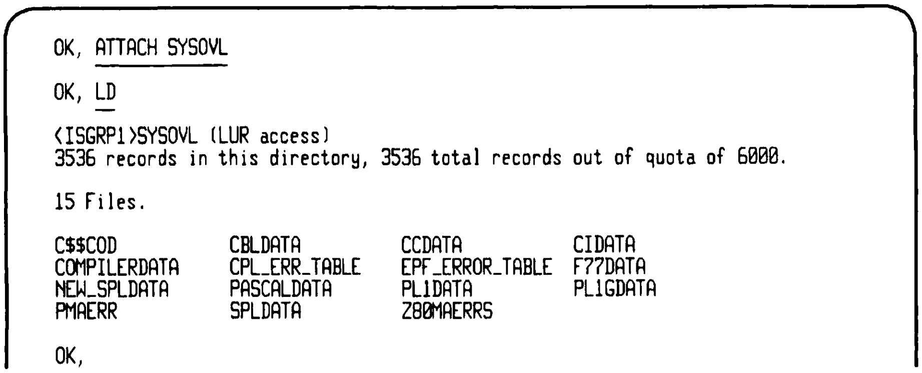
The Master File Directory (MFD): This is a special directory that contains the names of the top-level directories on a particular partition. There is one MFD for each partition. The name of the master file directory is MFD and is not to be confused with the name of the partition. The partition is named when you create it by using the MAKE command. In most installations, users do not have full access to the MFD level of the file structure. As an operator, however, you do most of your work at the MFD level.

The Top-level Directory: This directory is the major subdivision of the MFD, holding files, subdirectories, and information about the location and content of each file or subdirectory within it. In most cases, users are attached to a top-level directory when they log in. The directory to which a user is attached at login is referred to as the **origin directory** or **Initial Attach Point** (IAP).

The Subdirectory: These are subdivisions either of top-level directories or of other subdirectories. Users can create separate subdirectories for each user, department, project, or software product within a directory.

Example of Monitoring Directories

To check the contents of a directory, use the LD command with the pathname of the directory or attach to the directory with the ATTACH command and then use the LD command, as in the following example.



```
OK, ATTACH SYSOVL

OK, LD

<ISGRP1>SYSOVL (LUR access)
3536 records in this directory, 3536 total records out of quota of 6000.

15 Files.

C$$COD          CBLDATA         CCDATA          CIDATA
COMPILERDATA    CPL_ERR_TABLE   EPF_ERROR_TABLE F77DATA
NEW_SPLDATA     PASCALDATA      PL1DATA         PL1GDATA
PMAERR          SPLDATA         Z80MAERRS

OK,
```

To obtain a listing of a directory sorted in reverse chronological order, so that you can see which files and directories have been modified most recently, use the -SORT_DTM option on the LD command line. For more information on the LD command, see the *PRIMOS Commands Reference Guide.*

Files in the Master File Directory

Each Master File Directory holds a listing of a number of key system files and top-level directories. (Refer to Figure 4-5.) The key system files are described next.

The BOOT File: This file contains the bootstrapping procedure for booting PRIMOS from disk. It is used with every new boot, or startup, of PRIMOS.

The BOOT_RUN_FILE_TREENAME File: This file contains the pathname of the file used most recently for booting PRIMOS from disk. It does not exist, however, unless you have booted PRIMOS from this partition.

The BADSPT File: This file contains a list of all records that contain physical defects, or **badspots** such as scratches or areas with little or no coating. This file exists only on partitions that have known badspots, and only on Rev. 21.0 or later partitions, created in Nondynamic Badspot Handling (-AC) mode. Whenever data is written on a disk, the BADSPT file is searched in order to be sure that no information is copied onto unusable records.

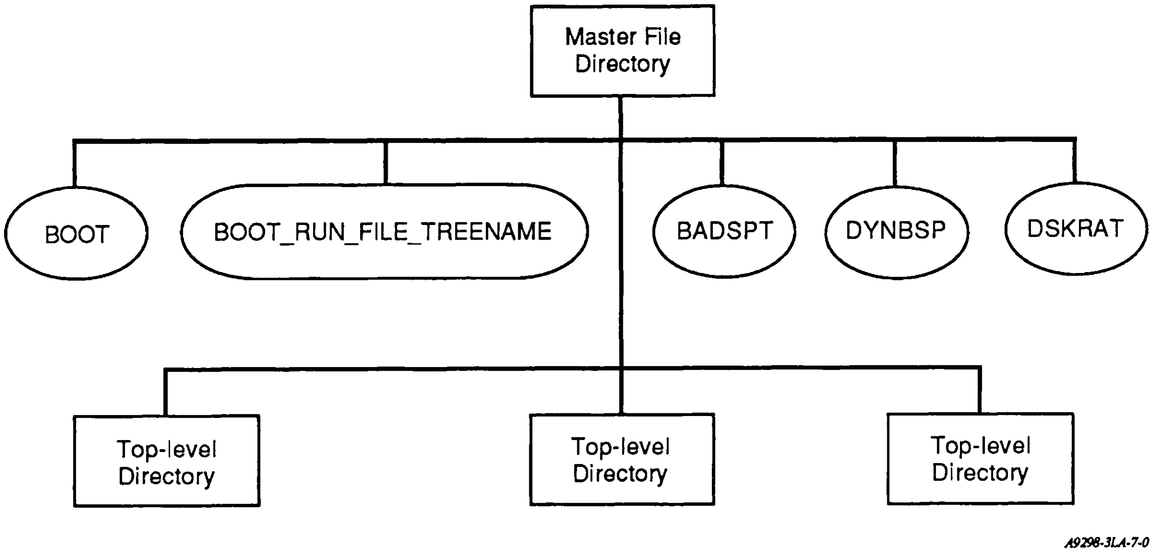


FIGURE 4-5. Key System Files in the Master File Directory

The DYNBSP File: This file, contained on Rev. 21.0 and later disks, is used to control access to two new files: the dynamic badspot (DBS) file and the remapped area (RMA) file. These three files are located on the **first partition** of a physical disk (the partition that contains the first surface – surface 0 – of the physical disk). The DBS and RMA files are not visible and are not in a listing of the MFD produced by an LD command. The DYNBSP file provides access checking of the DBS file by a specific ACL and provides a lock to control writing to the DBS file.

The DSKRAT File: This file is the Disk Record Availability Table, a list of available records on the partition. This table is dynamic; that is, it changes constantly as the partition's records are used or freed. A new DSKRAT file is automatically created every time a partition is created. It is used by FIX__DISK, the disk repair utility in PRIMOS, and by the PRIMOS file system. The DSKRAT takes as its filename the name of the partition on which it resides.

Some directories, and their associated subdirectories and files, are delivered on a master disk pack, master disk cartridge, or master magnetic tape; they are loaded as part of your Prime software. These are referred to as system directories and are discussed in a later section. Other system directories are created by the operator or the System Administrator for use by the system or by system users.

Important System Directories

Certain top-level directories are of particular interest to the operator. Referred to as **system directories**, they are the directories required to run PRIMOS, the utilities, and other software. Most of the system directories are located on the command device, as shown in Figure 4-6. These directories are described below.

The Directory DEVICE*: This directory contains a subdirectory that corresponds to each specific peripheral device (for example a tape drive or a printer) on the system that has device ACLs placed on it. Device ACLs are discussed in Chapter 6, System Resources.

The Directory SAD: This System Administrator Directory (SAD) contains all user profile and project information. You can boot a system without a SAD but users could not log in. You use EDIT_PROFILE to create the SAD, as described in the *System Administrator's Guide, Volume III: System Access and Security*. This directory is created when you first invoke EDIT_PROFILE.

The Directory LIBRARIES*: This directory contains all system library EPFs.

The Directory PRIRUN: This directory contains the PRIMOS runfiles (the files that are used to start up PRIMOS).

The Directory SEARCH_RULES*: Default **search rules** give each user process a sequence of locations to search for file system objects. For example, a directory name would be a search rule when the object of the search is a command runfile. Each process at initialization reads the presently active set of search rules lists.

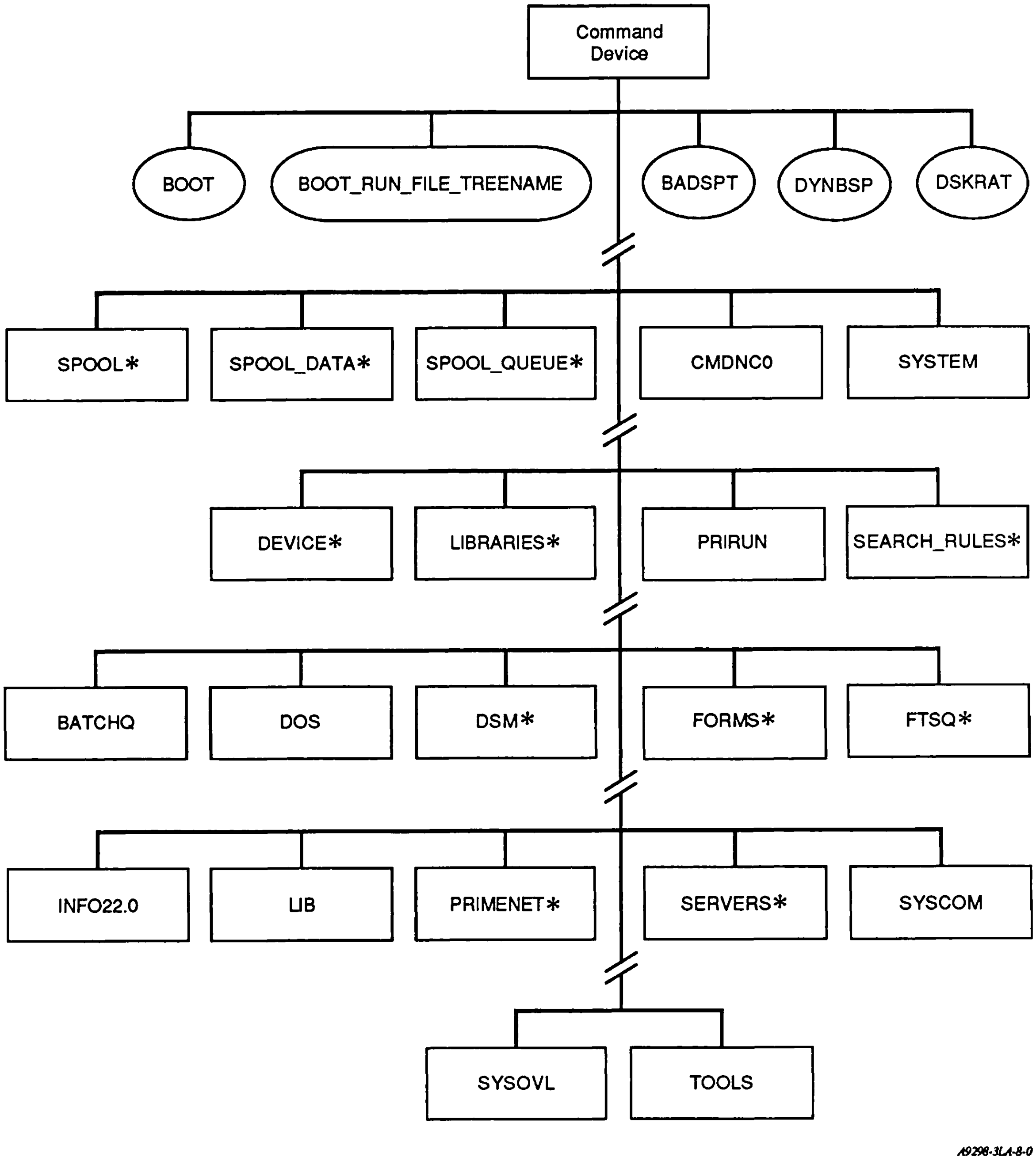


FIGURE 4-6. System Directories Located on the Command Device

The directory SEARCH__RULES*, which is created automatically by the installation program SYSTEM>INSTALL.STD.COMI, includes the Administrator search rules list, ADMIN$.ENTRY$.SR, and the following system default search rules files:

- ATTACH$.SR
- BINARY$.SR
- COMMAND$.SR
- ENTRY$.SR
- INCLUDE$.SR

The Directory SPOOL*: This directory contains Spooler subsystem files and subdirectories, including runfiles for the despooler phantoms and the files that control the environments of printer operations. The latter files specify the Spooler operating environments, list users controlling the Spooler, and list such things as forms used on a printer and the destination of spooled files.

The Directory SPOOL_QUEUE*: This directory contains the list of print requests awaiting printing. It may also hold two optional files: one to control who can see the entire spool queue with the SPOOL -LIST command, and the other to contain a list of names of local partitions where SPOOL__DATA* directories exist.

The Directory SPOOL_DATA*: This directory contains the copies of the files that are to be printed.

The Directory SYSTEM: This directory contains files for use by shared subsystem software, such as FORMS, and by compilers for high-level languages such as CBL and Pascal. The DISCS file, described later in this chapter, is also in this directory.

The Directory CMDNC0: This directory contains external PRIMOS commands, that is, commands that are not embedded in the operating system; examples of external commands are ED and FIX__DISK. Frequently, this directory contains special commands that have been custom-designed for your particular system. When you issue the LD command in the CMDNC0 directory, the files for the external commands appear in a format similar to the list below.

```
OK, LD

$$.RUN         AVAIL.SAVE     BATCH.RUN        BATGEN.RUN
CMPF.SAVE      CONCAT.SAVE    COPY.RUN         COPY_DISK.SAVE
CPMPC.SAVE     CRMPC.SAVE     DELETE.RUN       ED.SAVE
EDB.SAVE       EDIT_PROFILE.SAVE               FIX_DISK.SAVE
FILMEM.RUN     FILVER.SAVE    LD.RUN           JOB.RUN
FUTIL          HELP.RUN       MAGSAV.SAVE      LOAD.SAVE
LABEL.RUN      LATE.SAVE      PHYRST.SAVE      MAKE.SAVE
MAGNET.RUN     MAGRST.SAVE    PRMPC.SAVE       PHYSAV.SAVE
MRGF.SAVE      NSED           PSD.SAVE         PROP.RUN
PMA.SAVE       PRSER.SAVE     SET_DELETE.RUN   RUNOFF.RUN
PROTECT.RUN    PRVER.SAVE     SPOOL.RUN        SIZE.RUN
PSD20.SAVE     REVERT_PASSWORD.RUN             TERM.SAVE
RWLOCK.RUN     SEG.SAVE       SLIST.SAVE       SORT.RUN
TRAMLC.SAVE    UPCASE.SAVE    VPSD.SAVE        VPSD16.SAVE
```

CMDNC0 should be included in the COMMAND$ search list. Any commands that are not in CMDNC0 (such as ATTACH, RDY, and LOGOUT) are internal commands, that is, part of PRIMOS. PRIMOS uses a list of internal commands which it searches before going to the COMMAND$ search rules.

CMDNC0 also contains the system startup file, PRIMOS.COMI (or C_PRMO), and the system configuration file, usually named CONFIG.

Other Directories

Other directories, such as those listed below, are under the control of the operator.

Directory *Description*

BATCHQ Contains the files that are used whenever Batch jobs are run. They include the Batch monitor runfile, Batch queue definition files, and job submittal files.

DOS Contains the obsolete single-user operation system, PRIMOS II, in the file DOS.SAVE.

DSM* Contains Distributed Systems Management (DSM) files for DSM and the applications server, message text database, directories for applications software, databases for DSM and UMH (Unsolicited Message Handler) configuration, logs and journals, and the data files for the screen-based interface to System Information and Metering (SIM).

FORMS* Contains files needed to run the Forms Management System (FORMS). Must be installed to use FORMS. See the *FORMS Programmer's Guide.*

FTSQ* Contains File Transfer Service (FTS) runfiles, the configuration database, queues of transfer requests, and copies of users' files for transfer.

INFO22.0 Contains the files that summarize the major changes in the current revision of PRIMOS (Rev. 22.0).

LIB Contains all static-mode binary libraries available on the system. Should be on logical disk 0.

PRIMENET* Contains all files needed to run PRIMENET.

SERVERS* Contains the runfiles for the system servers such as the Login server, and for the Auditor if your system is using C2. This directory must be present.

SIT* Contains the system internationalization tools for DSM.

SYSCOM Contains parameter insert files for compilers.

SYSOVL Contains files required by CBL and the data files used by the FORTRAN 77, Pascal, PL/I, PL/I-G, and RPG compiler default driver programs.

T&MRUN Contains test and maintenance programs used by Customer Support representatives.

TOOLS Contains files and programs that can perform such tasks as converting your system to the current revision of PRIMOS. It also contains the driver programs for the PL/I-G, Pascal, and FORTRAN 77 compilers.

Operator Responsibility for Directories

Only you or the System Administrator should make additions to the above directories. Periodically (about once each month), you should check these directories to see that they are in order. To display the contents of the directories, use the LD command, as shown in the following section. Write the contents into a file by invoking the COMOUTPUT command before the LD command. You should compare the current contents of the system directory to the proper contents, a copy of which should be maintained in the system logbook.

ONLINE FILE SYSTEM MAINTENANCE

Monitoring the file system while the system is up and running is called **online maintenance**. Monitoring includes such things as checking the integrity of system directories, responding to user questions, and so on.

System directories that are important to the operator are discussed earlier in this chapter. You should check the directories to make certain that their contents are as you expected.

Sometimes, users receive error messages that are produced by the file system when they attempt to access files. Most of these error messages indicate user error; however, some of them indicate that the integrity of the file system is compromised. When this happens, you must attempt to restore that integrity.

You must monitor these areas of the file system:

- Access Control Lists (ACLs)
- Device access control lists
- Disk quotas
- Disk space utilization

The following messages indicate problems with these aspects of the file system:

`No information`	(ACLs)
`Insufficient access rights`	(ACLs)

Maximum quota exceeded	(Disk quotas)
The disk is full	(Disk space utilization)

ACLs and device ACLs are discussed in Chapter 5, The User Community and in Chapter 6, System Resources. Refer also to the *System Administrator's Guide, Volume III: System Access and Security.*

The following messages indicate problems with the physical integrity of the disk partition involved. Except where indicated, these messages may appear at user terminals as well as at the supervisor terminal.

- Pointer mismatch found (*not* the same as POINTER_FAULT$)
- The directory is damaged
- Directory too large
- Bad DAM file
- Bad truncate of segment directory
- Quota system may be incorrect; please run FIX_DISK (This message from the ADDISK command appears at the supervisor terminal only.)
- Segment directory error
- The file is too long
- Too many subdirectory levels
- Disk format does not support this revision of PRIMOS (This message from the ADDISK command appears at the supervisor terminal only.)

If any of these messages appear, you should perform offline maintenance of the disk or partition on which the error occurred, when it is convenient. This procedure is discussed below in the section, Maintaining File System Integrity.

Disk Quotas

To ensure equitable sharing of disk storage, System Administrators can set limits (called **quotas**) on the amount of storage space that a user's top-level directory can occupy on a partition. The SET_QUOTA command, which is used for this purpose, is discussed in detail in the *System Administrator's Guide, Volume I: System Configuration.*

In most cases, the system operator has the responsibility for monitoring and measuring the existing quotas and current storage use. The following commands allow you to examine the quota on a directory and the current storage space used by directories, files, and segment directories.

- LIST_QUOTA
- LD
- SIZE

The ways in which you use these commands to display quota and storage space information are discussed in the following sections.

Measuring Storage Space: Storage space is measured in disk records. A record contains 2048 bytes of user data. Thus, the number of records in a file system object equals the total number of bytes in the object, divided by 2048, and rounded up to the next whole number. A zero-length object (such as an empty directory or file) always contains one record.

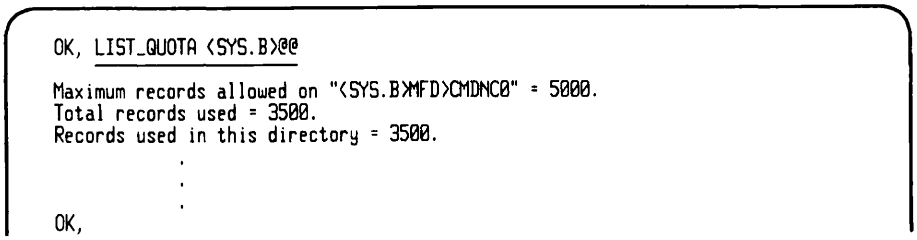
Using LIST_QUOTA: The LIST_QUOTA command provides the following information:

- The maximum quota on a directory
- The total number of records used by the entire subtree, beginning with and including the designated directory
- The number of records used by this particular directory

The format of the command is

LIST_QUOTA [*pathname*] [-BRIEF]
LQ

pathname gives the name of the directory on which quota information is requested. If *pathname* is omitted, the quota information on the current directory is listed. The -BRIEF option (abbreviated -BR) displays a one-line summary of the directory's quota status. For example, to list the quota information on all top-level directories on partition SYS.B, type the following:



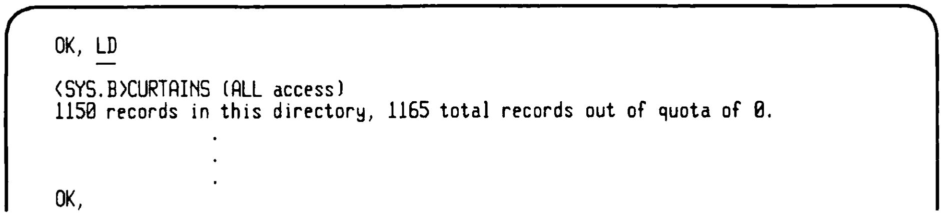
```
OK, LIST_QUOTA <SYS.B>@@

Maximum records allowed on "<SYS.B>MFD>CMDNC0" = 5000.
Total records used = 3500.
Records used in this directory = 3500.
              .
              .
              .
OK,
```

The -BRIEF option outputs a one-line summary of a directory's quota status, as shown here:

```
OK, LIST_QUOTA USER -BRIEF
Max:       200, Used:       178, Records:       65, USER
OK,
```

In this example, the maximum number of records allowed is 200, the total number of records used for this directory and its subtree is 178, and the number of records used by this directory alone is 65. If you omit the pathname from the command line, the pathname is omitted from the one-line summary.

Obtaining Quota and Storage Information With LD: The LD command provides quota and storage information on the second line of its display, as shown in this example:



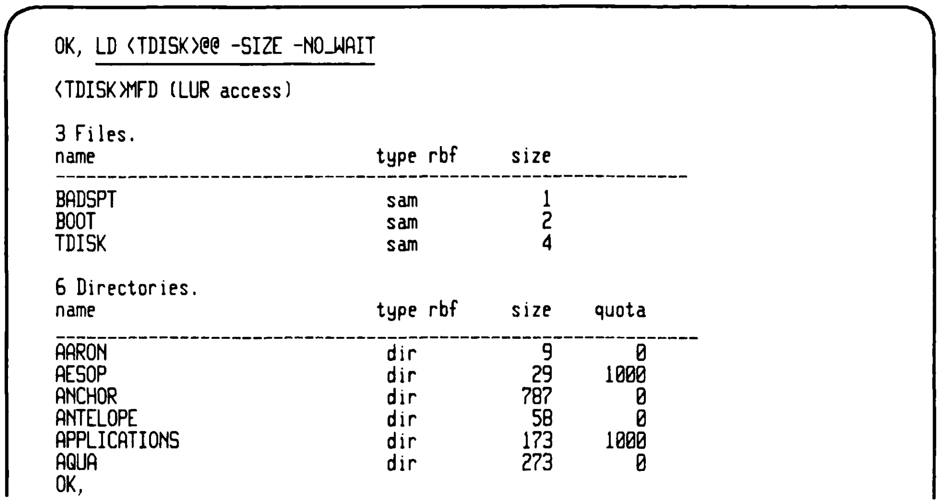
```
OK, LD

<SYS.B>CURTAINS (ALL access)
1150 records in this directory, 1165 total records out of quota of 0.
                    .
                    .
                    .
OK,
```

The number of records used by this directory, the total number of records used by the directory and its entire subtree, and the maximum number of records permitted for use by the directory and its subtree are indicated. If the third number is 0, there is no maximum limit other than the limit of the disk; that is, it is not a quota directory.

Use the -SIZE option with the LD command if you want to know how many records are in a file or a segment directory within a directory:

LD [*pathname*] -SIZE

You may use wildcards to get size information for an entire directory. A wildcard name is a pathname or objectname that contains one or two @ characters. In the following example, the @@ characters are wildcards calling for the display of information for *all* files and directories listed in the TDISK partition. See the *PRIMOS Commands Reference Guide* for complete information on using wildcards. The following example shows how to display information for all files and directories in a partition.



```
OK, LD <TDISK>@@ -SIZE -NO_WAIT

<TDISK>MFD (LUR access)

3 Files.
name                           type rbf     size
-------------------------------------------------------
BADSPT                          sam           1
BOOT                            sam           2
TDISK                           sam           4

6 Directories.
name                           type rbf     size    quota
---------------------------------------------------------
AARON                           dir           9        0
AESOP                           dir          29     1000
ANCHOR                          dir         787        0
ANTELOPE                        dir          58        0
APPLICATIONS                    dir         173     1000
AQUA                            dir         273        0
OK,
```

In this example, the file BADSPT contains one record, BOOT contains two records, and TDISK (the DSKRAT) contains four records. The AESOP and APPLICATIONS directories, with quotas of 1000 records each, contain 29 and 173 records. The nonquota directory, ANCHOR, contains 787 records. File system objects are displayed alphabetically.

By using a specific pathname or a wildcard pathname, you can request information on the size of either a single object or a specific group of objects.

You can obtain even greater detail with the LD -DETAIL command. Use this format:

LD [*pathname*] -DETAIL

Using SIZE: The SIZE command, like the LD -SIZE command, reports the number of records in an existing file, using a different display. You should be logged in with Read (R) access rights to the object whose size you wish to know. The command format is

SIZE *pathname* [-NORM]

pathname is the name of the object whose size you wish to know. It can be a wildcard name. -NORM presents records in normalized format (1 record = 880 bytes). SIZE can report on other file system objects as well. However, for directories, segment directories, and access categories, SIZE returns the number of entries in the object. Hence, the report returned by SIZE depends upon the type of object specified by *pathname*, as follows:

Object	*Report*
File	The size of the file in 2048-byte records (880-byte records if -NORM is specified). The number of words in the file (1 word contains 2 bytes) and the file type (SAM file or DAM file) are also displayed.
Directory	The number of top-level entries in the directory, the directory type password (pwd) directory or ACL directory and the size of the directory listing in words.
Segment Directory	The number of entries in the segment directory and the directory type (SAM SEGDIR or DAM SEGDIR). The maximum number of entries the segment directory can hold is also reported (*n* total). Multiplying this number by 2 yields the size of the segment directory in words. (For example, 65 total equals a size of 130 words.)
Access Category	The number of access pairs (identifier: rights) in the access category.

In all cases, SIZE displays the current pathname, so that you know which object SIZE is looking at when you use wildcards. For example, to obtain the size of all objects on the partition SYS.A, type

```
OK, SIZE <SYS.A>@@

   9 records in sam file    "<SYS.A>MFD>SYS.A" (8804 halfwords)
 153 entries in acl UFD     "<SYS.A>MFD>MFD" (4852 halfwords)
   2 records in sam file    "<SYS.A>MFD>BOOT" (1092 halfwords)
   8 entries in acl UFD     "<SYS.A>MFD>USR.1" (153 halfwords)
           .
           .
           .
OK,
```

What To Do if the Full Disk Condition Is Encountered: The System Administrator can assign directory quotas whose sum exceeds the capacity of the disk. This capability assumes that not all users will use their full storage allotment at the same time. In effect, users share part of their space. This technique provides efficient use of disk space, but it also makes it possible for users to completely fill the disk, even though none of them have reached their individual quotas.

If the disk is full when users attempt to store an object, users get the message `The disk is full.` If such a situation is reported, do the following:

1. Use the MESSAGE command to ask users to delete unnecessary files from their directories.
2. Report the situation to the System Administrator.

Monitoring Disk Space Utilization

The AVAIL command displays, for a specified partition, the total number of records that can be stored on the partition, the number of records not used and thus available, and the percentage of records used. Information is given as physical records (1 record = 2048 bytes).

The correct format for checking disk space utilization is

AVAIL [*disk*] [-NORM]

You can specify the *disk* argument in any one of the following ways:

Argument	*Definition*
partition	The name of any disk, or partition, on your system's network
*****	All started, or added, partitions that are listed in the file SYSTEM>DISCS
-LDEV ***nn***	The logical device number of any disk on your network, where *nn* is represented by a decimal number, such as 2, 53, or 146

If you enter the AVAIL command without arguments, information is displayed for the partition to which you are currently attached. For example:

```
OK, AVAIL

 Volume OLIO
  44442 total records
    1070 records available
  97.6% full
OK,
```

For compatibility with pre-Rev. 19.0 systems, this information is also available in normalized format (1 record = 880 bytes). You can use the -NORM option if you want records given in normalized format as shown in this example.

```
OK, AVAIL -NORM
 Volume OLIO
 103428 total records (normalized)
   2490 records available (normalized)
  97.6% full
OK,
```

If you use the command AVAIL *, PRIMOS reads the file SYSTEM>DISCS and displays a table of record utilization for all partitions listed there as shown in this example:

```
OK, AVAIL *

Volume   Total    Free   %   Comments
  ID     recs     recs   Full
---------------------------------------------
SYSACA  140733    1984  98.6   0    4463 Command device
ACCTNG   14814    3894  73.7   1     460 Accounting
ORIGIN   44442    1069  97.6   3   31460 Origin directories
OK,
```

The text listed under the `Comments` column is other information placed in the SYSTEM>DISCS file by the System Administrator. In this example, the comments give each partition's logical device number, physical device number, and an indication of its use.

If you request normalized format, the table appears as follows:

```
OK, AVAIL * -NORM

Volume    Total    Free   %      Comments
  ID      recs     recs   Full   normalized
---------------------------------------------
SYSACA   327524    4351  98.6    0    4463 Command device
ACCTNG    34476    9062  73.7    1     460 Accounting
ORIGIN   103426    2487  97.6    3   31460 Origin directories
OK,
```

Note

For non-ACL partitions, AVAIL requires that either the owner or the nonowner MFD password be XXXXXX, and that the DSKRAT (partition name) protection be set so that a user has Read access when attached to the MFD. In most cases, it is the nonowner password is set in this fashion.

For an ACL partition, user rights must be set to U on the MFD and to R on the DSKRAT file.

The DISCS File: AVAIL * does not work unless the file DISCS is built in the directory SYSTEM. The DISCS file is a list of partition names, in column form, that is created with an editor. In addition to the column listing partition names, any information can be included in separate columns, such as the following:

- The partition's logical device number (ldev)
- The partition's physical device number (pdev)
- Miscellaneous information, such as the purpose of each partition

The AVAIL command takes this information from the DISCS file and adds information on record utilization (determined from the system) to create its display. The DISCS file should be kept up-to-date relative to the way the partitions are started, or added. If it is not, the AVAIL * command gives inconsistent information.

Here is an example of a DISCS file:

```
OK, SLIST SYSTEM>DISCS

SYSACA   0   4463 Command device
ACCTNG   1    460 Accounting
ORIGIN   3  31460 Origin directories
OK,
```

If your system has DSM configured, you can use the SIM command LIST_DISKS to obtain the disk space utilization information as in this example:

```
OK, LIST_DISKS -AVAIL

[LIST_DISKS Rev. 21.0 Copyright (c) Prime Computer, Inc. 1986]

Executing at 14 July 90 16:52:56 Monday

** ENPUB2 **

Partition information for node: ENPUB2

   Ldev    Device   System     Pdev     Size in   No. free    %
  number    name     name     number    records   records    full
+------------------------------------------------------------------+
|     '0 | TPSYS  |        |    '2062 |   59256 |     1433 | 97.50 |
|     '1 | TPUSER |        |   '42062 |   59256 |    43820 | 26.00 |
|     '2 | PAGDEV |        |  '100463 |      16 |        9 | 43.70 |
+------------------------------------------------------------------+
OK,
```

See Chapter 7, Monitoring Your System, and the *DSM User's Guide* for further discussion of SIM commands.

MAINTAINING FILE SYSTEM INTEGRITY

FIX_DISK is a file system maintenance program that you use for any of the following purposes:

- To check that file system integrity is being maintained
- To compress the directory when there are unused records
- To find inconsistencies on a partition
- To repair inconsistencies that are found on a partition

Checking File System Integrity

You should check your file system integrity with FIX_DISK as often as is reasonable. The FIX_DISK command is documented in the *Operator's Guide to File System Maintenance.* If FIX_DISK finds any inconsistencies on the partition, it reports them. If it is necessary to run FIX_DISK on a partition, you are told this when you use the ADDISK command for the partition, as in this example:

```
OK, ADDISK 1060

Starting up revision 22 partition "IONIA".
(Quota system may be incorrect; please run FIX_DISK.)
OK,
```

For robust partitions that have been shut down improperly, the ADDISK message is similar to this example:

```
OK, ADDISK 4463

*** Robust Partition 4463 has not been properly shutdown.
*** Fast Fix_Disk has to be run before it can be added.
```

In this case, run FIX_DISK with the -FAST and -FIX options to repair the robust partition.

Because ADDISK commands are frequently included in the system startup command file PRIMOS.COMI (or C_PRMO), check the output generated during system cold start to see whether the parenthetical message was displayed after the message indicating that the partition was started.

In addition, you may get a message indicating that you should run FIX_DISK on a partition when you use COPY_DISK to restore the partition during a backup procedure. You also use FIX_DISK on target partitions as part of backup procedures. See the *Data Backup and Recovery Guide.*

Repairing File System Inconsistencies

If you specify the -FIX option on the FIX_DISK command line, FIX_DISK attempts to repair any inconsistencies. It is good practice to run FIX_DISK on the partition the first time without the -FIX option.

Two options are available at Rev. 22.0 for use with robust partitions: -MIN_EXTENT_SIZE and -MAX_EXTENT_SIZE, which allow you to reset the minimum and maximum extent size for CAM files on a partition. See the *Operator's Guide to File System Maintenance.*

FIX_DISK can also perform other useful functions, such as reducing the number of records in use by a directory by compressing the directory when it contains unused records.

5

THE USER COMMUNITY

Many of your tasks as an operator involve dealing with members of your system's interactive user community. As a computer operator, you meet the users in person, receive phone calls from them, or send and receive messages via the system software. You must understand the needs of users on your system, and be able to communicate effectively with them.

This chapter

- Defines interactive users, groups, projects, and user profiles
- Describes elements of PRIMOS security
- Explains how to respond to user requests
- Explains how to monitor interactive user status

INTERACTIVE USERS

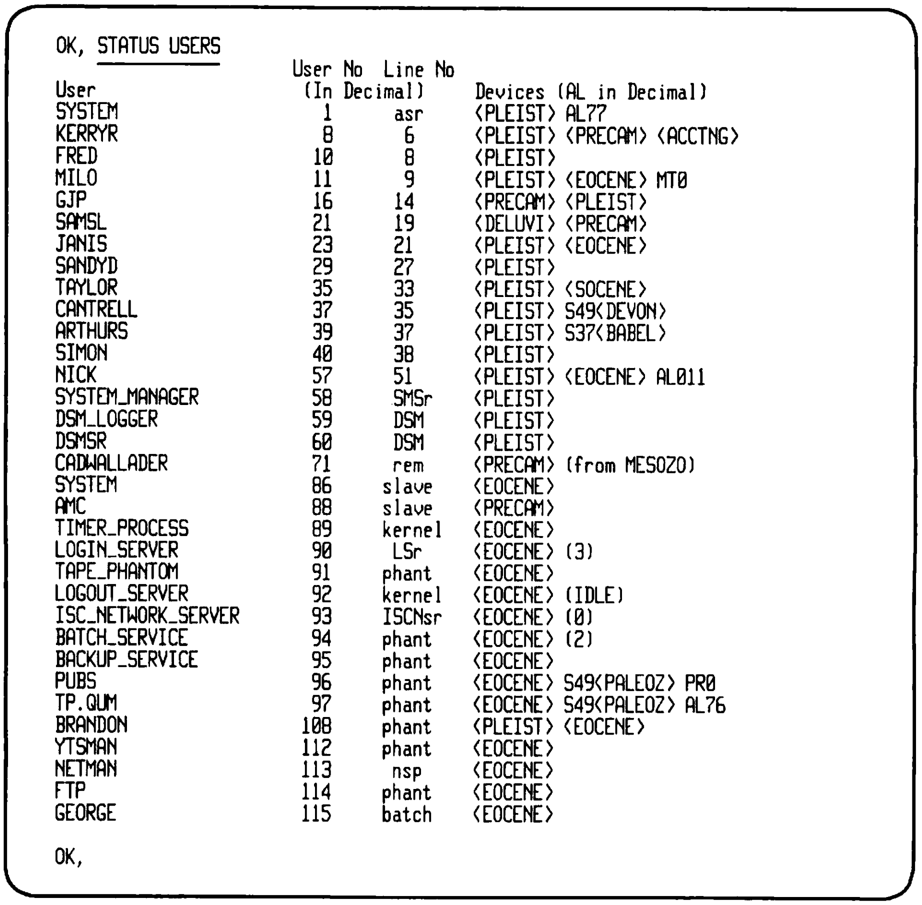
As discussed in Chapter 3, an interactive user is any user who is logged in at a terminal. (Refer to Figure 3-9 in Chapter 3.) An interactive user's name, also referred to as a **login name** or **user ID**, can contain a maximum of 32 characters, the first of which must be a letter. When users log in, they specify their user names and the passwords for those names.

While users are logged in, they are identified by their user names and user numbers. For instance, if a user sends a message to the supervisor terminal, the message includes the ID of that user.

MONITORING USER STATUS

The STATUS command, described in the *Operator's Guide to System Monitoring*, allows you to monitor the status of system users, as well as other aspects of the system. The information displayed indicates active users, active devices, active disks, network status, system status, open file units, assigned devices, and so on.

To determine the names and numbers of all users who are currently logged in to the system, use the STATUS USERS command as in this example:



```
OK, STATUS USERS
                        User No  Line No
User                    (In Decimal)     Devices (AL in Decimal)
SYSTEM                     1      asr    <PLEIST> AL77
KERRYR                     8       6     <PLEIST> <PRECAM> <ACCTNG>
FRED                      10       8     <PLEIST>
MILO                      11       9     <PLEIST> <EOCENE> MT0
GJP                       16      14     <PRECAM> <PLEIST>
SAMSL                     21      19     <DELUVI> <PRECAM>
JANIS                     23      21     <PLEIST> <EOCENE>
SANDYD                    29      27     <PLEIST>
TAYLOR                    35      33     <PLEIST> <SOCENE>
CANTRELL                  37      35     <PLEIST> S49<DEVON>
ARTHURS                   39      37     <PLEIST> S37<BABEL>
SIMON                     40      38     <PLEIST>
NICK                      57      51     <PLEIST> <EOCENE> AL011
SYSTEM_MANAGER            58      SMSr   <PLEIST>
DSM_LOGGER                59      DSM    <PLEIST>
DSMSR                     60      DSM    <PLEIST>
CADWALLADER               71      rem    <PRECAM> (from MESOZO)
SYSTEM                    86     slave   <EOCENE>
AMC                       88     slave   <PRECAM>
TIMER_PROCESS             89     kernel  <EOCENE>
LOGIN_SERVER              90      LSr    <EOCENE> (3)
TAPE_PHANTOM              91     phant   <EOCENE>
LOGOUT_SERVER             92     kernel  <EOCENE> (IDLE)
ISC_NETWORK_SERVER        93     ISCNsr  <EOCENE> (0)
BATCH_SERVICE             94     phant   <EOCENE> (2)
BACKUP_SERVICE            95     phant   <EOCENE>
PUBS                      96     phant   <EOCENE> S49<PALEOZ> PR0
TP.QUM                    97     phant   <EOCENE> S49<PALEOZ> AL76
BRANDON                  108     phant   <PLEIST> <EOCENE>
YTSMAN                   112     phant   <EOCENE>
NETMAN                   113      nsp    <EOCENE>
FTP                      114     phant   <EOCENE>
GEORGE                   115     batch   <EOCENE>

OK,
```

The names under the `User` column are the login, or user, names. The `User No` column shows the user number for each user. Each time a user logs in or a phantom is started, the system assigns a unique user number to that user. You need to have this number when you issue commands that do not accept user names or when more than one user is logged in with the same name.

The `Line No` column shows the asynchronous line number of the user terminals in decimal. Phantoms and remote users do not have user terminals on the system. In these cases, the `Line No` column shows the type of user, as indicated in the following chart.

User	*Process or Phantom*
`rem`	Remote user
`nsp`	The network server process, NETMAN
`slave`	A slave user or process working for a user from another system
`phant`	A user or subsystem phantom
`LSr`	The Login Server
`ISCNsr`	The InterServer Communications Network Server
`kernel`	The Logout Server phantom and the Timer Process phantom
`batch`	Indicates a running batch job by user GEORGE

The `Devices` column shows the partitions and other peripheral devices being used by each user. Names such as `<PLEIST>` refer to the partition in use by each user. Other names such as `AL011` indicate exclusive assignment of the device by the user. In this example, `AL011` means that user 57 has exclusive access to asynchronous line 11 and MTO means that user MILO has tape drive MTO assigned. A user might want to have exclusive access to an asynchronous line to transfer bulk data to another system, to do testing, or to have exclusive use of a printer for a period of time.

A parenthetical number to the right of the `Devices` column indicates the priority level at which a process is running. For example, LOGIN_SERVER is running at priority level 3. The `Devices` column also indicates other nodes from which remote users are logged in. For example, user 71 is logged in from MESOZO.

When To Use STATUS USERS

You might use the STATUS USERS command in these instances:

- To determine that users have released partitions before you shut the partitions down
- To check that all users have logged out before you shut down PRIMOS
- To check if unauthorized users have broken into your system
- To check if any peripheral device is assigned by a user

Monitoring the Number of Users

You can determine the total number of system users by using the USERS command, shown below. This total includes the number of interactive user(s) logged in remotely from or through the system.

```
OK, USERS
Users= 48
OK,
```

PRIMOS SECURITY

The PRIMOS security system provides the following:

- Security for an individual user's files
- Security for devices
- Rights of the user community to use the system
- A log of security events (C2)
- Protection of the hardware, software, storage tapes, and disks

Security for a user's files is achieved through the use of Access Control Lists (ACLs), which are discussed in the next section. The way in which the user community is given access to the system is discussed in two later sections, Project Assignments and User Profiles.

A general discussion of computer room environment and care of the hardware components of the system is in Chapter 1, in the section, The Computer Room.

System operator responsibilities to protect the software are discussed in Chapter 6, System Resources. The Security Audit facility is discussed in Chapter 7, Monitoring Your System.

Access Control Lists (ACLs)

Individual users can specify who can access their files. In certain circumstances, an individual may wish to grant Read (R), but not Write (W), access to a particular file to another user. Such access or restriction is specified in an **Access Control List** (ACL) for a file or directory. For complete information on ACLs for user files see the *PRIMOS User's Guide* and the *PRIMOS Commands Reference Guide.*

Table 5-1 lists the ACL rights that can be specified for files and directories. Here is an example of an ACL:

```
  SALLY:ALL
    JIM:LUR
  .BKPG:LURW
 .PURCH:LURA
  $REST:U
```

In this example, SALLY has ALL rights to the file or directory; whereas JIM has only LUR rights.

TABLE 5-1. ACL Access Rights

Symbol	*Right*	*Applies To*	*Meaning*
R	Read	Files	File can be read or executed.
W	Write	Files	File can be modified.
X	Execute	Local EPF runfiles (no effect on remote EPF files)	Executable Program Format (EPF) file can be executed, but cannot be copied with the standard file system utilities. Read (R) access automatically includes X access.
U	Use	Directories	User can attach to directory.
L	List	Directories	Directory contents can be listed.
A	Add	Directories	Directory entry can be added.
D	Delete	Directories	Directory entry can be deleted.
P	Protect	Directories	Access can be changed.
O	Owner	Files and directories	Owner can set all rights, except P and ALL, and can change RWLOCK.
ALL		Files and directories	User has all of the above rights.
NONE		Files and directories	No access is allowed.

Note

Before the implementation of the ACL system, the only protection for files was that given by the password check for access to the directories. Under the C2 security system, password directories are not allowed. The CONVERT_TO_ACLS utility converts any existing password directory to an ACL directory. Refer to the *System Administrator's Guide, Volume III: System Access and Security* for more information on security issues.

ACL Groups

Your System Administrator may have organized the user community on your system by using **ACL groups.** ACL groups serve two purposes:

- They make it easier for PRIMOS to check users' access.
- They allow the System Administrator to merge new users into existing ACLs by adding existing groups to users' profiles with the EDIT_PROFILE command.

An ACL group is a list of users who are grouped together for file access purposes. The name of an ACL group always begins with a period (for example, .BKPG or .PURCH). User IDs cannot begin with a period (.). Therefore, when you read an ACL, it is easy to tell which IDs represent individual users and which represent ACL groups.

In the example shown above, all users belonging to the .BKPG group have URW rights. The exception is SALLY or JIM, who have only those ACL rights specified for them, regardless of whether they belong to the .BKPG group. If an individual's rights are not as broad as the rights of the group to which that individual belongs, the individual ACL rights supercede the group rights for that individual.

Monitoring User Access

Three commands are available for the purpose of monitoring Access Control Lists (ACLs). The commands are listed below, followed by descriptions of their use.

Command	*Function*
LIST_GROUP **LG**	Lists the ACL groups to which you belong. Such groups determine access rights to certain files and directories.
LIST_ACCESS [*pathname*] **LAC**	Lists the access rights for any object. An object is a part of the file system tree structure, such as an MFD, a directory, or a file.
LIST_PRIORITY_ACCESS *diskname* **LPAC**	Reads the contents of the priority ACL on the partition named *diskname.*

The LIST_GROUP Command: As an operator, you should be a member of a group that has special operator's rights. In the following example, the operator is a member of the .ADMINISTRATORS group, which allows access to special system files and directories denied to other users. Group membership is defined by the System Administrator.

```
OK, LIST_GROUP
Groups are:  .ADMINISTRATORS
OK,
```

In the following example, the user who entered the LIST_GROUP command has the ACL rights of one group, .TPEOPLE.

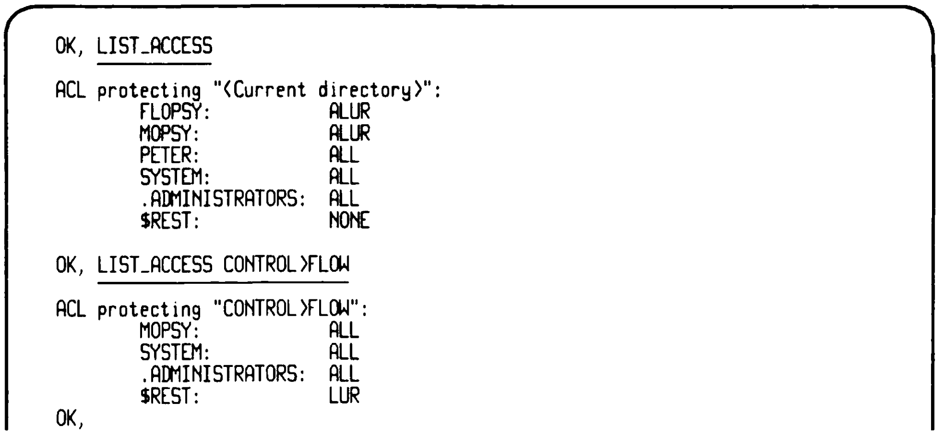
```
OK, LIST_GROUP
Groups Are:  .TPEOPLE
OK,
```

If a user attempts to access a file or directory and the system responds that the user has insufficient access, ask the user to issue the LIST_GROUP command. Either the user was mistakenly not assigned a group, or was assigned a group that is explicitly denied access to the file or directory he or she is attempting to reference.

The LIST_ACCESS Command: LIST_ACCESS lists your access rights to a file or directory. The format is

LIST_ACCESS [*pathname*]

If you omit *pathname*, access rights are given for the current directory, as shown here:



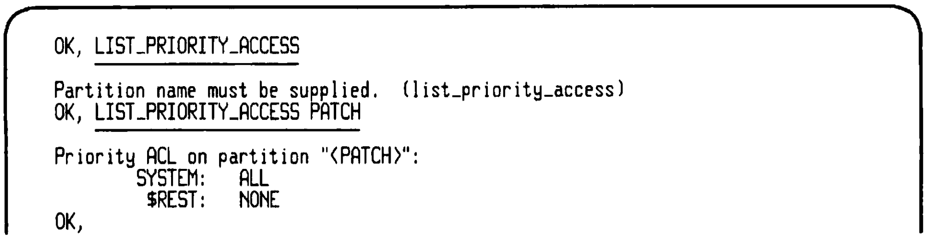
```
OK, LIST_ACCESS

ACL protecting "<Current directory>":
        FLOPSY:           ALUR
        MOPSY:            ALUR
        PETER:            ALL
        SYSTEM:           ALL
        .ADMINISTRATORS:  ALL
        $REST:            NONE

OK, LIST_ACCESS CONTROL>FLOW

ACL protecting "CONTROL>FLOW":
        MOPSY:            ALL
        SYSTEM:           ALL
        .ADMINISTRATORS:  ALL
        $REST:            LUR
OK,
```

In the first example the .ADMINISTRATORS group and users SYSTEM and PETER, have full access rights to the directory. Users FLOPSY and MOPSY can read files (R), attach to and list the contents of the directory (LU), and create new files or subdirectories (A). Other users of the system have no access rights.

In the second example, users SYSTEM and MOPSY, along with the group .ADMINISTRATORS, have all access rights. Other users of the system can list and use directories and can read files.

The LIST_PRIORITY_ACCESS Command: System Administrators and operators can override any user-defined ACL by creating a **priority ACL.** The priority ACL defines access for the entire partition. It is possible to prevent users from accessing even the MFD by using a priority ACL. You use the SET_PRIORITY_ACCESS (SPAC) command, although the SET_PRIORITY_ACCESS command is used primarily when doing system backups or installing software. See the *Operator's Guide to System Commands* and the *System Administrator's Guide, Volume III: System Access and Security.*

The LIST_PRIORITY_ACCESS command allows the operator and users to determine the contents of the priority ACL on any partition. You must always give the name of the partition, for example:

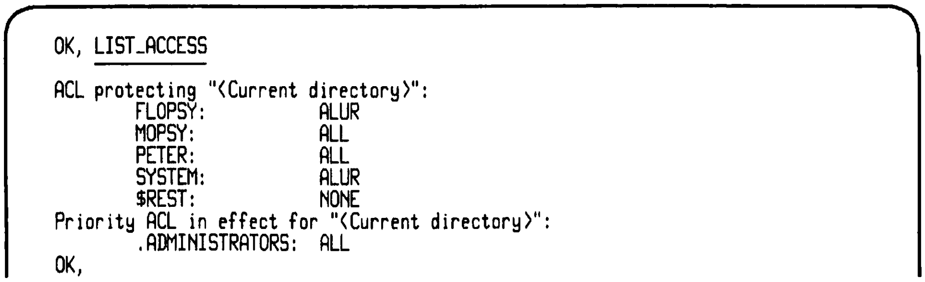


```
OK, LIST_PRIORITY_ACCESS

Partition name must be supplied.  (list_priority_access)
OK, LIST_PRIORITY_ACCESS PATCH

Priority ACL on partition "<PATCH>":
        SYSTEM:    ALL
         $REST:    NONE
OK,
```

If the partition PATCH is not protected by a priority ACL, the following message is displayed:

```
OK, LIST_PRIORITY_ACCESS PATCH
Priority ACL not found.  <PATCH> (list_priority_access)
ER!
```

When a priority ACL is active on a partition, the contents of that priority ACL are always displayed when the LIST__ACCESS command is issued, as shown here:

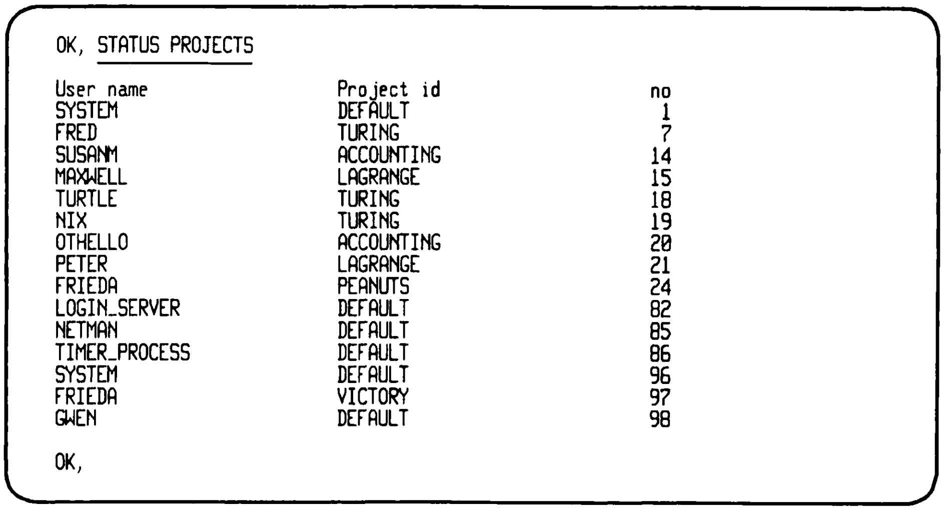


```
OK, LIST_ACCESS

ACL protecting "<Current directory>":
        FLOPSY:            ALUR
        MOPSY:             ALL
        PETER:             ALL
        SYSTEM:            ALUR
        $REST:             NONE
Priority ACL in effect for "<Current directory>":
        .ADMINISTRATORS:   ALL
OK,
```

Project Assignments

A Prime system must have at least one **project** on the system. A project is a collection of users working in the same area. The System Administrator may define several projects for the system. A user can belong to more than one project, but can be logged in under only one project at a time. This feature is often used to enhance system accounting.

When a user logs in, the system may ask the user for a project name. (The System Administrator determines whether or not users need to specify a project name at login time.) The groups to which the user belongs, the user's command environment attributes, and the user's origin directory depend upon the project specified by the user. If a user experiences problems when logging in or has insufficient access to files and directories, the problem may be that the user is trying to log in to the wrong project. To list the projects for all logged in users, issue the STATUS PROJECTS command, as follows.

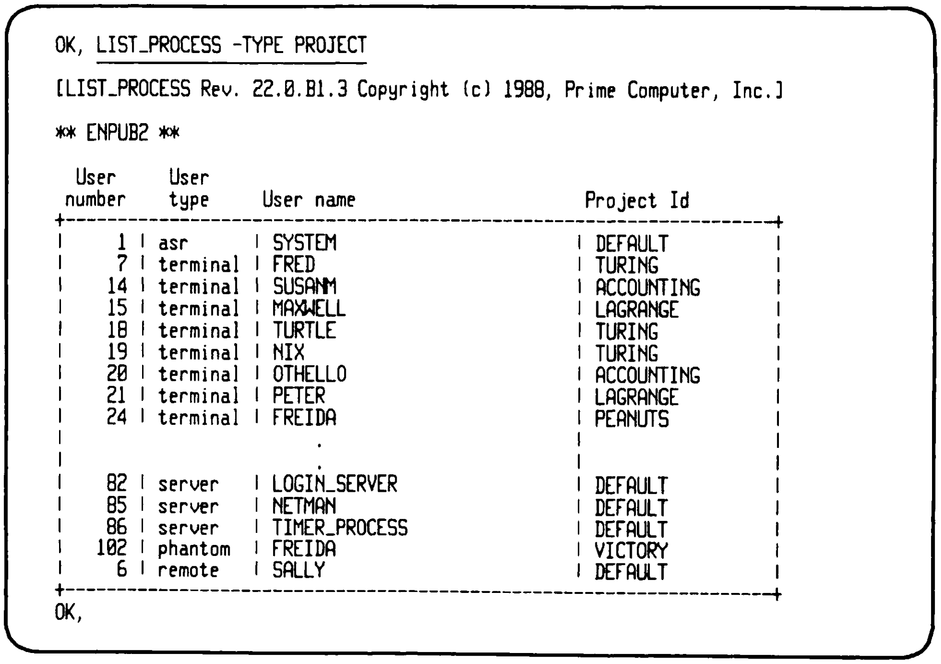


```
OK, STATUS PROJECTS

User name               Project id              no
SYSTEM                  DEFAULT                  1
FRED                    TURING                   7
SUSANM                  ACCOUNTING              14
MAXWELL                 LAGRANGE                15
TURTLE                  TURING                  18
NIX                     TURING                  19
OTHELLO                 ACCOUNTING              20
PETER                   LAGRANGE                21
FRIEDA                  PEANUTS                 24
LOGIN_SERVER            DEFAULT                 82
NETMAN                  DEFAULT                 85
TIMER_PROCESS           DEFAULT                 86
SYSTEM                  DEFAULT                 96
FRIEDA                  VICTORY                 97
GWEN                    DEFAULT                 98

OK,
```

The first column shows the user name, the second shows the project that the user is logged in to, and the third shows the user number (the number assigned by the system when the user logs in).

In the above example, note that there are two users named FRIEDA. The first is in project PEANUTS, the second, in project VICTORY. This indicates that user FRIEDA has two processes working in two different projects at the same time. This can happen when a user logs in to one project, starts up a phantom, logs out, and logs in to another project. It can also happen when a user is logged in on two terminals at the same time but with a different project on each.

Alternatively, you can issue the LIST_PROCESS command with the -TYPE PROJECT option, which displays the information in the following format:



```
OK, LIST_PROCESS -TYPE PROJECT

[LIST_PROCESS Rev. 22.0.B1.3 Copyright (c) 1988, Prime Computer, Inc.]

** ENPUB2 **

 User    User
 number  type      User name                       Project Id
+-------------------------------------------------------------------+
|     1 | asr      | SYSTEM                       | DEFAULT        |
|     7 | terminal | FRED                         | TURING         |
|    14 | terminal | SUSANM                       | ACCOUNTING     |
|    15 | terminal | MAXWELL                      | LAGRANGE       |
|    18 | terminal | TURTLE                       | TURING         |
|    19 | terminal | NIX                          | TURING         |
|    20 | terminal | OTHELLO                      | ACCOUNTING     |
|    21 | terminal | PETER                        | LAGRANGE       |
|    24 | terminal | FREIDA                       | PEANUTS        |
|                        .                        |                |
|                        .                        |                |
|    82 | server   | LOGIN_SERVER                 | DEFAULT        |
|    85 | server   | NETMAN                       | DEFAULT        |
|    86 | server   | TIMER_PROCESS                | DEFAULT        |
|   102 | phantom  | FREIDA                       | VICTORY        |
|     6 | remote   | SALLY                        | DEFAULT        |
+-------------------------------------------------------------------+
OK,
```

User Profiles

Each user who can log in to the system has a user (login) name. This user name is associated with a **user profile**. The user profile describes the systemwide attributes and one or more sets of project-specific attributes of a user. Systemwide attributes are always associated with a user, regardless of which project the user is logged in to. One set of project-specific attributes is also associated with each user. Project-specific attributes include the groups assigned to the user, the origin directory or Initial Attach Point (IAP) of the user, and the attribute limits for the user. The project-specific attributes of the user depend upon which project the user logs in to. User profiles are created or modified by the System Administrator or the Project Administrator using the EDIT_PROFILE utility.

When a user logs in, the user profile is checked for the user's IAP. This IAP must exist on the system to which the user is attempting to log in, and the user must have the right to attach to it; otherwise, the user is not logged in, and an error message is displayed.

If an IAP exists but a user is unable to log in, the origin directory may not be accessible either because

- It resides on a remote disk.
- It resides on a disk that is currently shut down.
- The directory has an ACL preventing the user from attaching to it. (The user was not given proper access to his/her own origin directory.)
- The directory may be damaged.

Refer to the *System Administrator's Guide, Volume III: System Access and Security.*

RESPONDING TO USER REQUESTS

To allow you to communicate with users, PRIMOS includes a message facility that is available through the MESSAGE command. Users request actions with this facility that only you, as an operator, can perform. Such requests are issued for the following actions:

- Sending broadcast messages to all users
- Adding new directories to the system
- Setting quotas on directories
- Adding or replacing software, for example in CMDNC0, LIB, and LIBRARIES*
- Incorporating shared segments
- Changing user priority or timeslice

When you receive a request, check with your System Administrator to be sure that you are allowed to honor the request, then record the request in the system logbook before you honor it.

Use the REPLY command to respond to user requests. For example, when a user requests the exclusive use of a tape drive, with the ASSIGN command, use the REPLY command to indicate which tape drive is being assigned to that user.

You use the message facility for the same reasons as users do, and particularly to send broadcast messages warning users of an impending shutdown of a partition or the system.

Sending Broadcast Messages

If a user discovers something about which all users should be told, such as a full disk, the user could ask you to send all users a message. From the supervisor terminal, you can send messages to

- All users on the local node of the network
- A specified user on any node of the network
- The supervisor terminal of a different network node (for operator-to-operator messages)

The MESSAGE command is useful for giving users general information (such as an impending system shutdown or a full disk), communicating with a single user (answering questions, requesting action), and for passing information between nodes (such as remote disk availability).

To send a message to all users stating that a partition is nearly full, type

```
OK, MESSAGE ALL -NOW -FORCE
BEEBLE PARTITION 99% FULL -- PLEASE DELETE UNNECESSARY FILES
OK,
```

Be sure not to include the supervisor terminal's kill character in the message. The default kill character is the question mark (?). For more information on the MESSAGE command, refer to the *Operator's Guide to System Commands.*

Adding New Top-level Directories to the System

Because access to MFDs is not usually granted to users, top-level directories can be added to MFDs only by the operator or the System Administrator. When a user makes a request to add a new top-level directory to the system, you should first determine from the user the new directory's name and the partition on which it is to reside. Although PRIMOS automatically checks the new directory name to ensure that it does not duplicate an existing directory name on that partition, you should check that no other local partition has a top-level directory of the same name. If several top-level directories have the same name, users must use the partition name to access the second directory.

If you create a new directory with the CREATE command, its quota is initially set to zero (unless you use the -MAX option); that is, it has no maximum quota. If you set a quota on a directory, you limit the storage allowance on any subdirectory within the directory.

If you set no limit on the directory, its storage capacity is limited only by the physical capacity of the disk with which it is associated. (Note that a quota of zero does not signify that the directory is allowed no storage at all; instead, it signifies the reverse.) Information on setting quotas is given below.

The access for a newly created directory defaults to the access at the MFD level. Therefore, you should normally set its access to allow ALL access for the owner of the directory.

Either work at the supervisor terminal or log in as a user (usually SYSTEM) at a user terminal, attach to the MFD on the appropriate partition, and generate the new directory with the CREATE command (explained in the *PRIMOS Commands Reference Guide*).

Note

> Only the System Administrator or a Project Administrator can specify a directory to be a user's Initial Attach Point (IAP) by using EDIT_PROFILE.

You must also perform all requests for directory name changes (by using the CNAME command) because access other than LUR to the MFD is not usually available to users.

Setting Quotas on Directories

To set maximum storage quotas on directories, use the SET_QUOTA command. Because you must have Protect (P) access rights, log in as the System Administrator or use the supervisor terminal. See the *Operator's Guide to System Commands* for a description of the SET_QUOTA command.

Adding and Replacing Software in System Directories

CMDNC0, SEARCH_RULES*, LIB, SYSTEM, and LIBRARIES* are usually ACL-protected directories under operator control. They contain essential system software, as explained in Chapter 3, The System Software. Use the COPY command to copy new software into these directories. Likewise, use a text editor to modify the files in the directory SEARCH_RULES*. All new or changed software should be debugged before installation.

Note all changes to these directories in the system logbook. Do not install new or changed software without first obtaining complete details of its operation. For commands, include command-line options and keywords as well as answers to any queries or prompts of the program. The proper position in loading sequences should be indicated for each library. This information should also be entered in the system logbook and distributed to interested users.

When installing a new command, be sure to add an appropriate help file. Users can obtain help on the command by typing

HELP *command*

Adding help files is explained in the *System Administrator's Guide, Volume I: System Configuration.*

Caution

When you install a new version of a command or a program, save a copy of the old version in a convenient directory until you have determined how the new version operates and are sure that the old version is no longer needed.

Incorporating Shared Segments

Subsystems that use shared segments are discussed in Chapter 3, The System Software. Normally, shared subsystems are incorporated into PRIMOS at system startup. At times, however, experimental subsystems need to be incorporated for test purposes. The appropriate command, issued from the supervisor terminal, is

SHARE ***pathname segment-number*** [*access-rights*]

The System Administrator assigns and coordinates shared segment usage. Shared segments contain software that is available to all users, such as languages, database management products, and word processors. See the *System Administrator's Guide, Volume I: System Configuration* for a list of shared segments. See the discussion of the SHARE command in the *Operator's Guide to System Commands* for complete details on its use.

Caution

Be sure to check the PRIMOS.COMI file to determine the segment numbers that are currently shared to ensure that you do not overwrite segments being used by another subsystem. Refer also to the list of shared segments recorded in your logbook, as described in the section, Keeping Your Logbook, in Chapter 2. Also, do not share into segments 0 through 1777_8, which contain PRIMOS and its databases.

Changing Priority or Timeslice

To increase efficiency and/or system performance, you can change process priorities or timeslices. You can give special priority to important jobs. You change priority and timeslice by using the CHAP command, which is described in the *Operator's Guide to System Commands.*

For example, to set the priority of user 12 to 2, and the timeslice to 2.3 seconds, type

```
OK, CHAP -12 2 27
```

The timeslice is specified in octal, as tenths of a second. The timeslice for a process is the total amount of time that the process receives service from the CPU before the next process is serviced. The first process is not serviced by the CPU again until the next timeslice for that process.

6

SYSTEM RESOURCES

This chapter specifies how to allocate system resources and discusses the operator interface to the following system resources:

- Magnetic tapes
- Assignable asynchronous lines
- The Spooler subsystem
- The Batch subsystem
- Distributed Systems Management
- The File Transfer Service (FTS)
- The PRIMENET network
- Network Terminal Service (NTS)

ALLOCATING SYSTEM RESOURCES

In addition to magnetic tape drives and assignable asynchronous lines, included in the above list, Prime system installations can include the following peripheral devices:

- User terminals
- Letter-quality printers
- Laser printers
- Parallel printers
- Serial line printers
- Plotters

- CAD/CAM workstations
- Synchronous communications boards
- Paper tape reader/punches
- Card reader/punches

PRIMOS manages all of these peripherals so that all users of the system can benefit equally from their availability. For example, consider a system with one printer and two users who both want to print files at the same time. The system cannot honor both print requests immediately.

To solve this problem, PRIMOS uses two approaches to manage peripherals. The first approach is to allow only one user at a time to operate a peripheral device. This approach is referred to as **exclusive assignment.** For example, while one user is using a paper tape punch, no other user is able to use that device. Exclusive assignment of devices prevents two users from punching one tape and causing data from two separate files to intermingle on the tape. It is cumbersome, however, because the user who is waiting must attempt to obtain exclusive access immediately after the first user relinquishes exclusive access and before another user can gain exclusive access.

The second approach is to allow any number of users to request operations to be performed on a peripheral, and to allow the requested operations to be performed in sequence as the peripheral device becomes available. This approach is called **request queuing.**

These approaches require you to monitor the operation of the physical peripheral device itself and its use by the user community.

Exclusive Assignment

When a user wants exclusive use of a peripheral, he or she must request exclusive access by using the PRIMOS command ASSIGN. (The PRIMENET Node Controller (PNC) cannot be assigned by a user, because it is always assigned to the network manager, NETMAN.) If another user already has exclusive access to the peripheral, the ASSIGN command returns the following error message:

```
OK, ASSIGN MT0
The device is in use.  MT0 (asnmt$)
ER!
```

In this case, the second user who requests exclusive access to device MT0 must wait until the first user relinquishes control. Once the first user gives up control, the second user can successfully assign the device, as follows:

```
OK, ASSIGN MT0
Device MT0 assigned.
OK,
```

The second user can then invoke programs that operate the device. For example, after assigning a magnetic tape drive, the user can invoke MAGSAV to save a file or directory, as described in the *Data Backup and Recovery Guide.*

You should monitor device assignment periodically to ensure that no one user is taking unfair advantage of the ASSIGN command and preventing other users from having time on a peripheral device. At the supervisor terminal, you can use the UNASSIGN command to return a peripheral device to the pool of available devices, even when another user has the device assigned.

The function of managing the assignment of magnetic tape drives is discussed in more detail in the section Magnetic Tapes, later in this chapter.

Assigning Disks: As an operator, you are primarily concerned with the assignment of two system peripherals – disks and tapes. Disks are not listed as peripherals in the preceding list, because they are considered system components rather than peripherals.

From time to time, you may need to perform operations other than normal user operations on disks. In these cases, you obtain exclusive access to a disk so that other users cannot reference it. The ASSIGN DISKS command is discussed in Chapter 4, The File System. You then use certain PRIMOS programs to examine and change the disk. PRIMOS itself is not able to access files on an assigned disk, but the program you run is able to do so.

Only the operator can assign disks. The procedure for doing so is explained in the *Operator's Guide to File System Maintenance.*

Device Access Control Lists

Device ACLs extend ACL protection to peripheral devices such as printers, plotters, tape drives, card readers, and card punches, and to assignable partitions of physical disks. For complete information on device ACLs, see the *System Administrator's Guide, Volume III: System Access and Security.*

The Directory DEVICE*: Device ACLs are implemented through a top-level directory called DEVICE*, which is created by the System Administrator. The DEVICE* directory contains properly named subdirectories that correspond to assignable partitions, tape drives, and other devices on the system. The list of devices is shown in Table 6-1.

TABLE 6-1. Device List for Device ACLs

Subdirectory	*Device Name Description*
CENPR	The serial printer.
CE2PR	The second serial printer.
CARDR	The serial card reader.
PTR	The paper tape reader/punch.
PUNCH	The card punch.
PR*n*	MPC printer *n*, where *n* ranges from 0 through 3, inclusive.
CR*n*	Parallel card reader *n*, where *n* ranges from 0 through 1, inclusive.
MT*n*	Magnetic tape unit *n*, where *n* ranges from 0 through 7, inclusive.
SMLC*n*	Synchronous Communications line *n*, where *n* ranges from 00 through 07, inclusive. Preceding zeros *must* be present.
SPARE*n*	Spare device *n*, where *n* ranges from 1 through 5, inclusive. These devices may be assigned, but presently do not correspond to any configured device.
PLOT	The plotter.
MG*n*	Megatek graphics display terminal *n*, where *n* ranges from 0 through 3, inclusive.
GS*n*	Vector General graphics display terminal *n*, where *n* ranges from 0 through 3, inclusive.
AL*n*	Asynchronous line number *n*, where *n* is normally a decimal number ranging from 0 through 1535. (Local line numbers range from 0 to 512; line numbers 1024 through 1535 are reserved for NTS assigned lines.) Omit any preceding zeros. Thus, for asynchronous line number 07, the device directory must be named AL7.
DK*n*	Disk partition *n*, where *n* is the octal pdev of the partition. When making a pdev assignable by means of the DISK command, you can also create, and set access on, a corresponding DK*n* device directory within DEVICE*. If you are altering a previous DK*n* directory either by increasing the size of the partition or by unassigning the partition, first be sure to update the device ACLs on the old DK*n*.
DEFAULT	A default directory that is checked when an assignable partition is assigned. If you do not create a specific DK*n* device directory for a given partition, the device ACLs mechanism provides access to it for any users with a U right to DEFAULT.

The System Administrator must set Use (U) rights on a device subdirectory in order to grant access to a requesting user. The ACLs set on DEVICE* are

```
system_administrator:PDALU
              SYSTEM:PDALU
               $REST:U
```

where *system_administrator* is the user name of the System Administrator.

Note

Any ACL rights other than U or NONE (for example LUR or ALL) set on the DEVICE* subdirectories are equivalent to NONE and thus any user with rights other than U is denied access to the device.

If the subdirectory corresponding to a requested device does not exist, or if the user does not have U access, PRIMOS issues the message `Insufficient access rights`, and denies access.

Administering Device Access: Before activating device ACLs, the System Administrator uses the commands SET_ACCESS or EDIT_ACCESS to provide device users with Use (U) access to a device directory and, thus, to the device. Use the LIST_ACCESS command with the device subdirectory name to monitor access to a device.

Only those persons allowed to control device protection have Protect (P), Add (A), or Delete (D) access rights to the DEVICE* directory.

The DEVICE_ACLS Command: Device access is activated by issuing the command DEVICE_ACLS (abbreviation DEVACL with the -ON option). When device access control is in effect, PRIMOS searches the local partitions for the top-level directory DEVICE*. If DEVICE* does not exist, PRIMOS displays this message:

```
Warning: Device ACLs are enabled, but DEVICE* could not be found.
```

If DEVICE* exists, PRIMOS checks the user's access rights to the appropriate subdirectory for that device in DEVICE*.

To turn off device access control, use the DEVACL -OFF command. DEVACL -OFF is the default at system cold start.

Request Queuing

A major drawback of the exclusive assignment approach is that while one user is using a device, another user who wants to use the device must wait until it becomes free and then attempt to obtain exclusive access before some other user does.

To solve this problem, PRIMOS provides **request queuing** for some peripherals. Users can request use of the device and continue other work. If the device is already in use, the request is processed automatically by PRIMOS when the device becomes available.

For example, instead of allowing a user to print a file directly on a printer, PRIMOS provides the Spooler facility whereby a user makes a request to print a file. This request is placed in the spool queue. The files are actually printed by a special PRIMOS phantom called the **despooler.** A despooler phantom is a process that controls one of the printers. Several despooler phantoms can run at the same time, and each despooler can search for jobs in queues on other systems in the same network, as well as in the local queue.

The phantom checks the spool queue to see whether there are any requests waiting that it can handle. The despooler phantom recognizes requests that it can process by examining their attributes. When the file is printed, the program removes the request from the queue.

This principle of queuing is used to manage printers and plotters. A similar principle is used to manage various uses of the synchronous communications boards and the PRIMENET Node Controller (PNC). Thus, the File Transfer Service (FTS) allows users to request that files be sent from one system to another. Like the Spooler, the File Transfer Service adds file transfer requests to a queue, and a subsystem phantom processes these requests.

Finally, PRIMOS provides queuing services, such as Batch and File Transfer Service. These subsystems queue requests for the use of Batch and FTP phantom processes.

MAGNETIC TAPES

Magnetic tapes provide a relatively inexpensive storage medium and are used extensively. Operators routinely perform several tasks related to magnetic tapes and magnetic tape drives. These include

- Setting tape drive assignment mode.
- Assigning and unassigning tape drives.
- Turning on tape drives.
- Mounting and dismounting tapes.
- Responding to special user options.
- Performing general maintenance of the tapes and drive unit.
- Performing backups and providing backup copies of files and programs. (See the *Data Backup and Recovery Guide.*)

The most important commands associated with the operator's magnetic tape responsibilities are

Command	*Function*
SETMOD	Sets drive assignment mode
ASSIGN	Allocates tape drives
REPLY	Replies to a user request for a tape drive
STATUS	Gives status of system use
UNASSIGN	Releases tape drive from user

The operator can issue the SETMOD, REPLY, and UNASSIGN commands only from the supervisor terminal. (You can issue the UNASSIGN command at any user terminal, but it affects only that user. From the supervisor terminal, it affects any user on the system.) These commands are discussed on the following pages. For more information regarding magnetic tape and magnetic tape drives, refer to the *Data Backup and Recovery Guide.*

Setting the Mode of Assignment

You can choose from three modes of tape drive assignment:

- Users can assign tape drives without operator intervention, unless special assistance is needed. This is the default mode.
- Users must channel all assignment requests through the operator.
- Users are not permitted to assign tape drives at all.

The SETMOD command establishes the assignment mode. It can be issued only at the supervisor terminal. If SETMOD is not issued, the default mode (user assignment) prevails. The three assignment modes are

Mode — *Description*

User mode

Users can assign tape drives without operator assistance unless options require special intervention. This is the default mode. The command to enter User mode is

```
SETMOD -USER
```

Operator Intervention mode Users must channel all assignment requests through the system operator. The command to enter Operator Intervention mode is

SETMOD -OPERATOR

No-assignment mode Users are not permitted to assign tape drives at all. The command to enter No-assignment mode is

SETMOD -NOASSIGN

The SETMOD command is described in the *Operator's Guide to System Commands.*

Allocating Tape Drives

Each magnetic tape operation requires the exclusive use of at least one tape drive. To reserve tape drives use the ASSIGN command. ASSIGN associates the drive's physical device number with the number of the user who issued the ASSIGN command. As long as the user number and device number are correlated within PRIMOS, the user has exclusive access to the drive. Access privileges are relinquished with the UNASSIGN command.

The ASSIGN command reserves magnetic tape drives for users, COMINPUT files, and CPL programs. ASSIGN is frequently used to request operator assistance in assigning a drive or mounting a tape. In addition to the default assignment, which simply designates a particular tape drive, the user can ask you to do the following:

- Assign any available tape drive.
- Assign a tape drive with certain features, such as special density settings.
- Assign a particular tape drive when it becomes available.
- Mount a particular tape on an indicated or available drive.
- Assign any tape drive, and give it a user-chosen logical device number, or alias, with which the user will subsequently reference the assigned tape drive.

Information on the ASSIGN command for operators is found in the *Operator's Guide to System Commands.* Information on the ASSIGN command for users is in the *PRIMOS Commands Reference Guide.*

Whenever a user's ASSIGN command line necessitates operator intervention, the request appears at the supervisor terminal.

Users may request assignment of magnetic tape drives in either of two ways:

- By physical device number (*n*), for example

```
ASSIGN MTn
```

- The following message appears at the supervisor terminal:

  ```
  ***** Magtape request *****

  From user-id (usernum) : ASSIGN MTn [options]
  ```

- By logical device number (*ldn*), for example

  ```
  ASSIGN MTX -ALIAS ldn
  ```

- The following message appears at the supervisor terminal as

  ```
  ***** Magtape request *****

  From user-id (usernum) : ASSIGN MTX -ALIAS ldn [options]
  ```

The *user-id* and *usernum* identify the originator of the request.

The message is repeated frequently at the supervisor terminal until you acknowledge it with the REPLY command, described below.

Note

> When a user sends an ASSIGN request that requires operator intervention, that user's terminal hangs until you respond to the user's request.

Responding to User Requests

When users request magnetic tape assignments via the ASSIGN command, they must be informed of the status of their requests. Use the REPLY command to respond to the requesting user. REPLY is preferred over the MESSAGE command when the user is assigning a magnetic tape because REPLY communicates successfully with Batch jobs, user phantoms, command files, or CPL files. By contrast, the message sent by a MESSAGE command can be read only by an interactive user. In addition, when a user uses the ASSIGN command with an option, the user's terminal hangs until you reply to that user by using the REPLY command. (The user could use Ctrl P to free the terminal; however, this aborts the request.)

The REPLY Command

You can issue the REPLY command only at the supervisor terminal. It allows you to do the following:

- Approve a simple request (in Operator Intervention mode).
- Inform the user which tape drive has been assigned when the user has requested any drive (MTX).
- Request repetition of an ASSIGN message.

- Inform a user that a special request has been fulfilled
- Deny a request

Use this procedure to respond to user requests:

1. Determine the tape drive to be used.
2. Perform all requested tasks.
3. Mount the correct tape.
4. Issue the appropriate REPLY command.

If you select User mode, you will have to respond either when options are requested or when drive assignments are requested by logical device number. If you select Operator Intervention mode, you must respond to all requests. If you select No-assignment mode, you do not receive requests from users, and they are unable to assign tapes.

Examples of ASSIGN Requests

ASSIGN requests to the system operator are of three types:

- Simple ASSIGN MT*n* requests
- ASSIGN MT*n* requests with options
- ASSIGN MTX requests

Responding to Simple ASSIGN MTn Requests: Requests appear at the supervisor terminal containing the user name, the user number, and a command line. For example:

```
***** Magtape request *****

from SHANIN (user 7): MT1
```

This example indicates that user SHANIN (designated by PRIMOS as user number 7) requests physical device MT1.

In User mode, this request would be approved or rejected (depending on MT1's availability) without the need for operator intervention, because no options are specified.

In Operator Intervention mode, the user's request appears at the supervisor terminal. You must always respond. If the request can be approved, inform the user (in this case, user 7) by issuing the command

```
REPLY -7 -TAPE GO
```

If the request cannot be approved, type

```
REPLY -7 -TAPE ABORT
```

The first response indicates that SHANIN now has exclusive access to physical device MT1. The second response indicates that the tape drive is not presently available.

Responding to ASSIGN MTn Requests With Options: More complicated requests require you to perform additional actions. The following message indicates that user HARRIET (user 11) has requested assignment of tape drive MT3, with the tape EXEC loaded, and with the write ring on. Also, user HARRIET is willing to wait until drive MT3 is available.

```
***** Magtape request *****

from HARRIET (user 11): MT3  -TPID EXEC  -RINGON  -WAIT
```

Follow these steps to fill the request:

1. Determine the availability of drive MT3.
2. Locate the tape identified as EXEC.
3. Insert the ring and mount the tape.
4. Issue the command REPLY -11 -TAPE GO.

User HARRIET now has exclusive use of tape drive MT3 with the tape EXEC mounted on it and with writing enabled on the tape.

Responding to ASSIGN MTX Requests: With requests that specify the MTX -ALIAS option, you get a message in the format

```
***** Magtape request *****

From BOB  (user 34): MTX -ALIAS MT0 -TPID JEN -DENSITY 1600
```

Respond by following these steps:

1. Locate the tape marked JEN.
2. Mount the tape on an available drive (assume here, MT1).
3. Set the density switch to 1600 bpi.
4. Issue the command REPLY -34 -TAPE 1.

User 34 now has the use of tape drive MT1, which is referred to by the user as MT0, the logical device number (ldn).

Information Gathering

Some typical areas of concern for you are listed below. Appropriate actions are indicated.

- To clarify an unintelligible request from a user, type

  ```
  REPLY -usernum -TAPE RESEND
  ```

  The ASSIGN command request from *usernum* reappears.

- To repeat the most recent magnetic tape request, type

  ```
  REPLY -TAPE RESEND
  ```

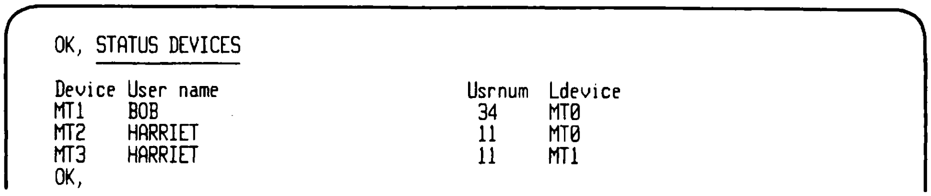
- To display all unanswered tape requests, type

  ```
  REPLY -ALL RESEND
  ```

- To determine the availability of a requested drive, use the STATUS DEVICES command, described in the next section.

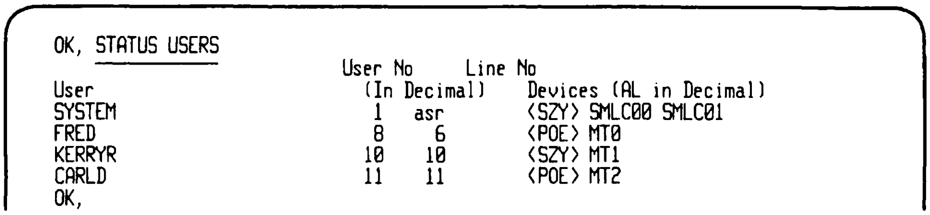
Determining the Current Status of Users and Magnetic Tape Drives

You can obtain a quick list of the magnetic tape drives currently in use by typing STATUS DEVICES or LIST_ASSIGNED_DEVICES. Only currently assigned magnetic tape devices are listed. The information returned by STATUS DEVICES looks like this:



```
OK, STATUS DEVICES

Device User name                     Usrnum  Ldevice
MT1    BOB                            34     MT0
MT2    HARRIET                        11     MT0
MT3    HARRIET                        11     MT1
OK,
```

You can also tell who has exclusive access to which peripheral devices by using the STATUS USERS command as in the following example. Peripheral devices include magnetic tape drives, card readers, and disks.



```
 OK, STATUS USERS
                        User No    Line No
User                     (In Decimal)    Devices (AL in Decimal)
SYSTEM                    1    asr       <SZY> SMLC00 SMLC01
FRED                      8     6        <POE> MT0
KERRYR                   10    10        <SZY> MT1
CARLD                    11    11        <POE> MT2
 OK,
```

This display indicates that users FRED, KERRYR, and CARLD are using tape drives 0, 1, and 2. See the *Operator's Guide to System Commands* for an expanded discussion of the STATUS command. See the *DSM User's Guide* for a description of the System Information and Metering (SIM) commands such as LIST_ASSIGNED_DEVICES.

Releasing Tape Drives

At times you must revoke exclusive access to a magnetic tape drive from a user. You can do this from the supervisor terminal with the UNASSIGN command, as in this example:

```
OK, UNASSIGN MT0
```

You can issue this command in all tape assignment modes. Only the user who assigned an alias can use the alias number when unassigning a drive. The actual device number must be specified in the UNASSIGN command at the supervisor terminal.

For example, suppose that user 17 assigns MT1 -ALIAS MT2 and also assigns MTX -ALIAS MT0. If you choose physical drive MT2 as MTX, the effective internal relationship can be represented as in the following table.

TABLE 6-2. Physical and Logical Device Numbers of Tape Drives

Usernum	*Physical Device Number*	*Logical Device Number*
17	MT1	MT2
17	MT2 (formerly MTX)	MT0

This representation is similar to the table displayed by STATUS DEVICES. Note that every magnetic tape drive has a default logical device number. This number is the same as the drive's physical device number, unless you change it with the -ALIAS option. You release these drives with the UNASSIGN command: UNASSIGN MT1 and UNASSIGN MT2.

In Operator Intervention mode, when a device is successfully unassigned from the supervisor terminal, the message `Device released` is displayed at the supervisor terminal. If a user successfully gives the UNASSIGN command, the message `Device MTn unassigned` is displayed.

In User mode, the message `Device released` signals a successful UNASSIGN command issued from the supervisor terminal.

Operator Use of Tapes

You will need to use magnetic tapes when you perform system backup and restore operations. The commands to back up and restore partitions to magnetic tape are BACKUP, BACKUP_RESTORE, MAGSAV, MAGRST, PHYSAV, and PHYRST. These commands, and the procedures for using them, are discussed in the *Data Backup and Recovery Guide.*

ASSIGNABLE ASYNCHRONOUS LINES

Asynchronous lines connect terminals, printers, and other devices with the CPU. The term asynchronous means that the devices that communicate over the line are not synchronized; data is sent and received one character at a time and each character is preceded by a start bit and followed by a stop bit.

Assignable asynchronous lines are a class of communications lines used for serial devices such as serial printers, plotters, card punches and readers, and personal computers. Assigned lines are required for serial devices. For a discussion of configuring and assigning asynchronous lines, see the *System Administrator's Guide, Volume II: Communication Lines and Controllers.*

Asynchronous lines can be assigned and unassigned with the ASSIGN and UNASSIGN commands.

Assigning Asynchronous Lines

To assign asynchronous lines, use the ASSIGN AYSNC command, as follows:

ASSIGN ASYNC -LINE *n* [*-TO z*]

n is the decimal number for the first line to be assigned and *z* is the decimal number of the last line to be assigned. All lines ranging from *n* through *z* are assigned as asynchronous lines.

Note

The ASSIGN ASYNC command assigns but does not configure an asynchronous line. Use the SET_ASYNC command to set or change the line configuration before assigning the line. See the *Operator's Guide to System Commands* and the *System Administrator's Guide, Volume II: Communication Lines and Controllers.*

Unassigning Asynchronous Lines

To unassign an asynchronous line, use the UNASSIGN ASYNC command, as follows:

UNASSIGN ASYNC -LINE *n* [*-TO z*]

n is the decimal number for the first line to be unassigned and *z* is the decimal number of the last line to be unassigned. All lines ranging from *n* through *z* are unassigned.

THE SPOOLER SUBSYSTEM

To allow users to print files at one or more printers in an orderly fashion, PRIMOS provides a Spooler subsystem. This subsystem, discussed in the *Operator's Guide to the Spooler Subsystem*, allows users to request that files be printed whenever a printer becomes available.

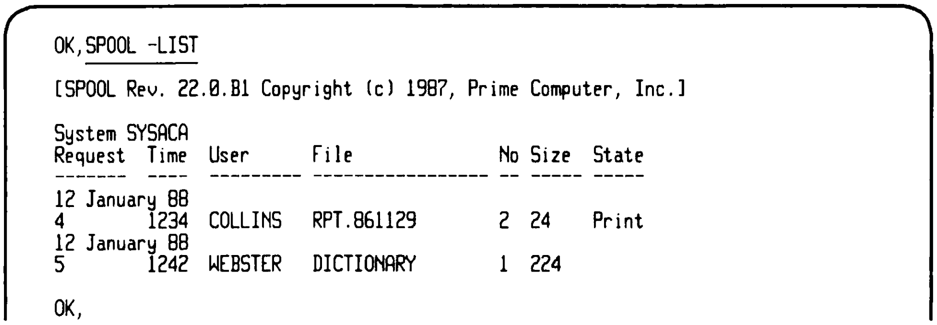
Read the *PRIMOS User's Guide* to understand how users apply the SPOOL command to issue print requests. The SPOOL command stores requests in the spool queue, where they wait until a printer has printed the files. When the requests are satisfied, they are removed from the spool queue.

Examining the Spool Queue

The contents of the spool queue are monitored with the following command:

SPOOL -LIST [*options*]

options include three levels of detail of the listing (-BRIEF, -DETAIL, and -FULL). The default is a brief listing as shown in the following example:



```
OK,SPOOL -LIST

[SPOOL Rev. 22.0.B1 Copyright (c) 1987, Prime Computer, Inc.]

System SYSACA
Request Time User      File              No Size  State
------- ---- --------- ----------------- -- ----- -----
12 January 88
4       1234 COLLINS   RPT.861129        2  24    Print
12 January 88
5       1242 WEBSTER   DICTIONARY        1  224

OK,
```

The default brief display gives the following information:

- The system name
- The time of the spool request
- The print request identification number
- The name of the user submitting the request
- The filename
- The number of copies (under the No column)
- The job size (number of copies times the file size in records)
- The state of the request or whether it is printing

If you specify the -ALL option, all queues in the local network are examined.

The following example shows the information given when you issue the -DETAIL option:

```
OK, SPOOL -LIST -DETAIL
[SPOOL Rev. 22.0.B1 Copyright (c) 1987, Prime Computer, Inc.]

System FOREST
Request  Time  User                             Copies  Size  State
-------- ----- -------------------------------- ------  ----- -------------
12 January 88
1         12:34  COLLINS                        1       24    Print
   File name   <TREE>BRANCH>TWIG
   Attributes  OS

12 January 88
10        12:42  WEBSTER                         1       224
   File name   <NEST>ROBIN>EGGS
   Attributes  OS

OK,
```

The more detailed listings give this additional information:

- A complete pathname of the spooled file
- Any attributes given explicitly or by default
- Any options included on the command line
- Whether the request is deferred to a later time

In the following example, a user has spooled a file, using the -ATT option to specify the attributes of the printer, the -ON option to specify a remote system, the -DEFER option to delay printing until 6:00 p.m., and the -NOTIFY option to receive notification that the file has finished printing. Use the 24-hour format with the -DEFER option to delay printing.

```
OK, SPOOL FLOWERS -ATT CARBON -ON DAISY -DEFER 1800 -NOTIFY
```

When you use the -DETAIL option to the SPOOL -LIST command, the spool queue information is displayed in a format similar to that shown below:

```
OK, SPOOL -LIST -ON DAISY -DETAIL

System DAISY
Request    Time   User                          Copies  Size  State
-------    ----   ----                          ------  ----  -----
133        11:26  CHARLES                       1       3
   File name   <FOREST>FLOWERS
   Attributes  CARBON
   Deferred until 18:00 on 09 February 88
   Options     -NOTIFY
OK,
```

Despooler Phantoms

Printers are controlled by phantoms. These phantoms use the ASSIGN command to acquire exclusive access to printers. For example, a phantom that prints on printer PR0 assigns device PR0. A phantom that controls a printer is called a **despooler phantom** because it runs a program called the despooler, which despools (takes out) file requests from the spool queue and sends them to the appropriate printer.

The despooler program periodically checks the spool queue to see whether any files are waiting to be printed. If so, the program starts to print one of them. When printing finishes, the program checks the spool queue again.

Printer Environments

Because many installations have more than one printer, the Spooler subsystem allows the System Administrator and the operator to control which files are printed on which printers. This specification is made by defining printer **environments.** Environments are defined in **environment files** and are usually set up by the System Administrator, but they may be set up by you or by a privileged user. Environment files reside in the SPOOL* directory.

An environment file defines the way in which any phantom using a printer will handle the files being printed. The definitions in the environment include

- Which line the phantom uses
- Which disks it searches for queued jobs
- The size of the jobs it may accept
- Which page margins it will use

By defining these attributes, the environment also defines the types of files the printer can handle. Thus, for example, one printer may accept only short files while another may print any file requiring extra-wide paper.

Whenever you start a despooler phantom with the PROP *environment-name* -START command, you select the environment it will use. You may change an environment at any time, but a printer may use only one environment at any given time.

Each environment on a system has a unique name. This name can contain a maximum of 16 characters, and can contain only the letters A through Z, the digits 0 through 9, and the special characters underscore (_), period (.), asterisk (*), pound sign (#), dollar sign ($), ampersand (&), dash (-), and forward slash (/). When a despooler phantom is started from the supervisor terminal, it takes the name of the environment file as its user name. A despooler phantom started from a user terminal takes the name of the user logged in at that terminal.

Remote Spool Queues

Many installations have more than one system in the network. Therefore, in addition to reading the spool queue on the local system, the Spooler subsystem is capable of searching all of the spool queues on the network, provided that the spool queues are Rev. 19.0 or later.

The commands in the environment file being used by the despooler phantom control access to remote spool queues by a despooler phantom. For details on configuring the queue search process, see the *Operator's Guide to the Spooler Subsystem.*

The PROP Command

The PROP command starts up or shuts down a despooler phantom. You can also use PROP to do other things, such as to suspend or continue a phantom, or stop printing the current file. You define printer environments using a text editor such as ED or EMACS.

When you use the PROP command to operate on a printer environment or a despooler phantom, specify the environment name on the command line. The name tells PROP the environment (despooler phantom) to which you are referring.

When a despooler phantom is running, it is said to be *controlling* a particular printer environment. To see which environments are running on your system, enter the PROP -STATUS command. It lists the currently active environments and displays an indicator of what each active environment is doing, as in this example:

```
OK, PROP -STATUS

[PROP Rev. 22.0 (c) Prime Computer, Inc., 1988]

TPBPR0         Stopping
TP.NPR         Hanging
TP.DBL         Idle
WHITE          Printing(DICTIONARY: page 74, copy 1 of 1)
LQP            Reset
OK,
```

In this example, the environment TPBPRO is stopping; TP.NPR is hanging and is waiting for a command before continuing; TP.DBL has no requests in the queues to print; WHITE is printing a file; and LQP is stopping and starting with a new environment. If an environment is stopped, it is not listed. To display inactive as well as active environments, use the -ALL option with the PROP -STATUS command.

Whenever you change the type of paper in a printer, stop the current environment, change the paper, and then start up a new printer environment. The new environment notifies the Spooler subsystem that a form change has been made and resets the despooler phantom to use the new environment. These steps prevent user files from being printed on the wrong paper.

See the *Operator's Guide to the Spooler Subsystem* for more information on using SPOOL and PROP and for more information on the Spooler subsystem.

User Print Requests

When users issue the SPOOL command to request that files be printed, they sometimes use the -ATTRIBUTE option to specify particular spooler attributes to be used. The Spooler subsystem matches the specified attributes to the list of accepted attributes for each environment being serviced. The phantom controlling the environment considers the file for printing only if the attributes specified by the user match attributes in that environment. If the user does not specify these attributes, the phantom uses the default attribute file, if it exists.

A user may spool a file that cannot be printed by any environment. This can happen either if the user specifies an invalid attribute, if the file is larger than a limit on file size that is specified in the environment, or if the environment is not running.

If a user reports that a file is not being printed, check the print request using SPOOL -LIST, and use PROP -DISPLAY to display the attributes for the environments on your system. To display the environments on other systems in the network, attach to the remote SPOOL* directory and use an editor to look at the environment files. This procedure tells you which environments are able to print the user's file. Environments may exist in which the request is eligible, but either these environments have no phantoms controlling them, or the phantoms may be printing other users' files. In this case, tell the user that the file will be printed later, when a printer becomes available.

It is also possible that no such environments exist; in that case, ask the user either to modify the print request by using the -MODIFY option of the SPOOL command, or to cancel the present request and spool the file again, using a valid combination of options and file size.

Operating Printers

In addition to overseeing the printers, you are usually responsible for

- Monitoring the spool queue with the SPOOL -LIST command. (See the *Operator's Guide to the Spooler Subsystem* and the *Operator's Guide to System Commands.*)
- Changing paper to print special forms requests. (Use the SPOOL -LIST command to see whether any such requests are outstanding. Schedule the printing of special forms for a specific time of day.)
- Reloading paper and ribbons in the printer as required.
- Vacuuming the printers frequently, as recommended in the documentation for the printer.
- Removing listings from the printer, separating them by user (banner name before each file), and placing them in a specified distribution area.

Plotters

In addition to queuing requests for printers, the Spooler subsystem is able to queue requests for plotters. Plotter environments are the same as printer environments, except that the device specified in a plot environment is a plotter or the PLOT command is used in the environment file. The user specifies attributes in the SPOOL command indicating that the file is to be plotted and not sent to a printer.

In a plotter environment, you or the System Administrator can specify whether the phantom controlling the environment should accept requests for both printers and plotters or for plotters only.

THE BATCH SUBSYSTEM

There are times when a user needs to do a large amount of computational processing. If the user performs this processing interactively at the terminal, he or she cannot begin any other tasks at that terminal until the processing is complete. Other users will notice a performance degradation, particularly if several users begin large computational jobs at once. In an extreme case, the system could spend a significant amount of time juggling these large jobs and less time actually performing them. In addition, the users would spend a significant amount of their time waiting for the jobs to finish.

To solve this problem, the Batch subsystem allows a user to submit a job into a queue. This **job** is a request to execute a command input (COMI) file or a CPL file. Frequently, the file submitted performs a large amount of processing. The Batch subsystem waits until other Batch jobs are finished before executing these new Batch jobs. The System Administrator sets up one or more Batch queues into which jobs may be submitted and defines the relative priorities of the queues. You monitor the Batch subsystem, and you may also be asked to prevent Batch jobs from executing during the peak hours of system usage.

Note

> Beginning at Rev. 21.0, the Batch subsystem must be an ACL-protected system; that is, BATCHQ must be an ACL directory.

Operator Responsibilities for the Batch Subsystem

The System Administrator is responsible for configuring the Batch subsystem and maintaining its database, as explained in the *Operator's Guide to the Batch Subsystem.* You are responsible for starting and stopping the Batch monitor when the system (or the Batch subsystem) is brought up or down, and for helping with users' jobs when necessary.

There are two main reasons for operator intervention in user jobs. If a job is holding up the queue (for example, because of an infinite loop or because the job is waiting for some unavailable resource), you can abort it. A user may ask you to hold a job in the queue until a particular resource becomes available, at which time you can release it.

In order for you to intervene in user jobs, you or the user logged in as SYSTEM must have the ACL group .BATCH_ADMIN$ assigned to you.

Batch Elements

The Batch subsystem consists of these elements:

- Jobs
- Queues
- The Batch monitor
- Batch phantoms

As noted previously, a user request to the Batch subsystem to execute a command file or a CPL file is called a job. This request is placed in a queue until it is honored by the **Batch monitor.** The Batch monitor honors the request by starting up a Batch phantom to process the job.

Every Batch job has a **job ID.** It consists of an **external name,** which is the name of the command file or the CPL file submitted by the user, and an **internal name,** which is assigned by the Batch subsystem to uniquely identify every job in the system. You use job IDs when you manipulate users' jobs. The System Administrator may define as many as 16 Batch queues, each with its own name and characteristics. Users who submit Batch jobs may specify the queues into which their jobs should be placed. If they do not specify queues, the job submission program automatically determines an appropriate queue for each job.

The program that actually starts up Batch jobs is called the Batch monitor. This program runs as a subsystem phantom. It is normally started up during system cold start, as part of the CMDNC0>PRIMOS.COMI file. The monitor also updates the queue when Batch phantoms log out, to show that the corresponding jobs are complete. The Batch monitor is always logged in as user BATCH_SERVICE.

To execute the requested command input (COMI) file or CPL file, the Batch monitor starts up a Batch phantom. This phantom is logged in with the same login name as that of the user who submitted the job, including the same project name and group names. Therefore, the Batch phantom has the same privileges as those enjoyed by the submitting user.

Batch Commands

Three essential commands in the Batch subsystem are

Command	*Function*
JOB	Submit, display, and control user jobs
BATCH	Start up, shut down, and display the state of the Batch monitor and subsystem
BATGEN	Define, modify, and delete Batch queues

In addition, two programs used by both the System Administrator and the operator are

Program	*Function*
INIT	Initialize the Batch database
FIXBAT	Repair and compress the Batch database

The use of these commands and programs by the operator is fully discussed in the *Operator's Guide to the Batch Subsystem* and in the *Operator's Guide to System Commands.* The use of the JOB, BATCH, and BATGEN commands by the user is discussed in the *Prime User's Guide* and the *PRIMOS Commands Reference Guide.* The use of the BATGEN command for the System Administrator and the operator is discussed in the *Operator's Guide to the Batch Subsystem.*

DISTRIBUTED SYSTEMS MANAGEMENT

Distributed Systems Management (DSM) is an integrated set of systems management facilities that you can use on networked and single systems. DSM commands can be invoked from any point on a network and they allow you to treat a network as a single administrative group. DSM commands and services are distributed to local and remote nodes through server processes that run on each system. These server processes are listed when you issue the STATUS USERS command or the SIM command LIST_PROCESS -TYPE SERVER. They are as follows:

- DSMSR
- DSM_LOGGER
- SYSTEM_MANAGER
- ISC_NETWORK_SERVER

Servers communicate with each other over the network through an inter-server communication mechanism, which is itself served by the ISC Network Server. DSM commands allow you to perform the following system administrative tasks:

- Administer event logging on all systems on the network
- Display system information for all nodes on the network
- Control remote systems from any terminal on the network

These three DSM functions are discussed in more detail in Chapter 7.

THE FILE TRANSFER SERVICE

File Transfer Service (FTS) allows users to request file transfers from one system in the network to another. Like Batch and Spooler, FTS accepts requests from users and queues them for execution. If one of the systems involved in the transfer is not up and running when the request is made, FTS attempts the transfer later.

FTS Elements

The File Transfer Service consists of the following elements:

- Requests
- Queues
- Systems
- FTS manager (YTSMAN)
- FTS servers

Users submit file transfer requests into request queues. These requests identify sites known to FTS as acceptable systems to which communication is possible. Refer to Figure 6-1, which illustrates how the FTS servers accomplish file transfers between two systems on a network.

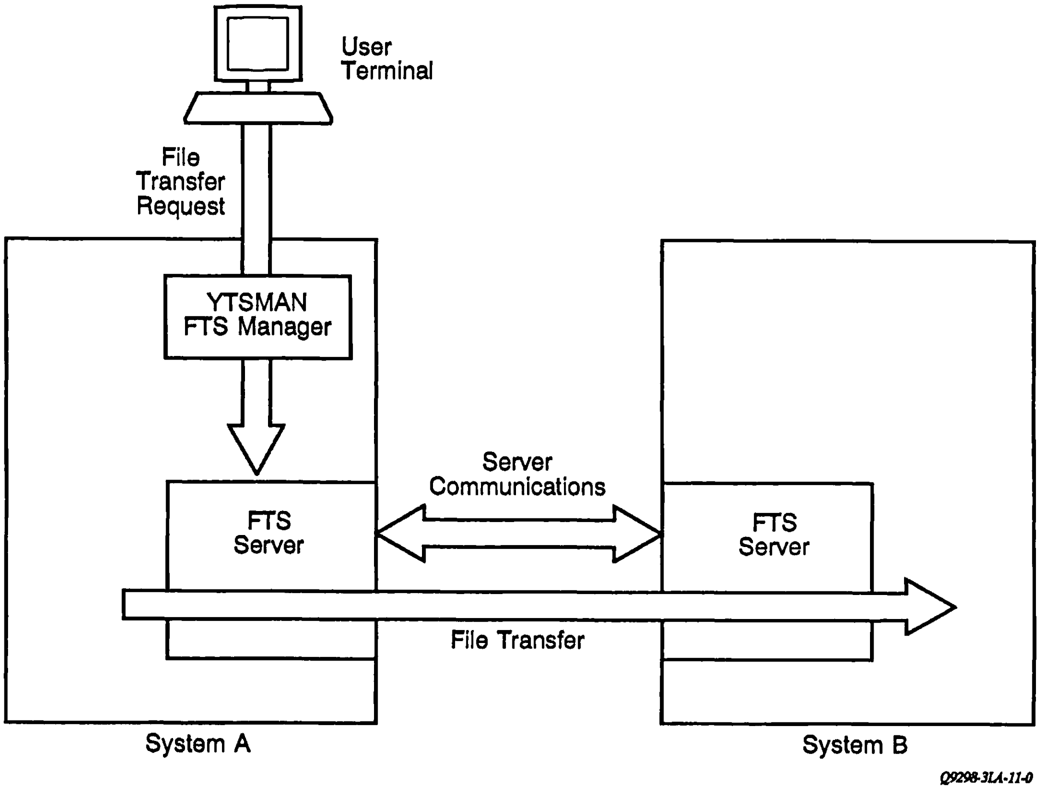


FIGURE 6-1. The File Transfer Service

When communication lines are open and not busy, the **FTS manager** (YTSMAN) chooses a request and passes it to an FTS server. The **FTS server** (FTP) performs the transfer by communicating with another FTS server on a remote node. The two servers pass the file data over the communications path; they also pass status information to ensure the correct transmittal of the file.

When the servers have completed the transfer, the FTS server that sent the file transfer reports back to that system's FTS manager. The request is then removed from the queue.

FTS Commands

Three FTS commands are available to you:

Command	*Function*
FTR	Submit, display, and control file transfer requests
FTOP	Start up, shut down, display, and control FTS servers and the FTS manager
FTGEN	Configure FTS queues and sites

Users can use only the FTR command. You and the System Administrator can use all three commands.

Operator Responsibilities for FTS

You are responsible for monitoring all aspects of the File Transfer Service, including the following:

- Ensure that File Transfer servers and the File Transfer manager are in operation.
- Monitor user requests.
- Monitor and archive FTS system log files.
- Make sure the FTSQ* directory has enough room to accommodate users' files.

Your responsibilities when you work with the File Transfer Service are discussed in detail in the *Operator's Guide to Prime Networks.*

Periodically, you should inspect the FTSQ* directory. The exact contents of this directory depend upon how your System Administrator has configured the FTS system. The directory contains log files that record the activity of each FTS server. Set the names of the log files in the queue and site configurations using the FTGEN command. Because these files have no limit as to their size, they may grow to such size that the FTSQ* directory no longer has room to hold copies of files being transferred for users. Therefore, log files should be periodically reviewed and archived to offline storage.

THE PRIMENET NETWORK

This section outlines the operational tasks required to maintain your system as a node in a PRIMENET network. Two categories of tasks are discussed:

- Using the ADDISK and SHUTDN commands
- Communicating with operators on other systems

At some installations, system operators also perform network-related tasks that are normally described as System Administrators' duties. For example, operators may configure the network or maintain network security. For information on these networking tasks, as well as descriptions of the various kinds of communications lines that PRIMENET supports, refer to the *PRIMENET Planning and Configuration Guide.* See the *User's Guide to Prime Network Services,* for an introduction to PRIMENET. For additional background information, see the *Operator's Guide to Prime Networks.*

Adding and Shutting Down Remote Partitions

As a system operator, you may be responsible for the following tasks:

- Starting up remote partitions on your system, using the ADDISK command
- Shutting down remote partitions on your system, using the SHUTDN command

The ADDISK and SHUTDN commands are used for both local and remote partitions. These two commands can be used only at the supervisor terminal. They are described in the *Operator's Guide to System Commands.* The information on ADDISK and SHUTDN in this chapter is of particular importance to operators of networked systems.

In order for a process on your system to access a remote partition, the following must occur:

- The remote system must be configured so that your system can see it.
- The operator on the remote system must use ADDISK to start up the partition on that system.
- You must start the remote partition on your system, using the ADDISK command.

The order in which these two operations are performed is unimportant. However, keep in mind that a partition that is not started up on its own system cannot be accessed by any other network node.

Remote File Access (RFA): RFA (formerly FAM II) allows users to access files and directories that reside on partitions connected to other nodes in the network, instead of being limited to the local system partitions only.

At Rev. 19.3 and beyond, PRIMOS supports only RFA. If your system is networked to a system running an older version of PRIMOS that uses FAM I, you must upgrade that system to use RFA in order for the two systems to communicate.

Adding Remote Partitions (ADDISK): ADDISK adds a specified partition name residing on a specified network node to the local logical device list. There is no check on the status of the remote node (running or not running) or on the existence of the partition. Thus, you need not wait until a remote node comes up in order to add one of that node's partitions.

When you add a partition with ADDISK, the partition name appears in the list on your system when you invoke the STATUS DISKS command. Because there is no check on the status of the remote system or on the existence of the partition, you cannot assume that every partition on the STATUS DISKS list has been started up and is accessible at this time. You must attempt to attach to a partition if you wish to confirm that the remote link and system are up and that the partition does exist.

When a remote partition is added, its physical device number does not appear on the STATUS DISKS list as does the physical device number of local partitions. Instead, its logical device number appears in the list.

Remotely added partitions acquire the write-protection status assigned to them on their local systems.

Shutting Down Remote Partitions (SHUTDN): SHUTDN removes a remote partition from the local list of logical partitions. Use of the SHUTDN command on a remote partition affects only local users of that partition; it does not affect any other users of that partition on the network. The remote partition is disconnected from the local system.

Communicating With Operators on Other Nodes

As a system operator, you may occasionally have to communicate with an operator on another node of your network. For example, you may need to confer concerning the accessibility of partitions between your systems. One way to contact other operators is with the MESSAGE command. For example, to send a message to the operator on system SYSA, you would issue the following command:

```
OK, MESSAGE -1 NOW -ON SYSA
Hi Marty, what's wrong with your PAYROL disk - can't attach to it!
OK,
```

For an explanation of the MESSAGE command, refer to Chapter 5, The User Community. See also the *Operator's Guide to System Commands.*

Note

> Remember not to use the terminal's kill character in the message. The default kill character is the question mark (?). Use the TERM -DISPLAY command to determine the kill character.

NETWORK TERMINAL SERVICE

Network Terminal Service (NTS) connects asynchronous terminals and other devices to 50 Series hosts over a Local Area Network (LAN), and provides connection management as well as normal PRIMOS terminal services. NTS terminals are not connected directly to any Prime host. They are connected to the LAN by a microprocessor-based LAN Terminal Server 300 (LTS). A set of LTS commands permits the terminal user to maintain a connection to any Prime host on the LAN.

NTS consists of three separate software components:

- PRIMOS at the host level
- The LAN Host Controller (LHC), which serves the LAN cable and its connected devices for the host
- The LAN Terminal Server (LTS), which connects your terminal to the LAN cable

The LHC is a standard Prime circuit board that links the 50 Series host to the LAN cable. The LTS is a standalone piece of equipment with its own microprocessor that connects up to eight asynchronous devices, such as terminals and serial printers, to the LAN. The devices are connected to the LTS and the LTS is connected to the LHC via the LAN cable.

You can determine if the Network Terminal Service is in operation by issuing the STATUS USERS command. The server phantom for NTS is listed in the output as NTS_SERVER, and the LAN Server is listed as a kernel process, as shown in the display in Chapter 5.

For more detailed information, see the *Operator's Guide to Prime Networks* and the *NTS User's Guide.*

NTS Features and Services

The NTS user commands allow users to examine the list of available NTS network hosts, connect to the host of their choice, log in and tailor terminal session characteristics, and use a variety of help facilities. In addition, these commands allow you, as an operator, to use the Network management facilities. These services are in addition to the normal PRIMOS asynchronous services that users can access across the LAN once they establish an NTS connection and log in to a specific Prime host. The following types of NTS commands allow you and users to use these basic NTS features and services.

- LTS connection, parameter control, and help commands
- NTS operator and user commands

NTS Monitoring and Management

A set of programs provides network monitoring and management services. Operators use these programs for NTS startup, monitoring and maintenance, and fault isolation. These programs consist of LTS downline load and upline dump, error and event reporting, statistics gathering, status commands, and a diagnostic loopback capability. The LTS downline load configures the terminal lines for NTS operation. The error and event reporting function logs errors and significant events to a single log file or to an operator's terminal within the network for diagnostic and periodic review. The loopback capability permits isolation of physical links responsible for network failures.

The commands that you use for these purposes, and which are discussed in the *Operator's Guide to Prime Networks*, are

- COMM_CONTROLLER
- START_NTS
- STOP_NTS
- SET_ASYNC

- LAN300 commands
- SIM commands

COMM_CONTROLLER: This command, with its five subcommands and options, allows you to do the following without having to warm start or cold start the system:

- Start up or shut down an ICS controller
- Downline load an ICS controller or an LHC or an LTS
- Upline dump the memory image of an LHC or an LTS to a disk file
- Verify the integrity of an ICS controller

START_NTS: Use this command to start NTS terminal activity for a Prime host node on the LAN. The START_NTS command requires a configuration file created by the network terminal configuration utility, CONFIG_NTS. In addition to starting NTS, START_NTS also initializes and starts the LAN300 network management services that are required for proper operation of NTS.

You can issue START_NTS at any time. Normally, START_NTS is part of the Prime system startup procedure. The System Administrator includes START_NTS in the system startup file, PRIMOS.COMI.

STOP_NTS: You can interrupt an NTS operation on a particular 50 Series host at any time, without interrupting any other host operations, by issuing this command. You can then change the network configuration or downline load any devices that the user might want, and then restart network operation using the START_NTS command. The ability to stop the network and reconfigure devices allows users to make changes to the LAN without shutting down the entire system.

SET_ASYNC: Use this command to configure loginable lines and assignable lines for NTS operation. Although primarily used by operators, it can be used by any knowledgeable user on that user's line.

LAN300 Commands: **LAN300 Network Management** is a collection of programs that serves two purposes for NTS:

- It provides network management functions such as LTS downline load, LTS naming and addressing, network monitoring, and event logging.
- It provides support functions to users including LTS status commands and diagnostic test commands.

The downline load function includes a set of programs to monitor the operating system of the terminal servers. Monitoring at initialization provides immediate operator notification of nonrecoverable faults. During normal operation, there is continuous monitoring by polling at five-second intervals for automatic fault detection and recovery. Summary statistics of these LAN300 operations are stored for periodic review. LAN300 also maintains a comprehensive set of performance statistics.

SIM Commands: The System Information and Metering (SIM) commands retrieve and display various amounts of information pertaining to a wide variety of network functions. The SIM commands are discussed in Chapter 7, Monitoring Your System.

7

MONITORING YOUR SYSTEM

PRIMOS provides these eight methods for monitoring your system:

- Performance measurement
- Event logging
- Supervisor terminal messages
- The Security Audit facility
- Tape dumps
- System status reports
- System information and metering
- The RESUS environment

MEASURING PERFORMANCE

At Rev. 22.0 you can use two methods to monitor the performance of your system:

- The USAGE command
- The PRIMON and PRIMAN commands

The USAGE command, which is described in detail in the *Operator's Guide to System Monitoring*, displays a measured sample of system performance. This tool is especially useful for determining the degree to which individual users and processes are using system resources and thus affecting system performance.

The PRIMON (PRIMOS Monitor) utility collects system metering information at intervals specified by the user. You can use PRIMON to present this information in one of two ways:

- An on-screen, dynamic display of system usage
- A file into which the data is read for later analysis

The PRIMON utility is discussed in more detail further on in this chapter.

The PRIMAN (Prime Analysis) utility can generate five different kinds of reports that are based on the data gathered and read into a file by PRIMON. Refer to the *PRIMAN User's Guide* for specific information about the PRIMAN utility.

The USAGE Command

The USAGE command allows operators and users to monitor several performance factors of PRIMOS operation. Both manual and automatic sampling modes are available, as are brief and long forms of display. In addition, you can use the USAGE command to monitor remote systems, as long as the remote system is running at Rev. 19.3 or later. These three types of usage sampling are described in the sections that follow. An example of a USAGE report is shown in Figure 7-1.

Automatic Sampling: Automatic sampling allows any user to observe system performance at equal sampling intervals. The USAGE program automatically times each interval, as specified by the user, and displays new information at the end of each interval.

Manual Sampling: Manual sampling allows any user to choose each sample interval individually. The intervals do not have to be identical.

With manual sampling, USAGE displays a prompt when you first invoke it. Thereafter, USAGE takes and displays a sample each time you enter a START command. After each sample is taken, USAGE pauses and returns you to command level, allowing you to enter other commands.

Remote Sampling: Remote sampling allows you to sample a remote node. You can request either the long or brief displays of USAGE output and choose either automatic or manual sampling. The remote system must be configured for RFA and RFA-enabled and must be running at Rev. 19.3 or later.

Interpreting USAGE Reports: USAGE is a diagnostic tool for determining where the problem is when system performance seems lower than normal. There are three major resources in a Prime system: the CPU, the disks, and memory. Any of these can cause performance problems. Systems experiencing bottlenecks are described as CPU-bound, I/O-bound, or memory-bound, respectively. The USAGE reports contain information pointing to specific symptoms to aid you in diagnosing the bottleneck. The interpretation of these reports is discussed in the *Operator's Guide to System Monitoring.*

Using the PRIMON Utility

Both the PRIMON utility and the PRIMAN analysis tool are separately priced products and are discussed fully in the *PRIMAN User's Guide.*

You may use PRIMON to observe current system activity or to collect data on system activity over a time period for submission to PRIMAN to generate reports. To invoke PRIMON, use the PRIMON command at a video display terminal (VDT). A number of options are available to control the display and to specify the sampling criteria. If you do not use any of the options, you are queried for your terminal type. After you enter your terminal type, PRIMON samples the system, displays the sampled information using the screen display default values, and continues to sample and display system information every 10 seconds. To stop PRIMON, enter a Q (quit).

A typical PRIMON screen display is shown in Figure 7-2.

SYSTEM AND NETWORK EVENT LOGGING

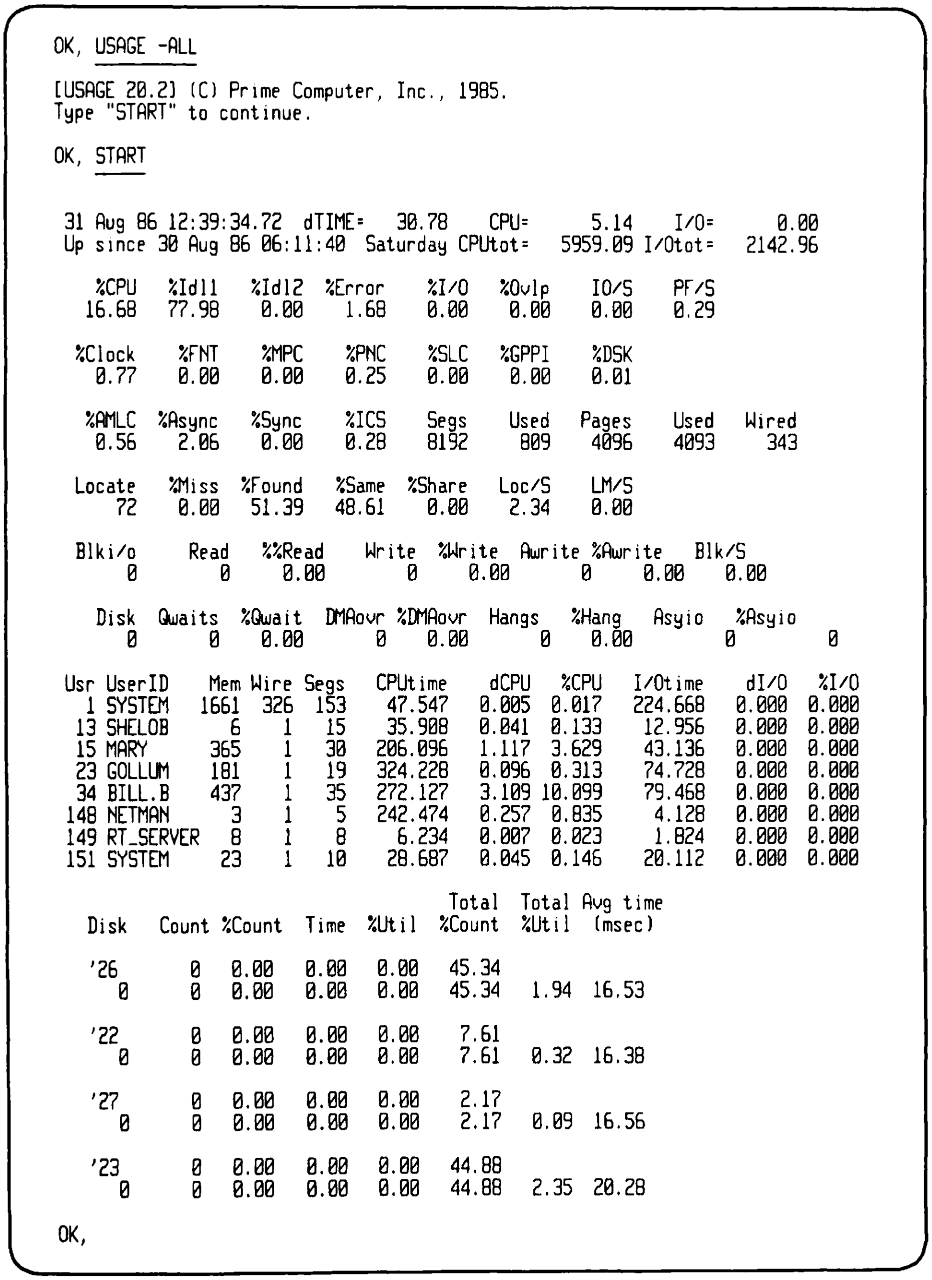
Each Prime computer running PRIMOS at Rev. 21.0 or later contains a Distributed Systems Management (DSM) logging mechanism that records information about significant system events, such as cold starts and warm starts, machine checks, and disk errors in a log file. This service has a facility for logging DSM messages in private or system logs anywhere on the network, along with utilities for administering and displaying those logs. For more information on DSM logging, refer to the *DSM User's Guide* and the *System Administrator's Guide, Volume III: System Access and Security.*

Starting DSM Logging

You start the DSM logging mechanism with the START_DSM command. START_DSM is normally included in the PRIMOS.COMI file, but it can be issued at any time. You should issue it prior to the START_NET command so that all network messages are logged. For more details on the START_DSM command and its options, refer to the *Operator's Guide to System Commands* and the *DSM User's Guide.*

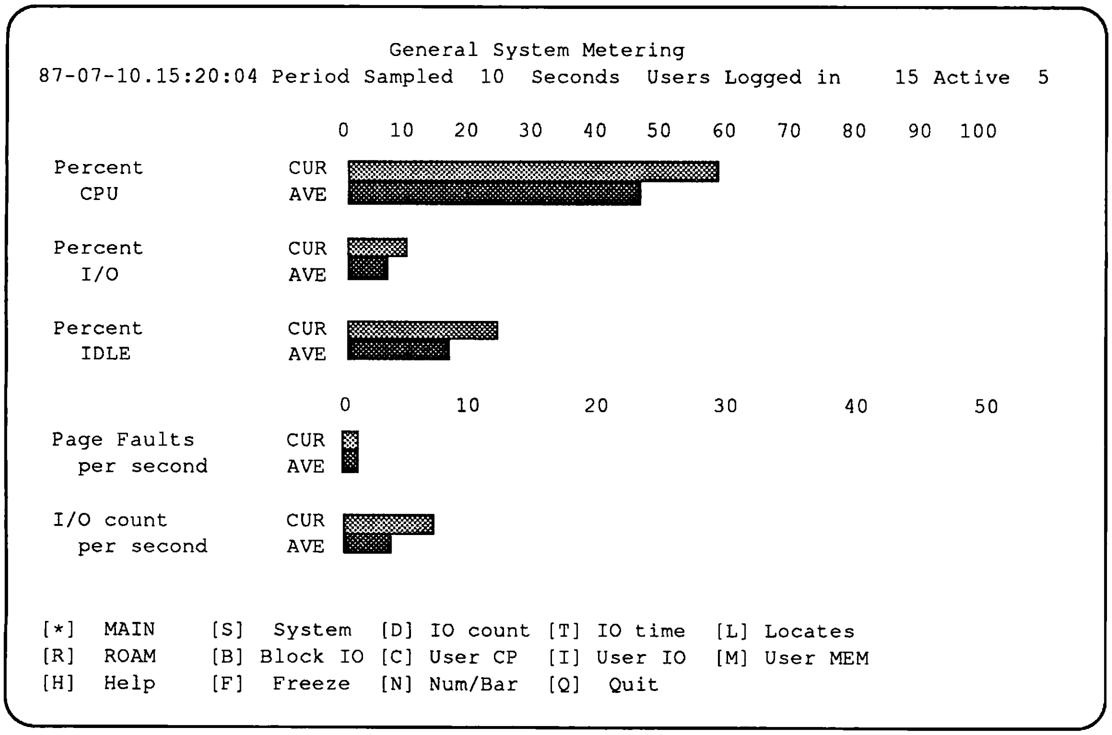
Storing Event Logs

System event logs are kept in the directory DSM*>LOGS>PRIMOS. Network event logs are kept in the directory DSM*>LOGS>NETWORKS. There is a single log file for system events and another for network events. Messages are appended continually to the appropriate file.



```
OK, USAGE -ALL

[USAGE 20.2] (C) Prime Computer, Inc., 1985.
Type "START" to continue.

OK, START


 31 Aug 86 12:39:34.72  dTIME=   30.78    CPU=      5.14    I/O=      0.00
 Up since 30 Aug 86 06:11:40  Saturday CPUtot=   5959.09 I/Otot=   2142.96

    %CPU   %Idl1   %Idl2  %Error    %I/O   %Ovlp    IO/S    PF/S
   16.68   77.98    0.00    1.68    0.00    0.00    0.00    0.29

  %Clock    %FNT    %MPC    %PNC    %SLC   %GPPI    %DSK
    0.77    0.00    0.00    0.25    0.00    0.00    0.01

   %AMLC  %Async   %Sync    %ICS    Segs    Used   Pages    Used   Wired
    0.56    2.06    0.00    0.28    8192     809    4096    4093     343

  Locate   %Miss  %Found   %Same  %Share   Loc/S    LM/S
      72    0.00   51.39   48.61    0.00    2.34    0.00

  Blki/o     Read   %%Read    Write   %Write Awrite %Awrite   Blk/S
       0        0     0.00        0     0.00       0     0.00    0.00

    Disk  Qwaits  %Qwait  DMAovr %DMAovr  Hangs   %Hang   Asyio   %Asyio
       0       0    0.00       0    0.00       0    0.00         0         0

 Usr UserID     Mem Wire Segs   CPUtime    dCPU   %CPU   I/Otime    dI/O   %I/O
   1 SYSTEM    1661  326  153    47.547   0.005  0.017   224.668   0.000  0.000
  13 SHELOB       6    1   15    35.908   0.041  0.133    12.956   0.000  0.000
  15 MARY       365    1   30   206.096   1.117  3.629    43.136   0.000  0.000
  23 GOLLUM     181    1   19   324.228   0.096  0.313    74.728   0.000  0.000
  34 BILL.B     437    1   35   272.127   3.109 10.099    79.468   0.000  0.000
 148 NETMAN       3    1    5   242.474   0.257  0.835     4.128   0.000  0.000
 149 RT_SERVER    8    1    8     6.234   0.007  0.023     1.824   0.000  0.000
 151 SYSTEM      23    1   10    28.687   0.045  0.146    20.112   0.000  0.000

                                      Total  Total Avg time
   Disk   Count %Count  Time  %Util  %Count  %Util  (msec)

   '26       0   0.00   0.00   0.00   45.34
      0      0   0.00   0.00   0.00   45.34   1.94  16.53

   '22       0   0.00   0.00   0.00    7.61
      0      0   0.00   0.00   0.00    7.61   0.32  16.38

   '27       0   0.00   0.00   0.00    2.17
      0      0   0.00   0.00   0.00    2.17   0.09  16.56

   '23       0   0.00   0.00   0.00   44.88
      0      0   0.00   0.00   0.00   44.88   2.35  20.28

OK,
```

FIGURE 7-1. Sample USAGE Output



```
                         General System Metering
87-07-10.15:20:04 Period Sampled  10  Seconds  Users Logged in    15 Active  5

                              0   10   20   30   40   50   60   70   80   90  100
 Percent             CUR
   CPU               AVE

 Percent             CUR
   I/O               AVE

 Percent             CUR
   IDLE              AVE

                              0          10         20         30         40         50
 Page Faults         CUR
   per second        AVE

 I/O count           CUR
   per second        AVE


[*]  MAIN     [S]  System  [D] IO count [T] IO time  [L] Locates
[R]  ROAM     [B] Block IO [C] User CP  [I] User IO  [M] User MEM
[H]  Help     [F]  Freeze  [N] Num/Bar  [Q]  Quit
```

FIGURE 7-2. PRIMON Screen Example

Administering and Controlling Event Logs

You can administer DSM logs using the DSM log management utility ADMIN_LOG. Use ADMIN_LOG to

- Create DSM logs
- Define and modify DSM log attributes
- Perform file maintenance tasks such as purging and deleting

Printing and Displaying Event Logs

The command DISPLAY_LOG replaces the pre-Rev. 21.0 commands PRINT_SYSLOG and PRINT_NETLOG. Use DISPLAY_LOG to

- Select messages from logs according to particular criteria
- Display the messages in various formats

You should write the buffer containing the DSM messages to a disk file from time to time by using the DISPLAY_LOG command.

SUPERVISOR TERMINAL MESSAGES

Many problems encountered by users, by PRIMOS, and by other parts of the system cause messages to be sent to the supervisor terminal. As the system operator, you are responsible for observing these messages and taking appropriate action.

These messages can be categorized as follows:

- VCP or Diagnostic Processor messages. (See the handbook for your CPU.)
- User requests (discussed in Chapter 6, System Resources).
- Magnetic tape assignment requests (discussed in Chapter 6).
- Batch messages. (See the *Operator's Guide to the Batch Subsystem.*)
- Spool messages. (See the *Operator's Guide to the Spooler Subsystem.*)
- FTS messages. (See the *User's Guide to Prime Network Services.*)
- Disk error messages. (See the *Operator's Guide to File System Maintenance.*)

If you are unsure about the meaning of a message, contact your System Administrator for assistance.

If You Use a Video Display Unit as a Supervisor Terminal

On some systems, the supervisor terminal is a Video Display Unit (VDU) rather than a hard-copy terminal. VDU terminals do not automatically produce a printed copy of operator commands and system messages; therefore, you should maintain a COMOUTPUT file as a record.

You or your System Administrator should insert the appropriate COMOUTPUT command into the system startup file PRIMOS.COMI (or C_PRMO). You should spool and delete this file about once a day to limit its size.

For more information on using a VDU as a supervisor terminal, see the *Operator's Guide to System Monitoring.*

Informative Messages

Most of the messages that appear at the supervisor terminal are meant to inform you of changes in system status. In general, these messages do not indicate problems that require your immediate attention.

THE SECURITY AUDIT FACILITY

Prime offers a separate audit trail subsystem that allows the System Administrator to verify the security of the system. The audit subsystem is fully described in the *System Administrator's Guide, Volume III: System Access and Security.*

The audit subsystem is the means through which the System Administrator examines security-related events and enforces user accountability. It includes these features:

- The Audit Collection facility
- The Audit Reporting facility
- The Audit Trail Backup facility
- The Crash Audit Recovery facility

The Audit Collection Facility

The **Audit Collection facility** audits the occurrence of selected events while the system is running and records them on either disk or tape. This facility enables data records, called **audit trails**, to be recorded in an audit file. Each audit trail is a record of specific security-related events that have occurred over a designated period of time. By examining an audit file, you can detect security violations and determine who is committing the violations. Also, you can create audit trails for selected events and selected users.

The interface to the audit collection mechanism is the SECURITY__MONITOR command. This command can be issued only from the supervisor terminal or by the System Administrator. SECURITY__MONITOR has options to

- Start and stop the monitor
- Select users, events, and event types to be audited
- Manage the audit file

The Audit Reporting Facility

The interface to the Audit Reporting facility consists of two commands: SECURITY__STATUS and PRINT__SECURITY__LOG.

The SECURITY__STATUS command provides information on the status of the security monitor. This command can be issued only from the supervisor terminal or by the System Administrator.

The PRINT__SECURITY__LOG command presents the data collected in an audit file that is no longer open for audit collection.

The Audit Trail Backup Facility

Within this facility, the TRANSFER__LOG utility allows the System Administrator to back up a number of separate audit trails to magnetic tape. The System Administrator also uses TRANSFER__LOG to recover audit files from magnetic tape.

The Crash Audit Recovery Facility

This facility enables the completion of a partially written security audit file after a system halt. The CRASH__AUDIT utility starts the actual recovery of audit trails. CRASH__AUDIT ensures that system buffers holding audit trails are written to an audit file if the system crashes.

Activate the Crash Audit Recovery facility by ensuring that

- A RINGO.MAP file is maintained on the system in the directory LOAD__MAPS*. (Maps for revisions of PRIMOS previous to Rev. 22.0 may exist in either PRIRUN or MAPs.)
- You start a tape dump after every unplanned system halt, before you perform a cold start of the system. See your CPU handbook for tape dump directions.
- After the system is cold started, submit the tape dump to the CRASH__AUDIT utility.

TAPE DUMPS

The monitoring methods mentioned above are useful while the system is running. If the system crashes, however, it is important that data in memory is collected on tapes for analysis.

To write all of memory out to tape, you can perform a **full tape dump**. When the system halts, issue two VCP commands: RUN 775, which uses tape drive MT0, and RUN 776, which uses tape drive MT1. Refer to the handbook for your CPU for more detailed instructions about performing a complete tape dump.

Because physical memory is getting larger, tape dumps can take a long time. Thus, it is now possible for you to get a **partial tape dump** by using the VCP command RUN 777. On some systems, you may also use the VCP command PARTIAL_TAPEDUMP. (Check the handbook for your CPU to determine which VCP command to use.)

Operator Commands for Specifying Additional Memory

When you use the RUN 777 command, specific segments are dumped to tape, as defined by the default values and by operator commands. Four operator commands allow you to specify additional memory to dump at the next RUN 777 command. These commands, which can be issued only from the supervisor terminal, are

- DUMP_SEGMENT
- DUMP_USER
- LIST_DUMP
- RESET_DUMP

DUMP_SEGMENT: This is an internal command that specifies which segments for all users are written to tape during a partial tape dump. The segments must be specified by their octal numbers. You may specify a maximum of 10 segment numbers on each command line.

DUMP_USER: This is an internal command that specifies which users will have all their segments 4000_8 through 7777_8 written to tape during a partial tape dump. You can specify a maximum of 10 user IDs on each command line.

LIST_DUMP: This is an internal command that displays the current parameters for a partial tape dump. These parameters are always the default parameters plus those added by the DUMP_SEGMENT and DUMP_USER commands.

RESET_DUMP: This is an internal command that resets the parameters for a partial tape dump to the default. The default is that the following segments are written to tape during a tape dump:

- Segments 0_8 through 1777_8 (the operating system)

RESET_DUMP: This is an internal command that resets the parameters for a partial tape dump to the default. The default is that the following segments are written to tape during a tape dump:

- Segments 0_8 through 1777_8 (the operating system)
- Segments 6000_8 through 6003_8 for all users
- Segments 4000_8 through 7777_8 for the process that is actively using the CPU at the time of the halt

You can add to the default values with the DUMP_SEGMENT and DUMP_USER commands. The LIST_DUMP command displays the current values.

Example of Tape Dump Commands

The four commands described above have a -HELP option to display their syntax. You can also enter the HELP command followed by one of the above commands to get a brief discussion of the command's operation. These commands and their options are described in the *Operator's Guide to System Commands.*

Here is an example using DUMP_SEGMENT, DUMP_USER, and LIST_DUMP.

```
OK, DUMP_SEGMENT -RANGE 4000 4004

OK, DUMP_USER NETMAN

OK, LIST_DUMP

Partial Tape Dump Parameters

Dump Segments For All Users

From      To

   0      1777
6000      6003
4000      4004

Dump User Segments

NETMAN
OK,
```

In addition to the default segments (0_8 through 1777_8, 6000_8 through 6003_8 and 4000_8 through 7777_8 for the active process), all user segments 4000_8 through 4004_8 and all of NETMAN user segments are to be dumped at the next partial tape dump. If you subsequently use the RESET_DUMP command, only the default segments would be dumped at the next RUN 777 command.

SYSTEM STATUS REPORTS

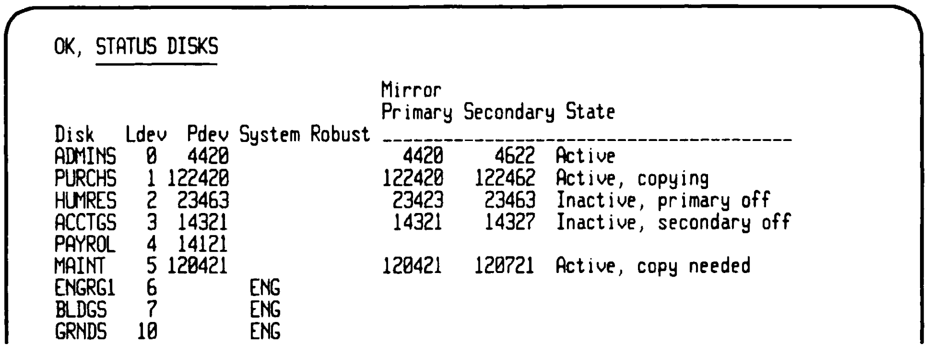
The STATUS command, described in the *Operator's Guide to System Monitoring*, allows you to monitor the status of the system. It allows you to answer such questions as

- Is anyone using the system? (This is useful when the system is about to be shut down.)
- Is anyone using a partition that is about to be backed up or shut down?
- Which partitions are currently started?
- Which user is using which terminal?
- Which tape drives are in use and by whom?
- Which remote users, phantoms, and slave processes are using the system?
- How are the system's communications controllers configured?

STATUS allows you to monitor the state of the system before you start any system operation. You can then make sure that users who may be affected by a system operation are warned before the process is started.

By specifying options to the STATUS command, you can obtain information on logged-in interactive users, active devices, active disks, network status, system status, open file units, and so on.

For example, when you specify the DISKS option, the system displays partition names, logical and physical device numbers, and node names of all currently started disk partitions, as shown in the following example. Also, STATUS DISKS displays information on mirrored and robust partitions.



```
OK, STATUS DISKS

                                Mirror
                                Primary Secondary State
Disk   Ldev  Pdev System Robust ----------------------------------------
ADMINS   0   4420                  4420      4622 Active
PURCHS   1 122420                122420    122462 Active, copying
HUMRES   2  23463                 23423     23463 Inactive, primary off
ACCTGS   3  14321                 14321     14327 Inactive, secondary off
PAYROL   4  14121
MAINT    5 120421                120421    120721 Active, copy needed
ENGRG1   6         ENG
BLDGS    7         ENG
GRNDS   10         ENG
```

The DSM SIM commands also allow you to monitor the status of the system. See the discussion of these commands in the section entitled System Information and Metering later in this chapter.

An Example of the STATUS ALL Command

When given from the supervisor terminal, the STATUS ALL command displays all the system information shown in the following example. Although this information is displayed in one piece, it is broken into sections here for ease of explanation.

System Identification: This section shows the system name, the version of PRIMOS currently in use, the copyright notice for PRIMOS, and the size of main memory in kilobytes.

```
OK, STATUS ALL

System ACCTNG is currently running PRIMOS rev. 22.0
Copyright (c) Prime Computer, Inc., 1988
8192K bytes memory in use
```

Open File Information: This section displays the name of the user and the local system name. At the supervisor terminal, the user ID is always SYSTEM, followed by the local system name (in this case ACCTNG). A list of all open file units is also displayed. (The COMOUTPUT file PRIMOS.COMO is open.)

```
User SYSTEM                        ACCTNG

File  File      Open File
Unit  Position  Mode Type  RWlock  Treename
COMO  000009650    w  DAM   NR-1W  <PLEIST>CMDNC0>PRIMOS.COMO
```

Device Information: This section lists the magnetic tape devices currently assigned. The Device column lists the physical device number. The User name column gives the user ID of the user to whom the device is assigned. The Usrnum column gives the user number. The Ldevice column lists the logical device number assigned by the user to the physical device (using the -ALIAS option of the ASSIGN command). If the user did not assign a logical number, the number listed under Ldevice the same as that under Device.

```
Device User name                    Usrnum Ldevice
MT0    SYSTEM                        1     MT0
MT1    GEORGE                       22     MT7
```

Communication Controller Information: This section lists the communications controllers. The Controller column displays the name of the controller such as AMLC, ICS1, ICS2, ICS3, MDLC, or LHC300. The Type column identifies the controller by type such as DMQ (AMLC controllers), downline load file number (ICS controllers), or PROM-set ID number (MDLC). The Device Address column gives the device address in octal. The Total-Lines column displays the total number of asynchronous and synchronous lines, including inoperable lines. The Bad-Lines column lists the number of failed lines.

```
                         Device    Total-Lines        Bad-Lines
Controller   Type        Address   Async      Sync    Async      Sync

ICS2         F-01        10        32         0       0          0
MDLC         5646        50        0          4       No Information
AMLC         DMQ         52        16         0       No Information
AMLC         DMQ         53        16         0       No Information
AMLC         DMQ         54        16         0       No Information
```

Active Partition Information: This section lists the partitions currently started up. The Disk column displays the name of the partition (also the name of the DSKRAT file). The Ldev column lists the logical device number associated with the physical device by the ADDISK command. You can add a maximum of 238 partitions (0 through 355_8) to a system. Logical device 0 must be the command device. The paging partitions are not necessarily included in this list if users cannot directly access them (see Paging Partition Information, below). The Pdev column lists the physical device number indicating the drive unit, controller, partition size, and offset. (See the *Operator's Guide to File System Maintenance.*) A blank space indicates that the partition is on a remote system. The System column lists the network node on which the partition is physically mounted; a blank means that it is mounted on the local system.

```
                                    Mirror
                                    Primary Secondary State
Disk    Ldev  Pdev   System Robust  ---------------------------------------
PLEIST   0    2460                    2460      2462  Active
OLIGOC   1   51460          Robust   51460     51462  Active,copying
PRECAM   2    3022
HOLOCN   3   61022          Robust   61022     61020  Inactive, primary off
PLIOCN   4  101022
ORDOVI   5           TEK2
SILUR    6           MKTG
DEVON    7           MKTG
PERMI   10           MNFG.A
JURI    11           MNFG.B
  .      .             .
  .      .             .
  .      .             .
LIBRY  353           ADMIN
ACCTG  354           ADMIN
PAYROL 355           ADMIN
```

Semaphore Information: This section gives semaphore information. Semaphores with negative numbers are reserved for and used by PRIMOS and its utilities; semaphores 1 through 64 are numbered semaphores (no access control); semaphores 65 and above are named semaphores to which numbers have been assigned, and the user number of users who have access to the semaphores. (See the *Subroutines Reference Guide, Volume III* for details on named and numbered semaphores.)

```
Sem. Value  Users
---- ------ -----
- 32      1
- 16 177777
- 15      1
  65      0   1
  66      1 143
  67      1 142
  68      1 141
   .      .   .
   .      .   .
   .      .   .
 120      0 141
 121      0 141
 122      0   1
 123      0 141
```

Network Information: Under PRIMOS, multiple network types can be in operation simultaneously. This section indicates those types currently in use. The node name is given along with the state of that node, either Up (in operation) or Down (not in operation). The local node is indicated by four asterisks (****).

```
Full duplex network

     Node       State
   ACCTNG       ****
   MX.B          Up
   TELENET       Up

Ring network

     Node       State
   ACCTNG       ****
   TEK2          Up
   MKTG          Up
   MNFG.A        Up
   MNFG.B        Up
   RES1          Up
   RES2         Down

Route-through network

     Node
   BELD1
   AUS1
   MRA.B
   BELD3

Public data network

     Node
   ATHNS
   CNBER
   RIO.A

NTS is not currently started
```

Paging Partition Information: This section displays the physical device numbers of the paging partitions (a maximum of eight) and the command device, COMDEV. COMDEV is the partition at logical device 0 at the time of system startup. This information is available only if you issue the STATUS command at the supervisor terminal.

```
PAGING PARTITIONS
  1    100461
  2    100463

Comdev = 2460
```

User and Process Information: This section lists the users currently logged in on the system. The `User` column displays the user ID. The `No` column lists the user number. The user number is a decimal number and is usually the line number (in decimal) plus 2. The `Line` column lists the asynchronous line number of the user terminal in decimal (dec). Special keywords are shown below.

```
                       User No  Line No
User                   (In Decimal)     Devices (AL in Decimal)
SYSTEM                    1       asr    <PLEIST> AL77
KERRYR                    8        6     <PLEIST> <PRECAM> <SYS562>
FRED                     10        8     <PLEIST>
MILO                     11        9     <PLEIST> <EOCENE>
GJP                      16       14     <PRECAM> <PLEIST>
SAMSL                    21       19     <DELUVI> <PRECAM>
JANIS                    23       21     <PLEIST> <EOCENE>
SANDYD                   29       27     <PLEIST>
TAYLOR                   35       33     <PLEIST> <SOCENE>
CANTRELL                 37       35     <PLEIST> S49<DEVON>
ARTHURS                  39       37     <PLEIST> S37<BABEL>
SIMON                    40       38     <PLEIST>
NICK                     57       51     <PLEIST> <EOCENE> AL011
SYSTEM_MANAGER           58      SMSr    <PLEIST>
DSM_LOGGER               59      DSM     <PLEIST>
DSMSR                    60      DSM     <PLEIST>
CADWALLADER              71      rem     <PRECAM> (from MESOZO)
SYSTEM                   86     slave    <EOCENE>
AMC                      88     slave    <PRECAM>
TIMER_PROCESS            89     kernel   <EOCENE>
LOGIN_SERVER             90      LSr     <EOCENE> (3)
TAPE_PHANTOM             91     phant    <EOCENE>
LOGOUT_SERVER            92     kernel   <EOCENE> (IDLE)
ISC_NETWORK_SERVER       93     ISCNsr   <EOCENE> (0)
BATCH_SERVICE            94     phant    <EOCENE> (2)
BACKUP_SERVICE           95     phant    <EOCENE>
PUBS                     96     phant    <EOCENE> S49<PALEOZ> PR0
TP.QUM                   97     phant    <EOCENE> S49<PALEOZ> AL76
BRANDON                 108     phant    <PLEIST> <EOCENE>
YTSMAN                  112     phant    <EOCENE>
NETMAN                  113      nsp     <EOCENE>
FTP                     114     phant    <EOCENE>
GEORGE                  115     batch    <EOCENE>

OK,
```

Line	*Meaning*
`asr`	User 1 or the supervisor terminal using the USRASR command
`Audit`	Security Monitor auditor process
`batch`	Batch job
`ISCNsr`	Interservice Communication server (ISC__NETWORK__SERVER)
`child`	Child process (spawned by PRIMIX™)

kernel	Timer process (TIMER_PROCESS), Logout server (LOGOUT_SERVER)
ncm	NTS connection manager (NTS_SERVER)
LSr	Login server (LOGIN_SERVER)
nsp	Network Server process (NETMAN)
phant	Phantom user
rem	User logged in remotely from another node in the network
rts	Route-through server (RT_SERVER)
slave	Network Process Extension (NPX) slave
SMSr	DSM System Manager server (SYSTEM_MANAGER)
DSM	DSM (DSM_LOGGER, DSMSR)

The Devices column lists all partitions and assigned devices in use by a particular terminal. A partition is considered to be in use if it contains the user's origin, home, or current directory, or if the user has any files open on that partition. Assigned devices are indicated with the same device abbreviations that the ASSIGN command uses (such as PR0 and MT2), except that assigned asynchronous lines are shown by an AL number and assigned partitions by a DK number.

Column 4 information may also include

- Remote logins from another system on the network (see user 71)
- User priority (default user priority is 1, which is not displayed; user 94 is running at priority 2; user 90 is running at priority 3)
- Use of a remote partition (see users 37 and 39)

SYSTEM INFORMATION AND METERING

Distributed Systems Management (DSM) is a set of services that provides for administration and management of Prime computer systems. One of these services is **System Information and Metering (SIM)**. SIM consists of 15 commands that allow you to monitor various aspects of your system, whether the system is standalone or networked.

Some SIM commands have their own particular options to allow you to specify the detail of your monitoring report. You can also use the 10 general SIM command options with any of the 15 SIM commands. For a detailed discussion of DSM and all of the SIM commands and their options, see the *DSM User's Guide*. The 15 SIM commands are as follows:

Command *Description*

LIST_ASSIGNED_DEVICES
Lists all devices that have been assigned. Options allow you to specify particular users by name or number (-USER) and particular devices by name.

LIST_ASYNC
Lists status and configuration of asynchronous lines. Options allow you to specify users by name or number (-USER) and lines by number.

LIST_COMM_CONTROLLERS
Lists the configuration of communications controllers.

LIST_CONFIG
Lists current PRIMOS configuration parameters. An option allows you to specify directives by name.

LIST_DISKS
Lists information concerning all partitions. Options allow you to specify partitions by name or partition users by name or number (-USERS), get information about local partitions only (-LOCAL) or about remote partitions only (-REMOTE).

LIST_LAN_NODES
Lists nodes on LAN300 local area networks. Options allow you to specify a list of LAN names (-LAN) on either host nodes (-HOST) or the LAN Terminal Server 300 (-LTS).

LIST_MEMORY
Lists physical memory usage in number of segments, resident pages, and wired pages per user process. Options allow you to specify users by name or number and types of users (-TYPE).

LIST_PRIMENET_LINKS
Lists status of PRIMENET links. Options allow you to specify names of nodes or of PSDNs and link device types by name (-LINK).

LIST_PRIMENET_NODES
Lists PRIMENET-configured nodes, node paths and access to the paths. Options allow you to specify node names and link device types (-LINK).

LIST_PRIMENET_PORTS
Lists assigned PRIMENET ports on which processes can receive calls. Options allow you to specify port numbers and port user names or numbers (-USER).

LIST_PROCESS Lists the environments of user processes, including the attach points, the abbreviation file, active COMI and COMO files, project group memberships, active remote IDs, and connect, CPU, and I/O times. Options allow you to specify users by name or number, projects by identity (-PROJ), process types (-TYPE), and whether you want detailed information (-DETAIL).

LIST_SEMAPHORES Lists the values of semaphores in use on the system. Options allow you to specify semaphores by number, users by name or number (-USER), and semaphore types (-TYPE).

LIST_SYNC Lists synchronous line configuration. An option allows you to specify line numbers.

LIST_UNITS Lists any user's open file units, the current attach points of all users, or the ID of users with a particular file open. Options allow you to specify a list of either user names or user numbers and a pathname prefix (-PATHNAME).

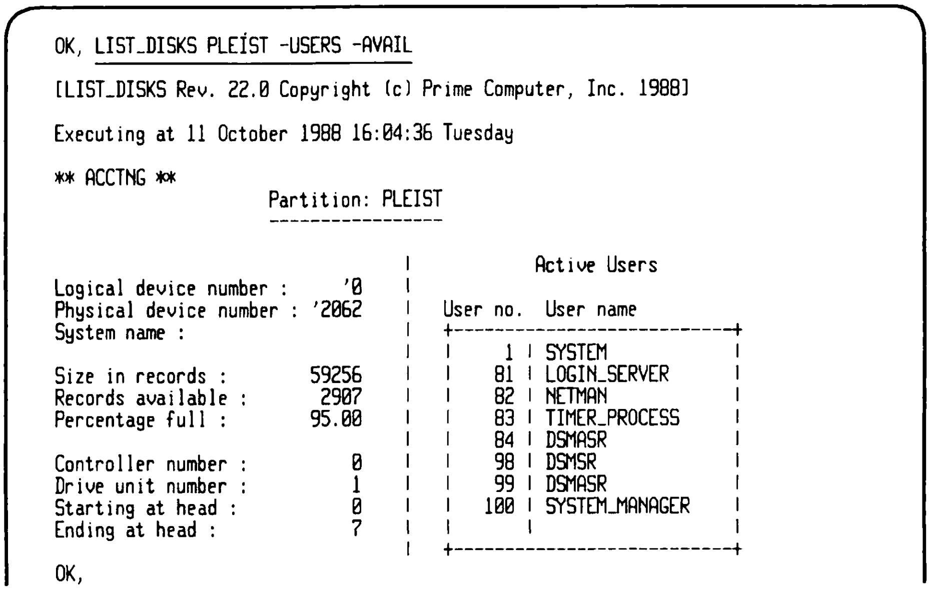
LIST_VCS Lists the state of active virtual circuits (VC) including the number of packets received and transmitted. Options allow you to specify particular virtual circuits, users by name or number (-USER), nodes (-NODE), ports (-PORT), and link devices (-LINK).

The 10 general SIM options that you can use with all of the SIM commands allow you to do the following:

- Specify the node group to which the command is to be directed (-ON).
- Write the information to disk by specifying a standard PRIMOS pathname (-PRIVATE_LOG).
- Write the information to a DSM system log (-SYSTEM_LOG).
- Suppress the prompt or query during the command output display (-NO_WAIT).
- Specify periodic execution of a command, with the interval between executions of the command determined in minutes (-FREQ).
- Specify a limit on the number of times that a command is to be executed in the periodic execution of commands. Used in conjunction with starting and stopping to implement periodic execution of a command (-TIMES).
- Set the date and time that command execution starts and stops (-START, -STOP).
- Display information on how to use the command (-HELP).
- Display abbreviated syntax information on how to use the command (-USAGE).

Examples of SIM Command Output

The example below shows the LIST_DISKS command in which the user specifies a particular partition and also specifies options to list all that partition's users and the availability of records on that partition.



```
OK, LIST_DISKS PLEÍST -USERS -AVAIL

[LIST_DISKS Rev. 22.0 Copyright (c) Prime Computer, Inc. 1988]

Executing at 11 October 1988 16:04:36 Tuesday

** ACCTNG **
                         Partition: PLEIST
                         -----------------

                                    |             Active Users
Logical device number :     '0      |
Physical device number : '2062      |   User no.  User name
System name :                       |   +--------------------------+
                                    |   |      1 | SYSTEM           |
Size in records :        59256      |   |     81 | LOGIN_SERVER     |
Records available :       2907      |   |     82 | NETMAN           |
Percentage full :        95.00      |   |     83 | TIMER_PROCESS    |
                                    |   |     84 | DSMASR           |
Controller number :          0      |   |     98 | DSMSR            |
Drive unit number :          1      |   |     99 | DSMASR           |
Starting at head :           0      |   |    100 | SYSTEM_MANAGER   |
Ending at head :             7      |   |        |                  |
                                    |   +--------------------------+
OK,
```

The display lists the characteristics of partition PLEIST, including the ldev, pdev, total size and records remaining, the unit numbers of the controller and disk drive associated with this partition, and the starting and ending surfaces of this disk partition.

In normal screen output, a `--More--` prompt appears after every 23 lines of output.

THE RESUS ENVIRONMENT

The **Remote System User (RESUS)** environment gives you access to the same command privileges at your own terminal that you would have at the supervisor terminal. The RESUS environment is part of Prime's Distributed Systems 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. For complete information on DSM, see the *DSM User's Guide.*

RESUS does not compromise system security in any way. Before beginning a RESUS session, you must enable RESUS at the supervisor terminal. RESUS can be enabled and disabled only at the physical supervisor terminal. Keeping RESUS disabled locks out all RESUS users, both local and remote, and ensures that the system can be controlled only from the supervisor terminal. A second level of security is provided by DSM's own security mechanism so that only specially authorized users have access to RESUS, even when it is enabled.

Through RESUS, an authorized user can issue the special PRIMOS operator commands and perform tasks such as adding disks, shutting down devices, and sharing segments from any terminal on any system in your DSM configuration group. You can use RESUS to control configured remote systems, or your own local system, from any convenient local user terminal.

During a RESUS session, your terminal is assigned to the User 1 process and replaces the User 1 functions of the supervisor terminal. In effect, your terminal becomes the *logical* supervisor terminal, while the real or *physical* supervisor terminal merely echoes what you type and the system's responses.

Once RESUS is enabled, these changes take place:

- Any authorized local or remote user can gain supervisor terminal privileges at a user terminal.
- The system can be controlled only from a local or remote user terminal and not from the supervisor terminal, except when the supervisor terminal is set to USER mode.
- The only commands that the physical supervisor terminal will process are RESUS -DISABLE and RESUS -DISABLE -FORCE.

Note

> Control Panel (CP) mode remains available at the supervisor terminal through the standard ESC ESC sequence, but RESUS does not provide remote access to CP mode from a user terminal.

Using RESUS

The PRIMOS command RESUS invokes the RESUS environment. For a complete description of the RESUS command's syntax and options, see the *Operator's Guide to System Commands* or the *DSM User's Guide.* There are six major steps in a RESUS session:

1. Enable RESUS at the physical supervisor terminal with the RESUS -ENABLE command.
2. Use the RESUS -STATUS command at a user terminal to check whether RESUS is enabled, and whether it is in use by someone else.
3. Begin the RESUS session at a user terminal with the RESUS -START command. If you do not use the -ON option to specify a remote node name, the local system is assumed. The RESUS -START command is not available either at the supervisor terminal or at a user terminal at which you are already using RESUS. You cannot control more than one system at a time through RESUS, and only one user can be in control of a system at any time.
4. Do your work as usual but keep in mind the following facts during a RESUS session.
   - You lose your personal abbreviations and pick up User 1's abbreviations, if any. Your ready and error prompts change to *systemname*.RESUS_OK> and *systemname*.RESUS_ER>.

- Your terminal takes on the terminal characteristics (for example, the kill and erase characters) of the physical supervisor terminal.
- RESUS does not provide access to CP mode. If you inadvertently press ESC ESC to invoke CP mode, your screen display freezes. Turn your terminal off and then on again to free the display.
- Certain PRIMOS commands should be used only with extreme caution in RESUS. (See the section Special Precautions With Some PRIMOS Commands later in this chapter.)

5. Terminate your RESUS session with the RESUS -STOP command. When the disconnection is complete, you receive a sign-off message and are returned to PRIMOS command level on the system where you are logged in. The system becomes available to other local or remote RESUS users.
6. Disable RESUS at the supervisor terminal with the RESUS -DISABLE command. Disabling RESUS on a system has no effect on the ability of users on that system to gain control of other systems where RESUS is enabled. The RESUS -DISABLE command is not honored if another RESUS user is already in control of the system. You must use the command RESUS -DISABLE -FORCE to forcibly disable the RESUS session.

Note

RESUS -DISABLE -FORCE bypasses normal operating system routines and allows local control of a system to be reestablished independently of PRIMOS. When a RESUS session is forcibly disabled, the User 1 process may be trapped in the most recently entered subsystem. You must restore the process to its normal state by referring to the record at the supervisor terminal.

You do not have to enable and disable RESUS before and after each RESUS session. You can enable RESUS at the beginning of the day and disable it at the end of the day, for example.

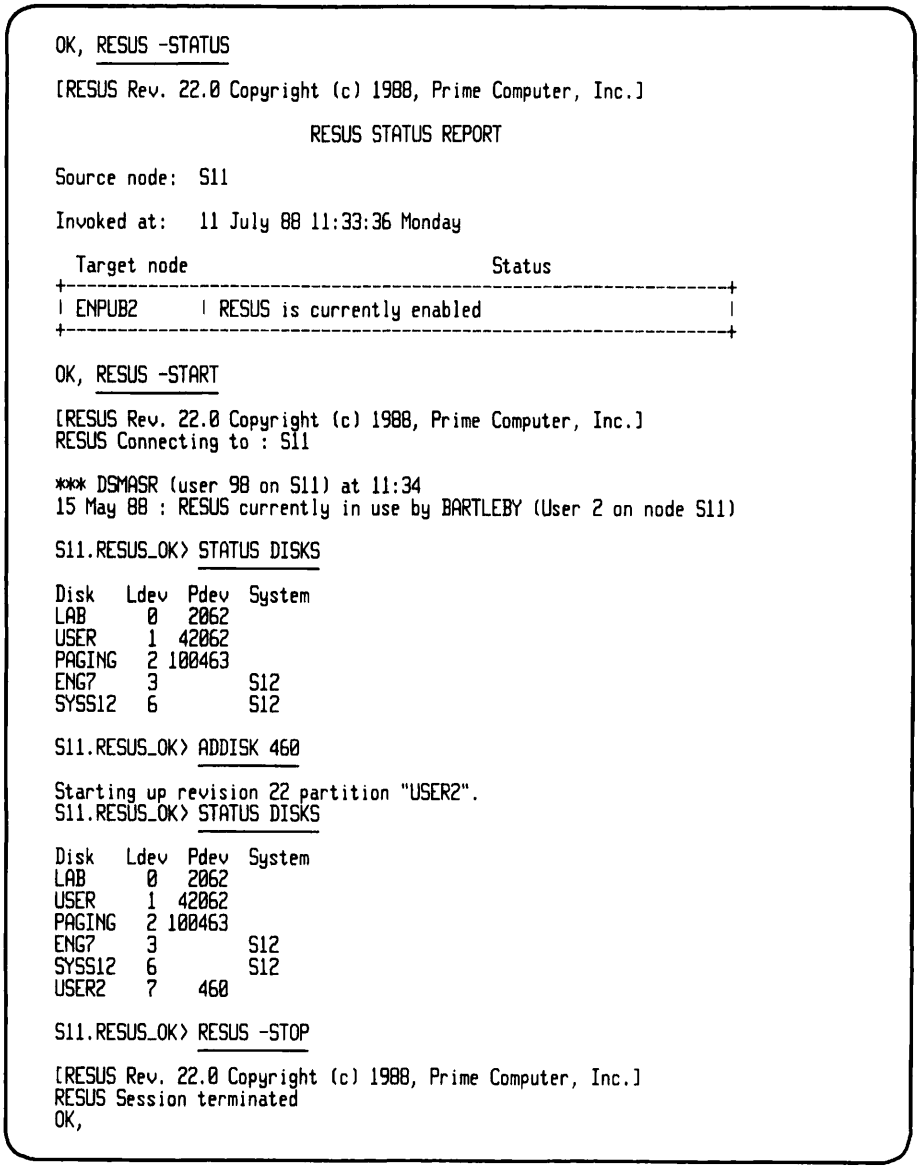
This six-step procedure is illustrated in the following sample session.

A Sample RESUS Session

At the supervisor terminal, enable RESUS:

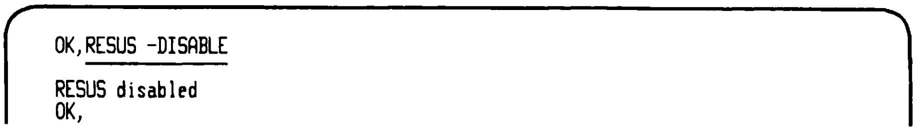
```
OK, RESUS -ENABLE

[RESUS Rev. 22.0 Copyright (c) 1988, Prime Computer, Inc.]
RESUS Enabled on S11
OK,
```

At the user terminal, start RESUS. In this example, an operator uses the ADDISK command from his or her own terminal.



```
OK, RESUS -STATUS

[RESUS Rev. 22.0 Copyright (c) 1988, Prime Computer, Inc.]
                                 RESUS STATUS REPORT

Source node:  S11

Invoked at:   11 July 88 11:33:36 Monday

  Target node                           Status
+--------------------------------------------------------------+
| ENPUB2        | RESUS is currently enabled                   |
+--------------------------------------------------------------+

OK, RESUS -START

[RESUS Rev. 22.0 Copyright (c) 1988, Prime Computer, Inc.]
RESUS Connecting to : S11

*** DSMASR (user 98 on S11) at 11:34
15 May 88 : RESUS currently in use by BARTLEBY (User 2 on node S11)

S11.RESUS_OK> STATUS DISKS

Disk    Ldev  Pdev  System
LAB      0    2062
USER     1   42062
PAGING   2  100463
ENG7     3          S12
SYSS12   6          S12

S11.RESUS_OK> ADDISK 460

Starting up revision 22 partition "USER2".
S11.RESUS_OK> STATUS DISKS

Disk    Ldev  Pdev  System
LAB      0    2062
USER     1   42062
PAGING   2  100463
ENG7     3          S12
SYSS12   6          S12
USER2    7     460

S11.RESUS_OK> RESUS -STOP

[RESUS Rev. 22.0 Copyright (c) 1988, Prime Computer, Inc.]
RESUS Session terminated
OK,
```

At the supervisor terminal, disable RESUS:



```
OK,RESUS -DISABLE

RESUS disabled
OK,
```

Special Precautions With Some PRIMOS Commands

RESUS is a special environment, a systems control facility that operates through the networking software. You should exercise caution when issuing the following commands during a RESUS session.

Command *Danger*

ICE The special RESUS prompts are lost for the remainder of the session and are restored only when RESUS is next enabled.

LOGOUT If the DSM server (DSMSR) is inadvertently logged out, supervisor terminal function can be temporarily lost. When you disable RESUS at the supervisor terminal, normal function is restored.

MIRROR_ON and
MIRROR_OFF These commands cause RESUS to hang because they may request input from the physical supervisor terminal's keyboard. Recover by disabling RESUS at the physical supervisor terminal (by using the RESUS -DISABLE -FORCE command) and answering the appropriate prompt.

NETLINK Your netlink session will be switched to the supervisor terminal and lost at your own terminal. If you enter NETLINK by accident while using RESUS, disable RESUS at the supervisor terminal, and quit the NETLINK session from there.

SET_ASYNC
AMLC You can unassign the line to the local terminal where RESUS is being used. You can recover control only by disabling RESUS at the supervisor terminal and reconfiguring the line.

STOP_DSM The operation of RESUS requires DSM to be running on the system.

TERM Any terminal characteristics set during a RESUS session remain in force on the supervisor terminal when the system returns to local control.

USRASR USRASR can hang the User 1 process and requires special recovery procedures.

Caution

Take care when using subsystems such as EMACS, which take advantage of special terminal characteristics, from a user terminal functioning as a supervisor terminal under RESUS. The user terminal must be identical to the supervisor terminal (for example, both must be PT200™ terminals). Otherwise, because the session echoes at the physical supervisor terminal, the terminal may lock. Return the logical supervisor terminal to User Terminal mode before using EMACS or any subsystem with these characteristics, unless you are certain the two terminals are of the same type.

Using RESUS at the Supervisor Terminal in USER Mode

You can use RESUS from the supervisor terminal in USER mode with the following restriction: before entering USER mode, issue the VCP command SYSOUT IGN to disable output to the supervisor terminal. If you do not, output is directed to the User 1 display buffer, and characters may be lost. The effect of SYSOUT IGN is that all output to the screen is ignored so that you have no record of your dialog. If you use the VCP command SYSOUT INT, screen output will be hopelessly jumbled. (See your CPU handbook for a discussion of these VCP commands.)

APPENDICES

A

PRIMOS COMMANDS

The basic unit of work for any user of PRIMOS is the **command**. Commands tell PRIMOS what you want it to do for you. To learn more about how to communicate with PRIMOS via commands, read the *PRIMOS User's Guide.* For complete information on PRIMOS commands for system users, see the *PRIMOS Commands Reference Guide.*

Some commands available to the operator are either not available or not useful to other users. These commands are described in the *Operator's Guide to System Commands.* Some commands provide you with information on the status of various parts of the system. You should use these commands periodically to monitor the status of the system and to ensure the system's smooth operation.

Following is an alphabetical list of system attributes and components and the PRIMOS commands that you invoke to display information on or change the status of these attributes and components.

At Rev. 21.0, Distributed Systems Management (DSM) services were introduced. DSM includes a subsystem for monitoring and obtaining information about all aspects of your system. This subsystem is called System Information and Metering (SIM). SIM consists of 15 commands to list various parameters. See Chapter 6, Monitoring Your System, and the *DSM User's Guide* for a further discussion of these commands.

TABLE A-1. System Attributes and Components Affected by PRIMOS Commands

Attributes and Components	*PRIMOS Command*
Access groups	LIST_GROUP
ACL protection, listing	LIST_ACCESS
ACL protection, setting	SET_ACCESS or EDIT_ACCESS
Active Batch jobs	JOB -STATUS or JOB -DISPLAY

TABLE A-1. System Attributes and Components Affected by PRIMOS Commands (continued)

Attributes and Components	*PRIMOS Command*
Assigned devices, user	STATUS USERS
	LIST_ASSIGNED_DEVICES
Assigned magnetic tape drives	STATUS DEVICES
	LIST_ASSIGNED_DEVICES
Asynchronous (user) line	STATUS USERS, LIST_ASYNC
Available records on a partition	AVAIL, LIST_DISKS
Batch jobs, active	JOB -STATUS or JOB -DISPLAY
Batch jobs, executing	BATCH -DISPLAY
Batch jobs, specific	JOB *job-ID* -DISPLAY
Batch queue names	BATGEN -STATUS
Batch queue parameters	BATGEN -DISPLAY
Batch subsystem usage	BATCH -DISPLAY
Configuration parameters	LIST_CONFIG
Command device	STATUS, STATUS DISKS, LIST_DISKS
Communication controllers	STATUS COMM, LIST_COMM_CONTROLLERS
Current revision number	STATUS SYSTEM
Current PRIMOS date and time	DATE
Deferred spool files	SPOOL -LIST [-ALL] -DETAIL
Devices, assigned, user	STATUS USERS,
	LIST_ASSIGNED_DEVICES
Device, command	STATUS, STATUS DISKS, LIST_DISKS
Devices, started	STATUS DISKS, LIST_DISKS
Devices, logical	STATUS DISKS, LIST_DISKS
Devices, mounted	STATUS DEVICE,
	LIST_ASSIGNED_DEVICES
Devices, physical	STATUS DISKS, LIST_DISKS
Devices, physical, user	STATUS USERS, LIST_DISKS
Devices, remote	STATUS DISKS, LIST_DISKS
Disk usage	USAGE -DISK, LIST_DISKS

TABLE A-1. System Attributes and Components Affected by PRIMOS Commands (continued)

Attributes and Components	*PRIMOS Command*
Disks mounted	STATUS DISKS, LIST_DISKS
Disks, remote	STATUS DISKS, LIST_DISKS
EPFs in use	LIST_EPF
Executing Batch jobs	BATCH -DISPLAY
File protection	LIST_ACCESS
File Transfer Server	FTOP -LIST_SRVR_STS
File transfer requests	FTR -STATUS or FTR -DISPLAY
File units in use	STATUS UNITS, LIST_UNITS
Free records on a partition	AVAIL, LIST_DISKS
Line, user (asynchronous)	STATUS USERS, LIST_PROCESS
Local node name	STATUS NET, STATUS SYSTEM LIST_PRIMENET_NODES LIST_PRIMENET_LINKS
Logical devices	STATUS DISKS, LIST_DISKS
Logins, remote	STATUS USERS, LIST_PROCESS
Login Server, starting	START_LSR
Login Server, stopping	STOP_LSR
Magnetic tape drives, assigned	STATUS DEVICES LIST_ASSIGNED_DEVICES
Memory usage	LIST_MEMORY
Mounted devices	STATUS DISKS, LIST_DISKS
Mounted disks	STATUS DISKS, LIST_DISKS
Network	STATUS NET, MONITOR_NET LIST_PRIMENET_NODES LIST_PRIMENET_LINKS
Network, type	STATUS NET LIST_PRIMENET_NODES LIST_PRIMENET_LINKS

TABLE A-1. System Attributes and Components Affected by PRIMOS Commands (continued)

Attributes and Components	*PRIMOS Command*
Node condition	STATUS NET
Node name, local	STATUS NET, STATUS UNITS
	LIST_PRIMENET_NODES
	LIST_PRIMENET_LINKS
Number of users	USERS
Number, user	STATUS USERS, LIST_PROCESS
Partition names	STATUS DISKS, LIST_DISKS
Phantom users	STATUS USERS, LIST_PROCESS
Physical devices	STATUS DISKS, LIST_DISKS
Physical devices, user	STATUS USERS
	LIST_ASSIGNED_DEVICES
Plot files, spool	SPOOL -LIST [-ALL] -DETAIL
Print files, spool	SPOOL -LIST [-ALL] -DETAIL
Printer names	PROP -STATUS [-ALL]
Printer environment parameters	PROP *printer-name* -DISPLAY
Priority ACL	LIST_PRIORITY_ACCESS
Priority, user	STATUS USERS
Protection, file	LIST_ACCESS
Quotas	LIST_QUOTA, LD -SIZE -DIR
Records available	AVAIL, LIST_DISKS
Records used	AVAIL, LIST_DISKS
Remote devices	STATUS DISKS, LIST_DISKS
Remote disks	STATUS DISKS, LIST_DISKS
Remote logins	STATUS USERS, LIST_PROCESS
Remote systems, logins to	STATUS USERS
Remote users	STATUS USERS, LIST_PROCESS
Segments in use	LIST_SEGMENT, LIST_MEMORY
Special form spool files	SPOOL -LIST [-ALL] -ATTR *form_type*
Specific Batch jobs	JOB *job-ID* -DISPLAY

TABLE A-1. System Attributes and Components Affected by PRIMOS Commands (continued)

Attributes and Components	*PRIMOS Command*
Spool files	SPOOL -LIST [-ALL]
Spool files, deferred	SPOOL -LIST [-ALL] -DETAIL
Spool files, special form	SPOOL -LIST [-ALL] -ATTR *form_type*
Spool files, user's own	SPOOL -LIST [-ALL] -USER *username*
Spool plot files	SPOOL -LIST [-ALL] -DETAIL
Spool print files	SPOOL -LIST [-ALL] -DETAIL
System name	STATUS SYSTEM, any SIM command
Terminals, configuration	LIST_ASYNC
Type of network	STATUS NET, LIST_PRIMENET_NODES
Units, file, in use	STATUS UNITS, LIST_UNITS
User-assigned devices	STATUS USERS
	LIST_ASSIGNED_DEVICES
User line (asynchronous)	STATUS USERS, LIST_PROCESS
User logins to other nodes	STATUS USERS, LIST_PROCESS
User number	STATUS USERS, LIST_PROCESS
User physical devices	STATUS USERS
	LIST_ASSIGNED_DEVICES
User priority	STATUS USERS, LIST_PROCESS
User's own spool files	SPOOL -LIST [-ALL] -USER *username*
Users, number of	USERS
Users, phantom	STATUS USERS, LIST_PROCESS
Users, remote	STATUS USERS, LIST_PROCESS
Volume names	STATUS DISKS
	LIST_ASSIGNED DEVICES
Your user ID	STATUS ME, LIST_PROCESS

B

GLOSSARY

Access Control List (ACL)
See ACL.

access rights
The degree of access that a user has on the system, specified in terms of which operations the user can perform. For example, a user with Read (R) access to a file can read that file.

ACL
A list of users and/or user groups and the access rights granted to them for a file, directory, or access category.

ACL group
A list of users who are grouped together for file access purposes. The System Administrator assigns users to groups and then specifies the access rights of the group. ACL groups can be systemwide or project-specific. ACL group names begin with a period. For example, .STAFF would be an ACL group name.

assigned device
A system device, such as a magnetic tape drive or a partition, that is under the exclusive control of a single user.

asynchronous line
A communications line that sends or receives data one character at a time. Refers to lines connected to an AMLC or ICS controller, as well as NTS lines connected to a LAN300 Host Controller. Asynchronous lines connect terminals, printers, and other devices to the CPU. *See also* synchronous line.

Batch job
A process started by a CPL or COMI file and executed by a batch phantom. Batch jobs, which can also be started interactively, are run by phantoms (in background) thus freeing the terminal for other interactive processes. *See also* interactive user, phantom process, user phantom.

Batch phantom
The phantom that runs a Batch job specified in a CPL or COMI file.

Batch monitor
The server that checks the Batch queue to see if Batch jobs are waiting to be run. *See also* phantom process, user phantom.

booting
Starting up the PRIMOS operating system. Same as cold start.

bootstrapping
See booting.

cache hit
A successful attempt by the CPU to find data in cache memory.

cache memory
The high-speed memory located on the CPU board. Data must be processed by the CPU from cache memory. Cache memory contains copies of information in the most recently referenced memory locations.

cache miss
An unsuccessful attempt by the CPU to find data in cache memory.

CMDNC0
A directory located on the command device (COMDEV) containing external PRIMOS commands, that is, those commands that are not embedded in the operating system. ED and FIX_DISK are examples of external commands. Both the system startup file (PRIMOS.COMI) and the configuration file (CONFIG) are located in CMDNC0.

cold start
Startup of PRIMOS including an initialization and configuration sequence. Used after certain types of halts or as a normal system startup. *See also* warm start.

COMDEV
See command device.

COMINPUT file
A command input file consisting of PRIMOS commands, utility subcommands, or dialog responses. Each line in the file corresponds to a line as it would be typed at a terminal. COMINPUT files may be executed using the COMINPUT command, as phantoms using the PHANTOM command, or as a Batch job.

command device
Logical device 0, that is, the first partition added to the system as specified by the COMDEV directive. Contains system directories required to run PRIMOS, the utilities, and the CMDNC0 directory, which contains external commands.

command input file
See COMINPUT file.

command output file
See COMOUTPUT file.

COMOUTPUT file
A file created using the COMOUTPUT command, which contains both the output stream directed to a user's terminal by PRIMOS and the input given to PRIMOS. Also referred to as a COMO file.

configuration directives
System parameters contained in the configuration file, which PRIMOS reads and processes at the beginning of system startup. Examples are PAGING, which specifies the paging device partitions, and COMDEV, which specifies the command device partition. The CONFIG command, the first instruction in the PRIMOS.COMI startup file, reads the configuration file.

configuration file
See configuration directives.

CPL file
A program written in Command Procedure Language (CPL) that executes sequences of PRIMOS commands or a combination of PRIMOS commands and CPL directives. A CPL file can be executed with the CPL or RESUME command, as a phantom, or as a Batch job.

despooler
The program that checks the spool queue to see if any files are waiting to be printed and sends any file requests to the appropriate printer.

despooler phantom
A process that controls a printer environment and, thus, controls the printer that is specified in the environment.

directive
See configuration directives.

directory
A file containing a list of all files within a partition, and their locations. Master File Directories, user file directories, and subdirectories are all examples of directories.

disk storage
A storage facility capable of storing large amounts of data on a physical disk medium for access by the system and its programs.

environment files
Files that contain information that is needed to implement a printer environment, including technical details of the output device, commands that control the header and footer pages of printouts, information about spool queues, and so on. Environment files are located in the SPOOL* directory.

exclusive assignment

Access to a system device that is limited to one user, as a result of using the ASSIGN command. This method of allocating system resources prevents two users from attempting to use a device at the same time. For example, if a user has assigned a tape drive, another user cannot access that tape drive until the first user has released it with the UNASSIGN command. *See also* request queuing.

external commands

Executable files located in the CMDNC0 directory. These commands can be PRIMOS commands, site-specific commands, or third-party software.

file

An organized collection of information stored on a disk (or on a peripheral storage medium such as tape). Each file has an identifying label called a filename.

FTS manager

A system server that monitors the file transfer queue for file transfer requests between nodes. When a file transfer request is in the queue and the communication lines are open and not busy, the FTS manager (YTSMAN) passes the file to an FTS server which, in turn, transfers the file to the FTS server on the node to which the file is being transferred.

FTS server

A phantom that communicates with and transfers files to the FTS server on another node.

halt

An unexpected cessation of PRIMOS processing. In this condition, PRIMOS does not respond to commands from either user terminals or the supervisor terminal; however, the Diagnostic Processor accepts VCP commands. During a halt, the STOP light (or PROC HALTED light) is on and a halt message appears at the supervisor terminal. *See also* hang.

hang

An unexpected cessation of PRIMOS processing. In this condition, PRIMOS does not respond to commands from either user terminals or the supervisor terminal. During a hang, the STOP light (or PROC HALTED light) on the System Status Panel is off and no halt message appears at the supervisor terminal. *See Also* halt.

Initial Attach Point (IAP)

The directory to which a user is attached at the time of login. Also called the origin directory.

interactive user

A user who is logged in to a terminal. *See also* phantom, phantom process.

internal command

A command that executes in PRIMOS address space. Examples are ATTACH and LOGOUT. Most internal commands do not overwrite the user memory image, and therefore do not prevent the user from restarting programs. Internal commands are embedded within PRIMOS itself, unlike external commands.

job ID
The identification number associated with a given Batch job. Each queue has its own set of job IDs, consisting of a number sign (#) followed by a number or letter that identifies the queue, followed by a four-digit number.

local user
A user who is logged in on a terminal that is directly connected to the local system. *See also* remote user.

logbook
A handwritten record of information about system status and operation. The contents may vary but should include information about hardware, the computer room environment, software, day-to-day operations, and halts.

logical disk
A partition that has been assigned a logical disk number either by the operator or during system startup. *See also* physical device number.

logical supervisor terminal
A user terminal that has been enabled by RESUS to perform the functions of the supervisor terminal. The logical supervisor terminal is able to control the system by issuing supervisor terminal commands.

login
The procedure for identifying yourself to PRIMOS as an authorized user of the system. User 1 (SYSTEM) is logged in automatically from the supervisor terminal at startup.

login name
Name given by a user when logging in to the system; the name identified by PRIMOS as that of a user who is authorized to use the system.

logout
The procedure for terminating a work session when you are finished working on the system. User 1 (SYSTEM) cannot be logged out from the supervisor terminal.

main memory
Memory locations on circuit boards in the CPU. When data is needed for a process, the CPU reads that data into main memory from disk storage.

Master File Directory (MFD)
A special directory that contains the names of the top-level directories on a particular partition. Each partition has one Master File Directory, whose name is always MFD.

network
A collection of independent computer systems that are connected to each other by various communications media (such as PDNs, LANs, and synchronous lines) and that communicate and share resources. An example is PRIMENET.

network server process
The phantom process that services network activity. The network server is always logged in under the name NETMAN.

No-assignment mode

One of three modes of tape drive assignment. This method disallows assignment of tape drives to users. Under this mode, no one can copy files to tape or restore files from tape. The SETMOD command establishes the assignment mode. User mode is the default. *See also* Operator Intervention mode, User mode.

node

Synonymous with the term system. In this book, node refers to a computer system other than your own that forms part of your network. The term is often used to distinguish your system from other systems in the network. For example, `Message from` *nodename* indicates that the message came from another system on the network, whereas `Message from` *systemname* identifies the message as having originated on the local system.

online maintenance

Monitoring the file system while the system is up and running. This includes checking the integrity of system directories, responding to user questions, and so on.

operator commands

Commands restricted to the System Administrator and system operators. You can use operator commands to control and monitor the system itself, control and monitor subsystems, and assist users with various tasks. *See also* user commands.

Operator Intervention mode

One of three modes of tape drive assignment. This method requires that users channel all assignment requests through the operator. The SETMOD command establishes the assignment mode. User mode is the default. *See also* No-assignment mode, User mode.

origin directory

See Initial Attach Point (IAP).

page fault

A request by a user program for data not in main memory, thereby forcing the operating system to read the data from disk.

page

A block of 2048 bytes (2 kilobytes). A page is the smallest unit moved in and out of main memory from disk storage. *See also* record.

paging

The technique of swapping data to a temporary storage area in disk storage, thus making more memory available to the system than actually exists. By paging the data to a paging partition, the system can bring the data back into main memory faster than if it had to retrieve the data from file partitions. *See also* paging partition, virtual memory.

paging partition

A special temporary storage area in disk storage. When all the locations in main memory are full and another process calls for data to be brought into main memory, the last recently used pages are swapped out to a paging partition. A system can contain as many as eight paging partitions.

partition

A sequence of surfaces that result from the subdivision of physical disks and that are used for the storage of specific data. Each partition is treated by PRIMOS as a separate logical device, made up of an even number of surfaces from the starting surface (but the last partition can have an odd number of surfaces).

phantom

A process that runs programs without user intervention. Phantoms can be started by users (with the PHANTOM command), by CPL or COMI files, or by subsystems. (For example, the BATCH subsystem starts a phantom to run a Batch job.) *See also* phantom process, user phantom.

phantom process

A process that runs unattached to a terminal, under the control of a command file or CPL file. A command file executed as a phantom (with the PHANTOM command) allows you to do other work at the terminal while the phantom process is running. *See also* user phantom.

physical device number (pdev)

An octal number representing a physical disk unit number. This is needed only for operator commands.

physical memory

The hardware parts of a computer system that are used to store large blocks of information. Physical memory consists of disk partitions (on one or more disk drives), main memory, and cache memory.

physical supervisor terminal

The real supervisor terminal. When RESUS is enabled, a user terminal becomes the logical supervisor terminal, and the physical supervisor terminal echoes anything entered at the logical supervisor terminal. *See also* supervisor terminal; logical supervisor terminal.

port

An information outlet connected to the CPU. Most of the ports on a system are connected to user terminals; one port on each system connects to a supervisor terminal. Some systems also have synchronous line ports, printer ports, and so on.

primary partition

One half of the mirroring pair of partitions. When two partitions are mirrored, all records are written to both partitions, so that if one partition fails, the data is retrievable from the other partition. *See also* secondary partition.

printer environment

Definition of how a printer is used and of how print requests made by SPOOL commands are matched with suitable printers. This includes information about type of paper, types of files the environment can handle, size range of files the environment is permitted to print, format of the output, and whether or not to convert the text to uppercase.

priority ACLs

Special access privileges to all files and directories on a partition, which can be set or removed by the System Administrator from any terminal, or by anyone from the supervisor terminal. *See also* ACLs.

process

A particular program running in a specific address space. Each user has a process in which to perform work.

project

A group of users who are grouped together by common need for access, command levels, and device use. Every system must have at least one project defined by the EDIT_PROFILE command. The default project is named DEFAULT.

quota

The maximum number of 2048-word records that the contents of a directory can occupy on a disk. A quota of 0 means that no limit exists on the number of records in the directory.

record

A description of storage capacity, 2048 bytes (2 kilobytes). Often used to describe the length of a file, as in "a 5-record file". Record sometimes refers to a physical location on a partition. Record numbers are used to identify bad spots on the partition so that the system won't try to use those areas.

remote user

A user whose terminal is attached to another node on the network but who is logged in remotely to the local system. A remote user appears as `rem` in the `Line No` column of the STATUS USERS display.

request queuing

A means of allowing any number of users to request operations to be performed on a peripheral device (for example, a printer). If the device is already in use, the request is processed automatically by PRIMOS when the device becomes available. Users can request use of the device and continue other work. *See also* exclusive assignment.

restoring a file

Copying a file or directory from tape to disk. This refers to a file or directory that had previously been archived to tape.

RESUS

(REmote System USer) A Distributed Systems Management (DSM) facility that allows any terminal on any node configured in a system's network to become the logical supervisor terminal and, thus, to control the system by issuing supervisor terminal commands.

secondary partition

One half of the mirroring pair of partitions. When two partitions are mirrored, all records are written to both partitions, so that if one partition fails, the data is retrievable from the other partition. *See also* primary partition.

sectors

A portion of a track on a partition surface. Equivalent to a record. The sector number is used to reference bad spots on partitions.

security logging

The use of the separately priced C-2 security system (the Security Audit facility) to monitor and record specified security events such as logins and attempts to attach to directories or read files.

segment

Unit of virtual memory, consisting of 128 kilobytes each, or 64 pages. Each segment is identified by a segment number (in octal). The maximum virtual address space for each user is 4096 segments. 2048 of these segments are shared PRIMOS or shared subsystem segments. The remaining 2048 are user segments.

server

A phantom that is started, either by the system startup file when the system is booted or by a command issued from the supervisor terminal. Servers run programs that must be run at all times to service subsystems. Examples are YTSMAN, the FTS server; NETMAN, the Network server; and LOGIN_SERVER, the server that processes login requests.

shared segments

The address space in virtual memory that is shared by all users. In the Prime virtual memory scheme, the first 2048 segments of user address space are PRIMOS and shared subsystem segments. *See also* unshared segments.

slave

A process representing a remote user who is using some resource on the local system. For example a user who is logged in to a remote node uses a slave to access a file on the local system. The process is visible to users on the local system as a slave in the `Line No` column of the STATUS USERS display.

spool

To place a file on the print queue via the SPOOL command.

subsystem

The programs, directories, and files that make up a utility. Subsystems perform one of the following functions: helping users do certain tasks, such as printing files, helping PRIMOS administer the system, and providing applications programs (such as Prime INFORMATION).

supervisor terminal

The terminal recognized by PRIMOS as the most privileged terminal on the system; always logged in as User 1 (with a user ID of SYSTEM) under PRIMOS. *See also* RESUS.

synchronous line

A communications line capable of sending blocks of characters rather than a single character at a time. Synchronous lines connect two systems or connect a system and a Public Data Network (PDN). *See also* asynchronous line.

system

The hardware and software components of a computer. In this book, the computer system with which the user (or operator) is currently dealing.

system configuration

The list of system characteristics established in the configuration file and read by the CONFIG command at startup.

system directories

The directories that are required to run PRIMOS, the utilities, and other software. Most system directories are located on the command device (COMDEV). Examples of system directories are the directory CMDNC0, the directory DEVICE*, and the directory SPOOL*.

system initialization

The procedure at startup or during a cold start whereby PRIMOS reads the PRIMOS.COMI file, which starts the subsystems, and the system configuration file, which establishes the system parameters.

tape backup

A copy to tape of files and directories which preserves their contents in case of a system malfunction. This is also used to transfer data from disk to tape so that the data can be transferred to another system that is not on the network.

tape dump

The writing of the contents of memory to tape after a system halt. This information, which may be a partial or full tape dump, is used for analysis of the cause of the halt.

timeslice

The amount of time given to each process by the CPU for processing, measured in tenths of a second. The default timeslice depends on each machine's model number; you can change the value of the timeslice by using the CHAP command.

track

A portion of a partition platter's surface that holds information. A surface consists of many information tracks; each track consists of one or more records.

unshared segments

The address space in virtual memory that is unique to each user. In PRIMOS, as many as 2048 unshared segments are available to each user, but only a small portion of that number is enabled by the System Administrator.

user

Any user process, including phantoms started by users or subsystems and people logged in at user terminals.

user commands

Commands that are available to any user; for example, any user can use the SPOOL command to send a print request to the printer. *See also* operator commands.

user ID

The name (maximum of 32 characters) registered with your System Administrator that enables you to use the system. You use this name to log in to the system. System servers, phantoms, and processes, as well as interactive users all have user IDs, which are listed in the User column of the STATUS USERS display.

User mode
One of three modes of tape drive assignment. Users can assign tape drives without operator intervention unless special assistance is needed. The SETMOD command establishes the assignment mode. User mode is the default. *See also* Operator Intervention mode, No-assignment mode.

user number
A unique number given to all users, including phantoms, servers, slaves, remote users, and local terminal users, when they are logged in. It is listed in the STATUS USERS display. This number is needed when you issue commands that do not accept user names. (For example, the LOGOUT command can take the user number as the argument.)

user phantom
A type of user that runs a process on the system, independently of a terminal, thus enabling the user at the terminal to continue with other work. Phantoms can be started by a user with the PHANTOM command or from a CPL or COMI file.

user profile
The attributes of an individual user contained in the User Profile Database, including system attributes and project attributes. It serves as a means of identifying and validating users, checking the ACL rights for file system protection, grouping users for purposes of accounting and file system control, and creating a unique environment for each user. The System Administrator creates a user profile with the EDIT_PROFILE command.

user terminal
Any terminal other than the supervisor terminal. User terminals can be used only when PRIMOS is running.

utility
A single program that is invoked with a single command and that provides the user with information or with a facility. Examples of commands to invoke utilities are EDIT_PROFILE, MAKE, and FIX_DISK.

virtual memory
Used to describe the ability of a system to use more main memory that it actually has by using paging partitions to transfer data back and forth between disk storage and main memory.

warm start
Restarting PRIMOS without having to complete the entire initialization and configuration sequence. This can be performed only after certain types of halts occur. *See also* cold start.

wired memory
Pages of data that remain in main memory so that the system always has access to them; such pages are never paged out.

INDEX

INDEX

SURVEYS

READER RESPONSE FORM

Operator's System Overview
DOC9298-3LA

Your feedback will help us continue to improve the quality, accuracy, and organization of our 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: