System Administration Tasks

HP 9000 Series 300/400 Computers

HEWLETT
PACKARD

HP Part No. B1864-90010
Printed in USA August 1992

First Edition
E0892

Legal Notices

The information in this document is subject to change without notice.

Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Warranty. A copy of the specific warranty terms applicable to your Hewlett-Packard product and replacement parts can be obtained from your local Sales and Service Office.

HEWLETT-PACKARD COMPANY
3000 Hanover Street
Palo Alto, California 94304 U.S.A.

Printing History

The manual printing date and part number indicate its current edition. The printing date will change when a new edition is printed. Minor changes may be made at reprint without changing the printing date. The manual part number will change when extensive changes are made.

Manual updates may be issued between editions to correct errors or document product changes. To ensure that you receive the updated or new editions, you should subscribe to the appropriate product support service. See your HP sales representative for details.

First Edition: August 1992 (HP-UX Release 9.0)

Contents

1. Introduction to System Administration

How to Use this Manual 1-1
Conventions Used in this Manual 1-2
What's in this Manual 1-3
What System Administrators Need to Know 1-6
A System Administrator's Responsibilities 1-7
Where to Find Other Information About System Administration 1-8
Using SAM 1-10
SAM Overview 1-11
A Typical SAM Task 1-13
Overview of Customizing the Object List 1-15
Changing the Object List Type 1-16
Changing the Format of the Object List 1-17
Displaying a Subset of Objects 1-18
Changing the Object List Order 1-20
Using SAM with an X Window System 1-21
Setting Up Your System 1-21
Korn and Bourne Shell 1-22
C Shell 1-22
Entering SAM 1-23
Exiting SAM 1-24
Customizing the SAM Interface 1-25
Using SAM with a Text Terminal 1-26
Entering SAM 1-26
Using Control Buttons 1-29
Using Softkeys 1-30
Exiting SAM 1-32
Entering a Functional Area 1-32
Selecting an Object 1-34
Opening a Menu 1-36

Choosing a Menu Item 1-37
Using Buttons and Checkboxes 1-37
Menu Buttons 1-37
Radio Buttons 1-38
Checkboxes 1-38
Navigating with Keys and Key Combinations 1-39
Changing Windows 1-40
Moving a Window 1-41
Resizing a Window 1-41
Iconifying a Window 1-41
Maximizing a Window 1-41
Opening a Window 1-41
Closing a Window 1-41
Using SAM for Remote System Administration 1-42
Adding and Removing Remote Systems 1-42
Configuring the Remote System 1-43
Logging SAM's Actions 1-44
Turning On SAM Logging 1-44

2. Constructing an HP-UX System
Assessing Users' Needs 2-1
User Survey 2-2
Installing HP-UX 2-4
Updating HP-UX 2-4
Installing and Updating Optional Software 2-4
Cluster Considerations 2-5
Installing HP-UX on a Cluster 2-5
Updating HP-UX on a Cluster 2-5
Installing and Updating Optional Software in a Cluster . . . 2-5
Adding, Removing, and Moving Peripherals 2-6
After Installing HP-UX 2-7
Creating a Recovery System 2-7
Recovery Devices 2-8
Using Cartridge Tape 2-8
Tools For Making a Recovery System 2-9
Procedure For Making a Recovery System 2-10
Using the mkrs Script 2-11
Examples of Creating a Recovery System 2-13

Setting the System Clock 2-14
Setting the Time Zone (TZ) 2-14
Setting the Time and Date 2-16
Problems You Can Cause by Changing the System Clock . 2-18
Setting Up File Systems 2-18
Setting Up On-Line HP-UX Reference (manpages) 2-19
Setting Up Networking 2-21
Adding Users and Groups 2-21
Setting Up Electronic Mail 2-22
Setting Up the Line-Printer Spooler 2-23
Setting Up news 2-24
Using HP VUE 2-25
Setting Up X Windows 2-26
Setting Up System Accounting 2-27
Customizing the System 2-28
Customizing System Startup 2-31
Editing the /etc/inittab File 2-31
Editing /etc/inittab in a Cluster 2-31
Editing the /etc/rc File 2-32
Customizing the Login Prompt (/etc/issue) 2-33
Posting a Message of the Day (/etc/motd) 2-33
Customizing Users' Login Environments 2-34
Customizing Users' Editing Environments 2-34
Setting Up Non-Standard Terminals 2-35
Creating a New terminfo File 2-37
Backing up the System 2-38
Reconfiguring the Kernel 2-38
When Do You Need to Reconfigure the Kernel? 2-39
Reconfiguring the Kernel Using HP-UX Commands 2-40
Reconfiguring the Kernel to Add/Remove Device Drivers Using SAM 2-46
Reconfiguring the Kernel to Modify System Parameters Using SAM 2-49
Reconfiguring the Kernel to Modify Special Devices Using SAM 2-51
Booting the Standalone or Cluster Server Backup Kernel Using the Boot ROM 2-54
Restoring the Cluster Client Backup Kernel 2-55
Adding and Removing Subsystems 2-56

Adding a Subsystem Using HP-UX Commands 2-56
Removing a Subsystem Using HP-UX Commands 2-58
Adding and Removing Subsystems Using SAM 2-59
Removing System Files 2-62
Important Points 2-62
How to Use rmfn 2-63

3. Starting and Stopping HP-UX
Starting HP-UX 3-2
Prerequisites and Conditions 3-2
Configuring Your System 3-3
Setting Initial Information 3-3
The Startup Process Might Check the File System 3-5
Turning On Your Computer 3-6
Starting an Alternate Operating System or Program 3-8
Shutting Down the System 3-9
Prerequisites and Conditions 3-10
Designating Shutdown Authorization 3-11
Customizing the Shutdown Process 3-11
Manual Procedures 3-12
Going to the Single-user State for Maintenance 3-12
Shutting Down the System Completely 3-13
Shutting Down the System to Activate a New Kernel 3-14
Using SAM to Shut Down the System 3-15
Using SAM to Halt or Reboot the System 3-15
Power Failure Considerations 3-16
Power Failure Related Tasks 3-16
Power Failure in a Cluster 3-17

4. Controlling Access to Your System
Terms Used in this Chapter 4-2
Overview of Controlling Access Your System 4-4
Controlling User Accounts and Groups 4-5
Primary Groups 4-7
Group Passwords 4-7
Special Groups 4-8
Controlling File Access 4-9
File Access Permissions 4-9

Access Control Lists 4-11
Controlling Run-Levels 4-12
Managing User Accounts and Groups Tasks 4-14
Adding a User Using SAM 4-16
Removing a User Using SAM 4-19
Customizing the SAM "Adding and Removing a User" Capabilities 4-21
Deactivating a User's Account Using SAM 4-24
Reactivating a User's Account Using SAM 4-26
Displaying/Modifying a User's Account Information Using SAM 4-28
Adding a Group Using SAM 4-30
Removing a Group Using SAM 4-31
Adding and Removing Users From Groups Using SAM . . . 4-33
Adding a User Using HP-UX Commands 4-34
Removing a User Using HP-UX Commands 4-47
Deactivating a User's Account Using HP-UX Commands . . . 4-51
Reactivating a User's Account Using HP-UX Commands . . . 4-53
Displaying/Modifying User's Account Information Using HP-UX Commands 4-55
Adding a Group Using HP-UX Commands 4-58
Removing a Group Using HP-UX Commands 4-61
Changing a User's Primary Group Using HP-UX Commands . 4-67
Adding Users to Groups Using HP-UX Commands 4-72
Removing Users From Groups Using HP-UX Commands . . . 4-74
Displaying/Assigning Special Group Privileges Using HP-UX Commands 4-79
Managing Run-Levels 4-83
Creating a New Run-Level Using HP-UX Commands 4-84
Changing System Run-Levels Using HP-UX Commands . . . 4-86
Entering the System Administration Run-Level 4-88
Returning From the System Administration Run-Level . . . 4-89

5. Managing Peripherals
Overview of Adding a Peripheral 5-4
Moving Peripherals Using SAM 5-5
Moving a Local Printer or Plotter 5-5
Moving a Tape Drive 5-8
Moving a Terminal or Modem 5-11
Moving a Disk Drive Used for File Systems and Swap 5-13
Removing Peripherals Using SAM 5-18
Removing a Local Printer or Plotter 5-18
Removing a Tape Drive 5-20
Removing a Terminal or Modem 5-22
Removing a Disk Drive Used for File Systems or Swap 5-24
Creating Device Files Using HP-UX Commands 5-27
Moving Peripherals Using HP-UX Commands 5-27
Moving a Local Printer or Plotter 5-27
Moving a Tape Drive 5-29
Moving a Terminal or Modem 5-31
Moving the System Console 5-32
Moving a Disk Drive Used for File Systems and Swap 5-34
Moving a Disk Drive Containing the Root File System 5-36
Removing Peripherals Using HP-UX Commands 5-39
Removing a Printer or Plotter 5-39
Removing a Tape Drive 5-40
Removing a Terminal and Modem 5-41
Removing a Disk Drive Used for File Systems and Swap . . . 5-42

6. Managing the File System
Terms Used in this Chapter 6-2
Overview of HP-UX File Systems 6-5
What Does "File System" Mean? 6-5
Mountable File Systems 6-6
Listing Mounted File Systems 6-8
Types of File Systems 6-9
Disk Layout 6-9
HP-UX System Files 6-10
Creating File Systems 6-13
Adding a Disk and Creating a File System Using SAM 6-14
How to Use SAM 6-14

Adding a Disk and Creating a File System Using SAM . . . 6-15
Adding a Disk and Creating a File System Using HP-UX Commands 6-17
1. Installing Your Disk 6-17
2. Creating the Block and Character Device Files for Your Disk 6-17
Examples, Creating Block and Character Device Files . . . 6-18
3. Initializing Your Disk Using mediainit 6-21
4. Creating a New File System Using newfs 6-21
Using -L or -S to Determine File Name Length 6-23
Overriding the Default mkfs File System Parameters . . . 6-24
Overriding the Default Block and Fragment Values . . . 6-24
Overriding the Default Reserved Disk Space 6-25
Overriding the Default Bytes Per Inode 6-25
Determining Disk Type 6-26
Example, Creating a File System Using `newfs` Without Options 6-27
Another Example, Creating a File System with Smaller Block Size 6-27
After Creating a File System 6-28
Mounting File Systems 6-29
The Mount Directory 6-29
Mounting and Unmounting File Systems Using SAM 6-30
Mounting and Unmounting Local File Systems Using SAM . . 6-30
Modifying a File System's Characteristics Using SAM 6-31
Using SAM to Mount an Existing File System on a Disk from Another System 6-32
Mounting File Systems Using HP-UX Commands 6-34
Syntax of the mount command 6-34
Using the mount Command to Add a File System 6-35
Example 6-35
Example 6-36
Adding a CD-ROM File System 6-36
Mounting and Unmounting NFS File Systems Using SAM . . . 6-38
Configuring a Local File System for Export 6-38
Enabling or Disabling the Server File System 6-39
To Make Remote Systems Clients of a Local File System . . . 6-39
Mounting Remote File Systems 6-39

Unmounting a Remote File System 6-40
Unmounting an Exported File System on a Server 6-41
Mounting NFS File Systems Using HP-UX Commands 6-42
Preparations for Mounting Remote File Systems 6-42
Example: Mounting an NFS File System 6-43
NFS Mount Problems 6-43
Unmounting an Exported File System 6-44
Automatically Mounting Your File Systems at Bootup 6-44
Making Entries for Mounting a File System in the Checklist File 6-45
Example 6-46
How /etc/checklist is Used 6-47
Unmounting a File System Using HP-UX Commands 6-48
Syntax of the umount Command 6-48
Example, Unmounting a File System 6-49
Unmounting Currently Mounted File Systems 6-49
Unmounting File Systems by Type 6-49
Automatically Unmounting Your File Systems at Shutdown . 6-50
Creating a LIF Volume 6-51
Prerequisites and Conditions 6-51
Manual Procedure for Making a LIF Volume 6-52
Moving File Systems from One Disk to Another 6-53
Example, Moving File Systems from Disk to Disk 6-53
Modifying File Name Length 6-55
Changing File Names: Potential Problems and Troubleshooting Suggestions 6-55
Enabling Long File Names Using SAM 6-57
Enabling Long File Names Using HP-UX Commands 6-58
Disabling Long Filenames 6-60
Displaying Current Disk Usage Information 6-61
Using SAM to Recover Disk Space 6-63
Using Disk Quotas 6-64
Planning for Disk Quotas 6-65
Setting Up Disk Quotas on a File System 6-65
Mount the File System 6-66
Edit /etc/checklist to Add "quota" Option 6-66
Create the "quotas" File in the File System's Root Directory 6-66
Establish Quotas for Users of the File System 6-67

Using edquota -p 6-68
Setting quotas for an individual user 6-69
Setting Time Limits for a File System's Users 6-69
Turning On Disk Quotas 6-70
Turning On Disk Quotas by Mounting the File System . . 6-70
Turning On Disk Quotas Using the quotaon Command . . 6-71
Turning Off Disk Quotas 6-72
Displaying File System Usage, Soft and Hard Limits 6-73
Reporting File System Usage 6-73
Reporting a Summary of Ownership 6-74
Reporting Individual Usage 6-74
What to Do When Reaching a Hard Limit 6-75
When Not In an Editor 6-75
When In an Editor 6-75
Checking Consistency of File System Usage Data 6-76
Checking Quotas When Starting the System 6-76
Running quotacheck Interactively 6-77
Checking File System Consistency 6-78
Using the fsck Utility 6-78

7. Managing Swap Space
Terms Used in this Chapter 7-2
Types of Swap Space 7-3
Device Swap 7-3
File System Swap 7-3
Calculating How Much Swap Space You Need 7-4
How Much Swap Do You Have? 7-5
Estimating Swap Space Needs (A Rule of Thumb) 7-6
Swap Space Default 7-7
Allocating Swap Areas: Guidelines 7-7
Guidelines for Selecting Device Swap Areas 7-7
Guidelines for Selecting File System Swap Areas 7-10
Guidelines for Using File System Swap in Clusters 7-11
Guidelines for Assigning Swap Priority 7-12
Adding, Removing, or Changing Device Swap Space 7-13
Changing Primary Swap 7-13
Specifying Primary Swap Devices in the dfile 7-14
Example 7-14

Specifying Secondary Swap Devices in dfile 7-15
Core Dump Areas 7-15
Reinstalling HP-UX to Increase Primary Swap Space 7-16
Using SAM 7-17
Adding Device Swap Using SAM 7-18
Adding Device Swap When Creating a File System on a Disk . 7-18
Adding a New Disk For Swap Using SAM 7-20
Making Changes to Device Swap Using SAM 7-22
Adding File System Swap Using SAM 7-23
Changing File System Swap Values Using SAM 7-24
Adding Device Swap with the /etc/swapon Command 7-25
Add Your Disk 7-26
Creating Device Files for Your Disk 7-26
Creating the Block Device File 7-27
Creating the Character Device File 7-27
Listing the Device Files 7-28
Determine the Overall Usage of the Disk 7-28
Determining the Priority for the Swap Device 7-30
Enabling Your Swap Device with the /etc/swapon Command . 7-30
Using the -f option 7-31
Using the -e option 7-31
Enabling Your Swap Device Each Time You Boot the System 7-31
Making Entries for Device Swap in the Checklist File 7-32
Example, Adding Device Swap Using /etc/swapon 7-33
Removing Device Swap Using HP-UX Commands 7-34
Adding File System Swap Using `/etc/swapon` 7-35
Adding File System Swap 7-36
Choosing a File System for Swap 7-36
Determine Mount Point Directory of the File System . . . 7-36
Choosing Values for /etc/swapon Parameters 7-37
Example, Setting Up File System Swap with /etc/swapon . 7-38
Making Entries for File System Swap in the Checklist File . 7-41
Removing File System Swap Using HP-UX Commands . . . 7-42

8. Backing Up and Restoring Your Data
Terms Used in this Chapter 8-2
Determining Which Data to Back Up 8-3
Included Files 8-4
Excluded Files 8-5
Graph Files 8-6
Determining How Often to Back Up Data 8-7
Full Backups vs. Incremental Backups 8-8
Backup Levels 8-8
Recovery Example Using Three Backup Levels 8-10
Recovery Example Using Two Backup Levels 8-11
Choosing the Type of Storage Device to Use 8-12
Automating the Backup Process 8-17
Restoring Your Data 8-18
Backing Up and Restoring Tasks 8-19
Backing Up Your System To a Local Device Using SAM . . . 8-20
Backing Up Your System To a Remote Device Using SAM . . 8-24
Setting Up an Automated Backup Schedule Using SAM . . . 8-28
Viewing Entries 8-30
Adding an Entry 8-31
Removing Entries 8-36
Override the Backup Schedule to Perform the Backup Now . 8-37
Restoring All Files From a Local Device Using SAM 8-38
Restoring Individual Files From a Local Device Using SAM . 8-41
Restoring All Files From a Remote Device Using SAM 8-44
Restoring Individual Files From a Remote Device Using SAM 8-47
Viewing the Index File on the Local Media Using SAM . . . 8-51
Viewing the Index File on a Remote Device Using SAM . . . 8-53
Viewing the Index Files on Your System Using SAM 8-55
Backing Up Your System Using HP-UX Commands 8-56
The `fbackup` Command 8-57
Examples Using the `fbackup` Command 8-60
Backing Up to a Hard Disk Using the `cpio` Command . . . 8-65
Backing Up To a Hard Disk or DDS Format Tape Drive Using the `dd` Command 8-67
Setting Up an Automated Backup Schedule Using HP-UX Commands 8-69
Creating an Automated Backup Schedule File 8-70

Activating Your Automated Backup Schedule 8-72
Displaying Your Automated Backup Schedule 8-73
Deactivating Your Automated Backup Schedule 8-74
Changing Your Automated Backup Schedule 8-74
Restoring Files Using HP-UX Commands 8-74
The `frecover` Command 8-75
Examples Using the `frecover` Command 8-77
Restoring Data From a Hard Disk Using the `cpio` Command . 8-80
Restoring Data From a Hard Disk Using the `dd` Command . . 8-81
Viewing the Index File on the Local Device Using HP-UX Commands 8-83
Recovering From a System Crash Using Your Recovery Tape . . 8-84
Other Backup and Restore Utilities 8-86

9. Managing Printers and Printer Output
What is the Line Printer Spooling System? 9-1
Terms Used in this Chapter 9-3
LP Spooler Overview 9-6
The Components of the LP Spooler 9-8
Printer Names 9-8
Printer Classes 9-9
Print Destinations 9-10
System Default Printer (Destination) 9-10
Printer Interfaces 9-11
Printer Models 9-11
Device Files 9-13
Line Printer Scheduler 9-13
Local Printer 9-14
Remote Printer 9-14
Network-Based Printer/Plotter 9-14
Print Request Identification Number 9-14
Remote Spooling 9-15
Priorities of Printers and Print Requests 9-17
Using Plotters with the LP Spooler 9-18
Controlling Data Flow Through the LP Spooler 9-19
Logging and Analyzing Printer Activity 9-20
Initial LP Spooler Set Up 9-21
Line Printer Spooler Tasks 9-22

Viewing Printers and Print Request Status Using SAM . . . 9-23
Adding a Local Printer Using SAM 9-25
Adding a Remote Printer Using SAM 9-30
Adding a Network-Based Printer Using SAM 9-33
Removing a Printer Using SAM 9-35
Starting and Stopping the LP Spooler Using SAM 9-37
Determining the Status of the LP Spooler Using SAM 9-39
Disabling a Printer Using SAM 9-40
Enabling a Printer Using SAM 9-42
Changing A Printer Fence Priority Using SAM 9-44
Setting Up the LP Spooler Using HP-UX Commands 9-45
Ensuring the Printer Driver is in the Kernel Using HP-UX Commands 9-46
Determining if a Device File Exists for your Printer Using HP-UX Commands 9-49
Adding a Local Printer Using HP-UX Commands 9-51
Adding a Remote Printer Using HP-UX Commands 9-56
Adding a Network-Based Printer Using HP-UX Commands . 9-61
Creating a Printer Class Using HP-UX Commands 9-62
Removing a Printer or Printer Class Using HP-UX Commands 9-64
Accepting and Rejecting Print Requests for a Printer Using HP-UX Commands 9-67
Enabling or Disabling a Printer Using HP-UX Commands . . 9-69
Setting a Printer Priority Fence Using HP-UX Commands . . 9-71
Starting and Stopping the LP Spooler Using HP-UX Commands 9-72
Canceling Print Requests Using HP-UX Commands 9-73
Moving *All* Requests Using HP-UX Commands 9-75
Moving Selected Print Requests Using HP-UX Commands . . 9-78
Viewing the Status of Printers and Print Requests Using HP-UX Commands 9-79
Changing the Priority of Print Requests Using HP-UX Commands 9-81
Displaying Statistics about Printer Activity Using HP-UX Commands 9-83

10. Communicating With the Users on Your System
Terms Used in this Chapter 10-2
Displaying Messages to Users Logging into Your System 10-3
  `motd` 10-3
  `news` 10-3
Communicating With a User Who is Logged into Your System . 10-4
Broadcasting a Message to All Users Logged into Your System . 10-4
Communicating With Users on Other Systems Using UUCP . . 10-5
Using Electronic Mail Systems 10-6

11. System Accounting Concepts and Tasks
What Is in This Chapter? 11-2
Installation and Daily Usage 11-3
  How to Install System Accounting 11-3
    Update /etc/rc 11-3
    Create crontab Entries 11-4
    Set PATH for Accounting Commands 11-5
  Summary of Daily Operation 11-5
Overview of System Accounting 11-7
  Definitions 11-7
    prime/non-prime connect time 11-7
    process accounting records 11-8
    total accounting records 11-8
  Introduction to Commands 11-9
    Installation 11-9
    Disk Space Usage Accounting 11-10
    Connect Session Accounting 11-10
    Process Accounting 11-11
    Charging Fees 11-12
    Summarizing and Reporting Accounting Information . . . 11-12
  System Data Flow 11-13
  Login and Directory Structure 11-15
    Logging In 11-15
    Directory Structure 11-15
Disk Space Usage Accounting 11-17
  Reporting Disk Space Usage 11-17
    acctdusg 11-17
    diskusg 11-19

Creating Total Accounting Records 11-22
acctdisk 11-22
dodisk 11-22
Connect Session Accounting 11-24
Writing Records to wtmp – acctwtmp 11-24
Displaying Connect Session Records – fwtmp 11-25
Fixing wtmp Errors – wtmpfix 11-27
Creating Total Accounting Records 11-27
acctcon1 11-27
prctmp 11-30
acctcon2 11-30
Process Accounting 11-32
Turning Process Accounting On 11-32
turnacct on 11-33
accton 11-33
Turning Process Accounting Off 11-34
turnacct off 11-34
accton 11-34
Checking the Size of pacct 11-34
ckpacct 11-35
turnacct switch 11-36
Displaying Process Accounting Records – acctcom 11-37
Definitions of Information Produced by acctcom 11-38
Report Format Options 11-42
Record Selection Options 11-44
Sample Reports 11-47
Command Summary Report – acctcms 11-48
Producing a Readable Report – the -a option 11-48
Other Options 11-50
Sample Report 11-51
Creating Total Accounting Records 11-52
acctprc1 11-53
acctprc2 11-54
Charging Fees to Users – chargefee 11-55
Summarizing and Reporting Accounting Information 11-56
Displaying Total Accounting Records – prtacct 11-56
Report Format 11-57
Example 11-59

Merging Total Accounting Files – acctmerg 11-60
Command Options 11-61
Example 11-62
Creating Daily Accounting Information – runacct 11-63
Files Processed by runacct 11-63
The States of runacct 11-64
Recovering from Failure 11-66
Restarting runacct 11-67
Daily Reports 11-68
Displaying runacct Reports – prdaily 11-69
Daily Line Usage Report 11-70
Daily Resource Usage Report 11-71
Daily and Monthly Command Summary 11-71
Last Login 11-71
Creating Monthly Accounting Reports – monacct 11-72
Updating the Holidays File 11-73
Fixing Corrupted Files 11-74
Fixing wtmp Errors 11-74
Fixing tacct Errors 11-75
Sample Accounting Shell Scripts 11-76
grpdusg 11-76
The Shell Script 11-77
acct_bill 11-78
Examples 11-78
Output Produced by acct_bill 11-79
The Shell Script 11-79
System Accounting Files 11-81
Files in the /usr/adm Directory 11-81
Files in the /usr/adm/acct/nite Directory 11-82
Files in the /usr/adm/acct/sum Directory 11-83
Files in the /usr/adm/acct/fiscal Directory 11-83

A. System Parameters

Logical Groups of Parameters A-2
Using SAM to Check or Change HP-UX Kernel Parameters . . A-3
Parameter Descriptions A-6
acctresume A-7
acctsuspend A-8
bufpages A-9
check_alive_period A-11
dos_mem_byte A-13
dskless_fsbufs A-14
dskless_node A-16
dst A-17
fpa A-18
fs_async A-19
maxdsiz A-20
maxfiles A-21
maxfiles_lim A-22
maxssiz A-23
maxswapchunks A-24
maxtsiz A-25
maxuprc A-26
maxusers A-27
mesg A-28
minswapchunks A-29
msgmap A-30
msgmax A-32
msgmnb A-33
msgmni A-34
msgseg A-35
msgssz A-36
msgtql A-37
nbuf A-38
ncallout A-40
ndilbuffers A-41
netisr_priority A-42
nfile A-43
nflocks A-44
ngcsp A-45

ninode A-46
nproc A-47
npty A-48
nswapdev A-49
nswapfs A-50
num_cnodes A-51
num_lan_cards A-53
parity_option A-54
reboot_option A-55
retry_alive_period A-56
scroll_lines A-58
selftest_period A-59
sema A-60
semaem A-61
semmap A-62
semmni A-64
semmns A-65
semmnu A-66
semume A-67
semvmx A-68
server_node A-69
serving_array_size A-71
shmem A-73
shmmax A-74
shmmin A-75
shmmni A-76
shmseg A-77
swchunk A-78
timeslice A-79
timezone A-80
unlockable_mem A-81
using_array_size A-82

B. Swap Space Computation

Swap Space Computation B-1
Swap Space Computation Worksheet B-3
Example B-6

C. Federal Information Processing Standard

Restricting the chown(1) Function C-1
Controlling the Group ID of New Files C-2
Truncating Filenames During Pathname Resolution C-3

Index

Figures

1-1. SAM Main Window 1-23
1-2. The Main Window in SAM's Text-terminal Interface 1-27
1-3. Highlighting a New List-item Choice 1-28
1-4. Highlighting a Control Button 1-30
1-5. A Subarea List Window 1-33
1-6. A Functional Area 1-34
1-7. Selecting an Object 1-35
1-8. A List of Menu Items 1-36
2-1. `rmfn`: "Partitions" Screen 2-63
6-1. Typical HFS File System Structure 6-5
6-2. Mounting an Auxiliary File System 6-7
7-1. Device Swap Space Configurations 7-9
7-2. Swapping to File Systems in a Cluster 7-12
8-1. An Example Directory Tree 8-4
8-2. Example of Using Incremental Backups 8-10
8-3. Example of Using Incremental Backups Supported by SAM . 8-11
8-4. An Example Directory Tree 8-60
8-5. An Example Directory Tree 8-77
9-1. Line Printer Spooler "Plumbing Diagram." 9-7
11-1. Disk Usage Accounting 11-13
11-2. Connect Session Accounting 11-13
11-3. Process Accounting 11-14
11-4. Charging Fees 11-14
11-5. Summarizing and Reporting 11-14
11-6. System Accounting Directory Structure 11-16

Tables

1-1. What is in Each Chapter of this Manual 1-3
1-2. Other Sources of System Administration Information 1-8
1-3. Function Keys for SAM's Text-Terminal Interface 1-31
1-4. Meanings of Selected Keys 1-39
2-1. Pseudo-Drivers 2-57
4-1. HP-UX Global and Local Shell Initialization Files 4-38
4-2. "Removing a Group" Task Decision Table 4-62
4-3. "Changing a User's Primary Group" Task Decision Table . . 4-68
4-4. "Removing Users From Groups" Task Decision Table 4-75
6-1. Root File System Subdirectories 6-10
6-1. Root File System Subdirectories (Continued) 6-11
6-1. Root File System Subdirectories (Continued) 6-12
6-2. File System Parameters 6-24
8-1. Determining Which Device to Use for a Backup 8-13
8-2. Disk Drive Storage Capacities 8-14
8-3. Magnetic Tape Storage Capacities 8-15
8-4. HP Format Cartridge Tape Storage Capacities 8-15
8-5. DDS Format (DAT) Tape Storage Capacities 8-16
8-6. fbackup command options 8-58
9-1. LP Spooler Models for Plotters 9-18
9-2. Series 300/400 Printer Drivers 9-29
9-3. Series 300/400 Printer Drivers 9-48
9-4. Series 300/400 Printer Drivers 9-49
9-5. Interpreting `lpana's` Output 9-84
A-1. . . . . A-2

1

Introduction to System Administration

This manual is written for the HP-UX System Administrator. It is written to assist system administrators, with differing levels of expertise, accomplish the various *tasks* associated with maintaining an HP-UX system.

Conceptual material is provided when it directly supports the task being described. For a more thorough coverage of the *concepts* behind administering an HP-UX system, see *How HP-UX Works: Concepts for the System Administrator*, HP part number B2355-90029.

This manual assumes that you are running the 9.0 Release of HP-UX. If you are not yet running Release 9.0, your first task should be to update to 9.0. For details on how to do this, see *Installing and Updating HP-UX*, HP part number B1864-90009.

How to Use this Manual

This manual describes the *tasks* associated with HP-UX system administration. Begin your search for a particular task description in the *Table of Contents*.

The System Administration Manager (SAM) utility can be used to perform many HP-UX system administration tasks. For those tasks, this manual presents both methods (the SAM method and the "HP-UX Commands" method). For information on how to use SAM, see "Using SAM".

Conventions Used in this Manual

This manual uses the following typographic conventions:

Boldface	Words defined for the first time appear in boldface. For example, **non-volatile memory** is not erased when the computer's power is shut off.
`Underlined Computer`	Underlined computer font indicates items you type. For example: `/etc/newfs`
`Computer`	Computer font within text indicates HP-UX commands and utilities. Computer font within text is also used to refer to SAM column titles.
Italics	Manual titles, emphasized words, parameters to an HP-UX command, and entries in the *HP-UX Reference* manual appear in italics.
(Return)	Words or letters in boxes refer to keys on the keyboard or a control button within SAM.
[ ]	Items enclosed in square brackets are optional.
|	A vertical bar means that you should choose one of the items on either side of the bar, but not both.
`Softkey`	Softkey font indicates menu items within the SAM interface.
"Double Quotes"	Indicate titles of sections within a manual, manuals, SAM windows, and SAM menubar menus.

What's in this Manual

This manual is organized as follows:

Table 1-1. What is in Each Chapter of this Manual

Chapter 1, "Introduction to System Administration" ■ Guidelines for using this manual ■ An Overview of using SAM: □ A typical SAM task description □ Customizing the object list □ X Window System interface □ Text terminal interface
Chapter 2, "Constructing an HP-UX System" Provides a general overview of what to set up after installing or updating from a previous release. It also contains kernel reconfiguration procedures and pointers to useful, related information.
Chapter 3, "Starting and Stopping HP-UX" Discusses how to start up (boot up) your system. It also covers how to properly shut down your system (to avoid file system corruption).
Chapter 4, "Controlling Access to the System" Discusses how to control access to your system and its resources. It contains information about users, groups of users, file access permissions, and run-levels.
Chapter 5, "Managing Peripherals" Provides an overview of: ■ adding a peripheral ■ removing a peripheral ■ moving a peripheral

Table 1-1. What is in Each Chapter of this Manual (continued)

Chapter 6, "Managing the File System" Provides information about: ■ creating new file systems. ■ mounting and unmounting file systems. ■ different types of file systems. This chapter also discusses **disk quotas**; a method of controlling the disk space used by individual users.
Chapter 7, "Managing Swap Space" Describes the tasks associated with managing swap space (part of HP-UX's virtual memory system). It also discusses the various types of swap space.
Chapter 8, "Backing Up and Restoring Your Data" Describes the tasks of backing up and restoring data as well as guidelines for deciding which device to use to back up your system.
Chapter 9, "Managing Printers and Printer Output" Describes the tasks associated with managing the line printer spooling system. The HP-UX line printer spooling system is used to control output to printers.
Chapter 10, "Communicating With the Users on Your System" Discusses various ways that you can communicate with the users of your system. As a system administrator, you may find it necessary to communicate with the users of your system (for example, to let them know about an upcoming event such as an operating system upgrade).
Chapter 11, "System Accounting" Provides information about the System Accounting subsystem which allows you to closely monitor the usage of the resources of your system (and if necessary, bill users for their resource usage).

Table 1-1. What is in Each Chapter of this Manual (continued)

Appendix A, "System Parameters" Describes numerous operating system parameters that can be used to "tune" the operation of your system.
Appendix B, "Swap Space Computation" Contains some additional (detailed) information (beyond what is in Chapter 7, "Managing Swap Space") about calculating how much swap space you need to allocate for your system. It should be needed only when disk space is very limited.
Appendix C, "Federal Information Processing Standard" Describes how to modify certain areas in HP-UX so that they conform to the Federal Information Processing Standard (FIPS).

What System Administrators Need to Know

This manual is intended to assist system administrators of all skill levels maintain their systems. However, there are basic skills that you should know before you attempt to administer an HP-UX system.

Specifically, you should know how to do the following things:

- Log in and out of your system.
- Move about the HP-UX directory tree (change directories).
- Distinguish between "absolute" and "relative" path names.
- Edit files using one of the HP-UX editors (such as `vi` or `ed`).
- Display the contents of files using `cat` or `more`.
- Search for text in files using `grep`.
- Move, copy, and remove files using `mv`, `cp`, and `rm` respectively.
- Use at least one of the HP-UX shells (such as `sh`, `csh`, `ksh`).
- Display manual reference pages using the `man` command.

If you need to learn more about the above topics, see:

A Beginner's Guide to HP-UX, HP part number B1862-90000

Using HP-UX, HP part number B2910-90001

Shells: User's Guide, HP part number B2355-90046

The Ultimate Guide to the `vi` *and* `ex` *Text Editors*, HP part number 97005-90015 (Benjamin/Cummings Publishing Co.)

A System Administrator's Responsibilities

The HP-UX System Administrator is responsible for installing and configuring the HP-UX operating system software, and for maintaining the system and repairing it when something goes wrong. More specifically, the HP-UX system administrator may need to do the following things:

- Install and test the hardware.
- Install the HP-UX operating system software.
- Configure the HP-UX operating system.
- Update the HP-UX operating system software.
- Allow users to access the system (provide user accounts, etc.).
- Add peripheral devices to the system.
- Monitor file system use and growth.
- Back up and restore files.
- Detect and correct file system errors.
- Assist others in using the system.
- Provide a backup system administrator to assist users (when the primary administrator is unavailable).

Where to Find Other Information About System Administration

The following table lists other manuals/books that can help you administer your system:

Table 1-2. Other Sources of System Administration Information

Title	Focus
Installing Peripherals, HP part number B1864-90011	Contains information about adding peripherals to your system and creating device files for those peripherals.
How HP-UX Works: Concepts for the System Administrator, HP part number B2355-90029	Provides detailed information about the *concepts* behind HP-UX system administration tasks.
Managing Clusters of HP 9000 Computers, HP part number B1864-90015	Discusses HP-UX system administration from the HP-UX cluster perspective. It should be used in conjunction with *this* manual when your computer is a member of an HP-UX cluster. Many HP-UX system administration tasks have special requirements (or differences) when your computer is a member of an HP-UX cluster.
Installing and Updating HP-UX, HP part number B1864-90009	Explains how to install (or re-install) HP-UX on your system. It also describes how to update HP-UX from a previous release.
HP-UX System Security, HP part number B1862-90009	Explains the special requirements for setting up HP-UX in a secure operating mode. If your system requires above-average security, use the *HP-UX System Security* manual as your primary system administration manual and use *this* manual as a secondary reference.

Table 1-2.
Other Sources of System Administration Information (continued)

Title	Focus
HP-UX Reference, HP part number B2355-90033	Provides a complete reference to HP-UX commands; the printed version of the manual reference pages. Commands in the reference are divided into numbered sections.
Owner's Guide for HP-UX Users	This manual presents much of the initial information you will need to get started with your particular HP 9000 machine. The document title and part number vary according to specific model you ordered.

Using SAM

SAM stands for *S*ystem *A*dministration *M*anager. This tool allows you to perform many system administration tasks without using the underlying HP-UX commands that are associated with the task. SAM can also save you time and keystrokes.

SAM can help you with tasks in the following areas:

- Working with users' accounts
- Working with groups of users
- Maintaining system security
- Working with file systems
- Configuring your swap space
- Adding or removing peripherals
- Working with the line printer spooler
- Backing up and recovering files (automated or manual system backups)
- Configuring network connections (LAN, X.25, FDDI, and TokenRing)
- Configuring UUCP communication
- Administering systems remotely from one location
- Configuring HP-UX clusters (SAM is required for converting a standalone system to an HP-UX cluster server and for several other cluster related tasks)
- Configuring the HP-UX kernel

Note SAM is an optionally loadable part of HP-UX. If you have not loaded SAM onto your system, you will not be able to use it. You can use the `update` program to add SAM to your system if you did not originally load it and currently want to use it. For details about how to do this, see the *Installing and Updating HP-UX* manual.

SAM Overview

SAM has two user interfaces, an X Window System interface and a text terminal interface. The two interfaces differ in the screen appearance and keyboard/mouse interactions. For text terminal systems, refer to "Using SAM with a Text Terminal".

SAM provides an on line help system to assist you when you need additional information. A procedure for accessing the SAM help system is provided later in this section. Refer to the SAM help system for information about navigating within SAM and the following primary components of SAM:

- SAM main window
- functional areas
- step menus
- message boxes
- checkboxes
- control buttons:

  (OK)

  (Apply)

  (Cancel)

  (Help)

  (Add)

  (Modify)

  (Remove)
- menu buttons
- grey areas
- "View" menu
- "Options" menu
- "Actions" menu
- "Help" menu

To get into the SAM help system:

1. Ensure that you have superuser capabilities.
2. Enter SAM; type:

   `/usr/bin/sam`

3. Activate the (Help) control button. SAM displays the help window. If necessary, resize the window to read the text. The help text reformats automatically.
4. Scroll the text until you see the "See Also" section.
5. Enter the "Using SAM (The System Administration Management Tool)" area.
6. Scroll the text until you see a list of additional SAM topics.
7. Enter the "SAM Overview" area.
8. Scroll the text until you see the following two sections:

   "Primary Components of the SAM User Interface"

   "Terms Used in Describing the SAM User Interface"

9. Enter and read each of these areas. The "Terms Used in Describing the SAM User Interface" area describes:
   - Highlighting objects
   - Choosing menu items
   - Turning on and off checkboxes
   - Activating control buttons

There are two additional methods to get information from the SAM help system:

1. You can choose one of the following items from the "Help" menu within a functional area:

   `Overview...` to get information about the current functional area.

   `Keyboard...` to get information about keyboard navigation within SAM.

   `Using Help ...` to get information about using the SAM Help system.

   `Product Information...` to display the version of SAM you are running.

2. You can press the (f1) *keyboard key* from within a dialog or message box. Pressing the (f1) key gives you context-sensitive information for the object field at the location of the cursor. For text terminals, refer to "Using SAM with a Text Terminal" to for keyboard key mappings.

A Typical SAM Task

A typical task using SAM consists of the following steps:

1. Ensure that you have superuser capabilities.
2. Run SAM; type:

   `/usr/bin/sam`

3. Enter a functional subarea by highlighting an item from the list in the SAM main window and activating the (Open) button. If you are given another list, repeat this procedure. For example, highlight `Peripheral Devices` and activate the (Open) button and then highlight `Tape Drives` and activate the (Open) button.
4. (optional) Customize the contents or format of an object list within a functional area. To customize the object list, see "Overview of Customizing the Object List".

5. (optional) Update the objects displayed by choosing `Refresh List` from the "Options" menu. This updates the data displayed.

   For example, if you are monitoring your print request in the print request queue, you would frequently update the displayed data by choosing `Refresh List` to reflect the current state of the print request queue.

6. Highlight an object or objects from the object list and then choose a task from the "Action" menu. If you are adding to the object list, you need not highlight an object before choosing a task from the "Actions" menu.

   For example, if you are performing user account tasks, you can choose from the tasks listed from the "Action" menu (`add`, `remove`, `modify`, `deactivate`, `reactivate`, and `task customization`).

7. Fill in dialog boxes and then activate the (Apply), (OK), or (Cancel) control button.

   Activating the (Apply) control button performs the task, but does not return you to the object list.

   Activating the (OK) control button performs the task and returns you to the object list.

   Activating the (Cancel) button returns you to the object list without applying changes or performing a task.

8. If SAM requires you to read a message before continuing, read the message and activate the (OK) button to proceed with the task

9. Exit SAM:

   - From the SAM main menu, activate the (Exit SAM) control button.
   - From the object list, choose `Exit` from the "List" menu and then activate the (Exit SAM) control button from the SAM main menu.

   If you have performed tasks that require you to generate a new kernel, SAM will prompt you to create the kernel and reboot the system.

   In the case of complex tasks, SAM displays a step menu. Each task in the step menu is required for the overall complex task. If there is a required order to the step menu, SAM allows you access to the step to be performed first and greys out the remaining tasks until you have completed the prerequisite task. If there is no particular order to the step menu, SAM allows you to access them in any order. When a step is completed, SAM summarizes the result of the tasks next to the step menu item.

Overview of Customizing the Object List

Customizing the object list allows you to:

- select the type of data you want to view. See "Changing the Object List Type".
- alter the format of the data displayed. See "Changing the Format of the Object List".
- conditionally display a subset of the total available data. See "Displaying a Subset of Objects"
- alter the order of the data displayed. See "Changing the Object List Order".

Once you customize the object list, you can preserve this view of the data for the next time you use SAM. If you do not explicitly preserve your changes to the object list, SAM returns to the default format the next time you use SAM.

Changing the Object List Type

To change the objects displayed within a functional area, choose an alternative object type from the "List" menu.

Note Changing the object list type from the "List" menu changes the associated tasks listed in the "Action" menu.

For example, within the "Users and Groups" functional area the "Actions" menu items for the users object list are:

`Add...`

`Remove...`

`Modify`,

`Deactivate..`

`Reactivate...`

`Task Customization`

In comparison, the "Actions" menu items for the groups object list are:

`Add...`

`Remove...`

`Modify`

Changing the Format of the Object List

To change the format of the object list:

1. Enter a functional area by highlighting an area from the list and activating the (Open) control button until an object list is displayed.
2. Choose `Columns...` from the "View" menu.

   For each column (attribute) in the object list, you can define:

   - a numeric column position (1 to the number of columns displayed) using a menu button.
   - justification (left *or* right) using a menu button.
   - width (in characters) by filling in the field.
3. Activate one of the following control buttons:

   (OK) to view the newly defined format and exit the "Columns" window.

   (Apply) to implement the newly defined format, but remain in the "Columns" window.

   (Cancel) to cancel the most recent change and return to the object list.

To preserve this view of the objects for the next time you enter this functional area of SAM:

1. Exit the "Columns" window by activating the (OK) or (Cancel) control button.
2. Choose `Save View as Default` from the "View" menu.

To return to the original listing of the objects:

1. Choose `Columns...` from the "View" menu.
2. Activate the (System Defaults) button and activate the (OK) control button.

Displaying a Subset of Objects

Selectively displaying elements is helpful for viewing the relative subset of total objects for your task. For example, within the "Users and Groups" functional area, you can display only those users with a user identification number below 20 belonging to user group *laboratory*. You define the criteria based on an operator (matches, not, greater than, or less than) and a field value. You can define your subset based on multiple attribute criteria. Multiple attribute criteria use the AND logical operation.

To selectively view objects that met particular criteria:

1. Choose `Filter...` from the "View" menu.
2. Choose one of the following operators for the field attribute(s):

   `matches`

   `not`

   `greater than`

   `less than`
3. For each field you defined an operator for, fill in the associated value to base the conditional operator.
4. Activate one of the following control buttons:

   (OK) to view the newly defined object list subset and exit the "Filter" window.

   (Apply) to implement the newly defined object list subset, but remain in the "Filter" window. The number of filtered items is displayed in the "Filter" window. For example:

   ```
   Current filter: showing 8 of 57 total items
   ```

   (Cancel) to cancel the most recent change and return to the object list.

To preserve this view of the objects for the next time you enter this functional area of SAM:

1. Exit the "Filter" window by activating the (OK) or (Cancel) control button.
2. Choose `Save View as Default` from the "View" menu.

To return to the original listing of the objects:

1. Choose `Filter...` from the "View" menu.
2. Activate the (System Defaults) button and activate the (OK) control button.

Changing the Object List Order

You can change the object list order (ascending or descending) based on the value of one or multiple attributes.

To change the object list order:

1. Choose `Sort...` from the "View" menu.
2. Based on the attribute on which you want to base the order of the object list, choose the priority from the attribute's `Priority` menu button.
3. For each priority defined, choose `Ascending` or `Descending` from the attribute's `Direction` menu button.
4. Activate one of the following control buttons:

   (OK) to view the newly defined object list order and exit the "Sort" window.

   (Apply) to implement the newly defined object list order, but remain in the "Sort" window.

   (Cancel) to cancel the most recent change and return to the object list.

To preserve this view of the objects for the next time you enter this functional area of SAM:

1. Exit the "Sort" window by activating the (OK) or (Cancel) control button.
2. Choose `Save View as Default` from the "View" menu.

To return to the original listing of the objects:

1. Choose `Sort...` from the "View" menu.
2. Activate the (System Defaults) button and activate the (OK) control button.

Using SAM with an X Window System

This section describes the following tasks for using SAM with and X Window System:

- Setting up your system
- Running SAM
- Exiting SAM
- Customizing the SAM interface

If you are using a text terminal, this section of the chapter does *not* apply to your terminal; refer to "Using SAM with a Text Terminal".

Setting Up Your System

There are three system requirements for using SAM with an X Window System:

1. The `SAM` fileset must be part of your HP-UX system. You can use the `update` program to add the SAM fileset to your system, see *Installing and Updating HP-UX*.
2. The `X11-RUN` fileset must be part of your HP-UX system. You can use the `update` program to add the `X11-RUN` fileset to your system, see *Installing and Updating HP-UX*.

Note The *SAM* and *X11-RUN* filesets must also be part of any system intended to be administered locally or remotely by SAM.

3. The `DISPLAY` environment variable must be set to reflect the display on which you want SAM to appear.

To view the current environment variable values for all shells, type `env`.

To view the current local shell variable values for all shells, type `set`.

Korn and Bourne Shell. To set the `DISPLAY` environment variable on the local system in the Korn and Bourne shell, type:

```
DISPLAY=hostname:0.0
export DISPLAY
```

hostname is the name returned from typing the `/bin/hostname` command on your local system.

Note In Korn and Bourne shells, subsequent changes to a shell variable are globally reflected after you have exported a variable with the `export` command.

Typically, the DISPLAY environment variable for the local system is set and exported in the `.profile` file. If you are running HP VUE, the DISPLAY environment variable for the local system is set in the `.vueprofile` file.

Note If the DISPLAY environment variable is not set, SAM will attempt to execute the text terminal interface.

C Shell. To set the `DISPLAY` environment variable on the local system in the C shell, type:

```
% setenv DISPLAY hostname:0.0
```

hostname is the name returned from typing the `hostname` command on the local system.

Typically the DISPLAY environment variable for the local system is set in the `.login` file. If you are running HP VUE, the DISPLAY environment variable for the local system is set in the `.vueprofile` file.

Note If the DISPLAY environment variable is not set, SAM will attempt to execute the text terminal interface.

Entering SAM

To start up the System Administration Manager (SAM):

1. Ensure that you have superuser capabilities.
2. Enter SAM; type:

   <u>`/usr/bin/sam`</u>

   SAM should respond with the following message:

   `Running SAM on DISPLAY=`*hostname*`:0.0`

To perform system administration tasks on a remote system using SAM, refer to "Using SAM for Remote System Administration".

Note SAM is an optionally loadable part of HP-UX. If you have not loaded SAM onto your system, you will not be able to use it. You can use the `update` program to add SAM to your system if you did not originally load it and currently want to use it. For details about how to do this, see the *Installing and Updating HP-UX* manual.

SAM presents you with the main window which looks similar to this:

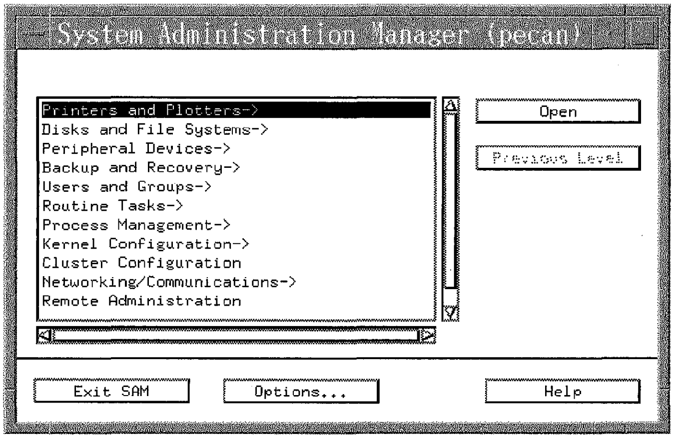


Figure 1-1. SAM Main Window

Exiting SAM

To exit SAM from the SAM main window (see Figure 1-1 in "Entering SAM") or in a functional subarea menu, activate the (Exit SAM) control button.

To exit SAM from a functional area with an object list displayed:

1. Choose `Exit` from the "List" menu.
2. Activate the (Exit SAM) button from the SAM main window.

To exit SAM from a dialog box:

1. Activate the (Cancel) button.
2. Choose `Exit` from the "List" menu.
3. Activate the (Exit SAM) button from the SAM main window.

You can also close the SAM main window with the window manager.

Customizing the SAM Interface

You can customize the following two features of the SAM interface:

- colors
- fonts

SAM colors and fonts are determined by the environment in which SAM is running. SAM requires only foreground and background color. However, if SAM is running under VUE, SAM will use VUE colors (for example, different colors for the menubar, dialog boxes, etc.). The VUE definitions for resources *supersede* the X11 resource definitions in your **`$HOME/.X11defaults`** file. To customize the resources for your VUE environment refer to the VUE documentation.

The `.X11defaults` file entries for customizing SAM colors are:

```
sam*foreground
sam*background
```

SAM uses two fonts, a proportional, sans-serif "system" font, and a monospace "user" font. The "system" and "user" fonts are implemented for the following primary components of the SAM interface:

"system"
- menubar
- menu items
- most labels and titles

"user"
- user input text
- control buttons
- static message text
- scrollable message text
- list boxes (object list and selection list items)
- list box column titles (object list and selection list column headings)

The entries for customizing SAM fonts are:

```
sam*userFont
sam*systemFont
```

Using SAM with a Text Terminal

A **text terminal** is a combination video display/keyboard. The video display of a text terminal is composed of **characters**—letters, numbers, and symbols. It may be able to use **graphics characters** to draw lines and other elements of simple images. Such a terminal is not capable of rendering the detailed **bit-mapped graphics** that are used by the X Window System.

SAM has a special interface for use on text terminals. Instead of using a mouse to navigate through the SAM screens, you must use particular keys (or combinations of keys) to move from one part of a screen to another and to move among screens.

The purpose of this section is to help you understand how to control SAM from the text-terminal interface.

Entering SAM

Note SAM is an optionally loadable part of HP-UX. If you have not loaded SAM onto your system, you will obviously not be able to use it. You can use the `update` program to add SAM to your system if you did not originally load it and currently want to use it. For details about how to do this, see the *Installing and Updating HP-UX* manual.

To start SAM, type:

```
/usr/bin/sam
```

In a few moments, SAM's main window (see Figure 1-2) will appear.

To perform system administration tasks on a remote system using SAM, see "Using SAM for Remote System Administration".

Figure 1-2 shows the appearance of the main window in SAM.

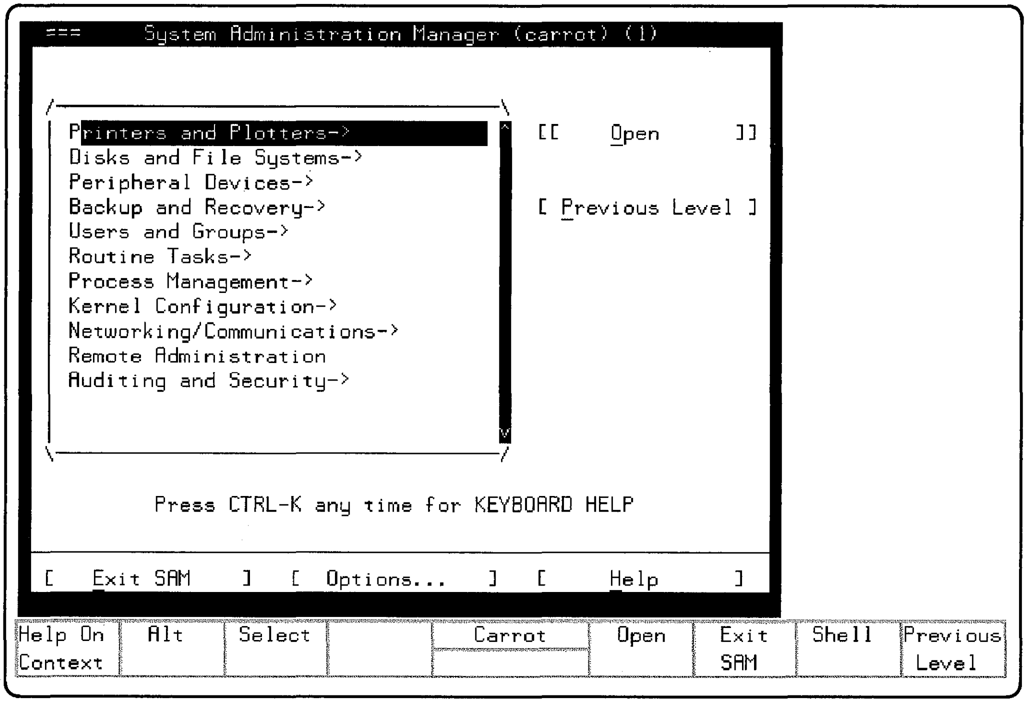


Figure 1-2. The Main Window in SAM's Text-terminal Interface

Note that there is a list of items within a box inside the window. `Printers and Plotters->` is **highlighted** (displayed in inverse video). A highlighted item can be thought of as having been designated for attention.

To choose another entry in this list, press the ▲ or ▼ arrow keys until the highlight is on your choice. For example, if you want to work with peripherals, move the cursor to the position shown in Figure 1-3:

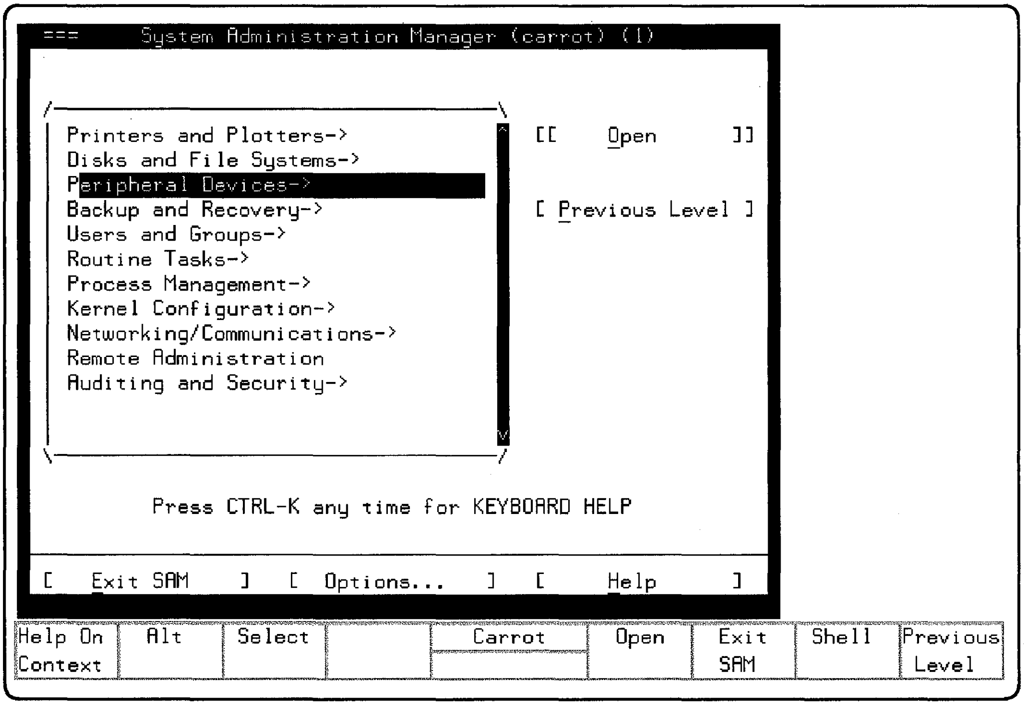


Figure 1-3. Highlighting a New List-item Choice

The highlight is now on the `Peripheral Devices->` list item.

Using Control Buttons

In the window are **control buttons** with these labels:

```
[[ Open      ]]

[ Exit        ]

[ Options... ]

[ Help        ]
```

Activate these buttons to make SAM carry out different actions.

Use the (Tab) key to return to "cycle through" all of the control buttons. To cycle through the control buttons in reverse order, hold down the (Shift) key while you press (Tab). Eventually you will return to the list of functional areas.

To activate a control button, do one of the following:

- **Highlight** the button by pressing the (Tab) key one or more times. When a button is highlighted, that indicates that is ready for activation.

  Activate the highlighted control button by pressing the (Return) on the keyboard.

- **Activate** a control button immediately by pressing a *mnemonic* key. For example, notice in Figure 1-3 that the letter `O` on the (Open) control button is underlined. Press the (O) key on the keyboard, and the (Open) control button is highlighted and activated immediately.

Figure 1-4 shows the appearance of the SAM main window when the Help control button is highlighted.

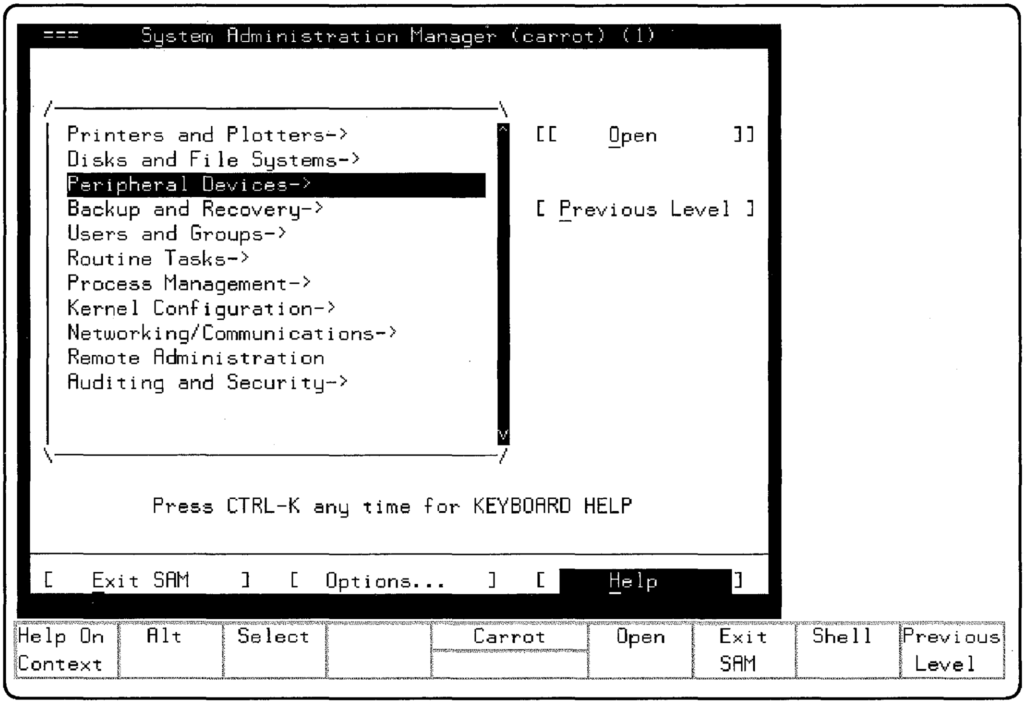


Figure 1-4. Highlighting a Control Button

Using Softkeys

Hewlett-Packard terminals (and some others) display eight **softkey labels** below the window area. The keyboard keys to which these labels correspond are in a row across the top of the terminal's keyboard, and they are usually labeled f1 through f8.

The labels may change when a new window appears. Table 1-3 lists the labels which you will see most often.

Note

VT-100 (and other ANSI-standard) terminals will not display the function-key labels.

The last column of Table 1-3 lists the keys or key combinations that give the equivalent result for these terminals.

Table 1-3. Function Keys for SAM's Text-Terminal Interface

Label	Meaning	Key(s)[1]	
		HP or Wyse	VT-100 or ANSI
`Help on Context`	Get help in understanding an element displayed on the screen	f1	Help or PF 2
`Alt`	Type alternate character	f2	PF 1
`Select`	Highlight an item or open a menu	f3 or Spacebar	Spacebar
`Menubar on/off`	Move cursor to menubar	f4	PF 1, Spacebar or PF 1, =
`Open`	Open the highlighted functional area or subarea	f5	Return
`Previous Level`	Return to the previous level of SAM	f8	(none)
`Shell`	"Escape" (temporarily) to a shell	f7	(none)
`Exit`	Exit the current window	f6	(none)
`Exit SAM`	Exit SAM entirely	f8	(none)

1 Keys are specified by the symbols which appear on their keycaps. Presence of a comma (",") between two keycaps means that the keys should be pressed in sequence.

Exiting SAM

To exit SAM:

- Activate any control button labeled (Exit SAM), or
- Press the softkey labeled `Exit SAM`.

The main window (and any other windows that may be open) will close, and the shell prompt will return.

Entering a Functional Area

From SAM's main window, highlight `Printers and Plotters->`.

Note If a functional area item ends in "`->`", you will be routed to a subarea list window. From there you will choose a functional subarea.

If you choose a functional area list item that does *not* end in "`->`", you will be presented with a functional area window immediately.

Press (Return). A subarea list window (like Figure 1-5) appears on your screen.

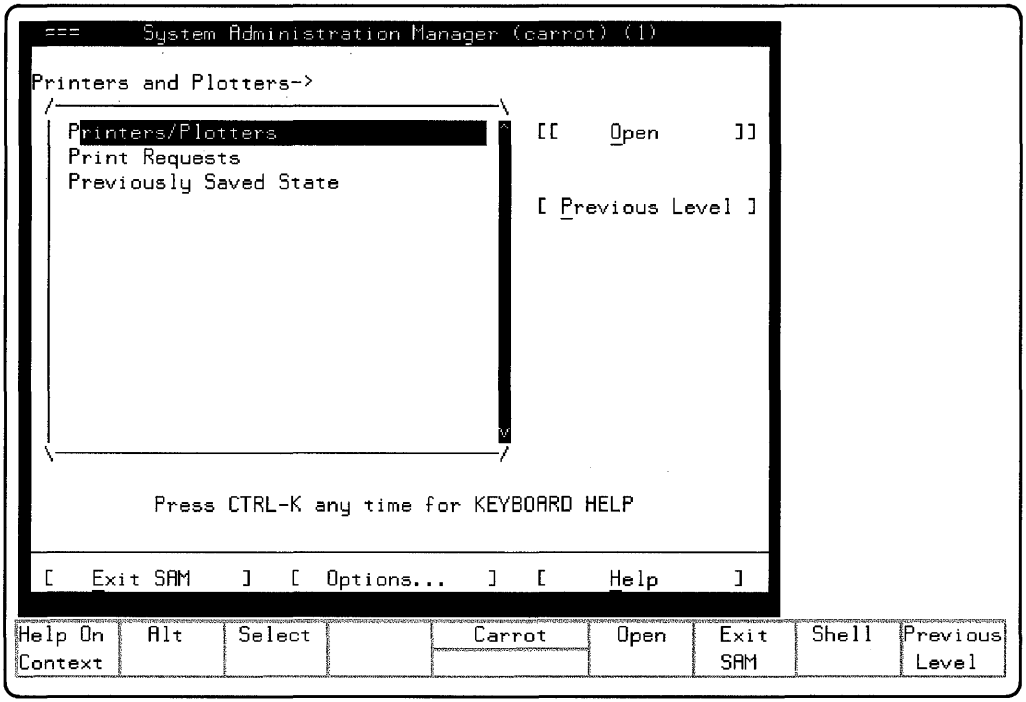


Figure 1-5. A Subarea List Window

Highlight the `Printers and Plotters` subarea. Press (Return). The "Printer/Plotter Manager" functional area appears. See Figure 1-6.

Selecting an Object. In the functional area illustrated by Figure 1-6, the cursor is on the first **object** in the **object list**.

Note Occasionally you may find that an object list is empty. You can use items from the "Actions" menu to add objects to the list in any functional area. See Figure 1-8 for an example of the items in an "Actions" menu.

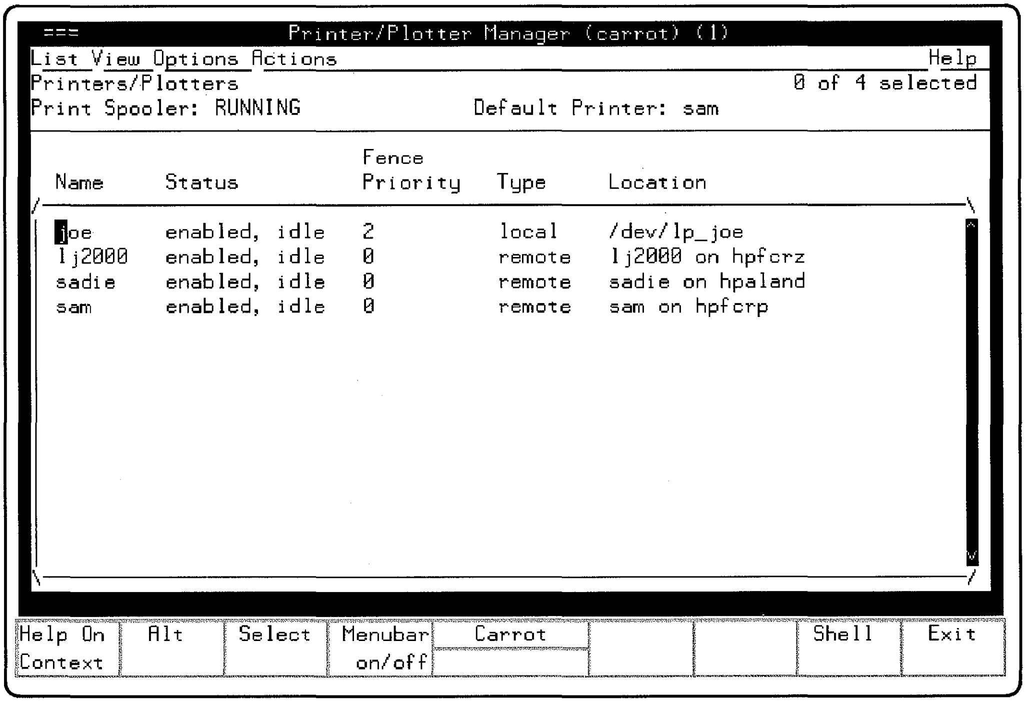


Figure 1-6. A Functional Area

Move the cursor to any item you wish SAM to act upon by using the ▲ and ▼ keys. Then highlight the item by pressing (Spacebar). Figure 1-7 shows one highlighted item in an object list.

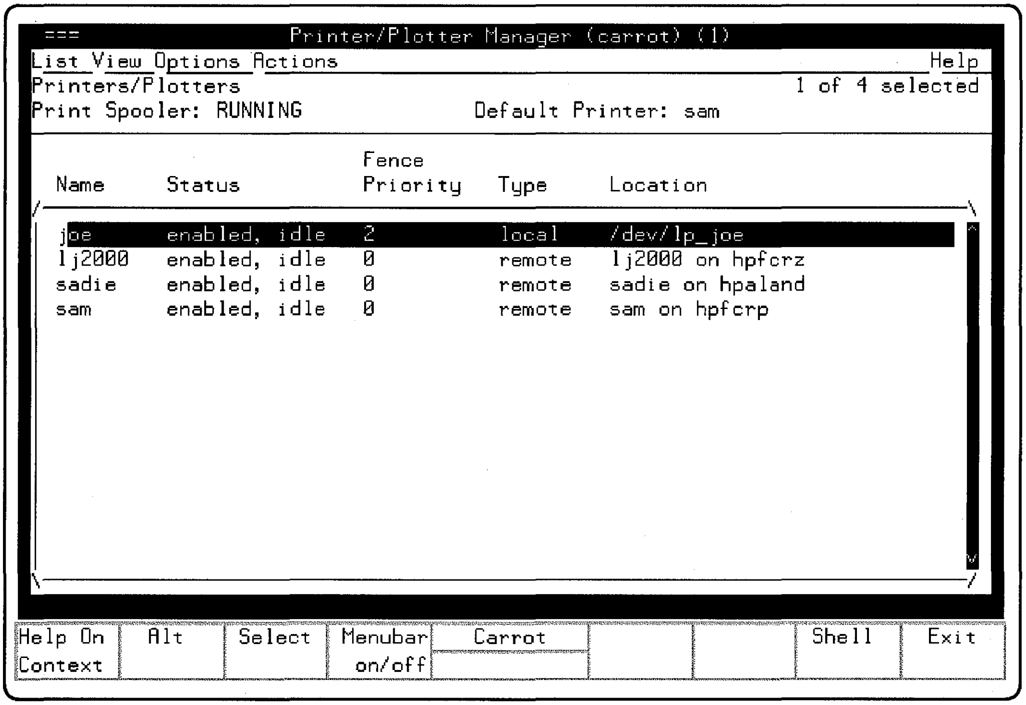


Figure 1-7. Selecting an Object

SAM can now work with the highlighted object. You can highlight more than one object at a time. For more information on selecting objects, see Table 1-4.

Opening a Menu. There is a **menubar** near the upper-left corner of the screen. It contains the titles "List", "View", "Options", and "Actions".

To move the cursor to the menubar:

- Press (f4) on HP or Wyse terminals
- Press (PF 1), then (Spacebar) on VT100 or ANSI terminals.

Each of the titles on the menubar has one or more **menu items** associated with it. To see the menu items associated with a particular title, use the (◀) and (▶) keys to highlight the title whose menu you wish to see, then press (Spacebar). See Figure 1-8 to see what an "Actions" menu looks like.

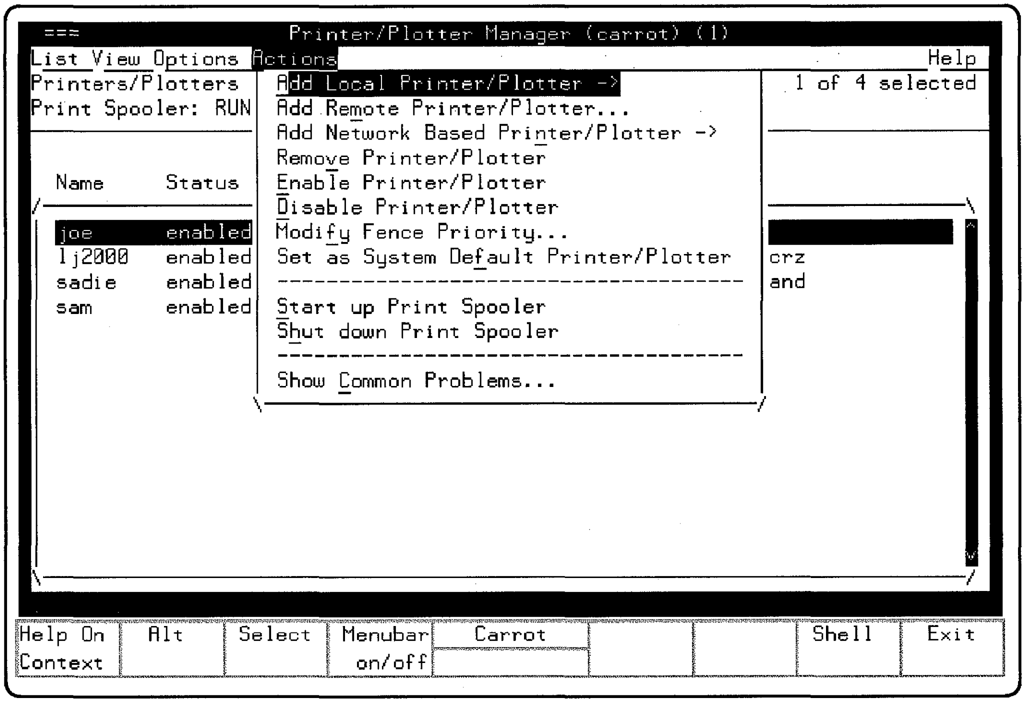


Figure 1-8. A List of Menu Items

Choosing a Menu Item. You can **choose** a menu item in either of two ways:

- **Highlight** the menu item of your choice by using the ▲ and ▼ keys. Notice that if you press either of the arrow keys many times, the highlight "cycles through" the menu over and over again.

  Choose the highlighted menu item by pressing the Return on the keyboard.

- If the menu item contains an underlined character, you can **choose** it immediately by pressing a *mnemonic* key. For example, notice in Figure 1-8 that the letter "A" in the `Add Local Printer/Plotter` menu item is underlined. Press the E key on the keyboard, and the `Add Local Printer/Plotter` menu item is highlighted and activated immediately.

Note You may not be able to highlight and choose some of the menu items. For example, an "Actions" menu item for removing a device cannot be chosen unless one of the objects in the object list is highlighted. These items may be presented at low intensity or in an alternate color, or they may be filled in with tildes ("~").

Using Buttons and Checkboxes

There are several features in SAM that have a special appearance and which exhibit special behavior.

Menu Buttons. Some screen buttons present a range of settings from which you must choose. These **menu buttons** differ in appearance from ordinary buttons by the presence of `->` after the button label. Menu buttons look like this:

`[` *label* `->]`

To "open " a menu button, highlight it and press Spacebar. The menu button expands into a small menu.

To choose an item from the menu, press the ▲ and ▼ keys to highlight your choice, then press Spacebar. The choice is displayed on the menu button.

Radio Buttons. Within the "List" menu, you may find two or more views of a functional area. Access to these alternate views is controlled by a **radio button** which may be turned "on" or "off". Radio buttons differ in appearance from ordinary buttons by the presence of a diamond shape to the left of the button label. A radio button looks like this when it is turned "on":

<*> *view_name*

A radio button looks like this when it is turned "off":

< > *view_name*

To turn a radio button on or off, , highlight the radio button with the ▲ or ▼ arrow keys and press Spacebar. The screen will change to another view of the functional area.

Radio buttons are *mutually exclusive*: within a "List" menu, only one button at a time may be turned on.

Checkboxes. A **checkbox** is an object which can be turned "on" or "off." Checkboxes differ in appearance from ordinary buttons by the presence of a square shape to the left of the button label. A checkbox looks like this when it is turned "on":

[x] *label*

A checkbox looks like this when it is turned "off":

[ ] *label*

To turn a checkbox "on" or "off", use the Tab key to move the highlight over the checkbox, then press Spacebar. If it was "on," the x in the checkbox disappears. If it was "off," an x appears in the checkbox.

Checkboxes are *not* mutually exclusive. You may turn "on" or "off" as many as you need.

Navigating with Keys and Key Combinations

You must use particular keys and combinations of keys to navigate and perform particular tasks in SAM. Table 1-4 lists the special meanings of the keys you must use to navigate within the windows in SAM's text-terminal interface.

Table 1-4. Meanings of Selected Keys

Action	Key(s)[1]	
	HP or Wyse	VT-100 or ANSI
Move the cursor one space to the right	▶	▶
Move the cursor one space to the left	◀	◀
Move the cursor up one line	▲	▲
Move the cursor down one line	▼	▼
Move the cursor to the next field	Tab	Tab
Move the cursor to the menubar	f4	PF 3
Scroll a list up one page	Shift-▲	(none)
Scroll a list down one page	Shift-▼	(none)
Scroll a list up one line	f2, ▲	PF1, ▲
Scroll a list down one line	f2, ▼	PF1, ▼
Scroll a list left one page	Prev	(none)
Scroll a list right one page	Next	(none)
Scroll a list left one character	f2, ◀	(none)
Scroll a list right one character	f2, ▶	(none)

1 Keys are specified by the symbols which appear on their keycaps. Presence of a comma (",") between two keycaps means that the keys should be pressed in sequence; presence of a hyphen ("-") between two keycaps indicates that the keys should be pressed simultaneously.

Table 1-4. Meanings of Selected Keys (continued)

Action	Key(s)[1]	
	HP or Wyse	VT-100 or ANSI
Highlight one item	f3 or Spacebar	Spacebar
Highlight all items in a list	f2, /	PF 1, /
Highlight a range of items	1. f2, f3 on first item 2. Move cursor 3. f2, f3 on last item	1. PF 1, . on first item 2. Move cursor 3. PF 1, . on last item or 1. Find on first item 2. Move cursor 3. Find on last item
Dehighlight one item	f3 or Spacebar	Spacebar
Dehighlight all items in a list	f2, \	PF 1, \
Open a menu on the menubar by using a **mnemonic** (first letter of menu)	f2, *mnemonic* key	PF 1, *mnemonic* key
Close a menu	f4 or Spacebar	PF 3 or Spacebar

Changing Windows

As you interact with SAM's text-terminal interface, you may have more than one window open at the same time. The interface allows you to perform various actions with windows: open, close, move, resize, and **iconify** (reduce the window to a small symbol on the screen).

These actions may be chosen from the **window control menu**. To open the window control menu:

- on a Hewlett-Packard or Wyse terminal, press f2, = or f2, Spacebar.
- on a VT-100/ANSI terminal, press PF 1, Spacebar or PF 1, =.

Moving a Window. Open the window control menu, highlight `move` and press (Spacebar). Notice that the four corners of the window have begun to "blink." Press any of the (▲), (▼), (◀), and (▶) to move the window to the desired location, then press (Spacebar).

Resizing a Window. Open the window control menu, highlight `resize` and press (Spacebar). Notice that the corners of the window have begun to "blink." (If one of the corners is not blinking, it indicates that the window cannot be resized in that direction.) Press any of the (▲), (▼), (◀), and (▶) to move the window corners to the locations that indicate the new size you require, then press (Spacebar).

Iconifying a Window. Open the window control menu, highlight `iconify` and press (Spacebar). The window disappears, but you can see that it is still available by opening the **window list menu** (see "Opening a Window"). If there is an uniconified window available, the cursor will move to that window.

Maximizing a Window. Open the window control menu, highlight `maximize` and press (Spacebar). The window is resized to fill the entire screen.

Opening a Window. To "raise" (open up) an iconified window:

- on a Hewlett-Packard or Wyse terminal, press (f2), (0).
- on a VT-100/ANSI terminal, press (PF 1), (0).

This opens the **window list menu**. This menu lists the titles of all visible or iconified windows. To choose the title of the window you wish to open, use the (▲) and (▼) cursor keys to highlight the desired window title, then press (Spacebar).

Closing a Window. Open the window control menu, highlight `close`, then press (Spacebar).

The window disappears, but it is added to the window list menu, and it may be opened as described in "Opening a Window".

Using SAM for Remote System Administration

SAM allows single-point administration of remote systems by executing SAM on the remote system while displaying on the local machine. Single-point administration refers to administering multiple remote systems from one location. There are no hardware related restrictions. You can use any HP 9000 Series 300/400/700/800 to remotely administer any other HP 9000 Series 300/400/700/800.

Adding and Removing Remote Systems

To add remote systems using SAM:

1. Run SAM; type:

   `/usr/bin/sam`

2. Highlight `Remote Administration` and activate the (Open) button.
3. Choose `Add System ...` from the "Actions" menu.
4. Fill in the dialog box information and activate the (Ok) button.

The local machine's `/etc/hosts` file must have an entry for the remote system.

To remove remote systems using SAM:

1. Run SAM; type:

   `/user/bin/sam`

2. Highlight `Remote Administration` and activate the (Open) button.
3. Highlight the system(s) in the object list to be removed.
4. Choose `Remove System(s) ...` from the "Actions" menu.

Additional Task Information. Choosing an item from the "Help" menu gives you information about:

- the current functional area.
- keyboard navigation within SAM.
- using the SAM help system.
- displaying the version of SAM you are currently running.

Activating the (Help) button from a dialog or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

Pressing the (f1) key gives you context-sensitive information for the object at the location of the cursor.

Configuring the Remote System

The remote system must meet the following requirements:

- The SAM fileset is installed.
- The local machine name is in the remote system's `/etc/rhosts` file.

Logging SAM's Actions

SAM provides a log file mechanism for tracking the actions SAM performed on your system. You can activate this tracking mechanism, define the log file name, level of detail, and log file size by activating the (Options...) control button from the SAM main window.

Turning On SAM Logging

To activate the logging mechanism:

1. Activate the (Options...) control button. The "Options" window appears.
2. Choose the level of log file detail (`Summary`, `Detail`, `Verbose`) from the `Logging level` menu button.
3. Fill in the log file name.
4. Choose the log file length (in bytes) (20000, 50000, 500000, or 2000000) from the `Maximum logfile size` menu button.
5. Turn on the `Save settings` check box if you want to preserve these values for the next time you enter SAM. If you do not turn on the `Save settings` check box, the default values are reset the next time you enter SAM.
6. Activate the (OK) control button.

Summary Level Log. The following listing illustrates the summary level log file entries for adding a new user to the system:

```
S:****** Adding user(s):
S:****** Successfully added user "newuser".
```

Detail Level Log. The following listing illustrates the detail level log file entries for adding a new user to the system:

```
S:****** Adding user(s):
D:          Executing (pid = 1152):
              addusr -u newuserA -g users -d /users/newuserA -i ",,," -s /bin/sh
            -p "" -v 203
D:          addusr:  Adding user "newuserA" to group "users".
D:          addusr:  Modifying "/etc/passwd":  login_name="newuserA" password=""
            aging="" uid="203" gid="20" gecos="" shell="/bin/sh"
            home_directory="/users/newuserA" audit_id="-1" audit_flag="0".
D:          addusr:  Creating home directory "/users/newuserA" for user
            "newuserA".
D:          addusr:  Calling "chown(2)":  chown(/users/newuserA,203,20)
D:          addusr:  Copying default files to directory "/users/newuserA".
D:          Child (pid = 1152) terminated with status 0x0
S:****** Successfully added user "newuserA".
```

Verbose Level Log. The following listing illustrates the verbose level log file entries for adding a new user to the system:

```
V:          Processing internal message UI_GENERIC_EXEC (0)
V:          Executing (pid = 1085):
              /usr/sam/bin/users_init
V:          Child (pid = 1085) terminated with status 0x0
V:          Processing internal message UG_GET_DEFAULT_UID (0)
V:          Processing internal message UG_GET_DEFAULT_UID (0)
V:          Processing internal message UG_VALIDATE_NEWUSER (0)
S:****** Adding user(s):
V:          Processing internal message UG_ADD_USER (0)
D:          Executing (pid = 1166):
              addusr -u newuserB -g users -d /users/newuserB -i ",,," -s /bin/sh
            -p "" -v 204
D:          addusr:  Adding user "newuserB" to group "users".
D:          addusr:  Modifying "/etc/passwd":  login_name="newuserB" password=""
            aging="" uid="204" gid="20" gecos="" shell="/bin/sh"
            home_directory="/users/newuserB" audit_id="-1" audit_flag="0".
D:          addusr:  Creating home directory "/users/newuserB" for user
            "newuserB".
D:          addusr:  Calling "chown(2)":  chown(/users/newuserB,204,20)
D:          addusr:  Copying default files to directory "/users/newuserB".
D:          Child (pid = 1166) terminated with status 0x0
S:****** Successfully added user "newuserB".

V:          Processing internal message UG_GET_DEFAULT_UID (0)
V:          Processing internal message UI_GENERIC_EXEC (0)
V:          Executing (pid = 1178):
              /usr/sam/bin/users_init
V:          Child (pid = 1178) terminated with status 0x0
V:          Processing internal message UG_GET_DEFAULT_UID (0)
```

2

Constructing an HP-UX System

This chapter explains how to build a new HP-UX system. It outlines what you need to do to create a functioning system, and tells you where you can find more detailed information if you need it. You should start on the first task, which is to assess your users' needs, before you assemble the components of the system.

Assessing Users' Needs

Most users think in terms of the job they have to do, not "I need FORTRAN, Graphics, a plotter, and 500,000 bytes of data storage." The sample survey that follows will help you to find out what your users need and to translate their needs into the hardware and software that comprise a functioning HP-UX system.

You may need to change the form to fit your particular situation.

User Survey

Name _ _ _ _ _ _ _ _ _ _ _ _ _ _   Location _ _ _ _ _ _ _ _

Phone _ _ _ _ _ _ _ _ _ _ _ _ _ _

Location where you will use the system: _ _ _ _ _ _ _ _ _ _ _ _ _

Which of the following best describes your job? (Please check all that apply):

_ Engineer/ Manager	Run existing application programs; enter data, create models.
_ Technical Data Entry Operator	Run existing application programs; enter data or automatically read data from instrumentation.
_ Secretary - Word Processing Operator	Run existing application programs; enter data/text.
_ Applications Programmer	Develop application programs.
_ Systems Programmer Support Person	Develop programs for improving computer system performance or for use by other programmers.

Describe your application (the program(s) you use or create):

_ _

_ _

What programming language(s) will you use?_ _ _ _ _ _ _ _ _ _ _ _

_ _

What applications software (such as graphics) will you use? _ _ _

_ _

_ _

What computer hardware or peripherals do you need?

_ Inkjet printer   _ Plotter

_ Impact printer

_ Graphics terminal

_ Laser printer

_ Removable mass storage devices

_ Other _ _ _ _ _ _ _ _ _ _ _ _ _

_ _ _ _ _ _ _ _ _ _ _ _ _

Are there other users with whom you want to share programs or data?

If so, list these users _

_ _

Will you generate or use large amounts of data? _ _ _ _ _ _ _ _ _

If so, how much must be "on-line" (accessible at all times)?

_ _

_ _

What long-term data storage does your application require?_ _ _ _

_ _

How many programs/processes will you be running at one time?_ _ _

_ _

Which programs are interactive, and which will you run in background mode? _

_ _

_ _

Can any programs be run overnight?_ _

_ _

Installing HP-UX

As the system administrator, you might be responsible for installing HP-UX. (On some systems, the operating system may be installed for you by a Hewlett-Packard Customer Engineer; and some systems come from the factory with the operating system installed.)

The manual *Installing and Updating HP-UX* provides instructions for installing HP-UX.

Updating HP-UX

As the system administrator, you will normally be responsible for updating your system from one version of HP-UX to another (for example from Release 9.0 to a subsequent release), although on larger systems you may decide to have your Hewlett-Packard Customer Engineer or Software Engineer do it for you.

Use the *update*(1M) utility to update the operating system to a new release. Full instructions are in the manual *Installing and Updating HP-UX*.

Installing and Updating Optional Software

You can use the *update*(1M) utility to add optional HP software (such as networking) to your system, or to update such software to a new release. `Update` is also the installation and update tool for some third-party software.

When adding and updating software, be sure to follow the supplier's directions. If the directions tell you to use `update`, use the manual *Installing and Updating HP-UX* for more information.

Cluster Considerations

If you are creating an HP-UX cluster, consult the *Managing Clusters of HP 9000 Computers*, HP part number B1864-90015, manual before you continue.

That manual explains how to configure a cluster server and add cluster clients and peripherals. It also provides instructions and guidelines for those aspects of system administration that are unique to a cluster as opposed to a workstation or standalone multi-user system. It's very important that you familiarize yourself with these differences before you attempt any cluster administration tasks.

Installing HP-UX on a Cluster

If you are creating a new HP-UX cluster configuration, you need to install HP-UX on the cluster server—but not on the cluster clients—following directions in *Installing and Updating HP-UX*. Then configure this new system as a cluster server. *Managing Clusters of HP 9000 Computers* has details. Refer to Chapter 4, "Setting Up a Cluster".

Updating HP-UX on a Cluster

Updating a cluster means updating HP-UX on the cluster server. The process is similar to updating a single workstation or multi-user system, but there are some important differences.

These differences are explained in *Managing Clusters of HP 9000 Computers*. First read Chapter 14, "Updating a Cluster",

Installing and Updating Optional Software in a Cluster

As with a standalone system, you can sometimes use the *update*(1M) utility to add or update optional software: the supplier's directions will tell you what installation tool you should use.

Normally, you should log in to the cluster server to do the installation or update and use a tape drive (or other installation device) attached to the server. You'll find details and an outline procedure in *Managing Clusters of HP 9000 Computers*, in Chapter 14, "Updating a Cluster".

Adding, Removing, and Moving Peripherals

By "peripherals", we mean hardware that you can add to your system, including terminals, printers, disk drives, tape drives, other storage and communication devices, and the interface cards they attach to.

On some systems, you might choose to have your Hewlett-Packard Customer Engineer (CE) or Software Engineer (SE) install a given peripheral, but often you will do it yourself.

To install a peripheral, you need the following manuals:

- The installation manual that came with the peripheral.
- The *Installing Peripherals* manual. Look up the particular peripheral you are installing in *Installing Peripherals*. This material contains the software driver and the device special file information for communication with the peripheral. The *Installing Peripherals* also contains information in Appendix A, "E/ISA Configuration", about the `eisa_config` utility necessary to configure your system to communicate with EISA or ISA interface cards on an HP 9000 Series 400 or Series 700 workstations.

Depending on the peripheral, and the system you are installing it on, you might need to rebuild your system's **kernel** to make it aware of the new peripheral—for example, you might need to add a new **driver**.

The **kernel** is the piece of software that controls the computer—it is often referred to more loosely as the operating system. You can reconfigure the kernel by means of HP-UX commands or by the menu-driven System Administration Manager (SAM) program.

A **driver** is a program that enables the kernel to communicate with a given type of peripheral.

If you do need to rebuild the kernel for the device you are adding, the *Installing Peripherals* will show you which device drivers need to be in your kernel and the device special files needed to communicate with your peripheral. Refer to the "Reconfiguring the Kernel Using HP-UX Commands" or "Reconfiguring the Kernel to Add/Remove Device Drivers Using SAM" sections later in this chapter for a general procedure for rebuilding an HP-UX kernel.

Refer to Chapter 5, "Managing Peripherals" of this manual for moving and removing a peripheral.

After Installing HP-UX

After you have installed HP-UX and added peripherals such as disk drives, tape drives, printers and terminals, you still have some work to do before your users can sit down at their terminals and workstations and do their jobs productively.

The sections that follow outline the most important tasks, and where necessary point you to sources of further information.

Creating a Recovery System

Once you have installed HP-UX, the first thing you should do (ideally before other users are allowed to begin using the system) is make a recovery system on removable media or on a hard disk drive.

A **recovery system** is a bootable subset of your HP-UX system. It contains only enough of the system to allow you to boot and to help fix your file system in an emergency.

For example, if you can't boot from your root disk because your root disk is corrupt or because you have forgotten your root password, your recovery system will be available to boot from and to repair your file system.

You can build a recovery system with the aid of the shell scripts explained on the next page. You can be in multi-user mode. *However*, you and other users should be aware that the process of building the recovery system affects system performance.

Recovery Devices

To build your recovery system, you can use the following devices:

- cartridge tape drives
- (DDS Format) DAT drives
- magneto-optical disk drives
- other hard disk drives

Using Cartridge Tape. Making a recovery system on cartridge tape takes only few minutes if you use the `-q` option of `mkrs` (described under "Using the mkrs Script"). Using the `-q` option requires that about 6 megabytes space be available in the `/tmp` directory to hold the image of the system before it is copied to tape.

If you do not use the `-q` option, the `mkrs` process can take hours (as long as 4-6 hours in the case of a 600-foot cartridge tape).

Note

- You cannot create a recovery system on flexible disks or nine-track magnetic tape.
- If you add or delete swap space to your system, you *must* create a new recovery system.

  The recovery system has a record of swap space addresses. If these addresses change, but are not changed in the recovery system, then when you boot the recovery system, it may overwrite and destroy your root file system.
- If you are running a trusted system, you must lock up the recovery system tape. Whoever boots from a recovery system has superuser capabilities, and there is no auditing.
- A new recovery system is required each time you update your system to a new release. Commands available on an older recovery system might be incompatible with newer systems.

Tools For Making a Recovery System

The programs needed to make a recovery system are:

`/etc/mkrs`	A shell script that creates the recovery file system.
`/etc/mkrs.data`	Defines the content of the recovery system.
`/etc/mkrs.init`	Limited version of the `init` program for booting a recovery system.
`/etc/mkrs.boot`	A LIF volume header for the recover system.
`/etc/mkrs.tool`	The recovery tool.

The recovery system has a boot area so you can boot using just the recovery system. The recovery system also has a small file system (defined by `/etc/mkrs.data`) containing the following files and directories:

`/hp-ux`	A minimal kernel.
`/bin`	Contains a small subset of HP-UX commands. The actual commands vary depending on your recovery medium. Use the `ls` command to list the files in your recovery system.
`/dev`	Contains the device files necessary for using the recovery system (block and character device files for the root disk and the recovery device).
`/disc`	This directory can be used to mount a file system.
`/etc`	Contains the tools and files necessary to fix your root file system: `sbtab`, `fsck`, `init`, `mknod`, `mount`, and `umount`. It also contains small `inittab`, `profile`, and `rc` files, which are necessary for booting.
`/tmp`	This directory is used for temporary file storage.

Procedure For Making a Recovery System

To create the recovery system:

1. Log in as the superuser, `root`.

   You will be using privileged commands, so you must have superuser privileges.

2. Determine whether the necessary device files in `/dev` exist for the recovery device and root device.

   The `mkrs` program requires device files for the recovery device and for the root device. Refer to the *Installing Peripherals* manual for a description of device files and creating device files.

   recovery device — If your recovery device is a DDS Format device interface, look for the device file `/dev/rmt/0m` or `/dev/rmt/0mn`.

   If your recovery device is a cartridge tape, look for the device files `/dev/update.src`, `/dev/rct/c0`, or `/dev/rct`.

   If none of these defaults exists on your system, or if any exists but corresponds to another device, you must either create one of them or supply the name of the device file associated with the recovery device as an option to `mkrs`.

   The recovery device file can be of either block or character type; the other type need not exist.

   root device — Use the device file that corresponds to the location of your root file system. When you type:

   ```
   bdf
   ```

   look for the device file that corresponds to `/`.

   Only the *block* device file need exist for the root disk.

3. Create the recovery system by using the `mkrs` script. See the following section, "Using the mkrs Script", for details on options and defaults.

   If `mkrs` doesn't exist on your system (you'll receive a message: `file not found`), use the information on adding filesets in in the manual *Installing and Updating HP-UX*, to add the `SYS-ADMIN` fileset to your system.

4. Boot the recovery system to verify that it works. For this step, you will need to shut down the system. To avoid inconveniencing users, you might test-boot the recovery system during off hours. Follow the procedure in Chapter 8, "Backing Up and Restoring Your Data".
5. Store the recovery system media in a safe, locked place.

   When you boot using the recovery system, you come up as the root user. This is potentially a serious security problem. It is up to you as the system administrator to keep this recovery system media safe, so you can use it if you need to, yet unauthorized people can't get at it.
6. If you loaded the `SYS-ADMIN` fileset just to create a recovery system, you may wish to recover the disk space used by `SYS-ADMIN`.

   To remove the fileset, follow the instructions in "Removing System Files" later in this chapter.

Using the mkrs Script

The `mkrs` command has the following syntax (no spaces allowed between the option flag and the argument):

`mkrs` [`-v`] [`-q`] [`-s`] [`-f`*rcdev*] [`-r`*rootdev*] [`-m`*series*]

where:

rcdev is the name of the device file for the device on which you will create your recovery system.

Note If you are using a DDS format (DAT) tape:

- you must explicitly specify the device file.
- you cannot use the drive in data compression mode.

The `mkrs` command looks for the following cartridge tape device files, in the order they appear, by default unless a device file is specified explicitly:

1. `/dev/update.src`
2. `/dev/rct/c0`
3. `/dev/rct`

If none of these defaults exists on your system, or if any exists but corresponds to another device, you must either create one of them or specify the recovery device file using the `-f` option.

The recovery device file can be either a block or a character device file. An error message results if you do not use one of the defaults and do not specify a recovery device file name.

Use the `-q` option to specify that the recovery system's image be created in the `/tmp` directory before being copied to the recovery media. The `-q` option is the default for a DDS Format tape recovery system. This option saves time due to seeking on cartridge and DDS Format tape media.

rootdev is the name of the device file for the root device.

The `mkrs` command looks for the following root device files, in the order they appear, by default unless a device file is specified explicitly:

1. `/dev/dsk/0s0` (if it exists as a block device file)
2. `/dev/root` (if it exists as a block device file; `mkrs` does not succeed if the `/dev/root` has a "magic" minor number; you must supply a device file with a specific minor number)
3. `/dev/hd` (if it exists as a block device file)

If none of these defaults exists on your system, or if any exists but corresponds to another device, you must either create one of them or specify the root device file using the `-r` option.

The root device file must be a block device file. The character device file need not exist. An error message results if a default root device file does not exist and you do not specify a root device file name.

series Normally not needed. If `mkrs` cannot determine the type of system you have it will send you an error message. If this happens re-execute `mkrs` using the `-m` option with the value 300 or 400, as applicable.

The `-s` option specifies that a smaller set of system files be placed on the recovery media; this applies when making a DDS Format (DAT) recovery system for a small memory system.

The `-v` (verbose) option specifies you want to see a running history of the construction of the recovery system.

Examples of Creating a Recovery System. To create a recovery system on a cartridge tape drive using the device file `/dev/update.src` and root device using the device file `/dev/dsk/0s0`, type:

```
mkrs
```

To create a recovery system on a DDS Format tape drive using the the device file `/dev/rmt/0m` and root device using device file `/dev/dsk/6s0`, type

```
mkrs -v -f/dev/rmt/0m -r/dev/dsk/6s0
```

Chapter 8, "Backing Up and Restoring Your Data" explains how to use the recovery tape to restore your system.

Setting the System Clock

Only the **superuser** can change the system clock. (The superuser is the person who can log in as `root`. This should be you, and one other person you nominate as a backup.)

Before you can set the clock, you must set the time zone environment variable (TZ).

Setting the Time Zone (TZ)

You can set the time zone with a declaration in any one of three files, `/etc/csh.login`, `/etc/rc`, or `/etc/profile`. (An application program can also set TZ by means of the `tzset` library routine.)

The TZ declaration takes the following forms in the files:

`/etc/rc`:

```
TZ=xxxhyyy
```

`/etc/profile`:

```
TZ=xxxhyyy
export TZ
```

`/etc/csh.login`:

```
setenv TZ xxxhyyy
```

where:

xxx is an alphabetic abbreviation of the standard time zone, usually three letters.

For example, MST for Mountain Standard Time.

h is the difference between standard local time and Greenwich Mean Time (GMT), in hours. Measured to the West, `h` is a positive number. Measured East, `h` is a negative number. This field can include a designation for minutes.

Some examples are:

3:30 for Newfoundland

7 for Mountain Standard Time

-9:30 for South Australia

yyy is an alphabetic abbreviation of the daylight time zone for your area, usually three letters (for example, `MDT` for Mountain Daylight Time).

Do not use this field if Daylight Savings Time is not observed in your geographic area.

The following U.S. examples should give you the idea:

- In the Eastern time zone, use `TZ=EST5EDT`
- In the Central time zone, use `TZ=CST6CDT`
- In Arizona, where Daylight Savings Time is not observed, use `TZ=MST7`

For more information on setting the time zone environment variable, refer to `TZ` under the *environ*(5) entry in the *HP-UX Reference*.

Note

`CST6CDT` has two meanings: "Central Standard Time" and "Canadian Standard Time."

This matters because the United States changes to daylight saving time on the first Sunday in April and Canada makes the same transition on the last Sunday in April. Canadian systems must use `CST6CDT#Canada` to distinguish between the two.

Setting the Time and Date

After you have set the time zone variable, terminate the `cron` process (if it is running) and enter the `date` command. Do this as follows:

1. Log in as superuser.
2. Kill the `cron` process.

   In an HP-UX cluster, terminate `cron` on each client. To terminate `cron`, first find the `cron` process information by entering:

   ```
   ps -ef | grep cron
   ```

   This gives the process ID (PID) for `cron`.

   To determine all `cron` processes for all clients in an HP-UX cluster, enter:

   ```
   cps -ef | grep cron
   ```

   Now terminate `cron` by entering:

   `kill` *pid*

   where *pid* is the Process ID associated with `cron` (for example, `16442`).
3. Set the time and date by entering:

   ```
   date mmddhhmm{yy}
   ```

   where:

`mm`	is a two-digit integer representing the month. For example, `03` represents March.
`dd`	is a two-digit integer representing the day of the month. For example, `02` represents the second day of the month.
`hh`	is a two-digit integer specifying the hour on a twenty-four hour clock. For example, `03` specifies 3:00 am and `14` specifies 2:00 pm.

`mm` is a two-digit integer specifying the number of minutes past the hour.

For example, `04` specifies four minutes past the hour.

`{yy}` is an optional two-digit integer specifying the last two digits of the year.

For example, `91` specifies 1991.

When **date** executes, it shows the time and date on your screen.

4. Restart `cron` if you terminated it in step 1.

   Enter:

   <u>/etc/cron</u>

Problems You Can Cause by Changing the System Clock

make: The `make` program is sensitive to a file's time and date information and to the current value of the system clock.

Setting the clock forward will not affect `make`, but setting the clock backward by even a small amount may cause `make` to behave strangely.

Backups: Incremental backups depend heavily on the date being correct because they rely on a dated file.

cron: Altering the system clock can cause unexpected results for jobs scheduled by `cron`.

- If you set the time back, `cron` does not run any jobs until the clock catches up to the point from which it was set back.

  For example, if you set the clock back from 8:00 to 7:30, `cron` will not run any jobs until the clock again reaches 8:00.

- If you set the clock ahead, `cron` attempts to catch up by immediately starting all jobs scheduled to run between the old time and the new.

  For example, if you set the clock ahead from 9:00 to 10:00, `cron` immediately starts all jobs scheduled to run between 9:00 and 10:00.

Setting Up File Systems

When you install HP-UX, the `install` program that builds your system comes with the file systems HP-UX needs, but you will need to create additional file systems for your users. Chapter 6, "Managing the File System", in this manual, explains how to do this.

Setting Up On-Line HP-UX Reference (manpages)

Every HP-UX command and system file is documented in the *HP-UX Reference*.

This manual, often referred to simply as the "manpages", comes in two forms: as a book, shipped with the core documentation shipped with your system, and as a set of files that allow you and your users to look up the entries on-line and to print them out individually. The on-line version requires some set-up. You have three methods to choose from:

1. Create a formatted version of all the manpages.

   The advantage of doing this is that users will get quick response when they call up a manpage on-line. The disadvantage is that the formatted versions take up a considerable amount of disk space (about as much again as the `nroff` originals from which they are created), which you may not have. However, once the pages have been formatted, you can recover disk space by getting rid of the `nroff` originals.

   This is a good method if you have enough disk space to hold both versions of the manpages for as long as it takes to finish formatting them.

   If you decide to do this, enter:

   `/etc/catman`

   The process of formatting all the manpages can take as long as five or six hours, so you might want to run it at a lower priority, in the background, or at night.

2. Format only certain sections of the manpages.

   This could give you the advantage of quicker access to heavily used sections without incurring the cost in disk space of formatting all sections.

   If you decide to do this, enter:

   `/etc/catman` *sections*

   (where *sections* is one or more logical sections in the *HP-UX Reference* such as 1).

3. Do not execute `/etc/catman` at all.

   Use this method if you can spare some disk space but do not want to use any more than is necessary.

   If you don't run `catman`, HP-UX formats each manpage the first time a user calls it up via the `man` command. The formatted version is added to the appropriate `cat` directory and used in subsequent accesses.

   If you decide to use this method, you must make directories to hold the formatted manpages. The following script creates these directories:

   ```
   cd /usr/man
   for num in 1 1m 2 3 4 5 7 8 9
   do
    mkdir cat$num
   done
   ```

When all the manpages have been formatted, you can remove the `nroff` source files.

Setting Up Networking

If your computer is to be part of a **network** (that is, if it will be connected to other computers via Local Area Network (LAN), Wide Area Network (WAN), or some other kind of link), you now need to establish the connection. A network link consists of both hardware (for example, a LAN card) and software (for example, the LAN/9000 and ARPA Services packages).

What you need to do at this point depends on the type of network you're using, and whether you're connecting the computer to an existing network or setting up a new one.

Hewlett-Packard documentation you may need includes:

- *Networking Overview*
- *Installing and Administering LAN/9000*
- *Installing and Administering FDDI/9000 Software*
- *Installing and Administering Token Ring/9000 Software*
- *Installing and Administering NFS Services*
- *Installing and Administering Network Services*
- *Installing and Administering ARPA Services*

If you have not administered a network before, start with *Networking Overview*.

Adding Users and Groups

It is now time for you to add **users** and **groups** to the system. These are the names of the data structures by which an HP-UX system recognizes a given person or class of people who use it.

There are SAM screens for setting up users and groups, or you can do it by means of HP-UX commands. Full directions are in Chapter 4, "Controlling Access to the System".

You add a user or group in a cluster just as you do on a standalone machine, but some of the implications may take you, and your users, by surprise. For example, a user who can log in on one computer in a cluster can log in on all of them. This applies to all users, including `root`.

Details are in *Managing Clusters of HP 9000 Computers*, in Chapter 13, "Managing Users in a Cluster".

Setting Up Electronic Mail

Electronic mail (or "email" as it is often called) can be run by any of these three utilities: `elm`, `mailx`, or `mail`. Any user can use any one of these.

- If your users will be exchanging messages only with each other, and will not need to send mail to users on other systems in a network, then you need not do any set-up.

  The mailer will do the initialization needed for each user when the user first invokes the mailer. However, you may want to supply each `mailx` and `elm` user with a customization file, setting up useful defaults. Depending on the mailer, the customization file should be:

  for `mail`: (none)

  for `mailx`: `$HOME/.mailrc` (That is, a file named `.mailrc` in the user's home directory.)

  (In addition, `mailx` uses a system-wide defaults file `/usr/lib/mailx/mailx.rc`.)

  for `elm`: `$HOME/.elm/elmrc`

- If your users will be sending and receiving mail over a network, you need to set up routing either through UUCP or ARPA Services.
  - □ To configure UUCP, follow directions in the manual *Remote Access*.
  - □ To configure ARPA Services, follow directions in *Installing and Administering ARPA Services*.
    - You will also need to install the ARPA Services `sendmail` utility. Chapter 6 of *Installing and Administering ARPA Services* contains the directions you'll need.

Setting Up the Line-Printer Spooler

You share printers among users via the line-printer spooler, which intercepts print requests, organizes them into a queue, and feeds them to the printer one by one. A printer that has been configured into the line-printer spooler is referred to as a **spooled** printer. Any printer Hewlett-Packard supports can be spooled.

If your system will have more than one user at any one time, you should spool the printer(s); if you don't, any listing sent to the printer while another listing is printing will be interleaved with it, garbling both listings.

Even if this will be a single-user system, you may still want to spool the printer, since spooling allows you to batch up print requests so you don't have to wait for one to complete before you can send the next.

If your system is part of a network, the line-printer spooler also lets you send print requests to, or receive them from, other computers in the network, allowing you to make the most efficient use of your printers.

Setting up the line-printer spooler is one of the more complicated tasks you need to do at this stage. Chapter 9, "Managing Printers and Printer Output" contains full explanations and directions. If you have not administered an HP-UX system before, or have not set up a spooled printer before, read the chapter carefully before you attempt the task.

Setting Up news

news is a utility that allows you to post messages for users to read (see also "Posting a Message of the Day (/etc/motd)" later in this chapter).

- To create a news item, create a file with your text editor and place it in the directory /usr/news.
- To make sure users know about news items they haven't read yet, do the following:
  - For Korn and Bourne shell users, edit /etc/profile to include the following statement:

    ```
    if [ -f /usr/bin/news ]
    then news -n    #notify if news.
    fi
    ```

  - For C shell users, edit /etc/csh.login to include the following:

    ```
    if ( -f /usr/bin/news ) then
       news -n    #notify if new news.
    endif
    ```

When they log in, if there are news items they haven't read, users will see a message like this:

news: *news_filename*

where *news_filename* is the name you gave the file in /user/news.

Users can enter news and the item or items will print on the screen. For more information, consult *news*(1) in the *HP-UX Reference*.

Using HP VUE

HP VUE enables users on an HP-UX system to manage and extensively customize their computer displays. HP VUE is based on the X Window System. Both HP VUE and X Windows are installed and configured at the time of HP-UX system installation.

The displayed computer screen can contain multiple windows, each of which can contain a running program. In this way, the displayed screen with windows is analogous to a work surface on which a person is working concurrently on several different tasks. With HP VUE, a user can switch to a different screen (a different work surface) and work with a different set of windows (a different set of tasks).

Refer to the following documents for information you might need to customize HP VUE on your system:

HP VUE User's Guide, HP part number B1171-90061

HP VUE Quick Start, HP part number B1171-90062

Using HP-UX, HP part number B2910-90001

Setting Up X Windows

X Windows is a package that allows the owner of a graphics workstation to interact with different applications on the same screen at the same time, on the analogy of a desktop on which a person is working concurrently on several different tasks.

X Windows is installed along with the operating system, and the only additional set-up you need to do is to allow users who want it to have X Windows as their default environment (so that the windows they specify in their `.x11start` file come up when they log in).

The easiest way to do this is to add the users in SAM, and respond `y` to the prompt `Login with X11 windows?`

If you respond `y`, SAM adds the following lines to the `.profile` file in a Bourne or Korn shell user's home directory:

```
# Add windows at login:
if [ "`who am i | grep console`" != "" ]
then
     exec /usr/bin/x11start
fi
echo "Press <Shift> <Ctrl> <Reset> simultaneously to exit all windows."
```

In the case of a C shell user, SAM adds the following lines to the `.login` file in the home directory:

```
# Add windows at login:
if ( "`who am i`" =~ *console* ) then
    exec /usr/bin/x11start
endif
echo "Press <Shift> <Ctrl> <Reset> simultaneously to exit all windows."
```

If you have already added the user, or if you choose not to use SAM, you can add the lines to the appropriate file yourself, or tell your users how to do it.

Setting Up System Accounting

System accounting, which is primarily intended for multi-user systems, allows you to:

- Monitor individual users' disk space usage.
- Record logins and logouts.
- Collect data about individual processes, such as memory usage and execution time.
- Charge fees for usage.
- Generate summaries and reports that you can use to analyze system performance and bill users for resource consumption.

If you need to set up system accounting, you should do so now. Details are in Chapter 11, "System Accounting".

Customizing the System

Customizing the system usually means editing a file, either to change the way the system behaves in general, or to modify the way a particular user interacts with it.

The most important files you can customize are:

`/etc/inittab`:
: Contains information about system run levels and also has an entry for each terminal.

  See "Editing the /etc/inittab File" later in this chapter.

`/etc/rc`:
: Defines actions taken during startup.

  See "Editing the /etc/rc File" later in this chapter.

`/etc/passwd`:
: Determines who can log into your system.

  You can add, delete and modify entries either by editing the file, or by means of SAM screens under the `Users` menu. Chapter 4, "Controlling Access to the System", contains more information.

`/etc/group`:
: Identifies the users that form a group, associates group IDs (GIDs) with group names, lists users, and associates those users with a group name and a group ID.

  There's more information in Chapter 4, "Controlling Access to the System".

`/etc/ttytype`: Used by the `tset` command as a database of terminal types on your system.

Edit this file when you add a new type of terminal or modem to your HP-UX system. For example:

```
300h console
2397 tty00
2397 tty01
```

This file is a context-dependent file in an HP-UX cluster (`/etc/ttytype+`). Make sure you are logged in to the cluster node to which the file applies when you edit it.

`.exrc`: Maps terminal characteristics and sets up key definitions for the `ex` family of HP-UX editors (`vi`, `ex`, and so on).

See "Customizing Users' Login Environments" later in this chapter.

`/etc/issue`: Determines what the user will see before the login prompt.

See "Customizing the Login Prompt (/etc/issue)" later in this chapter.

`/etc/motd`: Contains the message of the day.

See "Posting a Message of the Day (/etc/motd)" later in this chapter.

`/etc/profile`, `/etc/csh.login`: Executes automatically during the login process.

The `/etc/profile` file executes for Bourne, Korn, and restricted shell users. The `/etc/csh.login` file executes for C shell users.

See "Customizing Users' Login Environments" later in this chapter.

$HOME files: (Files in the user's home directory).

- `.profile`: Executes each time the user successfully logs in using the Bourne shell, Korn shell, or restricted shell.
- `.kshrc`: Korn shell script that supplements actions taken by the `.profile` file.

  Executes whenever a new Korn shell is spawned, if specified by the following statements in the user's `.profile`:

  ```
  ENV=$HOME/.kshrc
  export ENV
  ```

  The name `.kshrc` is merely a convention: whatever file you specify will execute.
- `.cshrc`: executes when a new C shell starts.
- `.login`: executes when a C shell user logs in, after `.cshrc`.
- `.environ`: executes when a user logs in using PAM.

  (PAM is a user interface to HP-UX and MSDOS, suitable for novices and infrequent computer users.)

See "Customizing Users' Login Environments" later in this chapter.

Customizing System Startup

When the system boots, it executes a series of programs and shell scripts. (Details are in Chapter 3, "Starting and Stopping HP-UX".) Of the files involved, you can customize `/etc/rc` and `/etc/inittab`.

Editing the /etc/inittab File

`/etc/inittab` is input to `/etc/init`, the first program HP-UX runs after obtaining control from the boot ROM. Use `/etc/inittab` to set system run-levels (see Chapter 4, "Controlling Access to the System").

You need to edit `/etc/inittab` whenever you add a new terminal to your system. For more information on `/etc/inittab`, see *inittab*(4) in the *HP-UX Reference*. An entry for a terminal whose device file name is `/dev/tty04` would look like this:

`04:2:respawn:/etc/getty tty04 H #`*comment to identify user*

When you start up the system, this terminal will receive a `login:` prompt, and the prompt will be redisplayed after the user logs out.

If you use SAM to add the terminal, SAM adds the `getty` line to `/etc/inittab`.

For instructions on adding a terminal, see *Installing Peripherals*, Chapter 5, "Installing Terminals and Modems". If you plan to use SAM to configure your terminal, additionally refer to Chapter 6, "Setting Up HP-UX for Terminals and Modems Using SAM" in the *Installing Peripherals* manual. If you decide to use HP-UX commands instead of SAM, additionally refer to Chapter 14, "Setting Up Devices Using HP-UX Commands" in the *Installing Peripherals* manual.

Editing /etc/inittab in a Cluster

In an HP-UX cluster, `/etc/inittab` is a context-dependent file. Edit `/etc/inittab` (or run SAM) on the client to which you are adding the terminal. (Context-dependent files are files that exist in different versions for different members of a cluster. Details are in *Managing Clusters of HP 9000 Computers*.)

Editing the /etc/rc File

The `/etc/rc` script is executed by the `/etc/init` program during system startup.

`/etc/rc` performs a number of functions, including setting the timezone and the date, and initializing system processes such as the **syncer daemon** and the **line-printer spooler**.

Edit `/etc/rc` to do any processing you might want this particular system to do when it boots.

For example, if you have Network Services, you might want to start the proxy server here.

You should put this processing in a separate script, such as `/etc/rc.local`, and call the script from `/etc/rc`. This way, it is easier to recreate your customization if `/etc/rc` is overwritten when you update HP-UX to a new release.

Customizing the Login Prompt (/etc/issue)

`/etc/issue` contains text users will see immediately before the `login:` prompt. Normally it identifies the system (by the **host name** from `/etc/hosts` if this is a networked system, and its "friendly" alias, if any), the release of HP-UX, and includes any other information you want to put there.

For example:

```
Folly [HP-UX Release A.09.0  9000/350]
```

This file is a context-dependent file in an HP-UX cluster, meaning that there is a separate version of the file for each member of the cluster. This allows you to identify each computer in a cluster distinctly.

Posting a Message of the Day (/etc/motd)

The message of the day appears each time a user logs in if the user's personal customization file (`/etc/profile` for Bourne and Korn shell users or `/etc/csh.login` file for C shell users) has the following line:

```
cat /etc/motd       # message of the day
```

Edit `/etc/motd` to display topical messages. For example:

```
Monthend reports due this week.
Going away party for Leslie on Wednesday.
Sign your time-sheets by Friday.
```

Customizing Users' Login Environments

/etc/profile and the .profile file in the user's home directory execute when a Bourne or Korn shell user logs in. When a C shell user logs in, /etc/csh.login executes, and so do the .cshrc and .login files in the user's home directory.

/etc/profile and /etc/csh.login should contain the defaults for variables such as the timezone setting, the terminal type, search path, and mail and news notification. These can be overridden if necessary in individual users' .profile or .login files.

.cshrc in the user's home directory performs additional set-up such as setting **aliases** (user-defined commands). .kshrc performs similar tasks for a Korn shell user if it is declared in the ENV variable.

When you add a new user, you may want to place default versions of these files in the user's home group. (If you use SAM to add a user, SAM puts the appropriate files in the home group for you.) You can use the sample files in the /etc/ directory (such as /etc/d.profile) as templates, editing them as you wish.

A Beginner's Guide to Using Shells has examples of all these files, with explanations of each entry in the default files.

Customizing Users' Editing Environments

This means editing the .exrc file in the user's home group to enable keyboard features such as the cursor arrow keys, and to set other options in the ex family of editors, including vi.

The .exrc file functions only if the EXINIT variable is *not* defined in the /etc/profile or $HOME/.profile files.

/etc/d.exrc is a sample .exrc file. You may want to customize the file and provide it to new users as a default. There's a commented version of the file in Chapter 11 of *The Ultimate Guide to the vi and ex Text Editors*, a Hewlett-Packard publication that you can order separately.

Setting Up Non-Standard Terminals

Files in directories under `/usr/lib/terminfo` enable you to use a wide variety of terminals, including terminals not manufactured by Hewlett-Packard.

To set a user up with a non-HP terminal, do the following:

1. Make sure the fileset NONHPTERM has been loaded:

    `ls /etc/filesets/NONHPTERM`

    If the fileset is not there, you can get it from your latest set of `update` media (the media on which you got the current release of HP-UX).

    Run the `update` program and select the NOHPTERM fileset. Chapter 5, "Updating HP-UX" in the manual *Installing and Updating HP-UX* shows how to load an individual fileset.

2. Find the file that corresponds to the terminal you want to set up, if the file exists.

    Suppose you want to set someone up with a Wyse (TM) 100 terminal. All supported terminals whose names begin with "w" are listed under `/usr/lib/terminfo/w`.

    Enter

    `ls /usr/lib/terminfo/w`

    and you'll see an entry for `wy100`. This is the `terminfo` file for the Wyse 100.

    If there is no `terminfo` file for the terminal you want to add, you can create one. See "Creating a New terminfo File" later in this chapter.

3. Find the terminal name in the file.

    For example,

    `more /usr/lib/terminfo/w/wy100`

    This will produce a screenful of special characters, but near the beginning you'll see `wy100|100|wyse 100`. This means you can refer to the Wyse 100 by any of the names `wy100`, `100` or `wyse 100`.

4. Set the user's `TERM` variable in the appropriate login script in their home directory: `.profile` for a Korn or Bourne shell user, or `.login` for a C shell user.

   For example (Bourne or Korn shell):

   ```
   TERM=wy100
   export TERM
   ```

   (C shell):

   ```
   set TERM wy100
   ```

   The default versions of these scripts prompt the user for the terminal type when he or she logs in, so rather than editing the script, you could simply tell the user to respond with the terminal name, for example:

   ```
   TERM = (hp) wy100
   ```

Creating a New terminfo File

If there is no `terminfo` file for the terminal you want to set up, you can create one. The *terminfo*(4) entry in the *HP-UX Reference* explains the rules for constructing a `terminfo` file.

You may want to copy an existing `terminfo` file. In this case, get into the directory containing the file you want to copy and create a ASCII version of the file.

For example, to make a copy the file `/usr/lib/terminfo/w/wy100`, do the following:

1. Log in as superuser.
2. Change directories:

   `cd /usr/lib/terminfo/w`

3. Make an ASCII version of the file:

   `untic wy100>`*filename*

   where *filename* is whatever you want to call the new file. Make it similar to the terminal's product name and model if you can.

4. Edit the file to reflect the capabilities of the new terminal.

   Make sure you change the name(s) of the terminal in the first line. See *terminfo*(4) for rules for entries.

5. Compile the new `terminfo` file:

   `tic` *filename*

For more information on using the `terminfo` compiler, refer to *tic*(1M) in *HP-UX Reference*.

Backing up the System

Now that you have built the system, you should do a full back up. This will allow you to reconstruct your system—kernel, system files, file system structure, user structures, and your customized files—should you ever need to. (If you often have to build a new system, the backup will also give you a basis from which to recreate the next system.)

SAM provides backup capability in addition to the several HP-UX tools available for back up. Each is explained in Chapter 8, "Backing Up and Restoring Your Data".

Reconfiguring the Kernel

This section describes:

- When you need to configure the kernel.
- Reconfiguring the kernel using HP-UX commands.
- Reconfiguring the kernel using SAM when:
  - adding/removing device drivers
  - modifying system parameters
  - adding/removing/modifying swap, dumps, and console devices

When Do You Need to Reconfigure the Kernel?

You need to reconfigure the kernel in the following situations:

- When you add a new peripheral to your system that requires a device driver that is not already configured in the kernel, you need to add that driver. By "peripherals", we mean hardware that you can add to your system, including terminals, printers, disk drives, tape drives, other storage and communication devices, and the interface cards they attach to. For adding a peripheral, refer to the *Installing Peripherals* manual.

  You may also want to remove a driver from your kernel if your system no longer uses any peripherals of that type. (This is not an absolute requirement, but it's desirable, since a smaller kernel is more efficient.)

- When you change kernel parameters, you need to reconfigure the kernel.

  When you first install your system, the configurable kernel parameters are set to default values. These values are correct for most systems, but under some circumstances you might decide to change one or more parameters—to accommodate a specialized application, for example, or an exceptionally large number of users.

  Refer to Appendix A, "System Parameters", which contains descriptions of all tunable parameters, their ranges, and how they interact with other parameters. Appendix A, "System Parameters" also contains a description of how to use SAM to change the tunable kernel parameters.

- If you add certain Hewlett-Packard software, such as LAN (Local Area Network) or NS (Network Services), you might need to reconfigure the kernel. In almost all cases, however, you should use *update*(1M) (the `/etc/update` program) to add a subsystem, rather than the method described in this chapter. For example, *config*(1M) and *mknod*(1M)) will add the subsystem "device drivers" to your kernel, and create the appropriate device special files, but will not get the software application and its files onto your system or do any other set-up needed.

  The *update*(1M) utility, on the other hand, helps you load the software and does the necessary configuration. Consult the manual that came with the software for installation instructions. *Installing and Updating HP-UX* contains more information on `update`.

- When you change the locations of the following kernel devices:
  - System console.
  - `root` (/) file system.
  - Primary swap.
  - Dumps.

Reconfiguring the Kernel Using HP-UX Commands

In the context of the following instructions, the term "standalone machine" refers to a machine that is *not* part of an HP-UX cluster. Instructions differ when reconfiguring a standalone machine, cluster server, or cluster client kernel.

Reconfiguring the kernel requires that you reboot your system. Note, however, the impact on other users *before* you shut down and reboot your system, especially the following:

- If others are logged into your system, rebooting it interrupts their work. If you have a small number of users or clients on your system, it is best to notify your users in person of the impending system shutdown. It is possible that users can be using an application and not be aware of the message sent by the `shutdown` command.
- If your system is a cluster server, or a swap server for other clients in a cluster, rebooting your system brings down the associated clients. See Chapter 10, "Booting and Shutting Down Clusters and Cluster Nodes" of *Managing Clusters of HP 9000 Computers*, HP part number B1864-90015, for details.
- If your system is a file server in a cluster, rebooting it makes any file systems mounted to the file server unavailable to clients. Again, See Chapter 10, "Booting and Shutting Down Clusters and Cluster Nodes" of *Managing Clusters of HP 9000 Computers*, for details.
- If your system is an Internet Protocol router, rebooting it affects any IP traffic routed through your system.

To reconfigure the kernel using HP-UX commands:

1. Ensure that you have superuser capabilities.
2. In an HP-UX cluster, ensure you are logged onto the machine for which a new kernel is being generated, client or server. This sets for the correct context for creating the `/hp-ux` context-dependent file and editing the `/etc/conf/dfile` context-dependent kernel configuration file. You can log in at the cluster node console or remotely log in to the cluster node from another location by using the `rlogin` command. See *Managing Clusters of HP 9000 Computers*, for additional cluster information.
3. Change your directory to `/etc/conf`:

   ```
   cd /etc/conf
   ```

Caution You *must* get out of the root directory because you will be creating a new kernel. Otherwise you will overwrite the currently executing kernel.

4. Make a backup copy of your current configuration description file (which is most commonly `/etc/conf/dfile`)

   Enter the following command for a standalone machine:

   ```
   cp /etc/conf/dfile /etc/conf/dfile.old
   ```

   Enter the following command for an HP-UX cluster server or client:

   ```
   cp /etc/conf/dfile /etc/conf/dfile.cluster_node_name.old
   ```

   where *cluster_node_name* is the name displayed by the `hostname` command to represent the hostname.

   We highly recommend the use of `/etc/conf/dfile` as the kernel configuration file so it remains up to date with the executing kernel, `/hp-ux`. Some system software depends on `/etc/conf/dfile` representing the currently executing kernel.

Note In a cluster, the `/etc/conf/dfile` is a CDF and should be used to recreate the kernel.

5. Edit the configuration description file (for example, `/etc/conf/dfile`) to:
   - add or remove device drivers
   - modify system parameters
   - add, remove, or modify special devices (root, console, swap, dump)
   - add or remove subsystems

   For additional information about the configuration description file, refer to *config*(1M) in the *HP-UX Reference*.

   In an HP-UX cluster, `/etc/conf/dfile` is a context-dependent file; see the *Managing Clusters of HP 9000 Computers* manual for more information.

6. Make a copy of the existing kernel.

Caution

- *Do not* perform this step if your system is booted from the `/SYSBCKUP` backup kernel. If you do, you could overwrite the only bootable kernel for your system.
- If you are creating a new cluster client kernel, do not copy `/hp-ux` to `/SYSBCKUP`. If you do, you will overwrite the cluster server's backup kernel.

If your system is a standalone or an HP-UX cluster server, enter:

`cp /hp-ux /SYSBCKUP`

If your system is an HP-UX cluster client, enter:

`cp /hp-ux /SYSBCKUP.`*custer_node_name*

where *cluster_node_name* is a unique two character abbreviation of the client hostname displayed by the `hostname` command.

Caution If you copy `/hp-ux` to `/SYSBCKUP` on a cluster client, you will overwrite the cluster server backup kernel.

Write down the filename of the backup kernel.

Note You must name your standalone or cluster server backup kernel `/SYSBCKUP` if you want to be able to boot the backup kernel from the Boot ROM.

---

7. Run `config` on the configuration description file you edited:

   <u>`/etc/config` *config_file*</u>

   where:

   config_file is the configuration description file, for example `/etc/conf/dfile` or `/etc/conf/dfile.`*cluster_node_name*.

   Executing `config` creates the files `conf.c` and `config.mk`. Be sure you have the correct version these files by typing `ll` (that is "el, el") from the `/etc/conf` directory and verifying the last modified date and time.

   Refer to *config*(1M) in the *HP-UX Reference* manual for additional information.

8. Create the new hp-ux kernel (the file `hp-ux`) in the current directory (`/etc/conf`):

   <u>`make -f config.mk`</u>

   As it is executing, `config.mk` displays the following two lines:

   ```
   Compiling conf.c  ...
   Loading hp-ux  ...
   ```

9. Bring the system into single-user mode using the `shutdown` command:

   ```
   cd /
   shutdown grace_period
   ```

   where *grace_period* is the number of seconds the system will wait before shutting down. Specifying a grace period is optional; the default is 60 seconds. The `shutdown` command sends all users currently logged into the system a warning message that the system is shutting down. You can rely on the system default message, or you can customize the message.

   Shutting down a cluster server causes all clients of the server to reboot. If you are shutting down a cluster server the following message is displayed:

   ```
   The following client cnodes are also rebooted:
    client1
    client2
    client3

   Do you wish to continue? (y or n)
   ```

10. Wait for the system to display from single-user mode.
11. Copy the new kernel to the / (`root`) directory:

    ```
    cd /etc/conf
    cp hp-ux /hp-ux
    ```

12. Halt the system:

    ```
    reboot -h
    ```

13. Turn off the computer. If you are installing or removing interface cards or peripheral devices, do it now. Refer to the documents shipped with the products being installed and the *Installing Peripherals* manual for specific instructions.

Warning **Be sure to follow the ESD (Electrostatic Discharge) precautions when handling cards and devices. ESD precautions are described in the hardware installation and configuration guides.**

14. Turn on the power. The system will attempt to boot the new kernel.

    If the new kernel fails to boot, boot the system from the backup kernel and repeat the process of creating a new kernel. See "Booting the Standalone or Cluster Server Backup Kernel Using the Boot ROM".

    To boot standalone machine or cluster server backup kernel select /SYSBCKUP from the boot ROM, see "Booting the Standalone or Cluster Server Backup Kernel Using the Boot ROM". The boot ROM does not support booting from context-dependent files or filenames other than /SYSHPUX and /SYSBCKUP.

    To boot cluster client from a backup kernel the backup kernel must be copied to `/hp-ux`. The cluster client can then boot the backup kernel by selecting /SYSHPUX from the boot ROM, see "Restoring the Cluster Client Backup Kernel".

    To boot a backup kernel select /SYSBCKUP from the boot ROM. The boot ROM does not support booting from filenames other than /SYSHPUX and /SYSBCKUP.

Reconfiguring the Kernel to Add/Remove Device Drivers Using SAM

To reconfigure the HP-UX kernel using SAM:

1. Login as superuser.
2. In an HP-UX cluster, ensure that you are logged onto the machine for which you are regenerating the kernel. This sets for the correct context for creating the `/hp-ux` context dependent file and optionally overwriting the `/etc/conf/dfile` context-dependent kernel configuration file.
3. Run SAM; type:

   `/usr/bin/sam`
4. Highlight `Kernel Configuration` and activate the (Open) control button.
5. Highlight `Drivers` and activate the (OK) control button.

   A list of drivers, their current status, and their pending status appear. Current status refers to a driver being in or *not* in (out of) the currently executing kernel. Pending status gives the status of the driver when you next regenerate the kernel (in or out).

6. Perform one of the two following tasks:
   - To *add* a driver (or drivers) to the kernel, highlight the diver (or drivers) you want to add and choose `Add Driver to Kernel` from the "Actions" menu.

     The "Pending State" column entry for the driver(s) changes to "In". You must recreate the kernel and install it to implement the change.
   - To *remove* a driver (or drivers) from the kernel, highlight the diver (or drivers) you want to remove and choose `Remove Driver to Kernel` from the "Actions" menu.

     The "Pending State" column entry for the driver(s) changes to the value "Out." You must recreate the kernel and install it to implement the change.
7. Choose `Create a New Kernel...` from the "Actions" menu.
8. Activate the (Yes) control button to confirm that you want to reconfigure the kernel now.
9. Choose one of the following:

   - `Create a new kernel now`

     This requires a reboot of your system. SAM prompts you to continue.
   - `Defer kernel creation until later`

     SAM preserves the request to reconfigure the kernel. If you attempt to exit the Kernel Configuration area of SAM before you have reconfigured the kernel, SAM prompts you to reconfigure the kernel or cancel your reconfiguration request.

   - `Cancel all kernel modifications`

10. Follow the prompts to regenerate and reinstall the new kernel. After SAM generates a new kernel, choose one of the following actions and activate the (OK) control button:
    - `Move the kernel into place and reboot the system now`
    - `Move the kernel into place but do not reboot the system`
    - `Exit without moving the kernel into place`

    There is an option to enable or disable overwriting the kernel configuration file, `/etc/conf/dfile`.

    If you *enable* overwriting the kernel configuration file, SAM moves `/etc/conf/dfile.SAM` to `/etc/conf/dfile`, overwriting any comments you have added to the configuration file.

    If you *disable* overwriting the kernel configuration file, `/etc/conf/dfile` will not represent your current kernel (`/hp-ux`) when you reboot your system. `/etc/conf/dfile.SAM` represents your current kernel configuration after you reboot your system.

    We highly recommend the use of `/etc/conf/dfile` for the kernel configuration file so that it remains up to date with the executing kernel, `/hp-ux`. Some system software depends on `/etc/conf/dfile` representing the currently executing kernel.

    If you do not want SAM to overwrite `/etc/conf/dfile`, because of comments you want to retain:
    a. Choose the SAM option to disable overwriting the kernel configuration file.
    b. Move the kernel into place (optionally rebooting the system).
    c. Copy your comments from `/etc/conf/dfile` to `/etc/conf/dfile.SAM`. Be careful to add only your comments to the file. At this stage, you want `/etc/conf/dfile.SAM` to reflect your current kernel configuration.
    d. Copy or save `/etc/conf/dfile.SAM` to `/etc/conf/dfile`.

    The kernel configuration file `/etc/conf/dfile` now represents the current `/hp-ux` kernel.

Reconfiguring the Kernel to Modify System Parameters Using SAM

See Appendix A, "System Parameters" for reference and discussion of specific tunable system parameters.

To reconfigure the HP-UX kernel using SAM:

1. Login as superuser.
2. In an HP-UX cluster, ensure that you are logged onto the machine for which you are regenerating the kernel. This sets for the correct context for creating the `/hp-ux` context dependent file and optionally overwriting the `/etc/conf/dfile` context-dependent kernel configuration file.
3. Run SAM; type:

   `/usr/bin/sam`
4. Highlight `Kernel Configuration` and activate the [Open] control button.
5. Highlight `Configurable Parameters` and activate the [OK] control button.
6. Highlight the parameter you wish to update and choose `Modify Configurable Parameter...`.
7. Choose one of the following:
   - `Specify new formula`
   - `Specify new value`
   - `Select formula/value from source file`
8. Fill in the new information and activate the [OK] control button.
9. Choose `Create a New Kernel...` from the "Actions" menu.
10. Activate the [Yes] control button to confirm that you want to reconfigure the kernel now.
11. Choose one of the following:
    - `Create a new kernel now`

      This requires a reboot of your system. SAM prompts you to continue.

- `Defer kernel creation until later`

  SAM preserves the request to reconfigure the kernel. If you attempt to exit SAM before you have reconfigured the kernel, SAM prompts you to reconfigure the kernel or cancel your reconfiguration request.

- `Cancel all kernel modifications`

12. Follow the prompts to regenerate and reinstall the new kernel. After SAM generates a new kernel, choose one of the following actions and activate the OK control button:

    - `Move the kernel into place and reboot the system now`
    - `Move the kernel into place but do not reboot the system`
    - `Exit without moving the kernel into place`

    There is an option to enable or disable overwriting the kernel configuration file, `/etc/conf/dfile`.

    If you *enable* overwriting the kernel configuration file, SAM moves `/etc/conf/dfile.SAM` to `/etc/conf/dfile`, overwriting any comments you have added to the configuration file.

    If you *disable* overwriting the kernel configuration file, `/etc/conf/dfile` will not represent your current kernel (`/hp-ux`) when you reboot your system. `/etc/conf/dfile.SAM` represents your current kernel configuration after you reboot your system.

    We highly recommend the use of `/etc/conf/dfile` for the kernel configuration file so that it remains up to date with the executing kernel, `/hp-ux`. Some system software depends on `/etc/conf/dfile` representing the currently executing kernel.

If you do not want SAM to overwrite `/etc/conf/dfile`, because of comments you want to retain:

a. Choose the SAM option to disable overwriting the kernel configuration file.
b. Move the kernel into place (optionally rebooting the system).
c. Copy your comments from `/etc/conf/dfile` to `/etc/conf/dfile.SAM`. Be careful to add only your comments to the file. At this stage, you want `/etc/conf/dfile.SAM` to reflect your current kernel configuration.
d. Copy or save `/etc/conf/dfile.SAM` to `/etc/conf/dfile`.

The kernel configuration file `/etc/conf/dfile` now represents the current `/hp-ux` kernel.

Reconfiguring the Kernel to Modify Special Devices Using SAM

Note

- SAM supports removing alternate swap devices.
- SAM supports modifying the location of primary swap.
- SAM does not support adding, removing, or modifying the root device.

See Chapter 7, "Managing Swap Space" for guidelines about configuring primary swap devices.

To modify special devices using SAM:

1. Login as superuser.
2. In an HP-UX cluster, ensure that you are logged onto the machine for which you are regenerating the kernel. This sets for the correct context for creating the `/hp-ux` context dependent file and optionally overwriting the `/etc/conf/dfile` context-dependent kernel configuration file.
3. Run SAM; type:

```
/usr/bin/sam
```

4. Highlight `Kernel Configuration` and activate the (Open) control button.
5. Highlight `Special Devices` and activate the (OK) control button.
6. Highlight the device you want to modify and choose `Modify Device Configuration` from the “Actions” menu.
7. Highlight and fill in the modifications you want to make and activate the (OK) control button. Refer to Chapter 7, “Managing Swap Space” for additional information to modify your primary swap device.
8. Choose `Create a New Kernel...` from the “Actions” menu.
9. Activate the (Yes) control button to confirm that you want to reconfigure the kernel now.
10. Choose one of the following:
    - `Create a new kernel now`

      This requires a reboot of your system. SAM prompts you to continue.
    - `Defer kernel creation until later`

      SAM preserves the request to reconfigure the kernel. If you attempt to exit SAM before you have reconfigured the kernel, SAM prompts you to reconfigure the kernel or cancel your reconfiguration request.
    - `Cancel all kernel modifications`

11. Follow the prompts to regenerate and reinstall the new kernel. After SAM generates a new kernel, choose one of the following actions and activate the OK control button:

    - `Move the kernel into place and reboot the system now`
    - `Move the kernel into place but do not reboot the system`
    - `Exit without moving the kernel into place`

    There is an option to enable or disable overwriting the kernel configuration file, `/etc/conf/dfile`.

    If you *enable* overwriting the kernel configuration file, SAM moves `/etc/conf/dfile.SAM` to `/etc/conf/dfile`, overwriting any comments you have added to the configuration file.

    If you *disable* overwriting the kernel configuration file, `/etc/conf/dfile` will not represent your current kernel (`/hp-ux`) when you reboot your system. `/etc/conf/dfile.SAM` represents your current kernel configuration after you reboot your system.

    We highly recommend the use of `/etc/conf/dfile` for the kernel configuration file so that it remains up to date with the executing kernel, `/hp-ux`. Some system software depends on `/etc/conf/dfile` representing the currently executing kernel.

    If you do not want SAM to overwrite `/etc/conf/dfile`, because of comments you want to retain:

    a. Choose the SAM option to disable overwriting the kernel configuration file.

    b. Move the kernel into place (optionally rebooting the system).

    c. Copy your comments from `/etc/conf/dfile` to `/etc/conf/dfile.SAM`. Be careful to add only your comments to the file. At this stage, you want `/etc/conf/dfile.SAM` to reflect your current kernel configuration.

    d. Copy or save `/etc/conf/dfile.SAM` to `/etc/conf/dfile`.

    The kernel configuration file `/etc/conf/dfile` now represents the current `/hp-ux` kernel.

Booting the Standalone or Cluster Server Backup Kernel Using the Boot ROM

If your system is a standalone or cluster server and the new kernel fails to boot, select the backup kernel using the boot ROM:

1. Turn the computer off and then on (cycling power).
2. Hold down the space bar during bootup to enter the boot ROM **attended mode**. This halts the automatic boot mechanism and allows you to manually select the operating system to load.
3. Type in the two-character code associated with the backup kernel `SYSBCKUP`.

Your backup kernel will begin to boot. When you are given the login prompt, login again and try to reconfigure the kernel again.

Caution If you reconfigure the kernel for the second time using the steps described in "Reconfiguring the Kernel Using HP-UX Commands", DO NOT create a backup of the current kernel. Since you are currently booted from the backup kernel, copying `/hp-ux` to a backup kernel could overwrite the only bootable kernel on your system!

Restoring the Cluster Client Backup Kernel

If your system is a cluster client and the new kernel fails to boot:

1. Log into the cluster server from another client or the server console.
2. Ensure that you have superuser capabilities.
3. Move the client's backup kernel to the `/hp-ux` context-dependent file. For example:

   `mv /SYSBCKUP.`*cluster_node_name* `/hp-ux+/`*c_node_name*

   where

cluster_node_name	is the client's full hostname as displayed by the `hostname` command

4. Reboot the cluster client by cycling the power.

The client's backup kernel will begin to boot. When you are given the login prompt, login again and try to reconfigure the kernel again.

Caution If you reconfigure the kernel for the second time using the steps described in "Reconfiguring the Kernel Using HP-UX Commands", DO NOT create a backup of the current kernel. Since you are currently booted from the backup kernel, copying `/hp-ux` to a backup kernel could overwrite the only bootable kernel on your system!

Adding and Removing Subsystems

In order to run certain Hewlett-Packard subsystems, you must not only install the software, but also reconfigure the kernel to make it aware of the subsystem. In general, you don't need to worry about this, because the `update` utility, which loads the software, also makes the necessary modifications to the kernel and to any other files in which the subsystem may require specific entries.

If you are about to install a new Hewlett-Packard subsystem, do not continue with this section. Instead, follow directions in the documentation that came with the product. Usually these documents will tell you to run `/etc/update`, and will contain all the information you need to install the software.

If you need more information on `/etc/update`, you'll find it in the manual *Installing and Updating HP-UX*.

Adding a Subsystem Using HP-UX Commands

Adding a subsystem is necessary only when you already have all the files a given Hewlett-Packard subsystem comprises on your system, and need to add the corresponding "pseudo-driver" to the kernel. A pseudo-driver is a piece of software that enables the kernel to communicate with the subsystem, which by comparison with a device driver controls a hardware device such as a disk drive).

This case could occur if you had disabled a subsystem by removing the pseudo-driver from the kernel, but had not removed the software. To enable the subsystem again, you could simply add the pseudo-driver back into the kernel, and then regenerate the kernel and reboot.

The configurable pseudo-drivers and the subsystems they support are as follows:

Table 2-1. Pseudo-Drivers

Driver Name	Used For:
nfs	Support for NFS networking
lla, lan0, lan1, lan01	Support for NS-ARPA networking (formerly the ieee802 and ethernet drivers)
dskless	Cluster code pseudo-driver
cdfs	CDROM subsystem driver
lan0, lan1, uipc, inet, netdiag1, netman, lla, lan01	Support for LAN
nipc	Support for NS networking
x25ip, x25pa	Support for X.25 networking

Table 2-1 shows which pseudo-drivers are used by which subsystems.

Caution If you have installed a new version of HP-UX since you removed the subsystem pseudo-driver form the kernel, you must not simply add the pseudo-driver back by editing the kernel generation file and creating a new kernel. The older subsystem might be incompatible with the new kernel, in which case the kernel build will fail.

Unless you are certain you have not updated HP-UX since you removed the pseudo-driver from the kernel, use `/etc/update` to recover the entire subsystem from the latest set of `update` tapes, or from the latest product tape if you got the product after the latest HP-UX release. We recommend this as the safest method in all cases.

Removing a Subsystem Using HP-UX Commands

If you are removing a subsystem (all the programs and data files) from the system, it's a good idea to remove the subsystem's pseudo-driver from the kernel as well. This will make the kernel smaller and it will run more efficiently.

Table 2-1 shows which pseudo-drivers go with which subsystems.

Reconfiguring the kernel using `config` removes only the pseudo-driver, not the software. To remove the software filesets, use the `rmfn` tool described in the later section, "Removing System Files".

Adding and Removing Subsystems Using SAM

To reconfigure the HP-UX kernel using SAM:

1. Login as superuser.
2. In an HP-UX cluster, ensure that you are logged onto the machine for which you are regenerating the kernel. This sets for the correct context for creating the `/hp-ux` context dependent file and optionally overwriting the `/etc/conf/dfile` context-dependent kernel configuration file.

Note For the CDFS and NFS subsystems, these *cannot* be added or deleted on a cnode. They can only be modified on the server. If SAM detects an attempt to add or delete one of these two on a cnode, an error message is presented which states you must make this change on the server for the whole cluster.

If SAM detects this change on a cluster server, you are warned that when the kernel is built to implement this change, a process runs on all the cnodes to similarly modify their kernels, and the whole cluster will have to be rebooted. This message is a confirmation message allowing you to decide not to make this change. The actual instructions about this cluster wide reconfig is given when building the new kernel.

---

3. Run SAM; type:

   `/usr/bin/sam`

4. Highlight `Kernel Configuration` and activate the (Open) control button.
5. Highlight `Subsystems` and activate the (OK) control button.

6. To add a subsystem:

   a. The subsystem file set must be loaded on the system; refer to *Installing and Updating HP-UX*.

   b. Highlight the subsystem you want to add and choose `Add Subsystem to Kernel` from the "Actions" menu. The "Pending State" column entry for the subsystem(s) should have the value "In."

7. To remove a subsystem, highlight the subsystem you want to remove and choose `Remove Subsystem from Kernel` from the "Actions" menu. The "Pending State" column entry for the subsystem(s) should have the value "Out."

8. Choose `Create a New Kernel` from the "Actions" menu.

9. Activate the (Yes) control button to confirm that you want to reconfigure the kernel now.

10. Choose one of the following:

    - `Create a new kernel now`

      This requires a reboot of your system. SAM prompts you to continue.

    - `Defer kernel creation until later`

      SAM preserves the request to reconfigure the kernel. If you attempt to exit SAM before you have reconfigured the kernel, SAM prompts you to reconfigure the kernel or cancel your reconfiguration request.

    - `Cancel all kernel modifications`

11. Follow the prompts to regenerate and reinstall the new kernel. After SAM generates a new kernel, choose one of the following actions and activate the OK control button:

   - `Move the kernel into place and reboot the system now`
   - `Move the kernel into place but do not reboot the system`
   - `Exit without moving the kernel into place`

   There is an option to enable or disable overwriting the kernel configuration file, `/etc/conf/dfile`.

   If you *enable* overwriting the kernel configuration file, SAM moves `/etc/conf/dfile.SAM` to `/etc/conf/dfile`, overwriting any comments you have added to the configuration file.

   If you *disable* overwriting the kernel configuration file, `/etc/conf/dfile` will not represent your current kernel (`/hp-ux`) when you reboot your system. `/etc/conf/dfile.SAM` represents your current kernel configuration after you reboot your system.

   We highly recommend the use of `/etc/conf/dfile` for the kernel configuration file so that it remains up to date with the executing kernel, `/hp-ux`. Some system software depends on `/etc/conf/dfile` representing the currently executing kernel.

   If you do not want SAM to overwrite `/etc/conf/dfile`, because of comments you want to retain:

   a. Choose the SAM option to disable overwriting the kernel configuration file.

   b. Move the kernel into place (optionally rebooting the system).

   c. Copy your comments from `/etc/conf/dfile` to `/etc/conf/dfile.SAM`. Be careful to add only your comments to the file. At this stage, you want `/etc/conf/dfile.SAM` to reflect your current kernel configuration.

   d. Copy or save `/etc/conf/dfile.SAM` to `/etc/conf/dfile`.

   The kernel configuration file `/etc/conf/dfile` now represents the current `/hp-ux` kernel.

Removing System Files

You can use the `rmfn` (remove functionality) utility to remove system software you don't need. The interactive screens of `rmfn` allow you to remove software in groupings at the level of **filesets** and **partitions**. (A fileset is a logical group of files that make up a piece of software functionality. A partition is a logical group of filesets.)

Before it removes filesets, `rmfn` checks fileset dependencies. If a fileset or partition you select for removal is required by other filesets, `rmfn` asks you if you want to remove these dependent filesets as well.

The `rmfn` command keeps a log of its actions in `/tmp/rmfn.log`.

Caution Although `rmfn` checks dependencies to prevent you from inadvertently removing functionality, you must still be cautious because `rmfn` removes major pieces of software quickly.

Important Points

- The filesets and partitions that `rmfn` displays depend on the contents of the directories `/etc/filesets` and `/system`. Do not change the contents of these directories or `rmfn` will display an inaccurate list of filesets.
- `rmfn` checks that removing the selected filesets will not harm the integrity of your system. For example:
  - `rmfn` will not allow you to remove a minimum set of filesets needed by the system. For instance, you cannot remove `UX-CORE`.
  - If you have a mirrored system, and select a mirrored fileset while the mirror is on, `rmfn` will not remove the fileset.
- The `rmfn` command will not remove files on a remote mounted system (NFS).
- As `rmfn` removes a symbolic link contained in a fileset, it does not remove a symbolic link's target file. A target file remains in tact until `rmfn` removes the fileset that contains it.

How to Use rmfn

To use the `rmfn` command, log in as superuser, and enter:

`/etc/rmfn`

The example below shows a typical `rmfn` menu screen.

To remove an entire partition, mark it with a `y`. To remove individual filesets within a partition, press Select Filesets and then mark the filesets you want removed with a `y`. (After you select individual filesets within a partition for removal, the partition is automatically marked with a `p` for partially selected.)

To prevent a fileset or partition from being removed (to keep it on your system), mark it `n`; `n` is the default choice for all filesets on the screen.

```
rmfn                               Partitions

Press "y" to select an entire partition for deletion.  Press "n" to undo a
selection.  Press the "Select Filesets" key to view the filesets within a
partition.  Press the "Start Removing" key when selection is complete.

Mark  Partition Name   Arch.  Partition Description           Size in Kbytes

 p    DIAGNOSTICS      300    Hardware Diagnostic Programs      37663
 n    NETWORKING       300    Networking Products                8919
 n    NLS              300    Native Language Support             472
 n    OS-ADMIN         300    Recommended Administration Cmds    2292
 n    OS-CORE          300    Recommended System Core            5517
 n    OS-FEATURES      300    Selectable OS Features             8176
 n    PROG-LANGUAGES   300    Programming Languages              8542
 n    REFERENCE-DOC    300    Reference Manual Pages              348
 n    SHARED-LIBS      300    Runtime Shared Libraries           2757
 n    WINDOWS          300    Windowing Products                  102

 Help            Shell    Start             View      Select               Exit
                          Removing          Selected  Filesets             rmfn
```

Figure 2-1. `rmfn`: "Partitions" Screen

`Help`	Explains how to the use the **rmfn** tool.
`Shell`	Lets you escape to the shell. Type `exit` to return to the **rmfn** screen.
`Start Removing`	Removes the selected filesets and partitions from your system.
`View Selected`	Lists the names and sizes of the partitions and filesets selected for removal.
`Select Filesets`	Allows you to individually select the filesets within a partition for removal.
`Exit rmfn`	Exits **rmfn**.

3

Starting and Stopping HP-UX

Starting and stopping HP-UX are routine tasks, but they are critical to the operation of your computer. When the system is turned on, you can allow the default operating system to boot, or selection other options. When you stop a system, you must use the appropriate shutdown process. Simply turning the system off can corrupt the file system. When you change the system to an administrative state, during shutdown, you can reboot (restart) the system without turning it off, or you can shut the system down completely.

The following table shows the sections of this chapter that describe these processes.

Section Name	How this Section Helps You
"Starting HP-UX"	Describes starting HP-UX, restarting HP-UX, and coordinating startup with turning on peripherals.
"Shutting Down the System"	Explains the situations and procedures for shutting down the system.

You can get additional information about these processes in the manual *How HP-UX Works: Concepts for the System Administrator*.

3

Starting HP-UX

You must start up HP-UX when the operating system has been completely shut down, as is required before you turn the computer off; or after you have partially shut down the operating system to perform system administration tasks.

Prerequisites and Conditions

Here are some points to consider:

- Some SAM tasks might restart (reboot) the system for you (for example, if you rebuild the kernel).
- To start your HP-UX system, you must have configured and installed the hardware and the software. See other chapters in this manual, as well as *Installing and Updating HP-UX* and *Installing Peripherals* for more information.
- Start up an HP-UX cluster server as you would a standalone system. This manual, and *Managing Clusters of HP 9000 Computers Sharing the HP-UX File System* contain additional information.
- The disk that contains the HP-UX file system can contain alternate HP-UX systems and other operating systems. If you want to boot a certain HP-UX system automatically, it must be the first system found by the bootROM.
- Your system must have certain files to start up properly (for example, `/etc/init`, `/etc/inittab`, `/dev/console`, `/etc/rc`). Without these files, the startup process will fail.
- The startup process might check the file system. This delays startup, and might require you to perform additional tasks.
- If your system will not boot, you can use your recovery system to get a partial system going.

Configuring Your System

Your computer might need to be configured before the operating system can recognize the I/O cards which are installed in your computer. Some computers require that you set switches on the CPU board, and others require that you change the addresses on a configuration table which appears on your monitor when you first turn on the computer.

Read your computer's owner's guide to determine how to configure your computer. You can determine if your computer is configured by setting switches on the CPU board, or by changing the addresses on a configuration table, by looking at the information which is first displayed on your monitor when your computer is turned on. If the words "Configuration EEPROM" is displayed on the screen during bootup, your computer can be configured by changing the addresses on a configuration table. If these words do not appear, you must set the switches on the CPU board in order to configure your system.

If your computer can be configured using the configuration table, see the *Installing Peripherals* manual for BootROM configuration information.

Setting Initial Information

The first time you boot HP-UX, the operating system will ask you to provide the following information:

- System Name.
- Internet Protocol (IP) Address (If networking is installed).
- Time Zone.
- Date.
- Time.

3

Be prepared by having the following information available:

- Your unique system name. This is the host name and must be less than nine characters long, contain only alphabetic characters, numbers, underscores, or dashes, and must start with an alphabetic character.
- Your internet protocol (IP) address. This address has four numeric components, each of which is separated by a period, and each number must be between 0 and 256. An example of an IP address is: 255.32.3.10. If you do not have networking installed, you will not be prompted for the IP address.
- Your time zone. This is the time zone where your system is located. For example: Pacific Standard Time.
- The current date and time.

If you do not know any of this information, you can use the default values provided, and then change the information later. However, this initial information will not be requested at later bootups, and you will have to enter the information manually following the instructions in chapter 2 of this manual.

The Startup Process Might Check the File System

During the startup process, the system executes `/etc/fsclean`. This command determines the shutdown status of the system and returns three possibilities:

1. If the file systems were shut down properly, the startup process continues and you see the following message: 3

   ```
   /etc/fsclean: /dev/dsk/0s0 (root device) ok
   file system is OK, not running fsck
   ```

2. If any file systems were not shut down properly, the startup process is interrupted and you see:

   ```
   /etc/fsclean: /dev/dsk/0s0 not ok
   run fsck
   FILE SYSTEM(S) NOT PROPERLY SHUTDOWN,
   BEGINNING FILE SYSTEM REPAIR.
   ```

   At this point, the system runs `/etc/fsck` in a mode that can correct certain inconsistencies in the file systems without your intervention and without removing data. The `fsck` command will either:

   a. repair and reboot the system, incorporating the changes, or

   b. you might be asked to run `fsck` manually. If you need to run `fsck` manually, see the chapter named "Managing the File System".

3. If `fsclean` detects any other errors (for example, not being able to open a specified device file), you get an error message. The startup process can end, and you will need to solve the problem. The *Solving HP-UX Problems* has information about possible problems in making HP-UX function.

Turning On Your Computer

Follow these steps to turn on your computer:

1. Turn on all peripherals you want to use. Wait until they are in the ready state. You must turn on the disk that contains HP-UX.
2. You have two possibilities for turning on the computer:
   a. If you have only a computer (no expander), turn it on and go to the next step.
   b. If your computer is attached to an expander, proceed as follows:
      i. The CPU and the user-interface card (the card having the keyboard and such) should be in the computer, not in the expander.
      ii. In any case, especially if the cards are not installed as described above, turn on the expander. Then, turn on the computer and go to the next step.
3. The bootROM initiates startup and displays a screen similar to the following:

```
Copyright 1989
Hewlett-Packard Company.
All Rights Reserved.

BOOTROM Rev. D
Bit Mapped Display
MC68030 Processor
MC68882 Coprocessor
Configuration EEPROM
HP-HIL.Keyboard
HP-IB
RAM 8388384 Bytes
DMA-CO
HP98644 (RS232) at 9
HP98265 (SCSI S 32) at 14
HP98625 (HPIB) at 15
HP98643 (LAN) at 21, 0800009AAAAAA
HP PARALLEL at 23

System Search Mode
RESET To Power-Up
```

4. You are then given the opportunity to automatically boot the operating system, or to halt the bootup process and selection an alternate operating system or program.

If you do nothing, the HP-UX operating system automatically takes control and completes the bootup process. Watch the startup messages. Compare what starts up with what you expect, and note possible problems. The exact messages depend on your configuration. The startup process ends when you see the login prompt. If you do not get the prompt, the system did not start up. You will need to determine why. During the startup process, the system will perform a file system consistency check of the root disk if the system was shut down improperly. If your system is spread over multiple disks, you should perform a consistency check on the other file systems according to procedures described in the chapter named "Managing the File System".

3

Starting an Alternate Operating System or Program

If you do not want to boot the first system found by the bootROM, you can select from alternate operating systems or programs.

1. Turn on your computer and hold down the spacebar as the computer boots up.
2. The startup process pauses to show a list of available systems. You can see more than one system (even non-HP-UX systems). The following example illustrates the idea of selecting a system from the attended mode:

`:HP7937, 1400, 0, 0`
`1H SYSHPUX`
`1D SYSDEBUG`
`1B SYSBCKUP`
	1H is probably your main HP-UX system. 1D is the debugger for the main system. 1B is the backup for the main system.

`:HP9144, 700, 1, 0` `2H SYSHPUX`	*An HP-UX system on a cartridge tape in an HP9144 drive, labeled 2H*

`:LAN, 21, hpfcma`
`3H SYSHPUX`
`3D SYSDEBUG`
`3B SYSBCKUP`
	3H is an HP-UX system that is available via your Local Area Network (probably a client in an HP-UX cluster). 3D is the debugger. 3B is the backup system.

   Use the label to select the system you want to boot. For example, typing `2H` starts up the system on the cartridge tape in the HP 9144 drive that lets you install HP-UX.

3. Once you select an HP-UX system other than one shown for an installation tape, the startup process is the same as the automated process described above, and the process ends when you get the login prompt.

Shutting Down the System

You should never just turn an HP-UX system off! Instead, shut the system down properly. Typically, you shut down the system down for one of two reasons:

1. Get into the single-user state so you can do system administration tasks such as update the system, reconfigure the kernel, or check the file systems, or
2. Shut down the system totally to perform a task such as installing a new interface card.

3

Prerequisites and Conditions

- Stopping the system improperly can corrupt (damage) the file systems. Never stop the system by turning it off!
- You can use SAM to shut down the system.
- Only the system administrator or a designated superuser should shut down the system.
- The `/etc/shutdown` command warns users of impending shutdown; halts daemons; kills unauthorized processes; unmounts file systems; puts the system in single user mode; and writes the contents of the I/O buffers to a disk. You see several messages during the process. You should watch them to note actions and possible problems.
- The `shutdown` command warns all users to log off the system, using a grace period you can specify. If you do not specify one, users get 60 seconds to log off. You should notify active users as to when the system will be shut down. Give them enough time to finish their work and log off. You can do this physically or use the `/etc/wall` or `/etc/cwall` commands. The chapter named "Constructing an HP-UX System" has information.
- In an HP-UX cluster, clients need only log off, but the shutdown process works better if you turn the cnodes off. Do not shut down the system from a client; do the work from the root server.
- If you use a network service, do not run `shutdown` from a remote system via `rlogin`. The shutdown process logs you out prematurely and returns control to the system console.
- See the *shutdown*(1M) entry in the *HP-UX Reference* manual for information about options and features.
- The *How HP-UX Works: Concepts for the System Administrator* manual has information on system shutdown concepts.

Designating Shutdown Authorization

You can designate which users are authorized to run `shutdown` by listing these users in the file `/etc/shutdown.allow`. If this file is empty, only the superuser has shutdown authority, but if this file is not empty, and the superuser login (usually **root**) is not listed in the file, then the superuser will not be permitted to shutdown the system. In an non-empty `shutdown.allow` file, only those users listed will have shutdown authority.

The following wildcards are allowed in the `shutdown.allow` file:

- `+` specifies that any host/user has shutdown authority.
- `%` specifies that any host in cluster has shutdown authority.

For example:

- `systemA user1` allows user1 to shut down systemA.
- `% user2` allows user2 to shut down any node in a cluster.
- `+ root` allows root to shut down any node.
- `systemC +` allows any user to shut down systemC.

Customizing the Shutdown Process

You can customize the shutdown process by placing Bourne shell scripts in the file `/etc/shutdown.d`. These scripts will be executed in an ASCII (machine-collated) order. These scripts are optional, and are not required to run `shutdown`.

Manual Procedures

Going to the Single-user State for Maintenance

3

1. As the root user, change to the root directory if not already there:

   ```
   cd /
   ```

2. Shut down the system. You have some alternatives for doing this. Also, the shutdown process asks if you want to send a message. If you elect to broadcast a message, respond with y and then type the message. When you finish, press [Return] (or [Enter]), and then [CTRL]-[D]. The following examples show alternatives for shutting down to the single-user state:

`shutdown`	*Shuts down to single-user state, allowing the default 60 second grace period*
`shutdown 0`	*Shuts down the system with no grace period*
`shutdown 30`	*Begins the shutdown to the single-user state after a 30-second grace period*

3. While the system is in the single-user state, perform the necessary system administration tasks. When you finish, you can start up the system without turning off anything by executing:

   ```
   reboot
   ```

   As always, watch the messages to see that everything is happening correctly.

   Some system administration tasks will do the rebooting for you.

Shutting Down the System Completely

1. As the root user, change to the root directory if not already there:

   ```
   cd /
   ```

2. Shut down the system. You have some alternatives doing this. Also, the shutdown process asks if you want to send a message. If you elect to broadcast a message, respond with `y` and then type the message. When you finish, press (Return) (or (Enter)), and then (CTRL)-(d). 3

   From the multi-user state, you can shut down the system completely:

   ```
   shutdown -h
   ```

   This process is rather harsh and sudden. It is generally better to take the system down in steps:

   a. Execute:

      `shutdown 20` *This gets the system into the single-user state, allowing a 20 second grace period*

   b. Execute:

      `reboot -h` *This brings the system to a complete stop*

      You know the system is shut down completely when the system displays `halted` and pressing a key takes no action.

3. When the system is halted, turn the system off as follows:

   a. If you have only a computer (no expander), turn the computer off. Then, turn the devices off as required.

   b. If you have a computer and an expander, turn the computer off, turn the expander off, and then turn the devices off as required.

4. When you want to start up the system again, see the earlier procedure for starting up HP-UX.

3

Shutting Down the System to Activate a New Kernel

You might want to shut down the system only to activate a new kernel. To do this, execute:

```
shutdown -r 0
```

The `-r` option causes the system to reboot immediately after the system gets into the single-user state.

Do not execute `shutdown -r` from run-level s. You must reboot using the `reboot` command.

Using SAM to Shut Down the System

You can use SAM to shut down the system. You can access SAM's shut down capability:

1. Highlight `Routine Tasks->` and activate the (OK) control button. 3
2. Highlight `System Shutdown->` and activate the (OK) control button.

In SAM's `System Shutdown->` window you can choose to:

- Halt the system
- Reboot (restart) the system
- Go to single user state

Using SAM to Halt or Reboot the System

The key things to consider when you reboot or shut down the system are:

- Choosing a grace period after issuing a warning message.
- Broadcasting a message to the other users on your system to give them time to end their activities and log off.

1. Activate the control button that corresponds to your action in the "Shutdown Type" control box.
2. Choose and activate an appropriate grace period in the "Time Before Shutdown" control box.
3. Activate the (OK) control button.
4. Note SAM's confirmation note and activate the (Yes) control button to proceed.
5. Type in the message to issue to the users when SAM prompts you and proceed to shut down. You will have one more opportunity to discontinue the shutdown process.

3

Power Failure Considerations

A local power failure means a power failure that halts the computer by affecting its central bus.

Remote power failures (affecting a remote bus) or device power failures (affecting a device) do not affect the system as a whole, unless the remote devices provide a vital system resource.

Power Failure Related Tasks

If you know power is going out soon: Shut down the computer and turn off power.

In a cluster, turn off root server, clients, and peripherals.

If local power fail occurs: If possible, TURN OFF all computer equipment affected by a power failure until power is completely restored. An electrical surge as power is coming back on could seriously damage hardware that has been left turned on.

Power Failure in a Cluster

1. When a local power failure occurs on a cluster root server, all the clients will panic. Make sure you switch off the root server and all other equipment that no longer has power.
2. When a local power failure occurs on an **auxiliary swap server**, the clients swapping to the auxiliary swap server will panic. Make sure you switch off the auxiliary server and all other equipment that no longer has power.

   An auxiliary swap server is a client to whose disks other clients are swapping.
3. When a local power failure occurs on an **auxiliary file server**, the locally mounted file systems will be unavailable until the auxiliary file server comes back up. Other cluster nodes that are not affected by the power failure will continue to function. Make sure you switch off the auxiliary server and all other equipment that no longer has power.

   An auxiliary file server is a client whose local disk is used for a file system but not for shared swap.
4. When a power failure occurs on a client that is not an auxiliary swap or file server, other cluster nodes that are not affected by the power failure will continue to function. Make sure you switch off the client and all other equipment that no longer has power.

To bring the cluster clients back up after a power failure on the root server or an auxiliary swap server, turn the server back on and wait for it to reboot, then reboot the clients.

4

Controlling Access to Your System

It is rare to find a computer installation where everyone has access to *all* of the computer's files, commands and hardware resources. It is therefore likely that you will want to control who has access to your system, its data and its commands.

Authorized users gain access to the system by supplying a valid user name (login name) and password.

For additional information about the login process and the `/etc/passwd` file, refer to *login(1)* and *passwd(4)* in the *HP-UX Reference* manual and Chapter 4, "Login" of *How HP-UX Works: Concepts for the System Administrator*, HP part number B2355-90029.

Terms Used in this Chapter

access permissions Values associated with each file that control who has permission to read, write (modify) or execute the file.

effective group If a user changes their default or primary group with the `newgrp` command, the new current group is the effective group (see **group** and **primary group** below).

group ownership The secondary ownership associated with each file, associating the file with a group (see **group**, below).

4

group Users on an HP-UX system can be grouped. If a group has access to a file, then any user who is defined as a member of that group will have access to the file. Users can be members of more than one group.

group_ID Also known as GID, is a unique number associated with each group (see **group**, above) that identifies the group to HP-UX. These group_ID numbers are defined in the `/etc/group` file.

log in Process used to gain access to the computer by supplying a user name and (if required) a password.

multi-user mode An HP-UX mode of operation that allows multiple users to access the system simultaneously. This is the "normal" mode of operation for HP-UX systems. See also **single-user mode**.

ownership Each file on the system has an owner. The owner controls access to the file by setting its access permissions. The owner is typically (but not always) the user who created the file.

primary group or default group A user can be a member of multiple groups, but only one of those groups is considered to be the user's primary or default group. In addition to being listed as a member of groups in the file `/etc/group`, an entry exists in the `/etc/passwd` file that indicates the user's primary group. When users first log into the system, they are affiliated with their primary group. Refer to the "Controlling User Accounts and Groups" and "Managing User Accounts and Groups Tasks" sections of this chapter for details.

run-level s See **single-user** mode.

run-level An HP-UX mode of operation. Modes of operation are defined in the file, `/etc/inittab`. The `/etc/inittab` file defines which terminals and processes are active at each run-level.

single-user mode A special HP-UX mode of operation that restricts user input to the system console. It is usually used by the system administrator to prevent others from accessing the system during special system administration activities when it is not advisable to have other system activity (for example, when updating the operating system to a new revision).

user_ID Also known as UID, is a unique number that HP-UX uses to identify a particular user. The user_ID number zero ("0") is used to identify the superuser. User_ID numbers between 1 and 99 are used by HP-UX subsystems. User_ID numbers above 99 are used for "normal" users.

user account The environment created on the system to allow the user access. Creating a user account involves updating the system to recognize the user's login name and password. You also need to give the user access to files, system resources, and applications.

Overview of Controlling Access Your System

Securing your data against deliberate, unauthorized access is only one reason for controlling access to your system. There are three levels of access control to your system. The following list of levels also includes reasons why you would want to control access at a particular level.

1. Controlling User Accounts and Groups

   By controlling who can log in to your system, you can prevent unauthorized users from running programs that consume valuable system resources (making them unavailable for the authorized users of your system). By creating and controlling groups of users, you can create unique group environments. Most systems are used for multiple purposes, and user groups allow you to customize according to multiple and varying group needs.

2. Controlling File Access

   By setting the appropriate access permissions for files and directories on your system, you can prevent them from being *accidentally* deleted or overwritten.

   By setting the appropriate ownership and group ownership for files (in addition to the file permissions) on your system, you can limit their use to specific users (or groups of users).

3. Controlling Run-Levels

   By configuring appropriate run-levels, you can activate different groups of terminals (and processes) for different situations (such as different work shifts).

Controlling User Accounts and Groups

Each user is defined by an entry in the file `/etc/passwd`. The `/usr/bin/vipw` command is the recommended editor for modifying the `/etc/passwd` file. The `vipw` command guarantees exclusive access to the `/etc/passwd` file. The `/etc/ptmp` file is created by the `vipw`, `chsh`, `chfn`, and `passwd` commands when access to the `/etc/passwd` file is granted. The `/etc/vipw` command requires the `EDITOR` environment variable set to `vi`.

If you are in single-user mode and the `vipw` command denies you access to the `/etc/passwd` file with an error message, "password file busy", delete the `/etc/ptmp` file and try the `vipw` command again. It is possible that the process that created this file terminated without removing this file. Refer to *vipw*(1M), *chsh*(1), *chfn*(1), *passwd*(1), and *passwd*(4) in the *HP-UX Reference* manual for additional information.

Users on your system can be divided into various working groups, so that files owned by members of a given group can be shared and yet protected from access by users who are not members of the group. A user can be a member of *more than one group*. A group can have a maximum of 200 members.

If you prefer not to divide the users of your system into separate working groups, it is customary to set up one group (usually called "users") and assign all users of your system to that group.

Users may change their current group by using the `newgrp` command. The new group is referred to as the **effective group** for the user. Changing to an effective group does not alter the user's primary group entry in the `/etc/passwd` file. The user can return to their primary group by specifying no parameters or options to the `newgrp` command.

Group information is defined in `/etc/group` and `/etc/logingroup`, which are ASCII files that you can edit with a text editor such as `vi`.

`/etc/group` defines for each group:

- group name
- encrypted password (optional)
- numerical group identifier (*group_ID*)
- comma-separated list of group members by user login name

For example:

```
root:*:0:
other:*:1:
bin:*:2:
sys:*:3:
adm:*:4:
daemon:*:5:
mail:*:6:
lp:*:7:
users:*:20:john,naomil,patrickd,kerschen,michelem,dennism,pvallis
pub:*:24:patrickd,naomil,dennism
```

Note that a blank line in the `/etc/group` file is not allowed. If a blank line appears in the `/etc/group` file, all entries after the blank line are ignored.

`/etc/logingroup` contains the identical information, but the group name and encrypted password fields are not used. It is common practice to link the `/etc/group` and `/etc/logingroup` files together using the `link` command (refer to *link*(1M) in the *HP-UX Reference*).

`/etc/group` is used by the `newgrp` command to check access privileges. If the user's login name appears in the access list of the group for which access is being requested, the access is granted thus changing the user's current group to the requested group. `/etc/logingroup` in contrast to `/etc/group` allows users listed in more than one group access to files belonging to other groups without changing their primary or effective groups.

For additional information about group related tasks, refer to the "Managing User Accounts and Groups Tasks" section of this chapter. For more details on the `/etc/group` and `/etc/logingroup` files, refer to the "Adding a Group Using HP-UX Commands" section of this chapter and *group*(4) in the *HP-UX Reference* manual.

Primary Groups

A user can be a member of multiple groups, but only one of those groups is considered to be the user's primary or default group. In addition to being listed as a member of the group in the file `/etc/group`, an entry exists in the file `/etc/passwd`, indicating which group is the user's primary group. When users first log into the system, they are affiliated with their primary group.

To change the *primary* (default) group that your user is a member of, you will need to change user's entry in the `/etc/passwd` file to reflect a new *group_ID* value. The *group_ID* uniquely identifies an entry in `/etc/group` and `/etc/logingroup`. For instructions, see the "Displaying/Modifying a User's Account Information Using SAM" or "Changing a User's Primary Group Using HP-UX Commands" section of this chapter.

4

Group Passwords

When a user first logs into your system, their default or primary group affiliation is the one pointed to by the *group_ID* entry (fourth field in `/etc/passwd`). A user may be a member of more than one group. To change which group a user is affiliated with, a user can use the `newgrp` command. `newgrp` will require a password if the *group has a password* and the *user does not*, or if the *group has a password* and the *user is not listed as being a member of that group* (in the file `/etc/group`). If the user only needs to access files in another group, a entry in the `/etc/logingroup` would permit access to other group's files without changing the user's effective group. See *group*(4) in the *HP-UX Reference* manual.

Note The use of group passwords is *not* encouraged, and they are rarely used. They encourage poor security practices.

Special Groups

Commands that permit access to all of the system's resources (and files) are usually restricted for use by superusers only. Although it is possible to have more than one superuser defined for your system (see "Adding a User Using SAM" or "Adding a User Using HP-UX Commands"), you may prefer to have only a subset of the superuser's capabilities available to a group of users. There are five types of **special privileges** that you can assign to a group of users using the `setprivgrp` command:

4

RTPRIO controls group access to the `rtprio` command and system call that allow the setting of real-time priorities.

MLOCK controls group access to the `plock` system call that allow processes to be locked in memory and allow the use of the `shmctl` system call SHM_LOCK parameter.

CHOWN controls group access to the `chown` command and system call that allow changing the ownership of files on the system.

LOCKRDONLY controls group access to the `lockf` system call that sets locks on files that are open for reading only.

SETRUGID controls group access to the `setuid` and `setgid` system calls. The `setuid` system call changes the real user ID of a process and the `setgid` system call changes the real group ID of a process.

For additional information refer to *rtprio*(1), *rtprio*(2), *plock*(2), *shmctl*(2), *chown*(1), *chown*(2), *lockf*(2), *setuid*(2), *setgid*(2), *setprivgrp*(2) and *setprivgrp*(1M) in the *HP-UX Reference* manual.

Any user whose current group_ID matches the group_ID of a privileged group will have access to the special capabilities assigned to that group. A group can have any one or a combination of the special privilege capabilities. Refer to the "Displaying/Assigning Special Group Privileges Using HP-UX Commands" section of this chapter for specific instructions.

Note

In an HP-UX cluster, group privileges apply only to the cluster node on which you set them. For example, if you want group `patrick` to have RTPRIO privilege on cluster clients `client1` and `client2`, then you must execute the `setprivgrp` command twice, once on `client1` and again on `client2`.

The CHOWN privilege is an exception: if a group has this privilege on the cluster server, it will have it on all cluster clients as well.

4

Controlling File Access

All of the files on an HP-UX system have access permissions, ownership, and group ownership associated with them. Together the permissions and ownerships determine who can access the file.

File Access Permissions

There are three types (modes) of file access:

read — Determines who can view the file's contents. For directories, read access allows access to the directory with the `cd` command.

write — Determines who can alter the file's contents. For directories, write access allows modify and remove privileges.

execute — If the file is an *executable program*, the execute permissions determine who can run the program. For directories, execute access allows listing the directory contents.

There are three sources of file access:

Owner — The owner is usually the person who created the file (unless ownership has since been changed using the `chown` command).

Group — Members of the group that the file belongs to.

Other — All other users on your system.

There are three commands that change file access privileges:

- `chmod`

  The `chmod` command changes the type of access (read, write, and execute privileges) for every access source (owner, group, or other). For example, you can give the owner of the file read, write, and execute privileges, restrict group members to read and execute, and give only execute privileges to all other users on the system. Only the owner of a file (or the superuser) can change its read, write, and execute privileges.

- `chown`

  The `chown` command changes file ownership. In order to change the owner, you must own the file or have superuser privileges. Special group privileges determines a group's ability to use the `chown` command on files not owned by the user. The `setprivgrp` command controls special group privileges. To use the `setprivgrp` command, refer to the "Displaying/Assigning Special Group Privileges Using HP-UX Commands" section of this chapter.

- `chgrp`

  The `chgrp` command changes file group ownership. In order to change the group, you must own the file or have superuser privileges.

Refer to *Using HP-UX* or *chmod*(1), *chown*(1), and *chgrp*(1) in the *HP-UX Reference* manual. Default file permissions are assigned by the system whenever you create a new file or directory, and these are governed by your `umask` setting. Unless set up otherwise by you or your system administrator, your default `umask` setting will be 0, which means that new *files* you create will have read/write permission for everyone (666 or -rw-rw-rw-) and new *directories* you create will have read/write/search permission for everyone (777 or `drwxrwxrwx`).

For additional information on file protection refer to Chapter 8, "HFS File System", in *How HP-UX Works: Concepts for the System Administrator*, HP part number B2355-90029. See also *ll*(1), *setprivgrp*(1M), and *umask*(1) in the *HP-UX Reference* manual.

Access Control Lists

Access control lists (ACLs) offer a finer degree of file protection than traditional file-mode protection. With ACLs, you can allow or restrict file access to individual users, unrelated to what group the users belong to, with the `chacl` command. Only the owner of a file (or the superuser) can create ACLs with the `chacl` command.

Since you can use both the `chmod` and the `chacl` commands to change access permissions, you need to be aware of how the two commands interact.

- The `chacl` command is a superset of the `chmod` command. Any specific permissions you assign with the `chacl` command are added to the more general permissions assigned with the `chmod` command. For example, suppose you use the `chmod` command to allow only yourself write permission to `myfile`. You can use the `chacl` command to make an exception and allow your manager write permission to `myfile` also. Users other than yourself and your manager will still be denied write permission as previously specified by the `chmod` command.
- Use `chmod` with the `-A` option when working with files that have additional permissions assigned with the `chacl` command. The additional permissions will be deleted if you fail to use the `-A` option with `chmod`.

For additional ACL information see *lsacl*(1), *chacl*(1), and *acl*(5) in the *HP-UX Reference* manual and Chapter 4, "Controlling User Access to Directories and Files", of *HP-UX System Security*, HP part number B1862-90009.

Controlling Run-Levels

A **run-level** is an HP-UX state of operation in which a specific set of processes (and their offspring) are permitted to run. This set of processes is defined for each run-level in a file called `/etc/inittab`.

Run-level 2 is the normal operating mode (often called **multi-user mode**). Users must log in to the system in order to gain access. Special processes called **getty**s run in this mode and post the "login" prompt on your system's terminals. When users log in to your system, the gettys initiate other processes (usually HP-UX shells) which in turn allow still other processes to be executed as users enter commands.

4

A special run-level called run-level "s" is also defined. Run-level "s" is a special system administration mode, called **single-user mode**. It is used for performing special tasks where it is desirable to have no one else on the system.

Run levels `s` and 2 are predefined. You can create new run-levels or change which processes can run at these predefined run-levels, if your needs require. You can define up to six run-levels (1-6). Most systems do not need to define additional run-levels, and modifications to the predefined run-level 2 are usually done to allow `getty` processes to run on terminals being added to a system.

To create a new run-level, make (or change) entries in the `/etc/inittab` file that define how you want the system to operate when the system is in that run-level. For information on the `/etc/inittab` file, refer to *inittab*(4) in the *HP-UX Reference* manual.

Note When you use SAM to add terminals to your system, SAM makes the entries in the file `/etc/inittab` for you.

Only the superuser can use the `init` command, which changes the system from one run level to another, but anyone having write permission to the file `/etc/inittab` can create new run-levels or redefine existing run-levels.

To protect your system from tampering, ensure that the permissions (and ownership) for the files `/etc/init` and `/etc/inittab` are:

```
-r-xr-xr-x   root   other          /etc/init
-r--r--r--   root   root           /etc/inittab
```

Note If your computer is a member of an HP-UX cluster, the file `/etc/inittab` is a context dependent file (CDF). This means that each computer in the cluster has its own (custom) version of the `inittab` file.

4

See the "Creating a New Run-Level Using HP-UX Commands", "Changing System Run-Levels Using HP-UX Commands", "Entering the System Administration Run-Level", and "Returning From the System Administration Run-Level" sections of this chapter for specific instructions. For additional information refer to Chapter 6, "Run-Levels", in *How HP-UX Works: Concepts for the System Administrator*, HP part number B2355-90029.

Managing User Accounts and Groups Tasks

There are two ways to perform user account and user group tasks on your system:

- Using the System Administration Manager (SAM)
- Using HP-UX Commands (editing a series of files and creating user directories)

Generally you should use the SAM method because it is simpler and faster than performing the task with commands. For information about running SAM and navigating within SAM, refer to Chapter 1, "Introduction to System Administration".

SAM allows you to control access to your system through its menu-selection and data-entry screens. By combining multiple "manual commands" into single tasks, SAM can save you time and keystrokes. SAM also eliminates the need to know command names and options.

Although HP-UX commands require you to learn more details than SAM does, you might need or prefer to use HP-UX commands, for the following reasons:

- HP-UX commands give you a greater degree of control.
- SAM might not be configured into your system. You *have* to use HP-UX commands.
- You might be more comfortable using HP-UX commands.

The following are tasks covered in this section:

- Adding a User
- Removing a User
- Customizing the SAM "Adding and Removing a User" Capabilities
- Deactivating a User's Account
- Reactivating a User's Account
- Displaying/Modifying a User's Account Information
- Adding a Group
- Removing a Group
- Changing a User's Primary Group
- Adding Users to Groups
- Removing Users From Groups
- Displaying/Assigning Special Group Privileges

Each task has an ordered list of instructions, an area for additional information if necessary, and specific examples. In some of the HP-UX commands method examples the `xargs` command is used with the `find` command. Output from `find` is piped to `xargs` instead of using the `-exec` *primary* option to the `find` command. This is because when a large number of files or directories are to be processed by a single command, the `-exec` *primary* spawns a separate process for each file or directory, whereas `xargs` collects filenames or directory names into multiple arguments to a single `chgrp` or `chown` command, resulting in fewer processes and greater system efficiency. Specify the full pathname to the command following `xargs` to guarantee expected command behavior. Refer to *find*(1) and *xargs*(1) in the *HP-UX Reference* manual for additional information.

Adding a User Using SAM

To add a user to your system:

1. Ensure that you have superuser capabilities.
2. Run SAM; type:

   `/usr/bin/sam`

   See Chapter 1, "Introduction to System Administration" for additional information about using SAM.

3. Highlight `Users and Groups->` and activate the (Open) control button.
4. Highlight `Users` and activate the (Open) control button.
5. Choose `Add ...` from the "Actions" menu.
6. Fill in the "Add a User Account" window fields and activate the (Apply) control button.
7. After reading the messages, activate the (OK) control button.

To return to the functional area list or functional subarea, choose `Exit` from the "List" menu.

Additional Task Information

SAM provides an on-line help system to assist you when you need additional information.

Activating the (Help) button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

From within a functional area, choosing an item from the "Help" menu gives you information about:

- the current functional area
- keyboard navigation within SAM
- using the SAM help system
- displaying the version of SAM you are currently running

From a dialog box (a window displaying fields to be filled in), pressing the (f1) key gives you context-sensitive information for the object at the location of the cursor.

Refer to "Customizing the SAM 'Adding and Removing a User' Capabilities" in this chapter for specific SAM customization instructions.

Note

Even though the user should be unique, there are a few circumstances where it is useful to have several `/etc/passwd` entries with the same user_ID number. For example, consider the following three `/etc/passwd` entries:

```
root:9WsbljlTvWbbw:0:3:Root User Account:/:/bin/sh
croot:NPt3HW.jBpVz2:0:3:Root User Account (C-Shell):/:/bin/csh
kroot:dGJbw/DBeDLdo:0:3:Root User Account (K-Shell):/:/bin/ksh
```

On the system with these entries in the `passwd` file, there are three separate accounts (`root`, `croot`, `kroot`) which have superuser capability. Depending on which one is used, the superuser will start up in either the Bourne Shell, the C Shell or the Korn shell.

4

Because all three accounts have the user_ID "0", the system views all three as the same user. When the system checks to see which user "owns" a file, it compares the "user_ID" associated with the file against the user_ID entries in the `/etc/passwd` file. When it does so, it scans the `/etc/passwd` file from beginning until it finds a user_ID match. This is why files created by the users `croot` and `kroot` (in the above example) will be listed (in the output of the `ll` command) as being owned by the user `root`.

Removing a User Using SAM

To remove a user from your system using SAM:

1. Ensure that you have superuser capabilities.
2. Run SAM; type:

   `/usr/bin/sam`

   See Chapter 1, "Introduction to System Administration" for additional information about using SAM.
3. Highlight `Users and Groups->` and activate the (Open) control button.
4. Highlight `Users` and activate the (Open) control button.
5. Choose `Remove ...` from the "Actions" menu.
6. Turn on the check box associated with the action regarding the user's files and activate the (OK) control button.
7. After reading the messages, activate the (OK) control button.

To return to the functional area list or functional subarea, choose `Exit` from the "List" menu.

Additional Task Information

SAM provides an on-line help system to assist you when you need additional information.

Activating the (Help) button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

From within a functional area, choosing an item from the "Help" menu gives you information about:

- the current functional area
- keyboard navigation within SAM
- using the SAM help system
- displaying the version of SAM you are currently running

From a dialog box (a window displaying fields to be filled in), pressing the (f1) key gives you context-sensitive information for the object at the location of the cursor.

Note

- SAM views a user as a specific *user_ID* (as opposed to a specific login name) and will not remove any user with the same *user_ID* as the superuser (*user_ID* 0). You should never remove the user called "root" from your system. If you have other superusers (users with the *user_ID* of zero) on your system you can remove them by simply removing their entry from the `/etc/passwd` file.
- If SAM detects that another user has the same UID (user_ID), SAM does not remove the user's files.
- SAM will *not* remove system directories, even if they are owned by a given user. And, SAM will *not* remove files across NFS mounts.
- SAM updates the `/etc/passwd` and `/etc/group` files, but does not update the `/etc/logingroup` file. If you use `/etc/logingroup`, edit the file to remove the user from all group entries.

Refer to "Customizing the SAM 'Adding and Removing a User' Capabilities" in this chapter for specific SAM customization instructions.

Customizing the SAM "Adding and Removing a User" Capabilities

To customize the procedure for adding and/or removing a user:

1. Ensure that you have superuser capabilities.
2. Run SAM; type:

   /usr/bin/sam

   See Chapter 1, "Introduction to System Administration" for additional information about using SAM.
3. Highlight `Users and Groups->` and activate the (Open) control button.
4. Highlight `Users` and activate the (Open) control button.
5. Choose `Task Customization ...` from the "Actions" menu.
6. Fill in the script file name to be executed in one or a combination of the before/after adding/removing a user fields.
7. Activate the (OK) control button.
8. After reading the messages, activate the (OK) control button.

Additional Task Information

SAM provides an on-line help system to assist you when you need additional information.

Activating the Help button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

From within a functional area, choosing an item from the "Help" menu gives you information about:

4

- the current functional area
- keyboard navigation within SAM
- using the SAM help system
- displaying the version of SAM you are currently running

From a dialog box (a window displaying fields to be filled in), pressing the f1 key gives you context-sensitive information for the object at the location of the cursor.

There are often additional steps (specific to your operations) that you may want to perform whenever you add or remove a user to your system. SAM allows you to set up shell scripts or executable programs which it will run for you before adding or removing the user, after adding or removing the user, or both before *and* after adding or removing the user.

There are strict permission and ownership requirements that must be followed for your custom script/program:

1. The file must be owned by root (group ownership not checked).

   Acceptable:

   ```
   -r-xr--r--   1 root    bin        994 May  3 07:44 ct_addnode.ex
   -r-xr--r--   1 root    other      994 May  3 07:44 ct_addnode.ex
   ```

   Unacceptable (areas that are highlighted):

   ```
   -r-xr--r--   1 bin     bin        994 May  3 07:44 ct_addnode.ex
   -r-xr--r--   1 joe     bin        994 May  3 07:44 ct_addnode.ex
   ```

2. The file must be writable and executable only by root (note that the file does not have to be writable, but if it is, it can only be writable by root).

   Acceptable:

```
-rwxr--r--   1 root     bin           994 May  3 07:44 ct_addnode.ex
-r-xr--r--   1 root     bin           994 May  3 07:44 ct_addnode.ex
-rwxr-----   1 root     bin           994 May  3 07:44 ct_addnode.ex
-r-x---r--   1 root     bin           994 May  3 07:44 ct_addnode.ex
-r-x------   1 root     bin           994 May  3 07:44 ct_addnode.ex
```

   Unacceptable (areas that are highlighted):

```
-rwxrw-rw-   1 root     bin           994 May  3 07:44 ct_addnode.ex
-rwxrw-r--   1 root     bin           994 May  3 07:44 ct_addnode.ex
-r-xr-xr-x   1 root     bin           994 May  3 07:44 ct_addnode.ex
-rwxr-xr--   1 root     bin           994 May  3 07:44 ct_addnode.ex
```

3. The file must reside in a directory path where all directories (that is, each directory in the directory path) are writable only by owner.

Suppose the custom command lies in directory `/usr/local/bin`. To successfully pass the validation, the permissions on `/usr`, `/usr/local`, and `/usr/local/bin` must all be "drwxr-xr-x". The permissions cannot be "drwxrwxr-x" or "drwxrwxrwx" (must be writable only by owner). This is typically a problem because `/usr/local` and `/usr/local/bin` are installed with permissions "drwxrwxrwx".

This means that the system administrators must take care in locating a directory (path) that meets the above requirements (`/usr`, `/usr/bin`, `/usr/sam`, `/usr/sam/bin`, `/usr/sam/config` are just a few examples of directories that at least meet the criteria when installed), or make one of their own that meets the requirements.

These restrictions are only applied at the time of SAM field validation of the command. Once SAM has registered a custom command to be used, the restrictions above are no longer checked by SAM for that command unless the user alters the custom script/program with SAM.

Deactivating a User's Account Using SAM

To deactivate a user's account:

1. Ensure that you have superuser capabilities.
2. Run SAM; type:

   `/usr/bin/sam`

   See Chapter 1, "Introduction to System Administration" for additional information about using SAM.
3. Highlight `Users and Groups->` and activate the (Open) control button.
4. Highlight `Users` and activate the (Open) control button.
5. Highlight the user entry in the object list you wish to deactivate.
6. Choose `Deactivate...` from the "Actions" menu.
7. Turn on the check box for the action regarding the user's files and activate the (OK) control button.
8. After reading the messages, activate the (OK) control button.

To return to the functional area list or functional subarea, choose `Exit` from the "List" menu.

Additional Task Information

SAM provides an on-line help system to assist you when you need additional information.

Activating the (Help) button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

From within a functional area, choosing an item from the "Help" menu gives you information about:

- the current functional area
- keyboard navigation within SAM
- using the SAM help system
- displaying the version of SAM you are currently running

From a dialog box (a window displaying fields to be filled in), pressing the (f1) key gives you context-sensitive information for the object at the location of the cursor.

Sometimes it is useful to temporarily suspend a user's ability to log into your system (such as when the user will be away for an extended period of time). The user's files remain on the system and intact, ready for the user when they return and you reactivate their account.

Deactivating a user's account means to make it so that *no login password is valid*.

Reactivating a User's Account Using SAM

To reactivate a user's account:

1. Ensure that you have superuser capabilities.
2. Run SAM; type:

   `/usr/bin/sam`

   See Chapter 1, "Introduction to System Administration" for additional information about using SAM.

4

3. Highlight `Users and Groups->` and activate the (Open) control button.
4. Highlight `Users` and activate the (Open) control button.
5. Highlight the user entry in the object list you wish to reactivate.
6. Choose `Reactivate...` from the "Actions" menu.
7. Optionally fill in a password for the user and activate the (OK) control button.
8. After reading the messages, activate the (OK) control button.

To return to the functional area list or functional subarea, choose `Exit` from the "List" menu.

Additional Task Information

SAM provides an on-line help system to assist you when you need additional information.

Activating the (Help) button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

From within a functional area, choosing an item from the "Help" menu gives you information about:

- the current functional area
- keyboard navigation within SAM
- using the SAM help system
- displaying the version of SAM you are currently running

From a dialog box (a window displaying fields to be filled in), pressing the (f1) key gives you context-sensitive information for the object at the location of the cursor.

Displaying/Modifying a User's Account Information Using SAM

To display or modify a user's account information:

1. Ensure that you have superuser capabilities.
2. Run SAM; type:

   `/usr/bin/sam`

   See Chapter 1, "Introduction to System Administration" for additional information about using SAM.
3. Highlight `Users and Groups->` and activate the (Open) control button.
4. Highlight `Users` and activate the (Open) control button.
5. Highlight the user in the object list.
6. Choose `Modify...` from the "Actions" menu.
7. To view the user's information, activate the (Cancel) control button after gathering the information you need.

   To modify the user's information, fill in the new information in the "Modify a User" window and activate the (OK) control button. After reading the messages, activate the (OK) control button. The following user information can be modified:

   a. login name (*user_name*)
   b. password
   c. user identification number (*user_ID*)
   d. primary group identification number (*group_ID*)
   e. comment
   f. login directory
   g. start up program

To return to the functional area list or functional subarea, choose `Exit` from the "List" menu.

Additional Task Information

SAM provides an on-line help system to assist you when you need additional information.

Activating the (Help) button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

From within a functional area, choosing an item from the "Help" menu gives you information about:

- the current functional area
- keyboard navigation within SAM
- using the SAM help system
- displaying the version of SAM you are currently running

From a dialog box (a window displaying fields to be filled in), pressing the (f1) key gives you context-sensitive information for the object at the location of the cursor.

Adding a Group Using SAM

1. Ensure that you have superuser capabilities.
2. Run SAM; type:

   `/usr/bin/sam`

   See Chapter 1, "Introduction to System Administration" for additional information about using SAM.
3. Highlight `Users and Groups->` and activate the (Open) control button.
4. Highlight `Groups` and activate the (Open) control button.
5. Choose `Add...` from the "Actions" menu.
6. Fill in the new group name and optionally highlight the users to be members of the newly created group.
7. Activate the (OK) control button if this is the only group you are adding. Otherwise, activate the (Apply) and subsequent (OK) control buttons to return to the "Add a Group" window.

To return to the functional area list or functional subarea, choose `Exit` from the "List" menu.

Additional Task Information

SAM provides an on-line help system to assist you when you need additional information.

Activating the (Help) button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

From within a functional area, choosing an item from the "Help" menu gives you information about:

- the current functional area
- keyboard navigation within SAM
- using the SAM help system
- displaying the version of SAM you are currently running

From a dialog box (a window displaying fields to be filled in), pressing the (f1) key gives you context-sensitive information for the object at the location of the cursor.

Removing a Group Using SAM

To remove a group:

1. Ensure that you have superuser capabilities.
2. Run SAM; type:

   `/usr/bin/sam`

   See Chapter 1, "Introduction to System Administration" for additional information about using SAM.
3. Highlight `Users and Groups->` and activate the (Open) control button.
4. Highlight `Groups` and activate the (Open) control button.
5. Choose `Remove ...` from the "Actions" menu.

   You can assign the group's files or another group if desired. Otherwise, SAM will reassign the group's files to the primary group of each of the file's owner.
6. After reading the messages, activate the (OK) control button.

To return to the functional area list or functional subarea, choose `Exit` from the "List" menu.

Additional Task Information

If the group SAM is removing is a user's primary group, SAM displays an error message and does not remove the group.

SAM provides an on-line help system to assist you when you need additional information.

Activating the (Help) button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

From within a functional area, choosing an item from the "Help" menu gives you information about:

- the current functional area
- keyboard navigation within SAM
- using the SAM help system
- displaying the version of SAM you are currently running

From a dialog box (a window displaying fields to be filled in), pressing the (f1) key gives you context-sensitive information for the object at the location of the cursor.

Refer to "Customizing the SAM 'Adding and Removing a User' Capabilities" in this chapter for specific SAM customization instructions.

Adding and Removing Users From Groups Using SAM

To modify a group's membership list:

1. Ensure that you have superuser capabilities.
2. Run SAM; type:

   ```
   /usr/bin/sam
   ```

   See Chapter 1, "Introduction to System Administration" for additional information about using SAM.
3. Highlight `Users and Groups->` and activate the (Open) control button. 4
4. Highlight `Groups` and activate the (Open) control button.
5. Choose `Modify...` from the "Actions" menu.
6. Follow the instructions displayed in the "Modify a Group" window and to add and remove members to and from a group.
7. Activate the (OK) control button.

To return to the functional area list or functional subarea, choose `Exit` from the "List" menu.

Additional Task Information

SAM provides an on-line help system to assist you when you need additional information.

Activating the (Help) button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

From within a functional area, choosing an item from the "Help" menu gives you information about:

- the current functional area
- keyboard navigation within SAM
- using the SAM help system
- displaying the version of SAM you are currently running

From a dialog box (a window displaying fields to be filled in), pressing the (f1) key gives you context-sensitive information for the object at the location of the cursor.

Adding a User Using HP-UX Commands

Generally you should use the SAM method because it is simpler and faster than performing the task with commands. For information about running SAM and navigating within SAM, refer to Chapter 1, "Introduction to System Administration".

To add a user to your system using HP-UX commands:

1. Ensure that you have superuser capabilities.
2. Make a copy of the `/etc/passwd` file so that it is easy to undo any mistakes that you might make:

   ```
   cp /etc/passwd /etc/passwd.old
   ```

   If you need to undo a mistake later, you can restore the "old" contents of the file using the command:

   ```
   cp /etc/passwd.old /etc/passwd
   ```

3. Create an entry in the file `/etc/passwd` for the new user using the text editor of your choice. HP recommends that you use the `vipw` command to ensure that you have exclusive access to the `/etc/passwd` file. The `/etc/vipw` command requires the `EDITOR` environment variable set to `vi`. Each user attribute must be colon-separated with no leading or trailing spaces. The one line entry must be in the form:

   user_name:*password*: *UID*: *GID*: *comment*: *login_directory*: *start_up_program*

   where:

   user-name — This is the user's login name (the one that they will enter at the `login:` prompt). The login name must have the following characteristics:

   - It must begin with an alphabetic character.
   - It can include up to eight alphanumeric characters.
   - It cannot contain blank spaces.
   - It cannot already exist on the system.

password

To ensure the user sets a password when they log in for the first time, place the characters ",.." in this field. For example:

```
bhewlett:,..:567:40:Bill Hewlett:/users/bhewlett:/bin/csh
```

Note

Putting an unencrypted password in the *password* field will *not* work. For example, if you want to assign a user the password "secret", the following entry will *not* allow the user to log in using the password "secret":

```
bhewlett:secret:567:40:Bill Hewlett:/users/bhewlett:/bin/csh
```

To set the password, use the `/bin/passwd` command.

To leave the new user's account without a password, do not put any characters between the colon (":") separators. For example:

```
dpackard::123:40:David Packard:/users/dpackard:/bin/csh
```

Caution

Leaving an account unprotected (without a password), even for a short period of time, is a security risk. If you entered ",.." in the *password* field, have the user log in as soon as possible to set a password for the account.

The `passwd` command is used to set or change the user's password.

UID

The *UID* (*user_ID*) is a *unique* integer value that the system uses to identify the user. If the *user_ID* is 0 (zero), then that user has superuser capabilities. When the system was shipped to you, the *user_ID* "0" was associated with the user `root`. By convention, the values 1 through 99 are reserved for system use. Therefore, when you are adding a new user to your system, pick for them any unused number greater than 99 (but less than 60000) for this field. *user_IDs* greater than 59999 are invalid.

GID — This value is the user's primary group *GID* (*group_ID*) as defined in the third field of the user's primary group entry in the `/etc/group` file. The *group_ID* is an integer value shared by all members of the same group. Refer to the "Adding a Group Using HP-UX Commands" section of this chapter for a description of the `/etc/group` and `/etc/logingroup` file formats.

comment — The *comment* field is used to log information about the identity of the user (or to identify this entry). Although this field is "free-format", using the following comma-separated subfield format is recommended:

User's Full Name, Office Location, Office Phone, Home Phone

login_directory — This is the absolute pathname to the directory that the user will be placed in when they first log in to the system. The directory need not exist when the entry to `/etc/passwd` is made. However, the directory *must* exist before the user can log in. This field can be no longer than 63 characters.

start_up_program — This field contains the name of a single command to be executed for the user when they log in; it should be an absolute pathname (for the command). This field can be no longer than 44 characters. Typically this is the name of a shell (`/bin/sh`, `/bin/csh`, `/bin/ksh`, etc.). However, the name can be that of any executable program or command. The command can be either a compiled program or a shell script, but no arguments to the command or script should be supplied. If the command field is left blank, `/bin/sh` is executed by default.

When the user logs in, the command listed in this field is executed and control is passed to that program. Once the program terminates, the user is logged out.

4. Create a login ("home") directory for the user with the **mkdir** command:

   /bin/mkdir [-p] [-m *mode*] *directory*

   where:

-p	specifies intermediate directories are created as necessary. Otherwise, the full path prefix of *directory* must already exist. The **mkdir** command requires write permission in the parent directory.
-m *mode*	specifies creating the directory as specified by *directory* with the file permissions are set to *mode*, which is a symbolic mode string.
directory	specifies the user login directory.

   The **login directory** is the directory that the users are *first* placed in when they log in to the system.

   The login directory that is defined for a user in the **/etc/passwd** file *must* exist when the user logs into the system or the login attempt will fail.

   It is not necessary for each user to have a separate login directory, but this is how systems are usually set up. It is easier to keep the files of the various users separated if each has their own login directory. This, in turn, makes it easier to work with a given user's files (for example when doing backups, determining how much disk space a given user is using, etc.).

5. Use the pwck command to verify that the **/etc/passwd** file has valid entries:

   /etc/pwck

   The pwck command validates the number of fields, login name, user ID, group ID, and whether the login directory and optional program name exist. Refer to *pwck*(1M) in the *HP-UX Reference* manual for additional information.

6. Create login (shell initialization) files for the user.

   In most cases, the *start_up_program* for a user will be one of the HP-UX shells (`/bin/sh`, `/bin/csh`, `/bin/ksh`, `/bin/rsh`, etc.). Each of these shells has a set of initialization files that they read when they begin executing as a user is logging in to the system. Table 4-1 lists the initialization file executed for each shell in the order they are executed.

Table 4-1. HP-UX Global and Local Shell Initialization Files

Shell	Initialization Files Executed at Login
/bin/sh	`/etc/profile` `$HOME/.profile`

/bin/csh	`/etc/csh.login`
	`$HOME/.cshrc`
	`$HOME/.login`

/bin/ksh	`/etc/profile` `$HOME/.profile`
/bin/keysh	`/etc/profile` `$HOME/.profile`
/bin/rsh	`/etc/profile` `$HOME/.profile`
/bin/rksh	`/etc/profile` `$HOME/.profile`

The `/etc/profile` and `/etc/csh.login` files contain global instructions/commands that you want executed for *every* user who logs into the system. These files are in the `/etc` directory so that they are accessible to all users. You should *not* copy them to each user's directory. The local initialization files are located in the user's login directory ($HOME). These local files typically contain shell commands and environment variable definitions that customize the user's environment and/or automatically run one or more programs for the user.

If the local initialization files exist in a user's directory, the shell attempts to execute the commands in the local files after completing the global files, but before the user receives the first shell prompt.

Examples of the local initialization files are located in the `/etc` directory. Their names begin with the characters "`d.`" (for example `d.profile`). You may copy these files to a user's login directory and customize them. When you copy these file to the user's login directory, rename the files without the `d` prefix.

7. Create or customize other initialization files for the user.

   Other programs such as the editor, `vi` and the various mail programs (`mail`, `elm`, `mailx`) have initialization files which you may also want to set up for the user.

   You may need to change the access permissions of particular files within the user's login directory. Refer to *Using HP-UX*. For additional information on file protection refer to Chapter 8, "HFS File System", in *How HP-UX Works: Concepts for the System Administrator*, HP part number B2355-90029. See also *ll*(1), *chmod*(1), *chown*(1), *chgrp*(1), and *umask*(1) in the *HP-UX Reference* manual.

8. Change the *file ownership* and *group ownership* of the new user's home directory and the files to the user's login name and primary group with the `chown` and `chgrp` commands respectively. You must change the ownership and group ownership of these new files to those of your new user so that *the new user* can access them.

   Change the *file ownership* of a file or directory with the `chown` command:

   `/bin/chown` [`-R`] *new_owner login_dir*

   where:

`-R`	specifies to recursively change the file ownership to *new_owner*. For each *login_dir*, the owner of the directory and all files and subdirectories in the file hierarchy below it are changed to *new_owner*.
new_owner	specifies the login name of the new user.
login_dir	specifies the login directory of the new user.

   Change the *group ownership* of a file or directory with the `chgrp` command:

   `/bin/chgrp` [`-R`] *new_group login_dir*

   where:

`-R`	specifies to recursively change the group ownership to *new_group*. For each *login_dir*, the group of the directory and all files and subdirectories in the file hierarchy below it are changed to *new_group*.
new_group	specifies the primary group of the new user.
login_dir	specifies the login directory of the new user.

9. Edit the `/etc/group` file, and optionally, the `/etc/logingroup` file to add the user's *user_name* to the names in the comma-separated list of members for the group(s). If you want the user to be able to access files belonging to another group other than their primary group without using the `chgrp` command, edit the `/etc/logingroup` file to add the user to all necessary groups.

Note

- A blank line in the `/etc/group` or `/etc/logingroup` file is not allowed. If a blank line appears in the files, all entries after the blank line are ignored. See "Adding Users to Groups Using HP-UX Commands" for specific instructions on editing the `/etc/group` and `/etc/logingroup` files.
- A group can have a maximum limit of 200 users.

4

10. Use the `grpck` command to check for inconsistencies and verify all entries in the `/etc/group` and `/etc/logingroup` files. This verification includes a check of the number of fields, group name, group ID, and whether all login names appear in the password file. The `grpck` command has the following format:

    `/etc/grpck` [*group_file*]

    where:

    group_file is the name of the group file to be checked. The default group file is `/etc/group`.

11. Have the new user log into the system so that you can verify that you have set up their environment correctly.

Additional Task Information

Refer to "Controlling User Accounts and Groups" for more information about the `vipw` command.

If the *comment* field information in the `/etc/passwd` file is entered in a comma-separated sub-field format, you can use the `/usr/bin/finger` command to display this information. If you need to modify the user's *comment* field information, you can modify the `/etc/passwd` file directly with the `vipw` command or you can use the `/usr/bin/chfn` command. The information in the *comment* field is referred to as "gecos" information. Refer to the "Displaying/Modifying User's Account Information Using HP-UX Commands" section of this chapter and/or *finger*(1) and *chfn*(1) in the *HP-UX Reference* manual for additional information.

Note

Even though the user should be unique, there are a few circumstances where it is useful to have several `/etc/passwd` entries with the same user_ID number. For example, consider the following three `/etc/passwd` entries:

```
root:9Wsbljl1TvWbbw:0:3:Root User Account:/:/bin/sh
croot:NPt3HW.jBpVz2:0:3:Root User Account (C-Shell):/:/bin/csh
kroot:dGJbw/DBeDLdo:0:3:Root User Account (K-Shell):/:/bin/ksh
```

On the system with these entries in the `passwd` file, there are three separate accounts (`root`, `croot`, `kroot`) which have superuser capability. Depending on which one is used, the superuser will start up in either the Bourne Shell, the C Shell or the Korn shell.

Because all three accounts have the user_ID "0", the system views all three as the same user. When the system checks to see which user "owns" a file, it compares the "user_ID" associated with the file against the user_ID entries in the `/etc/passwd` file. When it does so, it scans the `/etc/passwd` file from beginning until it finds a user_ID match. Files created by the users `croot` and `kroot` (in the above example) will be listed (in the output of the `ll` command) as being owned by the user `root` because `root` is the first of the three entries.

If you have several users sharing a login directory, the ownerships and permissions of the shell local initialization files may need to be adjusted so that all users sharing that login directory have read access to the local initialization files. There are several ways to do this. One way is to assign one of the users sharing the login directory to be the "owner" of the files, have all of the users sharing the directory be members of the same group, and give the group members read access to the files. For information about setting file permissions and ownership, see *Using HP-UX*. For additional information on file protection refer to Chapter 8, "HFS File System", in *How HP-UX Works: Concepts for the System Administrator*, HP part number B2355-90029. See also *ll*(1), *chmod*(1), *chown*(1), *chgrp*(1), *setprivgrp*(1M), and *umask*(1) in the *HP-UX Reference* manual.

Another way is to create ACLs (Access Control Lists) for the startup files. ACLs allow access control at the user level versus the group level. For additional ACL information see *lsacl*(1), *chacl*(1), and *acl*(5) in the *HP-UX Reference* manual and Chapter 4, "Controlling User Access to Directories and Files", of *HP-UX System Security*, HP part number B1862-90009.

Examples

To add new user accounts for *john*, *patrickd*, and *naomil* to the system:

1. Login as `root`.
2. Make a backup copy of the `/etc/passwd` file.

   ```
   cp /etc/passwd /etc/passwd.old
   ```

3. Update the `/etc/passwd` file to include the users' entries. HP recommends using the `/etc/vipw` command. The `/etc/vipw` command requires the `EDITOR` environment variable set to `vi`.

   To set the Korn and Bourne shell `EDITOR` environment variable, type:

   ```
   export EDITOR=vi
   ```

   To set the C shell `EDITOR` environment variable, type:

   ```
   setenv EDITOR vi
   ```

   Add the following entries to the `/etc/passwd` file:

   ```
   john:,..:342:20:John Smith, 125 Elm Street, 555-2324:/users/john:/bin/ksh
   naomil:,..:1667:20:Naomi Adams,540 Market Ave, 555-9078:/users/naomil:/bin/ksh
   patrickd:,..:24:Patrick Daly,421 Orange Road, 555-6140:/users/patrickd:/bin/ksh
   ```

   Note the primary group for *john* and *naomil* is `users` while the primary group for *patrickd* is `pub`.

4. Create a login directory for each of the new users:

   ```
   mkdir -p /users/john
   mkdir -p /users/patrickd
   mkdir -p /users/naomil
   ```

5. Check the `/etc/passwd` file format:

   ```
   pwck
   ```

6. Copy local initialization files to each user's login directory:

   ```
   cp /etc/d.profile /users/john/.profile
   cp /etc/d.profile /users/patrickd/.profile
   cp /etc/d.profile /users/naomil/.profile
   ```

7. Create or customize initialization files for the users.

8. Change the ownership and permissions of all of the files and subdirectories created in the login directories for *john*, *patrickd*, and *naomil* using the `chown` and `chgrp` commands with the `-R` option:

```
chown -R john /users/john
chown -R patrickd /users/patrickd
chown -R naomil /users/naomil
chgrp -R users /users/john
chgrp -R pub /users/patrickd
chgrp -R users /users/naomil
```

Check that ownership and permissions are correct in the new login directories use the `ll` command:

```
ll /users
drwxr-xr-x  17 john      users       2048 Feb  6 11:18 john
drwxr-xr-x   7 naomil    users       3072 Feb  5 15:57 naomil
drwxr-xr-x   9 patrickd users        5152 Feb  5 18:07 patrick
```

If you need to globally change the default owner, group, or other permissions on the files and subdirectories created for the new users, use the `chmod` command with the `-R` option. For example:

```
chmod -R u=rwx,g=x,o= /users/john/
```

or

```
chmod -R 710 /users/john/
```

For additional information about the `chown`, `chgrp`, and `chmod` commands, refer to *Using HP-UX*. See also *chown*(1), *chgrp*(1), and *chmod*(1) in the *HP-UX Reference* manual.

4

9. Update the `/etc/group` file, and optionally, the `/etc/logingroup` file to add the three users' login names to each users' primary group member list. Additionally, add *naomil* to the `pub` group and *patrickd* to the `users` group. For example:

```
root:*:0:
other:*:1:
bin:*:2:
sys:*:3:
adm:*:4:
daemon:*:5:
mail:*:6:
lp:*:7:
users:*:20:john,naomil,patrickd,kerschen,michelem,dennism,pvallis
pub:*:24:patrickd,naomil,dennism
```

   Note that a blank line in the `/etc/group` file is not allowed. If a blank line appears in the `/etc/group` file, all entries after the blank line are ignored.

   Users *patrickd* and *naomil* may access files belonging to both groups without changing their current group if the `/etc/logingroup` file has entries for both users in both groups. Otherwise, the `chgrp` command will be necessary for *naomil* and *patrickd* to access files belonging to another group.

10. Check the `/etc/group` file format:

    <u>/etc/grpck</u>

11. Instruct users *patrickd*, *naomil*, and *john* to log in.

Removing a User Using HP-UX Commands

Generally you should use the SAM method because it is simpler and faster than performing the task with commands. For information about running SAM and navigating within SAM, refer to Chapter 1, "Introduction to System Administration".

To remove a user from your system using HP-UX commands:

1. Ensure that you have superuser capabilities.
2. Decide the future of the user's files and directories. Your choices are: 4
   a. Remove the user's files and directories from the system
   b. Assign the user's files and directories to another user
   c. A combination of the above.

   Use the `find` command to get a list of the files on your system which are owned by the user you are removing:

   `/bin/find / -fsonly hfs -user` *user_name* `-print`

   where:

   user_name is the user's login name as defined in the user's `/etc/passwd` file entry.

Note In an HP-UX cluster, include the `-hidden` option to the `find` command to search context-dependent files (CDFs).

Files, especially those representing executable programs, can be shared among users in a group or among all of the users of the system. If you decide to remove the user's files, be sure that they will not be needed by other users of your system. Refer to *find*(1) in the *HP-UX Reference* manual for additional information.

3. Find and remove all ACL (Access Control List) entries for the user. To find and remove all of the ACL entries for the user `naomil` in the `users` group type:

   ```
   /bin/find / -fsonly hfs -acl naomil.users -depth -print | xargs chacl -d naomil.users
   ```

   For additional ACL information see *lsacl*(1), *chacl*(1), and *acl*(5) in the *HP-UX Reference* manual and Chapter 4, "Controlling User Access to Directories and Files", of *HP-UX System Security*, HP part number B1862-90009.

4. Search for and remove the user's login name from all entries in the `/etc/group` file. Optionally remove the user's login name from all entries in the `/etc/logingroup` file if it exists.

   Use the command `grep` (or the search command in your text editor) to find the entries in `/etc/group` that contain the *user_name* (login name) belonging to the user you are removing.

   Using a text editor, delete the *user_name* from those entries.

5. Use the `grpck` command to check for inconsistencies and verify all entries in the `/etc/group` and `/etc/logingroup` files. This verification includes a check of the number of fields, group name, group ID, and whether all login names appear in the password file. The `grpck` command has the following format:

   `/etc/grpck` [*group_file*]

   where:

group_file	is the name of the group file to be checked. The default group file is `/etc/group`.

6. Make a copy of the `/etc/passwd` file so that it is easy to undo any mistakes that you might make:

   ```
   cp /etc/passwd /etc/passwd.old
   ```

   If you need to undo a mistake later, you can restore the "old" contents of the file using the command:

   ```
   cp /etc/passwd.old /etc/passwd
   ```

7. Remove the user's entry in the `/etc/passwd` file using the `vipw` command.

8. Use the `pwck` command to verify that the `/etc/passwd` file has valid entries:

   ```
   /etc/pwck
   ```

   The `pwck` command validates the number of fields, login name, user ID, group ID, and whether the login directory and optional program name exist. Refer to *pwck*(1M) in the *HP-UX Reference* manual for additional information.

4

Additional Task Information

Note You should never remove the user called "root" from your system.

Refer to "Controlling User Accounts and Groups" for more information about the `vipw` command.

Examples

To remove user `michelem` from the system:

1. Login as `root`.

2. Change file ownership of all files in the login directory for `michelem` to `rykl` and remove *all* of the files on the rest of the system owned by user `michelem`.

   To change file ownership of *all* files and directories in the `/users/michelem` login directory to `rykl`:

   ```
   /bin/find /users/michelem -fsonly hfs -user michelem -depth -print | xargs chown -R rykl
   ```

   To remove files owned by `michelem` from the system:

   ```
   /bin/find / -fsonly hfs -user michelem !-type d -depth -print | xargs rm
   ```

   To remove *all* of the empty directories owned by user `michelem`:

   ```
   /bin/find / -fsonly hfs -user michelem -depth -print | xargs rmdir
   ```

3. Remove `michelem` from any Access Control List entries (ACLs):

```
/bin/find / -fsonly hfs -acl michelem.users -depth -print | xargs chacl -d michelem.users
```

4. Locate and remove the login name for the user `michelem` from all entries in the `/etc/group` file:

```
grep michelem /etc/group
```

The output might look like this:

```
photo:*:23:dennisp,janetn,michelem,stevens
therapy:*:23:kimz,michelem,bsmith
database:*:23:michelem,lynnf,rykl
```

After removing `michelem` from the group member lists, the updated `/etc/group` file entries should look like this:

```
photo:*:23:dennisp,janetn,stevens
therapy:*:23:kimz,bsmith
database:*:23:lynnf,earlg
```

5. Check the `/etc/group` file format:

```
/etc/grpck
```

6. Make a backup copy of the `/etc/passwd` file.

```
cp /etc/passwd /etc/passwd.old
```

7. Update the `/etc/passwd` file to delete the line containing the information for user `michelem`. HP recommends using the `/etc/vipw` command. The `/etc/vipw` command requires the `EDITOR` environment variable set to `vi`.

To set the Korn and Bourne shell `EDITOR` environment variable, type:

```
export EDITOR=vi
```

To set the C shell `EDITOR` environment variable, type:

```
setenv EDITOR vi
```

8. Check the `/etc/passwd` file format:

```
pwck
```

Deactivating a User's Account Using HP-UX Commands

To deactivate a user's account:

1. Ensure that you have superuser capabilities.
2. Make a copy of the `/etc/passwd` file so that it is easy to undo any mistakes that you might make:

   ```
   cp /etc/passwd /etc/passwd.old
   ```

   If you need to undo a mistake later, you can restore the "old" contents of the file using the command:

   ```
   cp /etc/passwd.old /etc/passwd
   ```

3. Edit the `/etc/passwd` file using the `vipw` command:
   a. Locate the entry in the `/etc/passwd` file that corresponds to the user's account that you are planning to deactivate.
   b. Replace the encrypted password in the second field with an asterisk "*" (fields are separated by colons ":").
   c. Save the `/etc/passwd` file and exit the editor.
4. Use the `pwck` command to verify that the `/etc/passwd` file has valid entries:

   ```
   /etc/pwck
   ```

   The `pwck` command validates the number of fields, login name, user ID, group ID, and whether the login directory and optional program name exist. Refer to *pwck*(1M) in the *HP-UX Reference* manual for additional information.

4

Additional Task Information

Note You should never deactivate the user called "root".

Deactivating a user's account means to make it so that *no login password is valid*.

Sometimes it is useful to temporarily suspend a user's ability to log into your system (such as when the user will be away for an extended period of time). The user's files remain on the system and intact, ready for the user when they return and you reactivate their account.

Refer to "Controlling User Accounts and Groups" for more information about the `vipw` command.

Examples

To deactivate the user account for *paul*, edit the `/etc/passwd` file. HP recommends using the `/etc/vipw` command. The `/etc/vipw` command requires the `EDITOR` environment variable set to `vi`.

To set the Korn and Bourne shell `EDITOR` environment variable, type:

```
export EDITOR=vi
```

To set the C shell `EDITOR` environment variable, type:

```
setenv EDITOR vi
```

The `/etc/passwd` file entry before deactivating user *paul*:

```
paul:sIgNXHLuFptVE:209:20:Paul Avonette,Mailstop F13,555-7086,:/users/paul:/bin/ksh
```

The `/etc/passwd` file entry after deactivating user *paul*:

```
paul:*:209:20:Paul Avonette,Mailstop F13,555-7086,:/users/paul:/bin/ksh
```

Check the `/etc/passwd` file format:

```
pwck
```

Reactivating a User's Account Using HP-UX Commands

To reactivate a user's account:

1. Ensure that you have superuser capabilities.
2. Make a copy of the `/etc/passwd` file so that it is easy to undo any mistakes that you might make:

   ```
   cp /etc/passwd /etc/passwd.old
   ```

   If you need to undo a mistake later, you can restore the "old" contents of the file using the command:

   ```
   cp /etc/passwd.old /etc/passwd
   ```

3. Edit the `/etc/passwd` file using the `vipw` command:
   a. Locate the entry in the `/etc/passwd` file that corresponds to the user's account that you are planning to reactivate.
   b. Replace the asterisk "*" in the second field of the file with the string ",.." (comma-dot-dot) which forces the user to set a new password for their account the next time they log in.
   c. Save the `/etc/passwd` file and exit the editor.
4. Use the `pwck` command to verify that the `/etc/passwd` file has valid entries:

   ```
   /etc/pwck
   ```

   The `pwck` command validates the number of fields, login name, user ID, group ID, and whether the login directory and optional program name exist. Refer to *pwck*(1M) in the *HP-UX Reference* manual for additional information.

Additional Task Information

Refer to "Controlling User Accounts and Groups" for more information about the `vipw` command.

Examples

To reactivate the user account for *paul*, edit the `/etc/passwd` file. HP recommends using the `/etc/vipw` command. The `/etc/vipw` command requires the `EDITOR` environment variable set to `vi`.

4

To set the Korn and Bourne shell `EDITOR` environment variable, type:

```
export EDITOR=vi
```

To set the C shell `EDITOR` environment variable, type:

```
setenv EDITOR vi
```

The `/etc/passwd` file entry before reactivating user *paul*:

```
paul:*:209:20:Paul Avonette,Mailstop F13,555-7086,:/users/paul:/bin/ksh
```

The `/etc/passwd` file entry after reactivating user *paul*:

```
paul:,..:209:20:Paul Avonette,Mailstop F13,555-7086,:/users/paul:/bin/ksh
```

Check the `/etc/passwd` file format:

```
pwck
```

Displaying/Modifying User's Account Information Using HP-UX Commands

To display a user's account information:

- Use the `finger` command to display the user's `/etc/passwd` file information:

  `/usr/bin/finger` *user_name*

  where:

  user_name is the user's login name as defined in the user's `/etc/passwd` file entry.

  or

- Use the `grep` command to display the user's `/etc/passwd` file information:

  `/bin/grep` *user_name* `/etc/passwd`

  where:

  user_name is the user's login name as defined in the user's `/etc/passwd` file entry.

To modify a user's account information:

1. Ensure that you have superuser capabilities.
2. Make a copy of the `/etc/passwd` file so that it is easy to undo any mistakes that you might make:

   ```
   cp /etc/passwd /etc/passwd.old
   ```

   If you need to undo a mistake later, you can restore the "old" contents of the file using the command:

   ```
   cp /etc/passwd.old /etc/passwd
   ```

3. Edit the `/etc/passwd` file using the `vipw` or `chfn` commands to update the following user information:
   - login name (*user_name*)
   - password
   - user identification number (*user_ID*)
   - primary group identification number (*group_ID*)
   - comment
   - login directory
   - start up program

   For a description of these fields, refer to the "Adding a User Using HP-UX Commands" section of this chapter.

   The `chfn` command has the following syntax:

   `/usr/bin/chfn` [*user_name*]

   where:

   user_name is the user's login name as defined in the user's `/etc/passwd` file entry.

   You must have superuser capabilities to use the `chfn` command to update other users' account information, but you can change your own account information without superuser capabilities.

4. Use the `pwck` command to verify that the `/etc/passwd` file has valid entries:

   `/etc/pwck`

   The `pwck` command validates the number of fields, login name, user ID, group ID, and whether the login directory and optional program name exist. Refer to *pwck*(1M) in the *HP-UX Reference* manual for additional information.

Additional Task Information

If you do not have superuser capabilities and you attempt the use the `chfn` command to update another user's account information, the error message "You are not allowed to change another person's finger entry." is displayed.

Refer to "Controlling User Accounts and Groups" for more information about the `vipw` command.

Examples

4

To display account information for user `jdoe`:

```
finger jdoe

Login name:  jdoe                        In real life:  John Doe
Bldg: Building 5
Directory: /users/jdoe                   Shell: /bin/ksh
On since Feb 10 11:17:04 on pty/ttys5 from mountian.net.ca
2 minutes 25 seconds Idle Time
No Plan.

grep jdoe /etc/passwd
jdoe:QAJZL4Xjg/BMM:1667:20:John Doe,Building 5,555-1234:/users/jdoe:/bin/ksh
```

To update the telephone number for user `jdoe` with the `chfn` command:

```
chfn jdoe
Default values are printed inside of of '[]'.
To accept the default, type <return>.
To have a blank entry, type the word 'none'.

Name [John Doe]:
Location (Ex: 42U-J4) [Building 5]
Office Phone (Ex: 1632) [1234]: 2233
Home Phone (Ex: 5555678) []:
```

Run `pwck` to check your `/etc/passwd` file format.

Adding a Group Using HP-UX Commands

To add a new group to your system using HP-UX commands:

1. Ensure that you have superuser capabilities.
2. Make a copy of the `/etc/group` file, and optionally, the `/etc/logingroup` file so that it is easy to undo any mistakes that you might make:

   ```
   cp /etc/group /etc/group.old
   cp /etc/logingroup /etc/logingroup.old
   ```

4

   If you need to undo a mistake later, you can restore the "old" contents of the files using the commands:

   ```
   cp /etc/group.old /etc/group
   cp /etc/logingroup.old /etc/logingroup
   ```

3. Create an entry for the new group in the `/etc/group` file with the editor of your choice. Optionally create an entry in the `/etc/logingroup` file to allow access to files belonging to other groups without changing the users' effective group. The `/etc/group` and `/etc/logingroup` one-line entries must have the following format:

   group_name: *group_password*: *group_ID*: *user1[,user2][,user3]...*

   where:

   group_name — This is the name of your new group. It must begin with an alphabetic character and can include up to 16 alphanumeric characters.

   group_password — It is recommended that you put an asterisk "*" in this field, which indicates that you will not be using group passwords.

   group_ID — Like the *user_ID* field in the file `/etc/passwd`, the *group_ID* is a *unique* integer, which is used by HP-UX to identify the group.

   user1,... — This is a list of comma-separated *user_names* (from the first field of the entries in the `/etc/passwd` file).

4. Use the **grpck** command to check for inconsistencies and verify all entries in the `/etc/group` and `/etc/logingroup` files. This verification includes a check of the number of fields, group name, group ID, and whether all login names appear in the password file. The **grpck** command has the following format:

   `/etc/grpck` [*group_file*]

   where:

   group_file — is the name of the group file to be checked. The default group file is `/etc/group`.

Additional Task Information

The `/etc/group` file is used by the **newgrp** command to check access privileges when a user is attempting to change their effective group. If the user's login name appears in the access list of the group for which access is being requested, the access is granted, thus changing the user's current group to the requested group. The `/etc/logingroup` file, in contrast to `/etc/group`, allows users listed in more than one group access to files belonging to other groups that they are members of without changing their primary or effective groups.

Note

- A blank line in the `/etc/group` or `/etc/logingroup` file is not allowed. If a blank line appears in the files, all entries after the blank line are ignored. Refer to the "Adding a Group Using HP-UX Commands" section of this chapter for a description of the `/etc/group` and `/etc/logingroup` files.
- A group can have a maximum limit of 200 users.

Optionally, add user entries to Access Control Lists (ACL). For additional ACL information see *lsacl*(1), *chacl*(1), and *acl*(5) in the *HP-UX Reference* manual and Chapter 4, "Controlling User Access to Directories and Files", of *HP-UX System Security*, HP part number B1862-90009.

Examples

The following listing is a sample /etc/group file:

```
therapy:*:20:dennisp,janetn,jdoe,stevens
photo:*:30:kimz,jdoe,bsmith
leader:*:59:blink,pgomez,stevens
manager:*:67:obones,jab,mlee,fjones
```

To add user group "users":

4

1. Login as root.
2. Make a backup copy of /etc/group and /etc/logingroup:

   ```
   cp /etc/group /etc/group.old
   cp /etc/logingroup /etc/logingroup.old
   ```

3. Create an entry in the /etc/group file for user group "users". For example:

   ```
   therapy:*:20:dennisp,janetn,jdoe,stevens
   users:*:23:michelem,rykl,karens,starsky,stevens
   photo:*:30:kimz,jdoe,bsmith
   leader:*:59:blink,pgomez,stevens
   manager:*:67:obones,jab,mlee,fjones
   ```

4. Check the /etc/group file format:

   ```
   /etc/grpck
   ```

5. Edit the /etc/logingroup file to enable user stevens to access files belonging to groups therapy leader, and users without changing effective groups:

   ```
   more /etc/logingroup
   therapy:*:20:stevens
   users:*:23:stevens
   leader:*:59:stevens
   ```

6. Check the /etc/logingroup file format:

   ```
   grpck /etc/logingroup
   ```

Removing a Group Using HP-UX Commands

To remove a group from your system:

1. Ensure that you have superuser capabilities.
2. Make a copy of the `/etc/group` file, and optionally the `/etc/logingroup` file, so that it is easy to undo any mistakes that you might make:

   ```
   cp /etc/group /etc/group.old
   cp /etc/logingroup /etc/logingroup.old
   ```

   If you need to undo a mistake later, you can restore the "old" contents of the files using the commands:

   ```
   cp /etc/group.old /etc/group
   cp /etc/logingroup.old /etc/logingroup
   ```

3. Make a copy of the `/etc/passwd` file so that it is easy to undo any mistakes that you might make:

   ```
   cp /etc/passwd /etc/passwd.old
   ```

   If you need to undo a mistake later, you can restore the "old" contents of the file using the command:

   ```
   cp /etc/passwd.old /etc/passwd
   ```

4. Use Table 4-2 to determine the next sequence of steps based on the status of the group members and their files.

   For each user that is a member of the group being removed, perform the steps that correspond to the matching combination of actions taken regarding the user account (table row) and files (table column).

Removing a Group Using HP-UX Commands

Table 4-2. "Removing a Group" Task Decision Table

	Delete User Files	Keep User Files
Delete User(s) From System	• For files matching the user and group ownership, remove all files and directories from the system using `find`, `rm`, and `rmdir`. • For the remaining files and directories owned by each user, remove them or reassign file ownership. Remove the files and directories using `find`, `rm`, and `rmdir`. Reassign file ownership using `find` and `chown`. • Edit `/etc/passwd` to remove user entries.	• For all files on the system owned by the user being removed with the group, change file and group ownership using `find`, `chown`, and `chgrp`. • Edit `/etc/passwd` to remove user entries.
Keep User(s) on System	• If the group to be removed is a user's primary group, edit the `/etc/passwd` file to reassign user(s) to a new primary group. • For each user assigned a new primary group, change the group ownership of the login directories using the `chown` command. • For each user assigned a new primary group, if there are files within the login directory that are to be preserved, change their group ownership to match the user's new primary group using `chgrp`. • For each user that is a member of the group being removed, delete the files owned by the user and belonging to the group being removed using `find`, `rm`, and `rmdir`.	• If removed group is a primary group for a user, edit the `/etc/passwd` file to reassign user(s) to a new primary group. • For each user assigned a new primary group, change the group ownership of the login directories using the `chown` command. • If the user *is* to retain access to the files belonging to the group being removed, change the group ownership of files owned by the user to a group that the user remains a member of using `chgrp`. • If the user *not* to retain access to the files belonging to the group being removed, change the file ownership to a user that is *not* a member of the original owner's group using `chown`. For the files changing owner, change the group ownership to new owner's group using `chgrp`.

Use the `find` command to globally search the system for files with particular file and group ownership:

```
/bin/find / -fsonly hfs -user user_name -group group_name -depth -print
```

Note In an HP-UX cluster, include the `-hidden` option to the `find` command to search context-dependent files (CDFs).

If you are globally reassigning file or group ownership of all files and directories, use the `find`, `xargs`, and the command to be executed globally (`rm`, `rmdir`, `chown`, `chgrp`, or `chacl`). For example:

```
/bin/find / -fsonly hfs -user user_name -group group_name -depth -print | xargs chgrp new_group
```

If you are not globally removing or changing file access permissions, use the `find` separately from the `rm`, `rmdir`, `chown`, `chgrp`, or `chacl` command.

5. Edit the `/etc/passwd` file to remove user entries if you are removing users from the system.
6. Remove Access Control List (ACL) entries for the group being removed using the `find` and `chacl` commands:

   ```
   /bin/find / -fsonly hfs -acl %.group_name -depth -print | chacl -d %.group_name
   ```

   where:

   group_name is the name of the group being removed.
7. Use the `pwck` command to verify that the `/etc/passwd` file has valid entries:

   ```
   /etc/pwck
   ```

   The `pwck` command validates the number of fields, login name, user ID, group ID, and whether the login directory and optional program name exist. Refer to *pwck*(1M) in the *HP-UX Reference* manual for additional information.
8. Edit the `/etc/group` file, and optionally the `/etc/loginigroup` file, to remove the group entry for the group you are removing. If users are being removed from the system, remove the user from any other groups.

9. Use the `grpck` command to check for inconsistencies and verify all entries in the `/etc/group` and `/etc/logingroup` files. This verification includes a check of the number of fields, group name, group ID, and whether all login names appear in the `/etc/passwd` file. The `grpck` command has the following format:

   `/etc/grpck` [*group_file*]

Additional Task Information

A blank line in the `/etc/group` or `/etc/logingroup` file is not allowed. If a blank line appears in the files, all entries after the blank line are ignored. Refer to "Adding a Group Using HP-UX Commands" for a description of the `/etc/group` and `/etc/logingroup` files. See also *group*(4) in the *HP-UX Reference* manual.

Refer to "Controlling User Accounts and Groups" for more information about the `vipw` command.

For additional ACL information see *lsacl*(1), *chacl*(1), and *acl*(5) in the *HP-UX Reference* manual and Chapter 4, "Controlling User Access to Directories and Files", of *HP-UX System Security*, HP part number B1862-90009.

Examples

Here is a sample `/etc/group` file:

```
therapy:*:20:dennisp,janetn,jdoe,stevens,kimz
users:*:23:michelem,rykl,karens,starsky,stevens
photo:*:30:kimz,jdoe,bsmith
leader:*:59:blink,pgomez,stevens
lab:*:67:obones,jab,mlee,fjones,bsmith
```

To remove the group "photo", the group members, and their files:

1. login as `root`.
2. Make a copy of `/etc/group` and `/etc/logingroup`:

   ```
   cp /etc/group /etc/group.old
   cp /etc/logingroup /etc/logingroup.old
   ```

3. Make a copy of the /etc/passwd file:

   ```
   cp /etc/passwd /etc/passwd.old
   ```

4. Remove all of the user files and directories with group ownership corresponding to the group being removed.

   To remove files:

   ```
   /bin/find / -fsonly hfs -user kimz -group photo ! -type d -depth -print | xargs rm
   /bin/find / -fsonly hfs -user jdoe -group photo ! -type d -depth -print | xargs rm
   /bin/find / -fsonly hfs -user bsmith -group photo ! -type d -depth -print | xargs rm
   ```

   To remove directories:

   ```
   /bin/find / -fsonly hfs -user kimz -group photo -type d -depth -print | xargs rmdir
   /bin/find / -fsonly hfs -user jdoe -group photo -type d -depth -print | xargs rmdir
   /bin/find / -fsonly hfs -user bsmith -group photo -type d -depth -print | xargs rmdir
   ```

   To list remaining files and directories owned by kimz, jdoe, and bsmith:

   ```
   /bin/find / -fsonly hfs -user kimz -depth -print
   ...
   /bin/find / -fsonly hfs -user jdoe -depth -print
   ...
   /bin/find / -fsonly hfs -user bsmith -depth -print
   ...
   ```

   To reassign the remaining file to other owners:

   ```
   /bin/find / -fsonly hfs -user kimz -depth -print | xargs chown stevens
   /bin/find / -fsonly hfs -user jdoe -depth -print | xargs chown janetn
   /bin/find / -fsonly hfs -user bsmith -depth -print | xargs chown mlee
   ```

5. Edit /etc/passwd to remove user entries for users kimz, jdoe, and bsmith. HP recommends using the /etc/vipw command. The /etc/vipw command requires the EDITOR environment variable set to vi.

   To set the Korn and Bourne shell EDITOR environment variable, type:

   ```
   export EDITOR=vi
   ```

   To set the C shell EDITOR environment variable, type:

   ```
   setenv EDITOR vi
   ```

6. Remove `kimz`, `jdoe`, and `bsmith` from all ACL entries:

```
/bin/find / -fsonly hfs -acl kimz.photo -depth -print | xargs chacl -d %.photo
```

or

```
/bin/find / -fsonly hfs -acl kimz.photo -depth -print | xargs chacl -d kimz.photo
/bin/find / -fsonly hfs -acl jdoe.photo -depth -print | xargs chacl -d jdoe.photo
/bin/find / -fsonly hfs -acl bsmith.photo -depth -print | xargs chacl -d bsmith.photo
```

7. Check the `/etc/passwd` file format:

```
pwck
```

8. Edit `/etc/group` to remove the "photo" group entry and the user entries in other groups for users `kimz`, `jdoe`, and `bsmith`.

9. Run `grpck`:

```
/etc/grpck
```

Changing a User's Primary Group Using HP-UX Commands

To change a user's primary group:

1. Ensure that you have superuser capabilities.
2. Make a copy of the /etc/passwd file so that it is easy to undo any mistakes that you might make:

   ```
   cp /etc/passwd /etc/passwd.old
   ```

   If you need to undo a mistake later, you can restore the "old" contents of the file using the command:

   ```
   cp /etc/passwd.old /etc/passwd
   ```

3. Determine the *group_ID* number of your user's *new* primary group by looking at the *new* primary group's entry in the /etc/group file. The third field of the group entry in the /etc/group file (fields are separated by colons ":") contains the *group_ID*.
4. Edit the /etc/passwd file using the vipw command to replace the primary group ID, *pri_group_ID* (fourth field), of your user's entry with the *new* primary group ID.
5. Use the pwck command to verify that the /etc/passwd file has valid entries:

   ```
   /etc/pwck
   ```

   The pwck command validates the number of fields, login name, user ID, group ID, and whether the login directory and optional program name exist. Refer to *pwck*(1M) in the *HP-UX Reference* manual for additional information.

6. Make a copy of the /etc/group file, and optionally the /etc/logingroup file, so that it is easy to undo any mistakes that you might make:

```
cp /etc/group /etc/group.old
cp /etc/logingroup /etc/logingroup.old
```

If you need to undo a mistake later, you can restore the "old" contents of the files using the commands:

```
cp /etc/group.old /etc/group
cp /etc/logingroup.old /etc/logingroup
```

4

7. Evaluate the access privileges needed on the files and directories owned by the user. Use Table 4-4 to determine the next sequence of steps based on the access need of the owner (rows) and the new and old primary groups (columns).

Table 4-3. "Changing a User's Primary Group" Task Decision Table

	New Primary Group Access	Old Primary Group Access
Retain Owner Access	• Change group ownership to the new primary group using `chgrp`.	No change. • Optionally, update the ACL entries to reflect the new primary group using `chacl -r`.
Deny Owner Access	• Change group ownership to the new primary group using `chown`. • Change file ownership to a user in the new primary group using `chown`. • Set ACLs to deny access using `chacl`.	• Change file ownership to a member of user's old primary group using `chown`. • Set ACLS to deny access using `chacl`, or globally deny other group access privileges using `chmod`.

Use the `find` command to globally search the system for files with particular file and group ownership:

/bin/find / -fsonly hfs -user *user_name* **-group** *group_name* **-depth -print**

Note In an HP-UX cluster, include the `-hidden` option to the `find` command to search context-dependent files (CDFs).

If you are globally reassigning file or group ownership of all files and directories, use the `find`, `xargs`, and the command to be executed globally (`chown`, `chgrp`, or `chacl`). For example:

/bin/find / -fsonly hfs -user *user_name* **-group** *group_name* **-depth -print | xargs chgrp** *new_group*

If you are not globally changing file access permissions, use the `find` separately from the `chown`, `chgrp`, or `chacl` command.

8. Edit the `/etc/group` file to add the user's login name to the entry which corresponds to their *new* primary group. If you do *not* want the user to continue to be a member of their *previous* primary group, you will also need to remove the user's login name from the list of user members of their previous primary group.

Note

- A blank line in the `/etc/group` or `/etc/logingroup` file is not allowed. If a blank line appears in the files, all entries after the blank line are ignored. Refer to the "Adding a Group Using HP-UX Commands" section of this chapter for a description of the `/etc/group` and `/etc/logingroup` files.
- A group can have a maximum limit of 200 users.

---

9. Use the `grpck` command to check for inconsistencies and verify all entries in the `/etc/group` and `/etc/logingroup` files. This verification includes a check of the number of fields, group name, group ID, and whether all login names appear in the `/etc/passwd` file. The `grpck` command has the following format:

   `/etc/grpck` [*group_file*]

   where:

   group_file is the name of the group file to be checked. The default group file is `/etc/group`.

Additional Task Information

Optionally, update the Access Control List (ACL) entries to replace, add, or delete the necessary file access permissions. For additional ACL information see *lsacl*(1), *chacl*(1), and *acl*(5) in the *HP-UX Reference* manual and Chapter 4, "Controlling User Access to Directories and Files", of *HP-UX System Security*, HP part number B1862-90009.

Refer to "Controlling User Accounts and Groups" for more information about the `vipw` command.

Examples

Here is a sample of the `/etc/group` file:

```
therapy:*:20:dennisp,janetn,jdoe,stevens
users:*:23:rykl,karens,starsky,stevens
photo:*:30:kimz,jdoe,bsmith
leader:*:59:blink,pgomez,stevens,jdoe
lab:*:67:obones,jab,mlee,fjones, michelem
```

Her is a sample of an `/etc/passwd` entry:

```
michelem:uNx.Q3QPMEqjs,Q1sF:342:67:M.Mansfield, 47LG, (415) 555-1101:/users/mmm:/bin/ksh
```

To change the primary group for user `michelem` from the "lab" group to the "users" group:

1. login as `root`.
2. Make a copy of the `/etc/passwd` file:

   ```
   cp /etc/passwd /etc/passwd.old
   ```

3. After looking at the `/etc/group` file, the new primary group (`users`) ID is 23.

4. Edit `/etc/passwd` to replace the existing *pri_group_ID* with the new primary group *pri_group_ID*, 23. HP recommends using the `/etc/vipw` command. The `/etc/vipw` command requires the `EDITOR` environment variable set to `vi`.

   To set the Korn and Bourne shell `EDITOR` environment variable, type:

   ```
   export EDITOR=vi
   ```

   To set the C shell `EDITOR` environment variable, type:

   ```
   setenv EDITOR vi
   ```

   The new `/etc/passwd` entry should be:

```
michelem:uNx.Q3QPMEqjs,Q1sF:342:23:M.Mansfield, 47LG, (415) 325-1101:/users/mmm:/bin/ksh
```

5. Check the `/etc/passwd` file format:

   ```
   pwck
   ```

6. Make a copy of the `/etc/group` file:

   ```
   cp /etc/group /etc/group.old
   ```

   Optionally, create a copy of the `/etc/logingroup` file.
7. Change file access privileges such that user `michelem` and the members of the new primary group have access to all of the user's files. Change the group ownership of all files owned by user `michelem` to the "users" group:

   ```
   /bin/find / -fsonly hfs -user michelem -group lab -depth -print | xargs chgrp users
   ```

   Change ACLs to replace user and old primary group entries with user and new primary group entries:

```
/bin/find / -fsonly hfs -acl michelem.lab -depth -print | xargs chacl -r michelem.users
```

8. Edit `/etc/group` to add user `michelem` to the new primary group "users." For this example, user `michelem` can remain a member of the previous primary group "lab".

   Optionally, edit the `/etc/logingroup` file.
9. Check the `/etc/group` file format:

   ```
   /etc/grpck
   ```

   Optionally, run `grpck` on the `/etc/logingroup` file.

Adding Users to Groups Using HP-UX Commands

To add users to a group (without changing the users' primary group):

1. Ensure that you have superuser capabilities.
2. Make a copy of the /etc/group file, and optionally the /etc/logingroup file, so that it is easy to undo any mistakes that you might make:

   ```
   cp /etc/group /etc/group.old
   cp /etc/logingroup /etc/logingroup.old
   ```

   4

   If you need to undo a mistake later, you can restore the "old" contents of the files using the commands:

   ```
   cp /etc/group.old /etc/group
   cp /etc/logingroup.old /etc/logingroup
   ```

3. Edit the /etc/group file, and optionally the /etc/logingroup file, to add the user's *user_name* to the names in the comma-separated list of members for the group(s) for which they are to be members. If you want the user to be able to access files belonging to another group other than their primary group without using the chgrp command, edit the /etc/logingroup file to add the user to all necessary groups.
4. Use the grpck command to check for inconsistencies and verify all entries in the /etc/group and /etc/logingroup files. This verification includes a check of the number of fields, group name, group ID, and whether all login names appear in the /etc/passwd file. The grpck command has the following format:

   /etc/grpck [*group_file*]

   where:

   group_file is the name of the group file to be checked. The default group file is /etc/group.

Additional Task Information

Note

- A blank line in the /etc/group or /etc/logingroup file is not allowed. If a blank line appears in the files, all entries after the blank line are ignored. Refer to the "Adding a Group Using HP-UX Commands" section of this chapter for a description of the /etc/group and /etc/logingroup file formats.
- A group can have a maximum limit of 200 users.

Optionally, update the Access Control List (ACL) entries to replace, add, or delete the necessary file access permissions. For additional ACL information see *lsacl*(1), *chacl*(1), and *acl*(5) in the *HP-UX Reference* manual and Chapter 4, "Controlling User Access to Directories and Files", of *HP-UX System Security*.

Examples

Here is a sample /etc/group file:

```
cats:*:15:donna,woody
naomil:*:20:mj,michelem,kerschen
```

To add users pixie and pepper to groups "cats" and "naomil":

1. login as root.
2. Make a copy of the /etc/group and /etc/logingroup files:

   ```
   cp /etc/group /etc/group.old
   ```

   Optionally, make a copy of the /etc/logingroup file.
3. Edit the /etc/group file to add the users pixie and pepper to the group member lists. For example:

   ```
   cats:*:15:donna,woody,pixie,pepper
   naomil:*:20:mj,michelem,kerschen,pixie,pepper
   ```

   Optionally edit the /etc/logingroup file.
4. Check the /etc/group file format:

   ```
   /etc/grpck
   ```

Optionally run grpck on the /etc/logingroup file.

Removing Users From Groups Using HP-UX Commands

Note If you are removing users from the system, see the "Removing a User Using HP-UX Commands" section of this chapter. If you are changing the user's primary group, see the "Changing a User's Primary Group Using HP-UX Commands" section of this chapter. Otherwise, this procedure assumes that you are *not* removing users from their primary groups.

4

To remove users from groups:

1. Ensure that you have superuser capabilities
2. Make a copy of the `/etc/group` file, and optionally the `/etc/logingroup` file, so that it is easy to undo any mistakes that you might make:

```
cp /etc/group /etc/group.old
cp /etc/logingroup /etc/logingroup.old
```

If you need to undo a mistake later, you can restore the "old" contents of the files using the commands:

```
cp /etc/group.old /etc/group
cp /etc/logingroup.old /etc/logingroup
```

3. List the files and directories owned by the user using the `find` command:

```
/bin/find / -fsonly hfs -user user_name -group group_name -depth -print
```

where:

user_name is the login name of the user as defined in the `/etc/passwd` file.

group_name is the group from which the user is being removed.

If the list of files is long you can redirect the output to a file or redirect the output to the `more` command. For example:

```
/bin/find / -fsonly hfs -user user_name -group group_name -depth -print | more
```

Note In an HP-UX cluster, include the `-hidden` option to the `find` command to search context-dependent files (CDFs).

4. Use Table 4-4 to determine the next sequence of steps based on the status of the group members and their files.

   For each user that is being removed, perform the steps that correspond to the matching combination of actions taken regarding the user account (table row) and files (table column).

4

Table 4-4. "Removing Users From Groups" Task Decision Table

	Delete User Files	Keep User Files
Delete User(s) From System	• For files matching the user and group ownership, remove all files and directories from the system using `find`, `rm`, and `rmdir`. • For the remaining files and directories owned by each user, remove them or reassign file ownership. Remove the files and directories using `find`, `rm`, and `rmdir`. Reassign file ownership using `find` and `chown`. • Edit `/etc/passwd` to remove user entries.	• For all files on the system owned by the user being removed with the group, change file and group ownership using `find`, `chown`, and `chgrp`. • Edit `/etc/passwd` to remove user entries.
Keep User(s) on System	• For each user, delete the files owned by the user and group combination using `find`, `rm`, and `rmdir`.	• If the user *is* to retain access to the files, change the group ownership of files owned by the user to a group that the user remains a member of using `chgrp`. • If the user is *not* to retain access to the files, change the file ownership to a user that is *not* a member of the current owner's group using `chown`. For the files changing owner, change the group ownership to new owner's group using `chgrp`.

Removing Users From Groups Using HP-UX Commands

Use the `find` command to globally search the system for files with particular file and group ownership:

```
/bin/find / -fsonly hfs -user user_name -group group_name -depth -print
```

Note In an HP-UX cluster, include the `-hidden` option to the `find` command to search context-dependent files (CDFs).

If you are globally removing files or reassigning file permissions, use the `find`, `xargs`, and the command to be executed globally (`rm`, `rmdir`, `chown`, `chgrp`, or `chacl`). For example:

```
/bin/find / -fsonly hfs -user user_name -group group_name -depth -print | xargs chgrp new_group
```

If you are not globally removing files or changing file access permissions, use the `find` separately from the `rm`, `rmdir`, `chown`, `chgrp`, or `chacl` command.

5. Remove Access Control List (ACL) entries for all users being removed from the group using the `find` and `chacl` commands:

```
/bin/find / -fsonly hfs -acl user_name.group_name -depth -print | xargs chacl -d user_name.group_name
```

6. Edit the `/etc/group` file, and optionally the `/etc/logingroup` file, to remove the user's *user_name* from the list of members for a group.

Note

- Do *not* remove the user's name from their primary group defined in the `/etc/passwd` file unless you are removing the user from the system. If you want to change the user's primary group, see the "Changing a User's Primary Group Using HP-UX Commands" section of this chapter.
- A blank line in the `/etc/group` or `/etc/logingroup` file is not allowed. If a blank line appears in the files, all entries after the blank line are ignored. Refer to the "Adding a Group Using HP-UX Commands" section of this chapter for a description of the `/etc/group` and `/etc/logingroup` file formats.

7. Use the **grpck** command to check for inconsistencies and verify all entries in the **/etc/group** and **/etc/logingroup** files. This verification includes a check of the number of fields, group name, group ID, and whether all login names appear in the password file. The **grpck** command has the following format:

   /etc/grpck [*group_file*]

   where:

   group_file is the name of the group file to be checked. The default group file is **/etc/group**.

Additional Task Information

For additional ACL information see *lsacl*(1), *chacl*(1), and *acl*(5) in the *HP-UX Reference* manual and Chapter 4, "Controlling User Access to Directories and Files", of *HP-UX System Security*, HP part number B1862-90009.

Examples

The following listing is a sample group file:

```
therapy:*:20:dennisp,janetn,jdoe,stevens
photo:*:30:kimz,jdoe,bsmith
leader:*:59:blink,pgomez,stevens
lab:*:67:obones,jab,mlee,fjones
```

To remove user **obones** from the **lab** group (which is not the user's primary group):

1. Login in as **root**.
2. Make a copy of the **/etc/group** file:

   ```
   cp /etc/group /etc/group.old
   ```

   Optionally, make a copy of the **/etc/logingroup** file.

Removing Users From Groups Using HP-UX Commands

3. List the files owned by the user obones and belonging to group lab:

```
/bin/find / -fsonly hfs -user obones -group lab -depth -print
...
...
```

4. Remove user obones from access privileges to the /users/development directory and its files, change the ownership of these files to a user belonging to the group from which you removed user obones. For example, change the file ownership of the project related files to user fjones:

4

```
chown /users/development blink
/bin/find /users/development -fsonly hfs -user obones -group lab -depth -print | xargs chown fjones
```

Enable only user obones to access his personal files by transferring the group ownership of personal files to another group in which obones is a member. If obones personal file's group ownership is not changed, any member of the group (for which obones is no longer a member) may gain access to the files depending on how the group permissions are set. To ensure privacy change the group ownership:

```
/bin/find /users/obones -fsonly hfs -user obones -group lab -depth -print | xargs chgrp photo
```

5. Remove obones.lab from any ACL entries:

```
/bin/find / -fsonly hfs -acl obones.lab -depth -print | xargs chacl -d obones.lab
```

6. Edit the /etc/group file to remove obones from the "lab" group entry. The following listing is how the file would appear after the edit:

```
therapy:*:20:dennisp,janetn,jdoe,stevens
photo:*:30:kimz,jdoe,bsmith
leader:*:59:blink,pgomez,stevens
lab:*:67:jab,mlee,fjones
```

7. Run grpck:

```
/etc/grpck
```

Optionally edit and run grpck on the /etc/logingroup file.

Displaying/Assigning Special Group Privileges Using HP-UX Commands

To display special group privileges use the `getprivgrp` command:

`/usr/bin/getprivgrp` [`-g` | *group_name*]

where:

`-g`	lists access privileges that have been granted to all groups. Otherwise, access privileges are listed for all privileged groups to which the requestor belongs.
group_name	is the name of the group as specified in the `/etc/group` file.

If *group_name* is supplied, access privileges are listed for that group only. If the requestor is not a member of the *group_name* specified, no information is displayed. The superuser is a member of all groups.

To assign special group privileges:

1. Ensure that you have superuser capabilities.
2. Assign special privileges using the `setprivgrp` command. There are three formats for the `setprivgrp` command.

Displaying/Assigning Special Group Privileges Using HP-UX Commands

One format of the `setprivgrp` command is:

`/etc/setprivgrp` *group_name* [*privilege*]

where:

group_name is the name of the group as specified in the `/etc/group` file.

privilege is one or more of the following privileges:

4

- *RTPRIO* gives access to the `rtprio` command and system call, which allows the setting of real-time priorities.
- *MLOCK* gives access to the `plock` system call, which allows processes to be locked in memory and allows use of the SHM_LOCK command (used with the `shmctl` system call).
- *CHOWN* gives access to the `chown` command and system call, which allows members of the group to change the ownership of files on the system.
- *LOCKRDONLY* gives access to the `lockf` system call to set locks on files that are open for reading only.
- *SETRUGID* gives access to the `setuid` and `setgid` system calls to change, respectively, the real user ID or real group ID of a process.

The other two formats of the `setprivgrp` command are:

`/etc/setprivgrp -g` [*privilege*]

`/etc/setprivgrp -n` [*privilege*]

where:

`-g`	specifies that *all* groups have access to the specified *privilege*(s).
`-n`	specifies that *no* groups have access to the specified *privilege*(s).
privilege	is one or a combination of the special privileges (RTPRIO, MLOCK, CHOWN, LOCKRDONLY, or SETRUGID).

For additional information refer to *rtprio*(1), *rtprio*(2), *plock*(2), *shmctl*(2), *chown*(1), *chown*(2), *lockf*(2), *setuid*(2), *setgid*(2), *setprivgrp*(2), and *setprivgrp*(1M) in the *HP-UX Reference* manual. Capabilities set by this command are not added to existing capabilities for the same group. If you want to add a capability for a particular group, you must respecify all capabilities that were already set for that group as well as the new capability.

Note Specifying no privileges removes all special privileges for the group.

Additional Task Information

Any user whose current *group_ID* matches the *group_ID* of a privileged group will have access to the special capabilities assigned to that group. A group can have any one, two or all five of the capabilities associated with it.

Note In an HP-UX cluster, group privileges apply only to the cluster node on which you set them. For example, if you want group `patrick` to have RTPRIO privilege on cluster clients `client1` and `client2`, then you must execute the `setprivgrp` command twice, once on `client1` and again on `client2`.

The CHOWN privilege is an exception: if a group has this privilege on the cluster server, it will have it on all cluster clients as well.

Examples

- To set real-time priorities and enable user processes to lock process text and data into memory for the `development` group:

```
setprivgrp development RTPRIO MLOCK
getprivgrp
global privileges: CHOWN
development: RTPRIO MLOCK
```

- To set real-time priorities and enable user processes to lock process text and data into memory for all groups:

```
setprivgrp -g RTPRIO MLOCK
```

- To deny real-time priorities and disable user processes to lock process text and data into memory for all groups:

```
setprivgrp -n RTPRIO MLOCK
```

For additional information, refer to *setprivgrp*(1M) and *getprivgrp*(1) in the *HP-UX Reference* manual.

Managing Run-Levels

A **run-level** is an HP-UX state of operation in which a specific set of processes (and their offspring) are permitted to run. This set of processes is defined, for each run-level, in a file called `/etc/inittab`.

The following list contains tasks covered in this section:

Creating a New Run-Level Using HP-UX Commands

Changing System Run-Levels Using HP-UX Commands

Entering the System Administration Run-Level

Returning From the System Administration Run-Level

Creating a New Run-Level Using HP-UX Commands

To create new run-levels:

1. Ensure that you have superuser capabilities.
2. Make a copy of the `/etc/inittab` file so that it is easy to undo any mistakes that you might make:

   ```
   cp /etc/inittab /etc/inittab.old
   ```

   If you need to undo a mistake later, you can restore the "old" contents of the file using the command:

   ```
   cp /etc/inittab.old /etc/inittab
   ```

3. Edit the `/etc/inittab` file with the editor of your choice to create a one-line entry in `/etc/inittab` with the following format:

   id:*rstate*:*action*:*process*

   where:

id	is a unique four-character identifier, used to identify an entry.
rstate	is a list of run-levels to which each entry applies.
action	is a action to be performed, such as `respawn`.
process	is the command that will be executed when that run-level is entered.

   Refer to *init*(1M) and *inittab*(4) in the *HP-UX Reference* manual for a detailed description of entries in the `/etc/inittab` file.

4. Edit the `/etc/inittab` file to change the `initdefault` entry in your test version to "s". By changing the `initdefault` entry to "s", you will come up in run-level "s" when you boot. You can *change* to run-level 2 after booting by executing `init 2`. If your new run-level 2 does not work, you can still reboot.

   Note that "s" is not a normal run-level. If you create this test version, you should replace the "s" with "2" after testing is complete. Run-level "s" is for system maintenance only.

   If you do not have a working state for the `initdefault` state, you may not be able to boot your system. After thoroughly testing your changes, *restore the original initdefault value.*

Examples

The following is an example `/etc/inittab` for a system that contains a system console and six terminals. The initdefault run-level is run-level 2. Run-level 2 is a multi-user run-level, with a `getty` on every terminal.

```
init:2:initdefault:
stty::sysinit:stty 9600 clocal icanon echo opost onlcr ienqak ixon icrnl ignpar </dev/systty
brc1::bootwait:/etc/bcheckrc </dev/console >/dev/console 2>&1 # fsck, etc.
slib::bootwait:/etc/recoversl </dev/console >/dev/console 2>&1 #shared libs
brc2::bootwait:/etc/brc >/dev/console 2>&1         # boottime commands
link::wait:/bin/sh -c "rm -f /dev/syscon; \
    ln /dev/systty /dev/syscon" >/dev/console 2>&1
cwrt::bootwait:cat /etc/copyright >/dev/syscon     # legal requirements
rc   ::wait:/etc/rc </dev/console >/dev/console 2>&1 # system initialization
powf::powerwait:/etc/powerfail >/dev/console 2>&1  # power fail routines
lp   ::off:nohup sleep 999999999 </dev/lp & stty 9600 </dev/lp
cons:012456:respawn:/etc/getty -h console console          # system console
vue :34:respawn:/etc/vuerc                        # VUE validation and invocation
t1:2:respawn:/etc/getty tty01 H
t2:2:respawn:/etc/getty tty02 H
t3:2:respawn:/etc/getty tty03 H
t4:2:respawn:/etc/getty tty04 H
t5:2:respawn:/etc/getty tty05 H
t6:2:respawn:/etc/getty tty06 H
```

Changing System Run-Levels Using HP-UX Commands

The following is a general procedure for changing the system from one run-level to another. You must be logged in at the system console as the superuser to change the system's run-level.

1. Warn all users who are currently logged in before you change run-levels.

   Changing to another run-level while users are logged on will kill (terminate) their processes if the run-level you are moving to does not contain `rstate` entries in `/etc/inittab` for their terminal. You can use the `write` or `wall` commands to communicate with the users. Note that the `wall` (write all) command immediately sends your message to the terminal of each user on the system.

   In an HP-UX cluster, users logged in to cluster clients are actually logged in to *different computers* than the one you're likely to use to issue the `write` or `wall` commands (as mentioned above). There is a special version of the `wall` command called `cwall` that is "cluster smart." It is used just like the `wall` command. See the *wall*(1M) and *cwall*(1M) in the *HP-UX Reference* manual.

   If each `getty` (terminal) entry has the new run-level in its `rstate` field, or if the `rstate` field is empty (implies all numbered run-levels), you don't need to ask them to log off; their processes will not be killed (unless your new run-level is run-level "s").

2. To change to a run-level other than run-level "s", use the command:

   `/etc/init` *new_run-level*

   where *new_run-level* is the number of the run-level you want to enter.

   To change to run-level "s", use the command:

   ```
   /etc/shutdown
   ```

Caution

- You should not change to run-level "s" without using the `shutdown` command (that is, do not execute `init s`). The `shutdown` command provides safeguards to "cleanly" bring your system to single-user mode (run-level "s").
- Run-level 0 is a special run-level reserved for system installation. Do not use run-level 0.
- If you are on a cluster client, changing run-levels has no effect on other nodes in the cluster. If you are on the root server of a cluster, changing run-levels *can* affect the cluster clients. In particular, if you change to run-level "s", the server will be unable to respond to the clients' requests. This means that the clients will panic and halt.

Entering the System Administration Run-Level

Many of the system maintenance tasks you perform as system administrator require the system to be in single-user mode (run-level "s") so that you can ensure that no one else is on the system while you're performing those tasks. In this run-level, the only access to the system is through the system console by the user `root`, and the only processes running on the system will be the shell on the system console, background daemon processes started by `/etc/rc`, and processes that you invoke. Commands requiring an inactive system (such as `fsck`) should be run in run-level "s".

Use the **shutdown** command, instead of **init s** when changing your system's run-level from any numbered run-level (run-levels 1 through 6) to run-level "s". The **shutdown** command kills all non-essential processes and brings the system *safely* to run-level "s" (without leaving system resources in an unusable state).

The **shutdown** command also allows you to specify a **grace period** to allow time for your users to terminate their work before the system goes down. The grace period is given (in number of seconds to wait) immediately following the command name. For example:

To enter run-level "s" with a grace period of 30 seconds, type in:

```
/etc/shutdown 30
```

This will automatically warn all users that they have 30 seconds to log off, kill all processes, and safely bring the system to run-level "s".

For details on how to use the **shutdown** command, see Chapter 3, "Starting and Stopping HP-UX" and *shutdown*(1M) in the *HP-UX Reference* manual.

Returning From the System Administration Run-Level

When you want to change your system's run-level *from* run-level "s" (single-user mode) to one of the other run-levels, it is best to do so by rebooting your system. You can use the `reboot` command to do this. You can also use the `init` command as described earlier in this chapter (See "Changing System Run-Levels Using HP-UX Commands") to change to the new run-level.

5

Managing Peripherals

Managing peripherals on your system is a very important system administration task. This chapter provides general guidelines and procedures for managing your peripherals. The purpose of this chapter is to give an overview of adding a peripheral and detailed instructions on moving and removing peripherals. There are references to other chapters of this book and other books in the documentation set that provide specific instructions and details.

The task guidelines covered in this chapter are:

- Overview of adding a peripheral
- Moving peripherals using SAM
- Removing peripherals using SAM
- Creating device files using HP-UX commands
- Moving peripherals using HP-UX commands
- Removing peripherals using HP-UX commands

This chapter describes special cases, for example, moving your system console or root disk to a different hardware address.

The *Installing Peripherals* manual has details on adding a peripheral to your system.

You can manage peripherals in either of two ways:

1. The System Administration Manager (SAM)
2. HP-UX commands

SAM configures the majority of all peripherals supported by HP-UX. For those devices that SAM supports, SAM creates the device files and adds the device driver to the kernel, if necessary.

When adding local printers and plotters with SAM, the device is automatically configured into the lp spooler.

When adding disk drives with SAM, you can create and mount file systems.

The peripherals that are not supported by SAM are:

- Graphics interface cards and graphics displays
- Flexible disk drives
- Scanjets/digitizers

For the devices that SAM does not support, SAM does not create device files, but you can use SAM to add the device drivers to the kernel.

SAM provides an on line help system to assist you when you need additional information.

Activating the (Help) button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

From within a functional area, choosing an item from the "Help" menu gives you information about:

- the current functional area
- keyboard navigation within SAM
- using the SAM help system
- displaying the version of SAM you are currently running

From a dialog box (a window displaying fields to be filled in), pressing the (f1) key gives you context-sensitive information for the object at the location of the cursor.

Refer to Chapter 1, "Introduction to System Administration", for additional SAM information.

Overview of Adding a Peripheral

There are two steps to adding a peripheral to your system:

1. You must physically connect the peripheral to your system and ensure that the peripheral's communication protocol is configured properly. Refer to the documentation shipped with the peripheral to locate the interface port, set and configure the communication protocol, and perform a self test (if applicable).
2. Your operating system must be configured to recognize the peripheral. Configuring your system includes:

   a. ensuring that the device driver for the peripheral is configured into the HP-UX kernel (typically `/hp-ux`). There can be more than one driver required in the kernel for the device.

   b. creating a device file or multiple device files.

   c. configuring HP-UX utilities to use the peripheral.

   SAM can perform all of these tasks for you.

Refer to the *Installing Peripherals* manual to add a particular peripheral to your system. The *Installing Peripherals* manual provides device driver and device file information.

Moving Peripherals Using SAM

Moving peripherals using SAM is different depending on the type of peripheral. Instructions for each of the following types of peripherals are included:

- local printer or plotter
- tape drive
- terminal or modem
- disk drive containing file systems or swap space

If users will be affected, notify the users on the system of the device location change, see the "Communicating With the Users on Your System" chapter of this manual.

Moving a Local Printer or Plotter

Moving a local printer on your system requires that you remove the printer from the lp spooler and then add the printer using the new hardware location encoded in the device file. When SAM removes a printer, SAM also removes the model script used to communicate with the printer located in the `/usr/spool/lp/interface` directory. Prior to removing the printer, you should preserve this file under another name and use it when adding the printer back to the lp spooler.

To move a local printer or plotter using SAM:

1. Ensure that you have superuser capabilities.
2. If users will be affected, notify the users on the system about the device being moved. See the "Communicating With the Users on Your System" chapter of this manual.
3. Copy `/usr/spool/lp/interface/`*printer_name* to a temporary location.

   ```
   cp /usr/spool/lp/interface/printer_name /usr/spool/lp/interface/printer_name.old
   ```

4. Run SAM; type:

   `/usr/bin/sam`

   SAM provides an on line help system to assist you when you need additional information.

   Activating the (Help) button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

   From within a functional area, choosing an item from the "Help" menu gives you information about:

   - the current functional area
   - keyboard navigation within SAM
   - using the SAM help system
   - displaying the version of SAM you are currently running

   From a dialog box (a window displaying fields to be filled in), pressing the (f1) key gives you context-sensitive information for the object at the location of the cursor.

   Refer to Chapter 1, "Introduction to System Administration", for additional SAM information.

5. Highlight `Printer and Plotters` and activate the (Open) control button.
6. Highlight `Printer/Plotters` and activate the (Open) control button.
7. Highlight the printer that you wish to move and choose `Remove Printer/Plotter`. SAM removes the device file if the device file is `/dev/lp_`*printer_name*; otherwise, the device file is not removed.
8. Exit SAM.
9. Turn off, unplug, and disconnect the printer or plotter.
10. Add the local printer to your system at the new hardware location; refer to the *Installing Peripherals* manual for specific instructions. When using SAM to add a printer, SAM also adds the printer to the lp spooler. If the printer is an HP-IB printer, ensure that the printer has a unique bus address.

Note Specify the temporary file (`/usr/spool/lp/interface/`*printer_name*`.old`) you created in step 3 for the model script.

---

11. Remove the temporary file (`/usr/spool/lp/interface/`*printer_name*`.old`) you created in step 3.
12. Update any software application configurations that use the relocated local printer. Refer to your software application documentation for specific instructions.

Refer to the "Managing Printers and Printer Output" chapter of this manual for additional information about adding and removing a local printer or plotter using SAM.

Note To return your system to the original configuration, repeat this procedure.

Moving a Tape Drive

Moving a tape drive on your system requires that you remove the tape drive and then add the tape drive using the new hardware location.

To move a tape drive using SAM:

1. Ensure that you have superuser capabilities.
2. Notify the users on the system about the system shutdown as a result of moving the tape drive. See the "Communicating With the Users on Your System" chapter of this manual.

Note It is recommended that you shut down and power off your computer while moving devices on the SCSI or HP-IB bus.

5

3. Run SAM; type:

   ```
   /usr/bin/sam
   ```

   SAM provides an on line help system to assist you when you need additional information.

   Activating the (Help) button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

   From within a functional area, choosing an item from the "Help" menu gives you information about:

   - the current functional area
   - keyboard navigation within SAM
   - using the SAM help system
   - displaying the version of SAM you are currently running

   From a dialog box (a window displaying fields to be filled in), pressing the (f1) key gives you context-sensitive information for the object at the location of the cursor.

   Refer to Chapter 1, "Introduction to System Administration", for additional SAM information.

4. Highlight `Peripheral Devices` and activate the OK control button.
5. Highlight `Tape Drives` and activate the OK control button.
6. Choose `Remove...` from the "Actions" menu. SAM does not remove the tape drive device file.
7. Exit SAM.
8. Remove any media currently loaded in the tape drive.
9. Shut down your system:

   cd /

   shutdown *grace_period_in_seconds*

   For additional information, see Chapter 3, "Starting and Stopping HP-UX" of this manual.
10. Halt the system:

    reboot -h
11. Turn off the computer.
12. Turn off, unplug, and disconnect the tape drive.
13. Physically move the tape drive. Refer to the documentation shipped with your tape drive if you intend to change the HP-IB or SCSI bus address. Ensure that each device on the SCSI or HP-IB bus has a unique bus address.

14. Turn on the tape drive.

Note For SCSI devices, it is important to power up your device before turning on your system.

---

15. Turn on the computer.
16. Log in and run SAM to add the tape drive to your system at the new hardware address. SAM will create a new device file for the tape drive and will not remove the old device file, unless you specify the same device file name.
17. Update any automated backup processes you have scheduled. See the "Backing Up and Restoring Your Data" chapter of this book for specific instructions.
18. Reload media into the tape drive.
19. Update any software application configurations that use the relocated tape drive. Refer to your software application documentation for specific instructions.

Moving a Terminal or Modem

Moving a terminal or modem on your system requires that you remove the terminal or modem and then add the terminal or modem using the new hardware location.

To move a terminal or modem using SAM:

1. Ensure that you have superuser capabilities.
2. If users will be affected, notify the users on the system about the device being moved. See the "Communicating With the Users on Your System" chapter of this manual. The terminal or modem to be moved cannot be in use, it must be inactive.
3. Run SAM; type:

   `/usr/bin/sam`

   SAM provides an on line help system to assist you when you need additional information.

   Activating the (Help) button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

   From within a functional area, choosing an item from the "Help" menu gives you information about:

   - the current functional area
   - keyboard navigation within SAM
   - using the SAM help system
   - displaying the version of SAM you are currently running

   From a dialog box (a window displaying fields to be filled in), pressing the (f1) key gives you context-sensitive information for the object at the location of the cursor.

   Refer to Chapter 1, "Introduction to System Administration", for additional SAM information.

4. Highlight `Peripheral Devices` and activate the (OK) control button.
5. Highlight `Terminals and Modems` and activate the (OK) control button.
6. Highlight the terminal or modem you intend to move and choose `Remove Device...` from the "Actions" menu. SAM removes the associated terminal and modem device file(s). SAM also updates the **/etc/inittab** file by removing the **getty** entry for the terminal or modem.
7. Exit SAM.
8. Turn off, unplug, and disconnect the terminal or modem.
9. Add the terminal or modem to the system at the new hardware location; refer to the *Installing Peripherals* manual. If you use SAM, SAM will create the necessary device files and entries in the **/etc/inittab** file.
10. Update any software application configurations that use the relocated terminal or modem. Refer to your software application documentation for specific instructions.

Moving a Disk Drive Used for File Systems and Swap

Note

- You can only change the hardware address of a disk used for a file system or swap using SAM.
- SAM does not support:
  - changing the hardware address of a disk drive containing the root file system. See "Moving a Disk Drive Containing the Root File System".
  - changing the hardware address of a disk that is labeled "unused". See "Moving a Disk Drive Used for File Systems and Swap".
  - changing the hardware address of a disk array.

To move a disk drive from one hardware address to another using SAM:

1. Ensure that you have superuser capabilities.
2. Back up the data on the disk. See the "Backing Up and Restoring Your Data" chapter of this manual for specific instructions.
3. Notify the users on the system about the system shutdown as a result of moving the disk drive. See the "Communicating With the Users on Your System" chapter of this manual.

Note It is recommended that you shut down and power off your computer while moving devices on the SCSI or HP-IB bus.

4. If your system is an NFS server and file systems on the disk you are moving are exported, unmount the file systems from the NFS client. If you do not unmount the file systems from the client, the client will receive NFS error messages when accessing the files on the disk.

   To find the NFS clients, log in to the NFS server and look at the `/etc/exports` file. Refer to *exports*(4) in the *HP-UX Reference*.

   Notify the users on the NFS client systems that data on the disk to be relocated will be temporarily inaccessible. See "Communicating With the Users on Your System".

   There are three methods to unmount the NFS client file systems:

   a. Enter the `Remote Administration` area of SAM on the NFS server and unmount the file systems remotely.

   b. Log in directly to each NFS client and run SAM to unmount the file systems.

   c. Log in directly to each NFS client and unmount the file systems using HP-UX commands.

   Refer to Chapter 6, "Managing the File System" for specific instructions on unmounting file systems.

5

5. Run SAM; type:

   `/usr/bin/sam`

   SAM provides an on line help system to assist you when you need additional information.

   Activating the (Help) button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

   From within a functional area, choosing an item from the "Help" menu gives you information about:

   - the current functional area
   - keyboard navigation within SAM
   - using the SAM help system
   - displaying the version of SAM you are currently running

   From a dialog box (a window displaying fields to be filled in), pressing the (f1) key gives you context-sensitive information for the object at the location of the cursor.

   Refer to Chapter 1, "Introduction to System Administration", for additional SAM information.

6. Highlight `Disks and File Systems` and activate the OK control button.
7. Highlight `CD-ROM, Floppy, and Hard Disks` and activate the OK control button.
8. Highlight the disk you intend to move.
9. Choose `Change a Disk Address...` from the "Actions" menu.
10. Highlight the interface to which the relocated disk will be attached. Fill in the hardware address, interface slot, and bus address, then activate the OK control button.

    SAM creates a new device file for the relocated disk and updates the `/etc/checklist`. SAM does not remove the old device file.

5

Note Your `/etc/checklist` file now reflects the future configuration of your system, *not* the current configuration of your system.

---

11. Exit SAM. SAM copied your original `/etc/checklist` file to `/etc/checklist.old`.
12. Shut down your system:

    ```
    cd /
    shutdown grace_period_in_seconds
    ```

    For additional information, see Chapter 3, "Starting and Stopping HP-UX" of this manual.
13. Halt the system:

    ```
    reboot -h
    ```

14. Turn off the computer.
15. Turn off, unplug, and disconnect the disk drive.
16. Physically move the disk drive. Refer to the documentation shipped with your disk drive if you intend to change the HP-IB or SCSI bus address. Ensure that each device on the SCSI or HP-IB bus has a unique bus address.

17. Turn on the disk drive.

Note For SCSI devices, it is important to power up your device before turning on your system.

---

18. Turn on the computer.
19. Update any software application configurations that use the relocated disk drive. Refer to your software application documentation for specific instructions.
20. If your system is an NFS server, remount the NFS client's file system(s) that were temporarily inaccessible. As superuser on the NFS client system, type:

    ```
    mount -a
    ```

21. Update any software application configurations that used the relocated disk drive. Refer to your software application documentation for specific instructions.

Removing Peripherals Using SAM

When SAM removes peripherals from the system, SAM removes the associated device files for

- printers and plotters with device filenames `lp_`*printer_name*.
- terminals and modems.

When SAM removes disk or tape drives, SAM does not remove the associated devices files.

SAM does not remove device drivers from the kernel when removing peripherals from the system.

If users will be affected, notify the users on the system about the device being removed. See the "Communicating With the Users on Your System" chapter of this manual.

5

Removing a Local Printer or Plotter

To remove a local printer or plotter using SAM:

1. Ensure that you have superuser capabilities.
2. If users will be affected, notify the users on the system about the device being moved. See the "Communicating With the Users on Your System" chapter of this manual.

3. Run SAM; type:

   `/usr/bin/sam`

   SAM provides an on line help system to assist you when you need additional information.

   Activating the (Help) button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

   From within a functional area, choosing an item from the "Help" menu gives you information about:

   - the current functional area
   - keyboard navigation within SAM
   - using the SAM help system
   - displaying the version of SAM you are currently running

   From a dialog box (a window displaying fields to be filled in), pressing the (f1) key gives you context-sensitive information for the object at the location of the cursor.

   Refer to Chapter 1, "Introduction to System Administration", for additional SAM information.

4. Highlight `Printer and Plotters` and activate the (Open) control button.
5. Highlight `Printer/Plotters` and activate the (Open) control button.
6. Highlight the printer that you wish to remove and choose `Remove Printer/Plotter`. SAM removes the device file if the device file is `/dev/lp_`*printer_name*, otherwise the device file is not removed.
7. Exit SAM.
8. Turn off, unplug, and disconnect the printer or plotter.
9. Update any software application configurations that used the removed local printer. Refer to your software application documentation for specific instructions.

5

Removing a Tape Drive

To remove a tape drive using SAM:

1. Ensure that you have superuser capabilities.
2. Notify the users on the system about the system shutdown as a result of removing the tape drive. See the "Communicating With the Users on Your System" chapter of this manual.

Note It is recommended that you shut down and power off your computer while removing devices from the SCSI or HP-IB bus.

---

3. Run SAM; type:

   `/usr/bin/sam`

   SAM provides an on line help system to assist you when you need additional information.

   Activating the (Help) button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

   From within a functional area, choosing an item from the "Help" menu gives you information about:

   - the current functional area
   - keyboard navigation within SAM
   - using the SAM help system
   - displaying the version of SAM you are currently running

   From a dialog box (a window displaying fields to be filled in), pressing the (f1) key gives you context-sensitive information for the object at the location of the cursor.

   Refer to Chapter 1, "Introduction to System Administration", for additional SAM information.

4. Highlight `Peripheral Devices` and activate the (OK) control button.
5. Highlight `Tape Drives` and activate the (OK) control button.
6. Highlight the tape drive you wish to remove from the object list.
7. Choose `Remove...` from the "Actions" menu. SAM does not remove the tape drive device file.
8. Exit SAM.
9. Remove any media currently loaded in the tape drive.
10. Shut down your system:

    `cd /`

    `shutdown` *grace_period_in_seconds*

    For additional information, see Chapter 3, "Starting and Stopping HP-UX" of this manual.
11. Halt the system:

    `reboot -h`
12. Turn off the computer.
13. Turn off, unplug, and disconnect the tape drive.
14. Turn on the computer.
15. Modify any automated backup processes scheduled by the `cron` utility that expect the tape drive to be present. See the "Backing Up and Restoring Your Data" chapter of this manual and *cron*(1M) in the *HP-UX Reference*.
16. Update any software application configurations that used the removed tape drive. Refer to your software application documentation for specific instructions.

5

Removing a Terminal or Modem

To remove a terminal or modem using SAM:

1. Ensure that you have superuser capabilities.
2. If users will be affected, notify the users on the system about the terminal or modem being removed. See the "Communicating With the Users on Your System" chapter of this manual. The terminal or modem to be removed cannot be in use, it must be inactive.
3. Run SAM; type:

   `/usr/bin/sam`

   SAM provides an on line help system to assist you when you need additional information.

5

   Activating the (Help) button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

   From within a functional area, choosing an item from the "Help" menu gives you information about:

   - the current functional area
   - keyboard navigation within SAM
   - using the SAM help system
   - displaying the version of SAM you are currently running

   From a dialog box (a window displaying fields to be filled in), pressing the (f1) key gives you context-sensitive information for the object at the location of the cursor.

   Refer to Chapter 1, "Introduction to System Administration", for additional SAM information.

4. Highlight `Peripheral Devices` and activate the (OK) control button.
5. Highlight `Terminals and Modems` and activate the (OK) control button.
6. Highlight the terminal or modem you intend to move and choose `Remove Device...` from the "Actions" menu. SAM removes the associated terminal and modem device file(s). SAM also updates the **/etc/inittab** file by removing the **getty** entry for the terminal or modem.
7. Exit SAM.
8. Turn off, unplug, and disconnect the terminal or modem.
9. Update any software application configurations that used the removed terminal or modem. Refer to your software application documentation for specific instructions.

Removing a Disk Drive Used for File Systems or Swap

Note SAM does not support removing the disk containing the root file system. See "Moving a Disk Drive Containing the Root File System".

To remove a disk drive using SAM:

1. Ensure that you have superuser capabilities.
2. Optionally, back up the data on the disk drive; refer to the "Backing Up and Restoring Your Data" chapter of this manual for specific instructions.
3. Notify the users on the system about system shutdown as a result of removing the disk drive. See the "Communicating With the Users on Your System" chapter of this manual.

Note It is recommended that you shut down and power off your computer while removing devices from the SCSI or HP-IB bus.

4. If your system is an NFS server and file systems on the disk you are moving are exported, unmount the file systems from the NFS client. If you do not unmount the file systems from the client, the client will receive NFS error messages when accessing the files on the disk.

   To find the NFS clients, log in to the NFS server and look at the `/etc/exports` file. Refer to *exports*(4) in the *HP-UX Reference*.

   Notify the users on the NFS client systems that data on the disk to be removed will be permanently inaccessible. See "Communicating With the Users on Your System".

There are three methods to unmount the NFS client file systems:

a. Enter the `Remote Administration` area of SAM on the NFS server and unmount the file systems remotely.

b. Log in directly to each NFS client and run SAM to unmount the file systems.

c. Log in directly to each NFS client and unmount the file systems using HP-UX commands.

Update the NFS client's `/etc/checklist` to remove any mount entries for file systems that are resident on the disk drive being removed. Refer to Chapter 6, "Managing the File System" for specific instructions to remove entries from the `/etc/checklist` file.

5. Run SAM; type:

   `/usr/bin/sam`

   SAM provides an on line help system to assist you when you need additional information.

   Activating the (Help) button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

   From within a functional area, choosing an item from the "Help" menu gives you information about:

   - the current functional area
   - keyboard navigation within SAM
   - using the SAM help system
   - displaying the version of SAM you are currently running

   From a dialog box (a window displaying fields to be filled in), pressing the (f1) key gives you context-sensitive information for the object at the location of the cursor.

   Refer to Chapter 1, "Introduction to System Administration", for additional SAM information.

6. Highlight `Disks and File Systems` and activate the (OK) control button.
7. Highlight `CD-ROM, Floppy, and Hard Disks` and activate the (OK) control button.
8. Highlight the disk you intend to remove and choose `Remove a Hard Disk Drive` from the "Actions" menu. SAM updates the **/etc/checklist** file to remove the mount entry. SAM does not remove the associated disk drive device file(s).
9. Exit SAM.
10. Shut down and halt your system:

    `cd /`

    `shutdown -h` *time_in_seconds*

5

11. Turn off your computer.
12. Turn off the disk drive.
13. Physically disconnect the disk drive.
14. Turn on the computer.
15. Log in. Ensure that you have superuser capabilities.
16. Update any software application configurations that used the removed disk drive. Refer to your software application documentation for specific instructions.

Creating Device Files Using HP-UX Commands

Refer to Chapter 11, "System Configuration" of *How HP-UX Works: Concepts for the System Administrator*, the *Installing Peripherals* manual, and the *mknod*(1M) command in the *HP-UX Reference*.

Moving Peripherals Using HP-UX Commands

Moving peripherals using HP-UX commands is different depending on the type of peripheral. Instructions for each of the following types of peripherals are included:

- printer or plotter
- tape drive
- terminal or modem
- system console
- disk drive containing file systems or swap
- disk drive containing the root file system

If users will be affected, notify the users on the system of the device location change. See the "Communicating With the Users on Your System" chapter of this manual.

Moving a Local Printer or Plotter

Moving a local printer on your system requires that you remove the printer from the lp spooler and then add the printer using the new hardware location encoded in the device file. When a printer is removed, SAM also removes the model script used to communicate with the printer located in the `/usr/spool/lp/interface` directory. Prior to removing the printer, you should preserve this file under another name and use it when adding the printer back to the lp spooler.

To move a printer using HP-UX commands:

1. Ensure that you have superuser capabilities.
2. If users will be affected, notify the users on the system about the device being moved. You will need to notify users, if you will be changing the printer name as well as the hardware address of the printer. See the "Communicating With the Users on Your System" chapter of this manual.
3. Copy `/usr/spool/lp/interface/`*printer_name* to a temporary location:

   ```
   cp /usr/spool/lp/interface/printer_name /usr/spool/lp/interface/printer_name.old
   ```

4. Remove the printer from the lp spooler; see the "Managing Printers and Printer Output" chapter of this manual. This procedure includes shutting down your lp spooler and disabling the printer.
5. Turn off, unplug, and disconnect the printer or plotter.
6. Add the newly located printer to the system at the new hardware address; see the *Installing Peripherals* manual or the "Managing Printers and Printer Output" chapter of this manual for additional information. if the printer is an HP-IB printer, ensure that the printer has a unique bus address.

Note Specify the temporary file (`/usr/spool/lp/interface/`*printer_name*`.old`) you created in step 3 for the model script when adding the printer to the system at the new hardware address.

---

7. Remove the temporary model script file (`/usr/spool/lp/interface/`*printer_name*`.old`) created in step 3.
8. If you changed the printer name, update any software application configurations that used the local printer. You may also need to update your software application if you refer to the hardware address of the printers on the system. Refer to your software application documentation for specific instructions.

Moving a Tape Drive

Moving a tape drive on your system requires that you remove the tape drive and then add the tape drive using the new hardware location.

Note It is recommended that you shut down and power off your computer while moving devices on the SCSI or HP-IB bus. For SCSI devices, it is important to power up your device before turning on your system.

To move a tape drive using HP-UX commands:

1. Ensure that you have superuser capabilities.
2. Notify the users on the system about system shutdown as a result of moving the tape drive. See the "Communicating With the Users on Your System" chapter of this manual.

Note It is recommended that you shut down and power off your computer while moving devices on the SCSI or HP-IB bus.

3. Remove any media currently loaded in the tape drive.
4. Shut down your system:

   ```
   cd /
   shutdown grace_period_in_seconds
   ```

   For additional information, see Chapter 3, "Starting and Stopping HP-UX" of this manual.
5. Halt the system:

   ```
   reboot -h
   ```

6. Turn off the computer.
7. Turn off, unplug, and disconnect the tape drive.
8. Physically move the tape drive. Refer to the documentation shipped with your disk drive if you intend to change the HP-IB or SCSI bus address. Ensure that each device on the SCSI or HP-IB bus has a unique bus address.
9. Turn on the tape drive.

Note For SCSI devices, it is important to power up your device before turning on your system.

---

10. Turn on the computer.
11. Log in. Ensure that you have superuser capabilities.
12. Add the tape drive to the system at the new hardware location; refer to the *Installing Peripherals* manual.
13. Modify any automated backup processes scheduled by the `cron` utility to reflect an updated device file for the tape drive. See the "Backing Up and Restoring Your Data" chapter of this manual and *cron*(1M) in the *HP-UX Reference*.
14. Reload media into the tape drive.
15. Update any software application configurations that used the moved tape drive. Refer to your software application documentation for specific instructions.

Moving a Terminal or Modem

Moving a terminal or modem on your system requires that you remove the terminal or modem and then add the terminal or modem using the new hardware location.

To move a terminal or modem using HP-UX commands:

1. Ensure that you have superuser capabilities.
2. If users will be affected, notify the users on the system about the device being moved. See the "Communicating With the Users on Your System" chapter of this manual. The terminal to be moved cannot be in use, it must be inactive.
3. Create a backup copy of the `/etc/inittab` file:

   ```
   cp /etc/inittab /etc/inittab.old
   ```

4. Turn off, unplug, and disconnect the terminal or modem.
5. Add the terminal or modem to the system at the new hardware location; refer to the *Installing Peripherals* manual.
6. Modify the `/etc/inittab` file to reflect the new device file for the terminal or modem.
7. Activate the updated `/etc/inittab` file; type:

   ```
   /etc/telinit q
   ```

8. Update any software application configurations that used the relocated terminal or modem. Refer to your software application documentation for specific instructions.

Moving the System Console

Moving the system console on your system requires that you update the Boot ROM console information in stable non-volatile memory.

Caution Making a mistake during this procedure could make your system inaccessible from the system console.

To move the system console using HP-UX commands:

1. Ensure that you have superuser capabilities.
2. This procedure requires you to reboot your system. Notify the users on the system about the system being unavailable for a short time. See the "Communicating With the Users on Your System" chapter of this manual.
3. Reboot your system:

   ```
   cd /
   /etc/shutdown -r time_period_in_seconds
   ```

4. Override the autoboot sequence. You need to enter the Boot ROM to perform system console hardware path configuration.
5. For Series 300 and Series 400 system consoles, select codes are scanned, starting with the built-in interfaces, until the first `remote` setting is encountered. If you are moving the system console from a built-in interface, you need to enter the Boot ROM to set the I/O configuration of the interface to `local`.
6. From the Boot ROM, save the configuration. Refer to the owner's guide shipped with your system.
7. Turn off the the system console and your computer.

8. Disconnect and reconnect the system console. Ensure that the hardware connections are properly seated.

   If you are moving your system console *to* an interface card, you need to check the hardware manual for the interface card to set the `remote` switch for the Boot ROM to recognize this interface as containing the system console.

   If you are moving your system console *from* an interface card, you need to set the `local` switch on the card to tell the Boot ROM that the system console is *not* located on the interface card.

   Look in the documentation shipped with the interface for the local and remote switch locations.

9. Turn on your system console and your computer. Your boot sequence should appear on your newly relocated system console.

Moving a Disk Drive Used for File Systems and Swap

Note	Moving the root disk is a special case and the instructions given in this section do not apply. Refer to "Moving a Disk Drive Containing the Root File System" in this chapter.

To move a disk drive used for file systems or swap using HP-UX commands:

1. Ensure that you have superuser capabilities.
2. Back up the disk drive to be moved; see the "Backing Up and Restoring Your Data" chapter of this manual.
3. Notify the users on the system about system shutdown as a result of moving the disk drive. See the "Communicating With the Users on Your System" chapter of this manual.
4. If your system is an NFS server and file systems on the disk you are moving are exported, unmount the file systems from the NFS client. If you do not unmount the file systems from the client, the client will receive NFS error messages when accessing the files on the disk.

   To find the NFS clients, log in to the NFS server and look at the `/etc/exports` file. Refer to *exports*(4) in the *HP-UX Reference*.

   Notify the users on the NFS client systems that data on the disk to be relocated will be temporarily inaccessible. See "Communicating With the Users on Your System".

   Log in directly to each NFS client and unmount the file systems using HP-UX commands. Refer to Chapter 6, "Managing the File System" for specific instructions on unmounting file systems.
5. Determine the hardware address for the new location. See Chapter 10, "System Architectures" in the *How HP-UX Works: Concepts for the System Administrator* manual.
6. Create a new device file for the disk using the `mknod` command. Refer to the *Installing Peripherals* manual for specific instructions for creating disk drive device files. The new hardware address will be reflected in the minor number.

7. Create a backup copy of the `/etc/checklist` file:

   `cp /etc/checklist /etc/checklist.old`

8. Edit `/etc/checklist` to update the device file associated with the file system to reflect the new device file.
9. Shut down your system:

   `cd /`

   `shutdown` *grace_period_in_seconds*

   For additional information, see Chapter 3, "Starting and Stopping HP-UX" of this manual.

10. Halt the system:

    `reboot -h`

5

11. Turn off the computer.
12. Turn off, unplug, and disconnect the disk drive.
13. Physically move the disk. Refer to the documentation shipped with your disk drive if you intend to change the HP-IB or SCSI bus address. Ensure that each device on the SCSI or HP-IB bus has a unique bus address.
14. Turn on the disk drive.

Note For SCSI devices, it is important to power up your device before turning bon your system.

---

15. Turn on the computer.
16. Log in. Ensure that you have superuser capabilities.
17. If your system is an NFS server, remount file system(s) on any NFS client systems. As superuser on the NFS client system(s), type:

    `/etc/mount -a`

18. Update any software application configurations that use the relocated disk drive. Refer to your software application documentation for specific instructions.

Moving a Disk Drive Containing the Root File System

moving using HP-UX commands| moving using HP-UX commands|

Moving a disk drive containing the root file system requires updating several system files and booting in attended mode to select the new root file system to boot from.

Note This procedure assumes that your root disk is accessible and functioning properly. This procedure does not describe repairing the data on your root disk.

To move the root disk drive using HP-UX commands:

5

1. Ensure that you have superuser capabilities.
2. Back up the disk drive to be moved; see the "Backing Up and Restoring Your Data" chapter of this manual.
3. Notify the users on the system about the system shutdown to move the root disk. See the "Communicating With the Users on Your System" chapter of this manual.

Note It is recommended that you shut down and power off your computer while physically moving devices on the SCSI or HP-IB bus.

---

4. If your system is an NFS server and file systems on the disk you are moving are exported, unmount the file systems from the NFS client. If you do not unmount the file systems from the client, the client will receive NFS error messages when accessing the files on the disk.

   To find the NFS clients, log in to the NFS server and look at the `/etc/exports` file. Refer to *exports*(4) in the *HP-UX Reference*.

   Notify the users on the NFS client systems that data on the disk to be relocated will be temporarily inaccessible. See "Communicating With the Users on Your System".

   Log in directly to each NFS client and unmount the file systems using HP-UX commands. Refer to Chapter 6, "Managing the File System" for specific instructions on unmounting file systems.

5. Determine the hardware address for the new location. See Chapter 10, "System Architectures" in the *How HP-UX Works: Concepts for the System Administrator* manual. 5

6. Create a new device file for the root disk using the **mknod** command. Refer to the *Installing Peripherals* manual for specific instructions for creating disk drive device files. The new hardware address will be reflected in the minor number.

7. Create a backup copy of the `/etc/checklist` file:

   ```
   cp /etc/checklist /etc/checklist.old
   ```

8. Edit `/etc/checklist` to update the device file associated with the root file system to reflect the new device file.

9. Shut down and halt your system:

```
cd /
/etc/shutdown -h time_in_seconds
```

10. Turn off the computer and the root disk drive.
11. Physically move and reconnect the disk drive to the new hardware address.
12. Turn on the disk drive.

Note For SCSI devices, it is important to power up your device before turning on your system.

---

13. Turn on the computer.

5

14. Override the autoboot sequence. You need to enter the Boot ROM to update the default boot hardware path configuration.
15. Reconfigure the Boot ROM's default boot hardware path to reflect your newly located root disk. Refer to your system's owner's guide to change the hardware path of the root disk.
16. Save the Boot ROM configuration. Refer to the owner's guide shipped with your system.
17. From the Boot ROM, boot from the newly located root disk. Refer to the owner's guide shipped with your system.
18. If your system is an NFS server, remount file system(s) on any NFS client systems. As superuser on the NFS client system(s), type:

```
/etc/mount -a
```

19. Update any software application configurations that use the relocated root disk. Refer to your software application documentation for specific instructions.

Removing Peripherals Using HP-UX Commands

If users will be affected, notify the users on the system of the device location change. See the "Communicating With the Users on Your System" chapter of this manual.

To remove peripherals:

1. Ensure that the device does not contain information critical to the operation of the system or users. For removing mass storage devices, copy critical data to another device.
2. Remove the device from your application software configuration. Refer to your software application documentation for specific instructions.
3. (optional) Remove the device from the HP-UX configuration:
   a. If there is no future need for a device of this type at this hardware address, remove the device file(s) associated with the device.
   b. If this is the only device of it's interface type and there is no future need for this device interface type on your system, reconfigure the kernel to remove the device driver. Removing the device driver can also reduce the physical size of the kernel (`/hp-ux`). See Chapter 2, "Constructing an HP-UX System".
4. Update any software application configurations that use the relocated local printer. Refer to your software application documentation for specific instructions.

Removing a Printer or Plotter

If you are removing a printer or plotter using HP-UX commands, see the "Managing Printers and Printer Output" chapter of this manual.

Update any software application configurations that use the removed printer. Refer to your software application documentation for specific instructions.

Removing a Tape Drive

To remove a tape drive using HP-UX commands:

1. Ensure that you have superuser capabilities.
2. Notify the users on the system about system shutdown as a result of removing a tape drive. See the "Communicating With the Users on Your System" chapter of this manual.

Note It is recommended that you shut down and power off your computer while physically removing devices from the SCSI or HP-IB bus.

---

3. Shut down your system:

   `cd /`

   `shutdown` *grace_period_in_seconds*

   For additional information, see Chapter 3, "Starting and Stopping HP-UX" of this manual.
4. Halt the system:

   `reboot -h`
5. Turn off the computer.
6. Remove any media currently loaded in the tape drive.
7. Turn off, unplug, and disconnect the tape drive.
8. Turn on the computer.
9. Log in. Ensure that you have superuser capabilities.
10. Remove/Modify any backup process scheduled by the `cron` utility that expect the tape drive to be present. See the "Backing Up and Restoring Your Data" chapter of this manual and *cron*(1M) in the *HP-UX Reference*.
11. Update any software application configurations that use the removed tape drive. Refer to your software application documentation for specific instructions.

Removing a Terminal and Modem

Note Removing the system console is not supported.

To remove a terminal or modem using HP-UX commands:

1. Ensure that you have superuser capabilities.
2. If users will be affected, notify the users on the system about the device being moved. See the "Communicating With the Users on Your System" chapter of this manual. The terminal or modem to be moved cannot be in use, it must be inactive.
3. Edit the `/etc/inittab` file to remove any `getty` entries for the terminal. Refer to *inittab*(4) in the *HP-UX Reference*.
4. Activate the updated `/etc/inittab` file; type:

   ```
   /etc/telinit q
   ```

5. Unplug and disconnect the terminal or modem.
6. Update any software application configurations that use the removed terminal or modem. Refer to your software application documentation for specific instructions.

Removing a Disk Drive Used for File Systems and Swap

Note Removing the disk containing the root file system is not possible. If you are moving the disk drive, see the "Moving a Disk Drive Used for File Systems or Swap" section of this chapter for further instruction.

To remove a disk drive using HP-UX commands:

1. Ensure that you have superuser capabilities.
2. Notify the users on the system about system shutdown as a result of removing a disk drive. See the "Communicating With the Users on Your System" chapter of this manual.

Note It is recommended that you shut down and power off your computer while adding to or removing devices from the SCSI or HP-IB bus.

3. If your system is an NFS server and file systems on the disk you are moving are exported, unmount the file systems from the NFS client. If you do not unmount the file systems from the client, the client will receive NFS error messages when accessing the files on the disk.

   To find the NFS clients, log in to the NFS server and look at the `/etc/exports` file. Refer to *exports*(4) in the *HP-UX Reference*.

   Notify the users on the NFS client systems that data on the disk to be relocated will be temporarily inaccessible. See "Communicating With the Users on Your System".

   Log in directly to each NFS client and unmount the file systems using HP-UX commands. Refer to Chapter 6, "Managing the File System" for specific instructions on unmounting file systems.
4. Update the `/etc/checklist` on all NFS client systems to remove the mount entries for file systems that are on the disk drive being removed.
5. Create a backup copy of the `/etc/checklist` file:

```
cp /etc/checklist /etc/checklist.old
```

6. Shut down your system; type:

   ```
   cd /
   shutdown grace_period_in_seconds
   ```

   For additional information, see Chapter 3, "Starting and Stopping HP-UX" of this manual.
7. Edit the **/etc/checklist** file to remove any mount entries for the disk being removed.
8. Halt the system:

   ```
   reboot -h
   ```

9. Turn off the computer.
10. Turn off, unplug, and disconnect the disk drive.
11. Turn on your system.
12. Log in. Ensure that you have superuser capabilities.
13. Update any software application configurations that use the removed disk drive. Refer to your software application documentation for specific instructions.

6

Managing the File System

As a system administrator responsible for managing your HP-UX file system, you will be performing the following major tasks:

- Creating file systems
- Adding and removing local and remote auxiliary file systems
- Monitoring and controlling the disk space consumed by users' files
- Moving a file system from one disk to another
- Adding or removing swap space in a file system (this is covered in the next chapter)

This chapter describes how to accomplish most of these tasks using both SAM and HP-UX commands. We recommend using the SAM utility because it enables you to perform many of these tasks easily and with less chance of errors.

There are some activities—those involving the use of disk quotas, for example—that the SAM utility cannot perform.

Terms Used in this Chapter

The following terms appear frequently in this chapter. You can scan the list now and refer to it later.

block device A hardware device that transmits and receives data in multiple-byte blocks (rather than by streams of individual bytes) or does block-buffered input/output.

block special file A special file associated with a mass storage device (such as a hard disk or tape cartridge drive) that transfers data in multiple-byte blocks, rather than in a series of individual bytes. See "device file."

CD-ROM file system A Read Only Memory file system on Compact Disk. You can read data from a CD-ROM file system, but you cannot write to one.

character special file A special file associated with I/O devices that transfer data byte-by-byte. Typical byte-mode I/O devices include printers, nine-track magnetic tape drives, and disk drives when accessed in "raw" mode. Disk drive access via character devices is typically faster than via block devices. Character device file are sometimes called "raw" device files.

cylinder On disk drives consisting of several disks, the arrangement of disk tracks under read/write heads that are in the same relative position.

device file A file used by the computer to communicate with a device. The file tells the operating system the location of the device and what device driver to use. There are block device files (used for transmitting data in multiple-byte blocks) and character device files (used for transmitting data byte-by-byte). Device files are typically stored in the `/dev` directory.

Block device files are stored in the directory `/dev/dsk`.

Character device file are stored in the directory `/dev/rdsk`.

device swap space A disk or disk section reserved exclusively as swap space.

disk quotas Disk usage limits that a system administrator can assign to users of a file system.

disk section A logical division or partition on a hard disk in which a file system or a swap location can be placed. On Series 300/400/700 computers, disks have only one section that can be used for file storage and/or swapping. (Series 600/800 computers, by contrast, can use disks that are partitioned in numerous sections.)

file system The organization of files on storage devices. The term "file system" can refer either to the entire file system tree or to a subsection of that file system contained on an individual disk, which can be mounted or unmounted from the tree.

fragment A part of a block. The end of a file that is not a whole block is typically stored as a fragment. The size of a fragment can be specified; the use of a small fragment size adversely affects performance but leaves less wasted space.

HFS file system A file system in which the files are arranged on a disk within hierarchical directories.

inode A data structure containing information about a file, such as file type, pointers to data, owner, group, and protection information.

kernel The actual operating system program that executes and runs, controlling the processes, hardware, file system, and so on.

long file names File names using more than 14 (but not exceeding 255) characters. Long file names are incompatible with file systems configured for short file names.

mount To add an auxiliary (removable) file system to an active existing file system.

mount directory A directory in an existing file system that serves as the root directory (the mount point) of a mounted file system.

mount point See **mount directory**.

NFS client A machine that mounts (via the network) a file system located on a remote **NFS server**.

NFS file system: A file system accessible over a network via the NFS Services product.

NFS server: A computer with local file systems that are being accessed via the network by remote computers, or **NFS clients**.

root directory: The highest level directory in a file system. In any mountable file system (any file system other than the `root` file system) the root directory is the mount directory.

The / directory, also known as the `root` directory, is the highest level in the HP-UX file system overall; the / file system cannot be unmounted because it contains the running operating system.

root file system: Or `root` (/); the file system that contains the kernel and other operating system files.

short file names: Files with names consisting of 14 or fewer characters. Short file names are compatible with file systems configured for long file names.

6

single-user mode: When a computer system is accessible to only one user, usually the system administrator.

swap space: Space on a disk used for storing the process image temporarily.

unmount: To remove an auxiliary file system from the existing file system.

Overview of HP-UX File Systems

This section briefly describes the types of file systems you will work with on your computer system. The manual *How HP-UX Works: Concepts for the System Administrator* discusses file systems conceptually and in detail.

What Does "File System" Mean?

In one sense, the word "file system" refers to the entire HP-UX file system tree, the organization of all files on the system.

The HP-UX file system is a hierarchical, upside down tree-like structure in which the files—like leaves—are at the bottom or the ends of a branching structure that leads upward through subdirectories to a single **root** (written "/") directory. A diagram of how a typical HP-UX file system structure appears to a user is shown in Figure 6-1.

```
                       /
     ---------------------------------------------
     |                 |                         |
    bin               usr                      users
     |                 |                         |
  -------         ------------            ----------------
  |     |          |          |            |              |
chown uname       adm        lib          bea            joe
                   |          |            |              |
         -----------    ---------     --------     ----------
         |         |    |        |    |      |      |        |
      messages  syslog  |        |  memos reports memos letters        |
                       mail    macros
                        |        |
                      -----   -----
                      |   |   |   |
                      |   |   an  mmt
                     bea joe
```

Figure 6-1. Typical HFS File System Structure

Mountable File Systems

The word "file system" also refers to the specific collection of files on a storage device such as a disk.

You can create the structure for a new file system on a disk by using the *newfs*(1M) command. You can also use SAM to create a file system. Once created, the file system, even though it is empty, encompasses the area on the disk in which it is created.

To use or access the file system, you need to **mount** that file system to the existing file system tree. Except for the `root` (/) file system on the system disk, you can mount and unmount all file systems on disks to and from the existing HP-UX file system tree.

You refer to an auxiliary file system by the name of the device file associated with the disk that contains the file system. You can **mount** the auxiliary file system by attaching it to a directory (the mount directory) in the root file system. Use the *mount*(1M) command, described later. You can also use SAM to mount and unmount file systems.

6

Figure 6-2 shows how you can mount a file system on one disk to the existing file system. In the example, the files on the disk, `/dev/dsk/cEd1s0` join the hierarchy of the existing file system at the mount directory `/users`.

```
BEFORE MOUNTING
     ---------------------          --------------------
     |       /           |          |       /          |
     |       |           |          |       |          |
     |  -------------    |          |  -------------   |
     |  |     |     |    |          |  |     |     |   |
     | bin   usr  users  |          | Al    Bea   Bob  |
     ---------------------          --------------------

           ROOT FILE SYSTEM            AUXILIARY FILE SYSTEM
           /dev/dsk/cEd0s0                /dev/dsk/cEd1s0

AFTER MOUNTING, using the command: mount /dev/dsk/cEd1s0 /users
                    ---------------------
                    |       /           |
                    |       |           |
                    |  -------------    |
                    |  |     |     |    |   /dev/dsk/cEd0s0
                    | bin   usr  users  |
                    ----------------|----
                           ---------|-----------
                           |  -------------    |
                           |  |     |     |    |
                           | Al    Bea   Bob   |   /dev/dsk/cEd1s0
                           ---------------------
```

Figure 6-2. Mounting an Auxiliary File System

You can unmount a file system, too, and then mount it again at a different mount point.

When users traverse the file system, they can move from the `/` directory to the files in `/users/Bob` as easily as they can move from `/` to the files in `/usr` even though `/usr` and `/users/Bob` are on different disks. As a user moves from one part of the HP-UX file system to another, it isn't apparent that the file system actually consists of separate file systems on different devices.

Listing Mounted File Systems

To see a list of the file systems mounted on your system, use the *bdf*(1M) command. For example:

```
bdf
Filesystem           kbytes    used   avail capacity Mounted on
/dev/dsk/cEd0s0      484960  239992  196472    55%    /
/dev/dsk/cEd1s0      237810   47943  166086    22%    /users
 .
 .
```

In the above example listing, the file system on disk with the device file `/dev/dsk/cEd1s0` is mounted at the mount directory `/users` on the root (`/`) file system in `/dev/dsk/cEd0s0` . You can see this in Figure 6-2.

6

Types of File Systems

The principal types of file systems used by HP-UX are the **HFS**—or high performance file system, the **NFS**, or network file system, and the **CDFS**, or CD-ROM file system.

HFS File Systems. HFS is an acronym for High-performance File System. HFS file systems physically reside on mass storage devices, usually hard disk drives.

NFS File Systems. NFS is an acronym for Network File Services. NFS file systems are remote HFS file systems that are accessible over a network that can be used in a local file system.

CD-ROM File Systems. CD-ROM is an acronym for Compact Disk Read-Only Memory. The information on the CD is virtually permanent; you can read data from a CD, but you cannot write to one. Data on a CD is prepared and mastered using a specialized publishing process. A CD-ROM file system (CDFS) allows easy retrieval of large amounts of information that requires no modification.

The arrangement of files in a CD-ROM file system is tree-like as in HFS file systems. You can use HP-UX commands to list, print, or copy files in the CD-ROM file system. However, some commands, such as `fsck` or `mkfs` for example, are not supported because of the read-only nature of a CD-ROM file system.

Disk Layout

When you add a disk to the system, you can designate how the space on the disk is to be proportioned between file system space and space for swapping (swap space is discussed in detail in the chapter, "Managing Swap Space"). The file `/etc/disktab` shows listing of the various possible layouts available for supported disks. Some examples in this chapter demonstrate the use of `/etc/disktab`.

HP-UX System Files

Many important system files are located in the directories and subdirectories of the `root` (/) file system, described in Table 6-1.

Table 6-1. Root File System Subdirectories

Directory	Contents
/bin	Compiled, often-used commands.
/dev	Block and character special device files used to communicate with devices. See *mknod*(1M) in the *HP-UX Reference*.
/etc	Most system administrator commands and configuration (customization) files.
/etc/newconfig	Customized configuration files and shell scripts during an update so you can use them for reference. You typically copy many of these files back into `/etc`. The `/etc/newconfig/README` file contains useful information about files in `/etc/newconfig`.
/etc/conf	Kernel configuration description files.
/etc/filesets	A list of loaded filesets.
/lib	Object code libraries and related utilities.
/mnt	User's home directories (usually).
/system	Revision lists and customize scripts from installation.
/tmp	Temporary files.
/usr	Commands and log files.
/usr/adm	System administration data files.

6

Table 6-1. Root File System Subdirectories (Continued)

Directory	Contents
/usr/bin	Commands not required to boot, restore, or repair the file system.
/usr/contrib	Files and commands contributed by user groups.
/usr/contrib/bin	Contributed commands.
/usr/contrib/lib	Contributed object libraries.
/usr/contrib/man	On-line documentation for contributed commands.
/usr/diag	Diagnostic tools.
/usr/include	High-level C language header files; the shared definitions.
/usr/include/local	Site-specific C language header files.
/usr/include/sys	Low-level, kernel-related C language header files.
/usr/lib	Less-used object-code libraries, utilities, lp commands, and miscellaneous data files.
/usr/lib/uucp	Configuration files for UUCP at install.
/usr/local	Localized, site-specific files.
/usr/local/bin	Localized, site-specific commands.
/usr/local/lib	Object code libraries for the site-specific commands.
/usr/local/man	On-line documentation for the site-specific commands.

6

Table 6-1. Root File System Subdirectories (Continued)

Directory	Contents
/lost+found	Orphaned files and directories created by **newfs** and used by **fsck**.
/usr/mail	Used by the mail facilities for your mail box.
/usr/news	System-wide news files.
/usr/spool	Spooled (queued) files for various programs.
/usr/spool/cron	Spooled jobs for **cron** and **at**.
/usr/spool/lp	Control and working files for the **lp** spooler.
/usr/spool/uucp	Queued work files, lock files, log files, status files, and other files for UUCP.
/usr/spool/uucppublic	Files freely accessible to remote systems via LAN and **uucp**.
/usr/tmp	Temporary large files.
/usr/man	All shipped on-line documentation.
/usr/man/cat1 ... cat9	On-line documentation that has already processed to speed up access.
/usr/man/cat1.Z ... cat9.Z	Compressed versions of **cat** directories.
/usr/man/man1 ... man9	The unformatted on-line documentation pages.
/usr/man/cat1.Z ... cat9.Z	Compressed versions of the on-line documentation pages.

Creating File Systems

You can expand your file system using one of the following methods:

- **Add a new disk drive and create a file system on it.** To add a disk to your system and create a file system on it, use either SAM or a combination of HP-UX commands directly.

  See the sections, "Adding a Disk and Creating a File System Using SAM" and "Adding a Disk and Creating a File System Using HP-UX Commands" later in this chapter.

- **Add a disk with an existing file system and mount the file system.** See "Using SAM to Mount an Existing File System on a Disk from Another System".

- **Mount an existing auxiliary file system that is now unmounted.** Use either SAM or HP-UX commands to do this.

  See the section "Mounting File Systems" later in this chapter.

We recommend you use SAM, when possible, because SAM can usually accomplish these tasks more easily and with less chance of error.

Adding a Disk and Creating a File System Using SAM

You can expand your file system by adding a new disk. The following lists the steps you might take to add a new disk using SAM.

How to Use SAM

To use SAM,

- Ensure that you have superuser capabilities.
- Type:

  `/usr/bin/sam`

  Activating the (Help) button from a dialog or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

  Choosing an item from the "Help" menu within a functional area gives you information about:

  - the current functional area
  - keyboard navigation within SAM
  - using the SAM help system
  - displaying the version of SAM you are currently running

Pressing the (f1) key gives you context-sensitive information for the object field at the location of the cursor.

See Chapter 1, "Introduction to System Administration" for additional information about using SAM. If you aren't familiar with SAM, take a moment to look at that overview material. There is a help system in SAM to assist you.

6

Adding a Disk and Creating a File System Using SAM

Note the following procedure creates a file system that uses the entire disk. If you want to create a file system and reserve space for swap, refer to the procedure described in the next chapter, "Adding Device Swap When Creating a File System."

Refer to the *Installing Peripherals* manual for instructions on adding your disk. When you have added the disk and restarted your computer, you can create a file system using SAM as follows:

1. Run SAM.
2. Highlight `Disks and File Systems->` and activate the (Open) control button.
3. Highlight `Local file Systems` and activate the (Open) control button.
4. When the list of local file systems is displayed, from "Actions" on the menu bar, choose `Add...`.
5. Highlight the disk you are adding from the list that appears in the "Select a disk" field.

   If the disk you are adding is not on the list of unused disks:

   - Activate the `Device Missing...` control box. SAM will now direct you through a diagnostic process that enables you to configure your disk.

     Some of the things SAM will ask you to check are:

     - Whether the device is turned on.
     - Whether the device was on when SAM started.
     - The connections.
     - Whether the driver for the disk is configured in the kernel.

   When you have successfully added your disk, you can resume.
6. Enter the name of a new or an existing empty directory in the field: `Mount Directory:`. This is where the new file system will join the existing file system hierarchy. If the directory you specify does not exist, SAM will create it for you.

7. Skip the `Modify Default Options......` control button, unless you want to change `When to Mount`, the `Access Permissions`, or the `Set user ID` default settings. If you want to modify the default options, SAM's (Help) can provide information.
8. Activate the (OK) control button to have SAM create the new file system.

   If there is any data in the disk section, SAM will ask you to confirm that it is alright to proceed with creating the file system.

   As SAM creates the new file system, it creates new device files for the disk, mounts the file system, and adds the file system to `/etc/checklist` (so you can have the file system mounted each time you boot the system).

   Activate (OK) to acknowledge SAM's actions and wait for SAM to add the new file system to the `Local File System` list. The file system is ready for use.

Adding a Disk and Creating a File System Using HP-UX Commands

Complete the following steps to expand your file system when adding a disk. The procedures employ the direct use of HP-UX commands. Details and examples for each of the steps will follow.

1. Install your disk.
2. Create block and character device files for the disk.
3. Run `mediainit` to initialize the disk, if necessary.
4. Run `newfs` to create the file system.

1. Installing Your Disk

To install your disk drive, refer to the documentation that came with your disk and to the *Installing Peripherals* manual. They will describe making the physical connections, determining the physical address of your disk, and adding the disk to your system's I/O configuration.

6

2. Creating the Block and Character Device Files for Your Disk

You need to have both *character* and *block* device files for the disk you are adding. For example, you will need to refer to the *character* device file when you use the `newfs` command to create the file system, and you will need to use the *block* device file with other commands such as `swapon`. Conceptual details about device files are in the manual *How HP-UX Works: Concepts for the System Administrator*.

You can create device files using the `/etc/mknod` command.

The `mknod` command has the following syntax:

`mknod` *name type major_number minor_number*

where:

name	The pathname for the file to be created.
type	Either `b` (for a block device) or `c` (for a character device).
major_number	Specifies the device driver number. Use the command `lsdev` to see a list of the major numbers for device drivers that are configured in your kernel.
minor_number	Specifies information about the device and its location in hexadecimal notation.

Examples, Creating Block and Character Device Files

- Creating the *block* device file.

  For this example, suppose you are adding an HP-IB disk to the interface card with a select code setting of 14, and have set the bus address on the disk to 2. To make the *block* device file for the disk, use the following command:

  ```
  /etc/mknod /dev/dsk/cEd2s0 b 0 0x0e0200
  ```

  In the device file name, `/dev/dsk/cEd2s0`, `/dev/dsk` is the directory for block device files. The device file, `cEd2s0`, has the following significance:

  - `c`*N*`d` - where *N* is a hexadecimal number (uppercase alphabetical characters) that signifies the disk's controller; that is, the select code set on the interface card.
  - *n*`s0` - where *n* is a hexadecimal number (uppercase alphabetical characters) that signifies the bus address set on the disk drive. `s0` signifies the section number; always `s0` for standard hard disks.

  There are other conventions for naming device files. For example, you can assign individual device file names for individual platters and sides of platters in the case of optical disk libraries, and you can assign device files to disks in hardware-based disk arrays. See *Installing Peripherals* for details if you are creating device files for these types of disks.

In the next fields, `b` specifies that the device file is being created for a block device and `0` is the major number for an HP-IB type disk used as a block device. Typing `/etc/lsdev` lists major numbers for drivers configured in the kernel; for example, you might see the following (an HP-IB disk, in this case, is a CS80 disk): following:

```
Character      Block      Driver
    .            .          .
    .            .          .
    4            0          CS80 disk
    .            .          .
```

The minor number is `0x0e0200`. This number signifies that the device is at select code 14 (`0e`) and uses bus address 2 (`02`). (`0x` indicates the number is hexadecimal; the final `00` doesn't apply to this example.)

Note

Detailed discussions of major and minor numbers are contained in the manual *Installing Peripherals*. See also *How HP-UX Works: Concepts for the System Administrator*.

- Creating the *character* device file.

  Just as you used `mknod` to make the block device file, you can use it to make the *character* device file. For example, you can use the following command:

  `/etc/mknod /dev/rdsk/cEd2s0 c 4 0x0e0200`

  `rdsk` is the directory used for the character device files for disks. `c` specifies the file is for character devices and `4` specifies the major number for a CS80 type disk used as a character device. Notice that the minor number and the device file name `cEd2s0`, are the same as were used when making the block device file.

- Listing the Device Files.

  You can list device files on your system.

  For example, listing the files with the `ll` command in `/dev/dsk` directory might yield the following:

```
total 0
brw-r-----   1 root     sys         7 0x0e0000 Aug  3 13:11 cEd0s0
brw-r-----   1 root     sys         7 0x0e0100 Jul 25 12:53 cEd1s0
brw-r-----   1 root     sys         7 0x0e0200 Aug 13 13:11 cEd2s0
```

  The third line in the listing shows the block device file created in the previous section.

6

3. Initializing Your Disk Using mediainit

New hard disks from Hewlett-Packard have been initialized at the factory. If your disk has been initialized, it is not necessary to initialize it again.

Caution *Do not* initialize a disk that contains data you need. Initializing will destroy any existing data on a disk.

It takes approximately an hour, maybe more, to initialize a disk. Refer to *mediainit*(1) in the *HP-UX Reference*.

4. Creating a New File System Using newfs

The recommended command for creating a file system on a disk is *newfs*(1M). The `newfs` command is a friendlier interface to the *mkfs*(1M) utility. Therefore, as you use `newfs`, you might be specifying `mkfs` options.

You can use `newfs` command without options, creating a file system based on the described in `/etc/disktab` for the type of disk you are adding. However, by using the options, you can use `newfs` to:

- Choose a maximum file name length, long or short.
- Modify the `mkfs` options that specify the way space is used in a file system.
- Determine the way the space on a disk is divided between a file system and swap space.

The `newfs` utility has the following syntax:

`newfs` [`-L` | `-S`] [`-n`] [`-v`] [*mkfs-options*] *device_file disk_type*

where:

-L	Creates a file system with long file names (up to 255 characters).
-S	Creates a file system with short file names, 14 characters maximum. By default, `newfs` will create the same type as the `root` file system. See the next section "Using -L or -S to Determine File Name Length".
-v	Specifies verbose mode, which lists `newfs` actions.
mkfs-options	These options override the default `mkfs` parameters (the `newfs` utility calls `mkfs`). Table 6-2 later in this section describes these parameters. The following are those most commonly changed. -b *blksize* — block size in bytes, defined in `/etc/disktab` -f *fragsize* — fragment size in bytes, defined in `/etc/disktab` -m *minfree* — default is 10% of file system space reserved from normal use -i *nbpi* — default is 2048 bytes per inode
device_file	The *character* device file name for the disk on which you are creating the file system.
disk_type	The type of disk, as defined in `/etc/disktab`.

6

Using -L or -S to Determine File Name Length

- Choosing File Name Length.

  By default, `newfs` creates a file system of the same type as the `root` (/) file system. However, you can explicitly specify the type of file system with either `-L`, which indicates a file system that allows long file names, or `-S`, which indicates a file system that permits only short file names.

- Long vs. Short File Names.

  When configured with the short file names, HP-UX file systems are compatible with earlier system releases that are not configured to accept long file names. Typically, file systems are configured with short file names.

  Generally, long file names (the 255 character limit) provide flexibility in naming files. Also, files created on other systems that allow long file names can be moved to your system without being renamed.

  Avoid long file names if:

  - You plan to use applications that read directory file information and do not use portable directory routines like those described in *directory*(3C) in *HP-UX Reference*. If these applications assume that directories are in an array of fixed-size entries, they will not work with long file names. To correct this, rewrite the application to correct the assumptions about directories using the directory file information required by long file names.
  - Programs (with no source code available) that were developed for or compiled on releases of HP-UX that do not support long file names will be run on the system.
  - Other systems in your organization run versions of HP-UX that impose a 14 character limit on file name length. In this environment, you might want uniformity across the systems so that files can be moved between systems.

See the section later in this chapter entitled "Modifying File Name Length".

Overriding the Default mkfs File System Parameters

Table 6-2 provides a reference for the `mkfs` file system parameters.

Table 6-2. File System Parameters

Parameter	/etc/disktab Names	Range	Default
file system size	s0#	defined in /etc/disktab	none
block-size	b0#	4096 bytes (4KB), 8192 bytes (8KB), 16,384 bytes (16KB), 32,768 bytes (32KB), or 65,536 bytes (64KB)	8192 bytes (8KB)
frag-size	f0#	1024 (1KB) to 8192 (8KB); fragment size must be at least one-eighth block-size	1024 bytes (1KB)
% space reserved	N/A	0 to 100	10 %
number of bytes per inode	N/A	1 to (function of file system size and other parameters)	2048 bytes (2KB)

The following sections discuss overriding the `mkfs` parameters.

Overriding the Default Block and Fragment Values. Configuring blocks and fragments represent a time/space trade-off. The larger the block size, the greater the access speed. However, more disk space is wasted. You can use one of the following suggested block and fragment combinations for the listed file systems (block size/fragment size):

- `/tmp` is usually 8K/8K to allow quick access. Most files in this directory are temporary. Therefore, wasting space is not a problem here.
- `/usr` is 8K/1K, which is the median trade-off between speed and space utilization.
- `/mnt` is usually 4K/1K because files that reside here are typically small and remain for a long time.

Table 6-2 describes the ranges. The `newfs -b` *blksize* parameter specifies the block size in bytes and the `newfs -f` *fragsize* parameter specifies the fragment size in bytes.

Overriding the Default Reserved Disk Space. The value of *minfree* is the percentage of disk space reserved for the superuser when the file system fills up. It allows the superuser to reserve space for system use. The file system throughput degrades as the number of choices for free blocks is reduced. By setting *minfree* at 10%, which is the default, you are ensuring that the file system throughput will not degrade significantly.

Decreasing the value of the *minfree* parameter lets you write to an additional percentage of file system space. The lower the percentage, the greater the possibility that your file's blocks will be scattered on the disk. Performance decreases as the disk fills up.

Overriding the Default Bytes Per Inode. The *nbpi* parameter dictates the relationship between the number of data bytes on the disk and the number of inodes allocated on the disk. Each file requires an inode. If you increase the number of bytes per inode, you are asking for fewer inodes. The default is to create one inode for every 2048 bytes of data space.

If your system has many small files, you can decrease the average number of bytes per inode. This gives you more inodes, and lets you create more (but smaller) files. Having many inodes takes more space on your file system.

If your system has a few large files, you can increase the space available for data by increasing the average number of bytes per inode.

Determining Disk Type

The `/etc/disktab` file describes the file system layouts and parameters for supported disks; the value you specify for *disk_type* in the `newfs` command line must match an entry in `/etc/disktab`. For the HP 2203A disk, `/etc/disktab` lists five configurations.

The listing in the file looks like the following:

```
# HP2203A has 671 MBytes
#         256 Bytes/sector
#         113 sectors/track;  16 heads;  1449 cylinders;
#       Total: 654948 1K sectors
hp2203A|hp670H|hp2203|hp22030:\
        :64 MBytes reserved for swap & boot:ns#113:nt#4:nc#1304:\
        :s0#589408:b0#8192:f0#1024:\
        :se#256:rm#4002:
hp2203A_96MB|hp670H_96MB|hp22030_96MB:\
        :96 MBytes reserved for swap & boot:ns#113:nt#4:nc#1231:\
        :s0#556412:b0#8192:f0#1024:\
        :se#256:rm#4002:
hp2203A_42MB|hp670H_42MB|hp22030_42MB:\
        :42 MBytes reserved for swap & boot:ns#113:nt#4:nc#1353:\
        :s0#611556:b0#8192:f0#1024:\
        :se#256:rm#4002:
hp2203A_noreserve|hp2203A_noswap|hp670H_noreserve|hp670H_noswap:\
        :no swap or boot:ns#113:nt#4:nc#1449:\
        :s0#654948:b0#8192:f0#1024:\
        :se#256:rm#4002:
hp22030_noreserve|hp22030_noswap:\
        :no swap or boot:ns#113:nt#4:nc#1449:\
        :s0#654948:b0#8192:f0#1024:\
        :se#256:rm#4002:
###############################################
.
.
```

For example, the listing that reads `hp2203A_96MB` describes the disk layout geometry for an HP 2203A disk that will reserve 96MB of disk space for swap.

Example, Creating a File System Using `newfs` Without Options

If you decide to accept the file system defaults, no options are required for the `newfs` command.

In the examples that follow, let's assume you want to add a disk and use it in part for a file system and in part for swap. You have connected an HP 2203A disk to the HP-IB internal interface card. After checking the optional disk layouts for the HP 2203A in `/etc/disktab`, you determine that the layout that reserves a space of 42 MB for swap and boot is appropriate.

So, using the character device file you created previously, issue the `newfs` command to create the file system:

```
newfs /dev/rdsk/cEd2s0 hp2203A_42MB
```

Now, you can add the new file system to your existing file system. See "Mounting File Systems" later in this chapter. Also, the swap area can now be enabled for use; refer to Chapter 7, "Managing Swap Space".

Another Example, Creating a File System with Smaller Block Size

Let's assume that you want to set up a file system that will contain many small files. To avoid wasting space, you decide to set up the file system with a smaller file system block size. You check the `/etc/disktab` file and find the following description for your HP 2203A disk:

```
hp2203A_42MB|hp670H_42MB|hp22030_42MB:\
        :42 MBytes reserved for swap & boot:ns#113:nt#4:nc#1353:\
        :s0#611556:b0#8192:f0#1024:\
        :se#256:rm#4002:
```

The default block size (`b0#`) is 8192 bytes. You can specify a block size of 4096 bytes when you issue the `newfs` command:

```
newfs -b 4096 /dev/rdsk/cEd2s0 hp2203A_42MB
```

The file system built matches the description in `/etc/disktab` with the exception of the block size, which is now 4096 bytes.

6

After Creating a File System

After you have created a file system, you can add it, or mount it, to your existing file system by using SAM or the the HP-UX `mount` command. The next section in this chapter, "Mounting File Systems," explains how to do this.

If you created a file system on your disk and used an option from `/etc/disktab` that specified a swap area, you can enable that swap area by using SAM or the `swapon` command. Refer to Chapter 7, "Managing Swap Space" for discussion and examples.

6

Mounting File Systems

Mounting a file system links the file system contained on a specific device to a directory (the mount directory) in the existing file system tree. Once mounted, a file system becomes accessible to users. Figure 6-2 earlier in this chapter shows the relationship of a mounted file system to the existing file system.

Unmounted file systems are inaccessible to users. Unmounting a file system removes its files from the existing file system's hierarchy. The files themselves remain on the disk and can be accessed by mounting the file system again. Mounted file systems are automatically unmounted at shutdown time. The / file system cannot be unmounted.

You can use SAM or use HP-UX commands directly to mount or unmount file systems.

If you create a file system using *newfs*(1M), you can mount it using the *mount*(1M) command. See "Mounting File Systems Using HP-UX Commands".

The Mount Directory

The mount directory becomes the root directory for the file system you add. The mount directory should be an empty subdirectory on the existing file system. Create the directory using *mkdir*(1M) if it does not exist. To specify the mount directory, indicate the full absolute path name.

If you specify a non-empty directory for the mount point, any files in the mount point directory will be inaccessible when the new file system is mounted. The files will still exist, but they will remain inaccessible until you unmount the overlaying file system. Therefore, do not mount a file system over data that you will need later.

Mounting and Unmounting File Systems Using SAM

You can mount and unmount local file systems using SAM. Local file systems are file systems present on disks that are connected directly to the computer.

When you use SAM to create a file system, you have the option to mount the file system at that time, each time you boot the system, or both.

You might want to change some of the file system's characteristics, in which case it must be unmounted and remounted with the changed characteristics. SAM can do this automatically. If you want to change the file system's permissions, for example, SAM can automatically unmount the file system, change its permissions, and remount it.

Note If you want to access file systems located on remote computers, you can "NFS mount" them. Sam also enables you to do this. Go to the section, "Mounting and Unmounting NFS File Systems Using SAM".

Mounting and Unmounting Local File Systems Using SAM

6

1. Run SAM.
2. Highlight `Disks and File Systems->` and activate the (Open) control button.
3. Highlight `Local File Systems` and activate the (Open) control button.
4. Highlight the file system you want to mount or unmount.
5. From "Actions" on the menu bar, choose `Modify...`.
6. In the field labeled "When to Mount", modify the `Now` or `At Every System Boot` control buttons.

   If you indicate you do not want the file system mounted "At Every System Boot," SAM removes an entry from the `/etc/checklist` file.

Note You cannot unmount the `/` file system.

Modifying a File System's Characteristics Using SAM

Once you have added your file system, you might find that you want to:

- Discontinue having the file system automatically mounted when the system boots.
- Change the mount point directory for a file system.
- Unmount the file system temporarily.
- Change the permissions for a file system.
- Change the "set user ID" condition.
- Modify other file system options.

You can implement these changes from the `Modify a File System Screen` in SAM.

1. Run SAM.
2. Highlight `Disks and File Systems->` and activate the (Open) control button.
3. Highlight `Local File Systems` and activate the (Open) control button.
4. Highlight the file system you want to mount or unmount.
5. From "Actions" on the menu bar, choose `Modify...`.
6. Make changes you want to make by activating the appropriate control buttons for when to mount, access permissions, and set user ID conditions.

   Enter other options you want implemented for the file system in the field: `Additional Options:`. For example, you can enter "`quota`" to turn on disk quotas for this file system. (Except for activating the `quota` mount option, SAM does not perform disk quota activities. Refer to the sections "Using Disk Quotas").

Using SAM to Mount an Existing File System on a Disk from Another System

If you move a disk that contains a file system from one system to another, you can use SAM to mount the file system. However, you must add the disk to your system first.

1. Add the disk to your system following the procedure in the *Installing Peripherals* manual. Make sure the disk is turned on.
2. Run SAM.
3. Highlight `Disks and File Systems->` and activate the (Open) control button.
4. Highlight `CD-ROM, Floppy, and Hard Disks->` and activate the (Open) control button.
5. Highlight the new disk that will appear on the list of disks. At this time, the list will indicate that the disk is "unused."
6. From "Actions" on the menu bar, choose `Add a Hard Disk Drive...`.
7. In the next screen, activate the "Select a Disk to Add ... " menu bar. From the list that SAM presents, highlight the disk you are adding and activate the (OK) control button.
8. Activate the "Set Disk Usage and Options ... " menu.
9. In the "Use disk for" field, choose "File System."
10. Enter a mount directory name in the "Mount Directory" field. The mount directory is where the file system on the disk you are adding will join the existing file system hierarchy. If the directory you specify does not exist, SAM will create it for you.
11. Make sure to deactivate the "Create new file system" control button, because the file system already exists.

12. Skip the "Modify Defaults" control button, unless you want to change the defaults for when the file system is mounted, the permissions, or the set user ID condition. To review the defaults, activate the control button, view the settings, and activate the (Cancel) button.
13. Activate (OK) to mount the file system on the added disk.
14. The new disk will now show "`hfs`" under the "Use" column on the list of "CD-ROM, Floppy, and Hard Disks." The file system is ready to use if you had chosen to have it mounted now.

6

Mounting File Systems Using HP-UX Commands

If you are not using SAM to mount a file system, you can use the **mount** command. See *mount*(1M) in the *HP-UX Reference*. The **mount** command attaches an auxiliary file system existing on a specific device to a mount directory in the existing local file system. The auxiliary file system can be on a disk connected to your system or it can be a file system that is part of a remote file system (that is, an NFS type file system).

The **mount** command updates the file **/etc/mnttab**, which lists the existing mounted file systems. The contents of **/etc/mnttab** are displayed when you enter the command **mount** without arguments.

Syntax of the mount command

The *mount*(1M) command has the following basic syntax:

`mount` *sfname directory*

where:

6

sfname is the name of the block device file associated with the device containing the file system to be mounted. For example, you might specify the disk with the block device file, /dev/dsk/cEd2s0.

If you are specifying a system on a remote file system, use the form: *host:path*. For example,

```
hpfcd:/build
```

See the section, "Mounting and Unmounting NFS File Systems Using SAM".

directory the mount point directory, that is, the directory in the existing file system where the file system is to be mounted.

The **mount** command has many options that are fully described in the *mount*(1M) manual page in *HP-UX Reference*. The examples that follow will show the use of some options.

Using the mount Command to Add a File System

To use the mount command to add a file system, follow the steps outlined below. Examples follow.

1. If necessary, connect the disk containing the file system to your computer. To install your disk, refer to the documentation that came with your disk. The *Installing Peripherals* manual will help you verify that the device driver required for your disk is configured in the system's kernel.
2. Determine the device file for the disk containing the file system. If device files for the disk do not exist, you can create them using the mknod command.
3. Determine the mount point directory for the file system. Use the mkdir command to create the directory if it does not yet exist.
4. Determine which mount command options—if any—to use when you mount the file system.
5. Use the mount command to add the file system.
6. Edit the file /etc/checklist to have the file system mounted when you boot your system.

6

Example

Suppose you want to add the file system on an HP-IB disk that has the device file /dev/dsk/c7d2s0. The disk contains the files of most of the users of the system, so you will specify the empty directory /users as the mount point directory for file system. Type:

```
mount /dev/dsk/c7d2s0 /users
```

This command mounts (attaches) the file system on the disk using the device file /dev/dsk/c7d2s0 to the mount point /users.

After mounting the file system, you can edit the /etc/checklist file so that the file system is automatically mounted each time you boot the system. Refer to the section "Automatically Mounting Your File Systems at Bootup" for details concerning adding entries to the /etc/checklist file. For the file system mounted above, you would add a line in the checklist file such as:

```
/dev/dsk/c7d2s0   /users   hfs   defaults   0   3   # users
```

Note If an HFS file system has been unmounted improperly and not checked for inconsistencies with the *fsck*(1M) utility, the `mount` command will not be able to mount the file system. Run `fsck` on that file system before attempting to remount it. For information on using the `fsck` utility, refer to Chapter 6, "File System Problems" and Appendix A, "Using the fsck Command" in the *Solving HP-UX Problems* manual. Also see *fsck*(1M) in the *HP-UX Reference*.

Example

Suppose you want to mount a file system and have that file system be read-only. You would use the command:

```
mount /dev/dsk/cEd2s0 /users -o ro
```

In this example, the read-only option is specified by `-o ro`; the `-o` signifier must precede many `mount` command options. You can specify other options (such as options for setting user ID execution or disk quotas), which must be preceded by `-o`.

6

For this file system, you can add a line in the `/etc/checklist` file such as:

```
/dev/dsk/cEd2s0   /users   hfs   ro   0   3   # users
```

See the section "Automatically Mounting Your File Systems at Bootup" for a detailed discussion of making entries for the `/etc/checklist` file.

Adding a CD-ROM File System

Before you can mount CD-ROM file systems, your system's kernel must be configured for the `cdfs` subsystem.

Note In an HP-UX cluster, CD-ROM file systems can be mounted only on the cluster server.

Suppose you wanted to mount a CD-ROM file system at the mount directory `/users/reference`. If the appropriate device file for the disk is `/dev/dsk/cEd4s0`, you would enter:

```
mount /dev/dsk/cEd4s0 /users/reference -t cdfs
```

where `-t` specifies that a file system of the type `cdfs` is being mounted.

Note CD-ROM file systems are read only.

To have a `cdfs` file system mounted automatically at bootup, you can:

- Include a listing for the file system in `/etc/checklist`
- Add a line in the `/etc/rc` file, in the section called `localrc()`

  See "Automatically Mounting Your File Systems at Bootup".

Mounting and Unmounting NFS File Systems Using SAM

You can mount and unmount NFS file systems using SAM.

Before you can mount file systems located on a remote system, or before a remote system can mount a file system on a local machine, NFS Services software must be installed and configured on both local and remote systems. Refer to the manual *Installing and Administrating NFS Services* for the necessary and detailed information.

When configuring NFS file systems in SAM,

- Note that a machine can be an NFS server (export file systems), an NFS client (mount remote file systems), or both.
- Both for the **NFS Server** (the system where the file systems reside, which is the machine exporting the file sytems) and for the **NFS Client** (the machine where remote file systems are mounted), entries must exist in the `/etc/hosts` file. SAM makes these entries automatically.

Configuring a Local File System for Export

6

Configuring a local file system for export means that the local machine will be the server for a local file system that can be mounted by remote clients.

1. Highlight `Disks and File Systems->` and activate the Open control button.
2. Highlight `Networked File Systems (NFS)->` and activate the Open control button.
3. Highlight `Local File Systems Exported` and activate the Open control button.
4. From "Actions" on the menu bar, choose `Add...`.
5. Enter the name of the local file system to export in `Local Directory Name:` field. Accept the default settings on the remainder of the fields, unless you want to modify them.
6. Activate OK to set up the local file system to be exported.

Enabling or Disabling the Server File System

You can enable or disable an exported file system from being mounted by clients. In the "Local File System Exported" Screen:

1. Highlight the file system for export.
    a. If the NFS server is "Disabled," from "Actions" on the menu bar, choose `Enable NFS Server`. This enables a local file system to be mounted on remote systems.
    b. If the NFS server is "Enabled," from "Actions" on the menu bar, choose `Disable NFS Server`. This disables a local file system to be exported to remote systems.

To Make Remote Systems Clients of a Local File System

1. Highlight the file system for export.
2. From "Actions" on the menu bar, choose `View Directory Access`.
3. Add the machine name in the appropriate field for the type of access desired.

6

Mounting Remote File Systems

Mounting a remote file system means that a local machine becomes a client for a file system that is being exported from a remote server.

1. Highlight `Disks and File Systems->` and activate the (Open) control button.
2. Highlight `Network File Systems (NFS)->` and activate the (Open) control button.
3. Highlight `Remote File Systems Mounted` and activate the (Open) control button.
4. From "Actions" on the menu bar, choose `Add Remote Directory...`.
5. Enter a name in the `Remote System Name` field.
6. Enter a name in the `Remote Directory Name` field.

7. Enter a name in the `Local Directory Name` field.

   Accept the default settings on the remainder of the fields, unless you want to modify them.

8. Activate (OK) to enable the local file system to be exported.

Unmounting a Remote File System

1. Highlight `Disks and File Systems->` and activate the (Open) control button.
2. Highlight `Network File Systems (NFS)->` and activate the (Open) control button.
3. Highlight `Remote File Systems Mounted` and activate the (Open) control button.
4. Highlight the remote file system to be unmounted.
5. From "Actions" on the menu bar, choose `Modify...`. Deactivate the `now` control button in the "When to Mount" field.
6. Activate (OK) to unmount the remote file system.

Unmounting an Exported File System on a Server

To unmount a file system that is currently being exported to one or more clients:

1. Have the file system unmounted from each and every client. From each client:

   a. Run SAM.

   b. Unmount the remote file system. Use the procedure described in "Unmounting a Remote File System".

Note Unmounting an exported file system on which users of remote client systems have open files could result in lost data.

---

2. From the server, disable the exported file system.

   Because it is a local file system on the server, you can unmount the file system using the procedure described in "Mounting and Unmounting Local File Systems Using SAM".

6

Mounting NFS File Systems Using HP-UX Commands

You can use the `mount` command to mount file systems located on a remote system.

Preparations for Mounting Remote File Systems

Before you can mount file systems located on a remote system, NFS Services software must be installed and configured on both local and remote systems. Refer to the manual *Installing and Administrating NFS Services* for the necessary and detailed information.

Note the following about using `nfs` file systems.

1. Both for the **NFS Server** (the system where the file systems reside, which is the machine exporting the file systems) and for the **NFS Client** (the machine where remote file systems are mounted), entries must exist in the `/etc/hosts` file. (See *hosts*(4) in *HP-UX Reference*.)

   Note that a machine can be an NFS server (export file systems), an NFS client (mount remote file systems), or both.

6

2. The **NFS Server** must list both the file systems and the NFS Clients that can mount the file systems in the file `/etc/exports`. (See *exports*(4) in *HP-UX Reference*.)

   Entries in the `/etc/exports` file require the following syntax: the file system name must be flush left and the client machine names are to follow, separated by single spaces. An entry in `/etc/exports` that lists only a file system name (no machine names) indicates that all machines can access the file system. (Review *exports*(4) in *HP-UX Reference* for guidelines and cautions concerning the use of the `-async` option.)

   For example, to allow machines called `rolf` and `egbert` to remotely mount the `/usr` file system, edit the file `/etc/exports` on the server machine and add the line:

   ```
   .
   /usr rolf egbert
   .
   ```

Example: Mounting an NFS File System

To mount the remote file systems `/users/jpsouza` on the remote system `hpedc2` to the mount directory `/users/jpsouza` on your local file system, enter:

1. Create the mount directory if it does not already exist:

   ```
   mkdir /users/jpsouza
   ```

   Note that the mount directory should be empty. A mounted file system will mask files in a mount directory, making them unavailable until you unmount the file system.

2. Mount the remote file system:

   ```
   mount hpedc2:/users/jpsouza /users/jpsouza
   ```

   This will make the files in the directory `/users/jpsouza` on remote machine `hpedc2` accessible from your local machine.

When mounting NFS file systems, you can use options that affect mounting conditions, user permissions, and so on. All options are thoroughly described in the manual *Installing and Administrating NFS Services*. (See also *mount*(1M) in *HP-UX Reference*.)

6

NFS Mount Problems

When the `mount` command succeeds, it is silent. Otherwise, you will receive an error message. If the attempt to mount a remote file system fails, be sure to verify that:

- The client machine has an entry in NFS server's `/etc/exports` file that allows it to mount the remote file system.
- The mount directory exists, is not currently being used as a mount point, or that no files in the directory are in use.

Unmounting an Exported File System

To unmount a file system that is currently being exported:

1. Have the file system unmounted from each and every client. From each client, unmount the remote file system.

   ```
   umount hpfcf8:/users
   ```

Note Unmounting an exported file system on which users of remote client systems have open files could result in lost data.

---

2. Unmount the file system from the server.

Automatically Mounting Your File Systems at Bootup

To automatically mount your file systems at bootup, do the following:

6

- List the file systems you want automatically mounted in the `/etc/checklist` file. See "Making Entries for Mounting a File System in the Checklist File" and the entry for *checklist*(4) in the *HP-UX Reference*.
- Enter the `mount -a` command (if it is not already present) in the `/etc/rc` script.
  - □ For `hfs` type file systems, add the line

    ```
    /etc/mount -a -t hfs
    ```

    in the `hfsmount()` section of the `/etc/rc` file.
  - □ For `cdfs` file systems, you can add the line

    ```
    /etc/mount -a -t cdfs
    ```

    in the the `localrc()` section of the `/etc/rc` file.

Making Entries for Mounting a File System in the Checklist File

Before reading the discussion on making `/etc/checklist` entries, you can enter the command:

`/etc/mount -p`

This displays information about all of the currently mounted file systems in `/etc/checklist` format.

You can also see the same information by simply typing `mount` without options; the display will not be formatted, however. Look at the following example entry in an `/etc/checklist` file:

```
/dev/dsk/cEd1s0    /users    hfs   defaults 0 2 # users
```

An entry for a file system in the `/etc/checklist` file has seven fields separated by blank spaces. In all but the last of the fields, you need to put either an entry or , in some fields, a placeholder. The following describes making entries for each field.

- First field: Enter the *block device file* corresponding to the disk used for the file system.
- Second field: Enter the mount point *directory*; this directory is located in the existing file system and will serve as the root directory for the mounted file system.
- Third field: Enter the *type* of the entry, the *type* must be one of the following depending on the type of file system:

  `hfs` (local high-performance file system)
  `nfs` (file system available through NFS Services)
  `cdfs` (CD-ROM file system)

  It is also possible to enter `ignore` in this field when you want to retain the entry for the file system in the `checklist` file, yet do not want the file system mounted at the time the system boots. You can mount the system later.

- Fourth field: Enter *options*, which include the following:

defaults	use all default options (rw,suid).
rw	read-write (default).
ro	read-only.
suid	set user ID execution allowed (default).
nosuid	set user ID execution not allowed.
quota	enable disk quotas.
noquota	disable disk quotas (default).

  These options correspond to the options used with the `mount` command. More options are available for use with the NFS type file systems; check in *mount*(1M) in the *HP-UX Reference*. Disk quotas are discussed later in detail. See the section "Using Disk Quotas".

- Fifth field: This field is reserved for future use by backup utilities. `0` is a placeholder.
- Sixth field: Assign a pass number of 1 for the root file system and larger numbers to other file systems. The pass number is used by the `fsck` command issued with the `-p` command. The `fsck` utility ignores file systems with pass numbers of 0, which is typically used for NFS file systems.
- Seventh field (optional): Enter a comment preceded by the `#` character.

6

Example

The following is a sample `checklist` file for a system using two disks; notice that one disk is used for both a file system and swapping:

```
more /etc/checklist

/dev/dsk/cEd0s0    /        hfs    defaults    0 1   # root
/dev/dsk/cEd0s0    /swap    swap   defaults    0 0   # swap
/dev/dsk/c7d1s0    /users   hfs    defaults    0 2   # users
```

How /etc/checklist is Used

At boot up, the `/etc/bcheckrc` and `/etc/rc` file system scripts are executed from `/etc/inittab`. The `/etc/bcheckrc` script checks each file system listed in `/etc/checklist` and determines whether the file system was properly shutdown. If a file system appears to have been previously shutdown improperly, `bcheckrc` runs `fsck` during the startup process. The `/etc/rc` script mounts all file systems listed in `/etc/checklist`.

Unmounting a File System Using HP-UX Commands

To unmount a file system, use the *mount*(1M) utility. All files on the particular file system to be unmounted must be closed. Attempting to unmount a file system that has open files (including your working directory) causes the *umount*(1M) utility to fail without unmounting the file system.

Use the *ps*(1) utility with `-ef` options or the *fuser*(1M) utility to check for open files. If there are open files, take necessary actions to close the files. You might need to execute these commands more than once to ensure that all files are closed.

Syntax of the umount Command

The `umount` command has the following syntax:

`umount` *sfname*

or

`umount` *directory*

6

where:

sfname — is the pathname of the block device file for the device containing the file system to be unmounted or the name of a remote file system in the form: *host:path*.

directory — is the directory where the file system is mounted.

When using `umount` to unmount a file system, you can specify either the name of the mount directory or the block special file of the disk containing the file system.

Note — Always unmount file systems contained on a mass storage device before removing the device from the system. Removing a device containing mounted file systems (for example, disconnecting or turning off the power to a disk, or removing a disk pack from a mass storage device) will likely corrupt the file systems.

Example, Unmounting a File System

To unmount a local HFS file system on the disk with the device file `/dev/dsk/c7d3s0` mounted at the mount point directory `users`, issue the command:

```
umount /dev/dsk/c7d3s0
```

or

```
umount /users
```

To unmount a remote NFS file system, you can issue a command such as:

```
umount hpfcf8:/users
```

Unmounting Currently Mounted File Systems

The `umount` command removes the specified file system from the `/etc/mnttab` file. If you wish to unmount all your currently mounted file systems contained in the `/etc/mnttab` file execute:

```
umount -a
```

Unmounting File Systems by Type

6

Or, to unmount currently mounted file systems of a particular type, you can use the `-t` option. For example, to unmount all NFS file systems, use the command:

```
umount -a -t nfs
```

Note The root (/) file system cannot be unmounted.

Note It is recommended that you remove the file system entry in the file `/etc/checklist` for the file system you have just unmounted.

If you have unmounted a file system and you do not wish to remove the entry from the `/etc/checklist` file, you can enter `ignore` in the *type* field. The file system will not be mounted when the system boots but can be mounted later.

Automatically Unmounting Your File Systems at Shutdown

When you execute the *shutdown*(1M) command, the system unmounts all of the file systems listed in the `/etc/mnttab` file. The `shutdown` utility uses `umount -a` to unmount file systems. File systems are also unmounted when you use the *reboot*(1M) command. For more information on *shutdown*(1M) refer to Chapter 3, "Starting and Stopping HP-UX".

Creating a LIF Volume

The LIF format (Logical Interchange Format) is an HP standard mass-storage format that can be used for the interchange of files among the various types of Hewlett-Packard computer systems. It is supported on Series 300, 700, and 600/800 computers. See *lif*(4) in *HP-UX Reference* for discussion of this format and its characteristics.

Prerequisites and Conditions

- If your media has never been initialized, you must use `mediainit` to initialize the media, then use `lifinit` to create a LIF volume.
- A LIF volume can be created directly on a disk or within the HP-UX file system as a regular file.
- Test previously initialized media to see if it is a LIF volume *before* you initialize a disk. Assuming the media to check is associated with `/dev/rdsk/c7d4s0`, execute:

  ```
  lifls -l /dev/dsk/cEd0s0
  ```

  Note that you must be superuser to list information about device files.

  You get one of the following responses:

  - For an initialized disk that is a LIF volume and contains files, you see a listing. For example, you might see:

    ```
    volume BOOT data size 25 directory size 1
    filename   type   start   size    implement  created
    ===============================================================
    SYSHPUX    -5822  3       25      ffff0800   91/03/17 19:50:08
    SYSDEBUG   -5822  3       25      ffff0800   91/03/17 19:50:08
    SYSBCKUP   -5822  3       25      ffff0800   91/03/17 19:50:08
    SYSTEST    -5822  3       25      ffff0800   91/03/17 19:50:08
    ```

  - For an initialized disk that is a LIF volume and has no files, you see an empty line.

6

- For an uninitialized disk, you might see:

```
lifls: Can't list /dev/rdsk/c7d3s0; not a LIF volume
```

You should continue, or not, depending on what you see.

There are no SAM procedures related to the use of LIF files.

Manual Procedure for Making a LIF Volume

1. Become the root user.
2. Use *lifinit*(1) to create a LIF volume according to the following syntax:

   `lifinit` [`-v`*nnn*] [`-d`*mmm*] [`-n`*VOL_NAME*] *FILE_NAME*

   If you use the last two parameters, use characters limited to uppercase letters (`A-Z`), digits (`0-9`), and the underscore character (`_`). Limit the volume name to six characters, the file name to ten characters.

   a. The following example writes a LIF volume header to the disk associated with the device file named `/dev/rdsk/c7d3s0`:

   ```
   lifinit /dev/rdsk/c7d3s0
   ```

   b. The following example writes a LIF volume header (named WORK) to an HP-UX file (named TMP), where the volume size is 270,336 bytes and the number of directories is 240.

   ```
   lifinit -v270336 -d240 -nWORK TMP
   ```

3. The manual *HP-UX Reference* has more information about the options used with *lifinit*(1).

6

Moving File Systems from One Disk to Another

You might want to move the data in a file system on one type of disk to a file system on another type of disk. For example, you might want to move a file system to a larger disk.

The following steps outline how to copy data from one disk to another disk of a different type. An example follows.

1. Back up files from the current disk onto tape.
2. Add your new disk to your system.
3. Create new file systems using the `newfs` command on your new disk.
4. Edit the `/etc/checklist` files to create entries for new file systems.
5. Mount your new file systems.
6. Restore the files backed up on tape to your new file systems.

Example, Moving File Systems from Disk to Disk

Let's assume you want to copy data from your current disk, a Model HP 7935, to a Model HP 7937FL disk. You have a file system on the HP 7935 disk, which has the device file `/dev/dsk/c7d2s0`. By looking at the file `/etc/checklist`, you can determine the mount point directory for the file system. For example,

```
more /etc/checklist

.
/dev/dsk/c7d2s0      /usr/users    hfs rw 0 3 # users
.
.
```

Copy this file system to the new disk as follows:

1. Back up your file system onto tape.

   The files you want to move to the new disk are now in the `/usr/users` file system. To back up these files to the 6250 bpi magnetic tape drive unit, use the following command:

   ```
   /etc/fbackup -0f /dev/rmt/0h -i /usr/users
   ```

Detailed information about performing backup is in Chapter 8, "Backing Up and Restoring Your Data".

2. Add the new disk to your system and make your new file system.

   Refer to the documentation that came with your disk and to the *Installing Peripherals* manual. Use either SAM or `newfs` to make the new file systems on your new disk. Refer to the earlier section in this chapter "Creating/Removing File Systems."

   For example, after adding your new disk, creating its device files, and initializing it, you could use the `newfs` command:

   ```
   newfs /dev/rdsk/c7d3s0 hp7937
   ```

3. Edit `/etc/checklist`.

   After you have created the file systems on your new disk, edit the file `/etc/checklist`. Change the device file to reflect your new disk. For example, change `/dev/dsk/c7d2s0` to `/dev/dsk/c7d3s0`. Editing this file tells the system to automatically mount the new file system each time you boot your system.

6

4. Mount new file system.

   Now, mount the new file system by running the command:

   ```
   mount /dev/dsk/c7d3s0 /usr/users
   ```

5. Restore your backed up files to the file system on the new disk.

   Load the tape with your files on the tape drive and restore the files to their new file system. You can use the following commands.

   ```
   /etc/frecover -xf /dev/rmt/0h -i /usr/users
   ```

Modifying File Name Length

The procedures to convert a file system from the use of short file names to the use of long file names (and vice versa) are described in the following sections. Refer also to the section "Changing File Names: Potential Problems and Troubleshooting Suggestions".

Changing File Names: Potential Problems and Troubleshooting Suggestions

Here are some potential problems and troubleshooting suggestions:

- A program opens directories and reads the directory entries directly. Change the program to use directory library routines or use **get directories** system calls.

- A program assumes that the maximum length of a file name (in a buffer) is 14 characters. For example, **char filename**[14] or **char filename**[**DIRSIZ**] (**MAXNAMLEN** should be used for the buffer size, if only a few buffers are involved).

  If you want to store more than a few file names, enable the DIRSIZ_MACRO compilation flag. When DIRSIZ_MACRO is enabled, DIRSIZ is a macro instead of a constant of 14. The macro accepts an argument that is a pointer to a struct direct and returns the size of the file name rounded to a 4-byte boundary. You can then allocate more memory for the file names.

- A program includes <**dir.h**> and uses **struct direct**. The struct direct for systems that support long file names is a variable length structure and the struct direct for systems that support only short file names is a fixed-size structure.

  You can include **ndir.h** and use directory libraries.

- A program assumes there is only one file system magic number. (The magic number for a system that supports long file names is different from the magic number for a system that supports only short file names.)

  Change the program to allow the new magic number for long file names.

- A program uses **MAXNAMLEN** and assumes it has a value of 14 (when you convert to long file names, you need a **MAXNAMLEN** of 255).

  Recompile the program.

- A program uses **DIRSIZ** and assumes it is a constant of 14 (meaning the maximum file name length is 14 characters).

  Instead of **DIRSIZ**, use **MAXNAMLEN** to dictate the maximum file name length on a system that supports long file names. (For systems that support only short file names, use **DIRSIZ_CONSTANT** to dictate the maximum file name length.)

Enabling Long File Names Using SAM

Caution The process used to convert a file system to long file names is not reversible. Changing a file system back to short names requires that you perform the series of steps described in the section "Disabling Long Filenames".

1. Back up your entire file system before you use SAM to convert the length of your file names. (You should do a backup before you perform any operation that alters the file system).
2. Get into single-user mode. You can use SAM to get to single-user mode, although you must reenter SAM after you reach single-user mode to convert to long file names.

   `shutdown`

3. Run SAM.
4. Highlight `Disks and File Systems ->` and activate the OK control button.
5. Highlight `Local File Systems` and acivate the OK control button.
6. Highlight the file system you want to convert.
7. From the "Actions" on the menu bar, highlight `Convert to Long File Names`.

   SAM issues a warning about the irreversibility of converting to long file names, giving you an opportunity to stop the task.

8. Activate OK when SAM reports the task is completed.

Enabling Long File Names Using HP-UX Commands

If you have an HP-UX file system that allows only short file names, use the *convertfs*(1M) utility to convert the file system to allow long file names.

Caution The process used to convert a file system to long file names is not reversible. Changing a file system back to short names requires you perform the series of steps described in the section "Disabling Long Filenames" .

Follow these steps:

1. Back up your entire file system before you use the `convertfs` utility. (You should do a backup before you perform any operation that alters the file system).
2. Shut your system down to single-user state by typing: `shutdown`

Note When `convertfs` runs on file systems containing inconsistencies, the file systems might become corrupted. It's a sound precaution to correct the inconsistencies by running `fsck` on file systems before converting them.

6

3. Unmount all of your file systems:

   `umount -a`
4. Execute the `convertfs` utility:

   `convertfs`

You will receive these messages:

```
Warning: certain programs might not work with long file names.

Converting the file system will cause a system reboot. The system
should be shut down into single user state and all non-root file systems
should be unmounted before this utility is run.

Do you wish to continue? [y/n]
```

If you have your system in single-user state and have all non-root file systems unmounted, answer `y`.

The utility will then ask you if you want to convert all of the normally mounted file systems listed in `/etc/checklist`. If you answer "no" to this prompt, `convertfs` will ask whether you want to convert each file system in `/etc/checklist`. Respond to the prompt for each file system.

The `convertfs` utility modifies the superblocks and reformats the directories in the file systems you want to convert. After modifying each file system, `convertfs` executes `fsck` so that the file system can again be mounted.

Note

Although the `convertfs` utility allows just one (or a few) file systems to be selected for conversion to long file names, we recommend that you convert all or none of your normally mounted file systems listed in `/etc/checklist`. This prevents inconsistencies and undesired events (such as the overwriting of files) that can occur if you mix long and short file names on the same system.

If you have converted the root file system, `convertfs` reboots the system so that the changes made to the file system superblock will not be overwritten by an update of the superblock in the system memory.

6

You can also execute `convertfs` with the name of the specific file system you want to convert:

```
convertfs /dev/rdsk/cEd2s0
```

The `convertfs` utility converts the named file system without prompting for input.

After you reboot the system or remount the converted file systems, you can use long file names on the converted file systems. The `newfs` and `mkfs` utilities create new files of the same type as the root file system. If you converted the root file system, all new file systems you create allow long file names. If you need a file system with short file names, use the **-S** option to either `newfs` or `mkfs`. (Refer to either *newfs*(1M) or *mkfs*(1M) in the *HP-UX Reference* for more details.)

Disabling Long Filenames

When you use *convertfs*(1M) to convert to long file names, you cannot use the utility to convert back to short file names. If you must convert back to short file names after using `convertfs`, the file system should not have any file names longer than 14 characters. Recreate the file system with short names using the **-S** option to `newfs` or `mkfs` and then recover the original files from the backup media. If the root file system needs to be converted back to short file names, it must be reinstalled. Be sure to save any files customized for your system so these files can be recovered after the reinstallation.

The following four steps describe the process of converting your file system to short file names:

1. Examine all file names to make sure they have 14 or fewer characters. Use the `mv` command to rename files with long names so that they have names of 14 or fewer characters.
2. Backup your entire file system after you have shortened the file names.
3. Recreate the file system with short file names by executing `newfs` with the -S option.
4. If the root file system must be changed, reinstall it from the installation tape.

Displaying Current Disk Usage Information

1. Use the *bdf*(1M) to list all currently mounted file systems and key information about them. Enter:

   ```
   bdf
   ```

   The output resembles:

   ```
   Filesystem          kbytes    used   avail capacity Mounted on
   /dev/dsk/cEd0s0     484960  243777  192687    56%   /
   /dev/dsk/cEd1s0     237810   48481  165548    23%   /graphics
   /dev/dsk/cEd2s0     277954  129787  134269    49%   /users
   /dev/dsk/cEd3s0     121663   23257   86239    21%   /tmp
   /dev/dsk/cEd4s0     461664  320936   94561    77%   /usr
   ```

   The column headed "Filesystem" lists the block device files for all mounted file systems, whether they are locally or remotely mounted.

   The values in the next three columns are reported in kilobytes. You can multiply these values by 1024 to find the values in bytes. Divide them by 1000 and round off the result to find the value in megabytes.

   The values under "used" and "avail" add up to the total space available to users, and the percentage under "capacity" corresponds to the value under "used." The total of "used" and "avail" equals 90% of the value under "kbytes." The difference is the "minfree" area that, by default, is reserved for system administration use and allows for efficient file system performance.

   The "Mounted on" column lists the file systems' the mount directories.

2. Use *df*(1M) to see the amount of free space left in a file system. For example, you can use `df -t /users` to see usage information for a mounted file system, `/users`:

   ```
   df -t /users
   ```

   ```
   /users  (/dev/dsk/cEd2s0 ):  288480 blocks       128796 i-nodes
                                879996 total blocks  147456 total i-nodes
                                503516 used  blocks   18660 used i-nodes
                                    10 percent minfree
   ```

   The top line shows the available space (in 512-byte sized blocks) and the number of available file system i-nodes. Divide by the number of 512-byte blocks by 2 to get the number in kilobytes.

6

While the examples provide suggestions, HP-UX has many commands for exploring the system. In general, you can find them in sections 1 and 1M of the *HP-UX Reference*.

The following commands explain how to get information about disk usage. Some commands generate long lists, which you might want to redirect to a file or pipe to `more` to view the information one screenful at a time.

- Use *du*(1) to monitor users who are increasing their disk usage. The `du` utility displays information in 512-byte blocks.

  ```
  du -s /users/*
  ```

  ```
  184 /users/jamieo
  92 /users/michelem
  10 /users/rykl
  10 /users/alisonm
  ```

- Use *du*(1) and *sort*(1) to list files in decreasing size.

  ```
  du -s /users/michelem | sort -nr
  ```

  ```
  92 /users/michelem
  24 /users/michelem/checklist.man
  14 /users/michelem/shutdown.man
  12 /users/michelem/swapon.man
  10 /users/michelem/umount.man
  10 /users/michelem/mount.man
  6 /users/michelem/convertfs.man
  ```

- Use *find*(1) to locate files over a particular size. The following example displays files larger than .5 Mbytes:

  ```
  find / -size +1000 -print > big-files
  ```

- Use `find` to locate files older than *n* days. The following example displays files not written or accessed in 90 days:

  ```
  find / -mtime +90 -atime +90 -print > aging-files
  ```

Using SAM to Recover Disk Space

SAM provides the means to remove old or useless files that can accumulate on your system, wasting valuable disk space.

1. Run SAM.
2. Highlight `Routine Tasks->` and activate the Open control button.
3. Highlight `Disk Space Recovery->` and activate the Open control button.
4. You can now choose, using the Open control button, one of the following activities:
   - `Log File Trimming->`
   - `Large File Removal`
   - `Core File Removal`

   These tasks are straightforward. SAM can help you decide how to remove these files on the basis of type, size, and date.

6

Using Disk Quotas

As the system administrator, you can use disk **quotas** to limit the number of files and file blocks a user can own on an HFS or NFS file system. Disk quotas are established on a per-file-system basis. You must have superuser privileges to set up disk quotas. For each user, you can set limits for the number of files (by limiting the number of inodes) that can be created and for the number of file system blocks that can be used.

Each user can have a **soft limit** and a **hard limit**. A soft limit is a preferred limit that a user can exceed for a limited time, while a hard limit is an absolute limit. If a user reaches hard limits or fails to reduce usage below soft limits before a specified time, he or she will be unable to create files or increase file system block usage.

For each file system enabled with quotas, the operating system maintains statistics on limits and usage. A user can check his or her quota status at any time. As system administrator, you can increase or decrease a user's limits at any time.

Caution By using the `chown` command to change the ownership of files, a user can bypass disk quota limits. For example, a user can use the `chown` command to make `root` the owner of a file; this file, now owned by `root`, will not be considered in the file system usage computed for the user who created it.

A solution to this potential problem is to reserve the use of the `chown` command to privileged users. See *setprivgrp*(1M). Also, see Chapter 4, "Controlling Access to the System".

By editing the `/etc/checklist` file, you can have quotas turned on automatically for each file system when you boot your system. You can turn quotas off and turn them back on again at any time, though this is discouraged because of the system overhead required to recompile usage.

SAM does not have the capability to perform tasks involving quotas.

Planning for Disk Quotas

- Choosing file systems for disk quotas. Typically, you will want to set disk quotas on file systems that would otherwise become full without limitations on their use. This means that file systems containing the home directories and files of several users are suitable for disk quotas. It is not recommended that you set up quotas for the `/tmp` file system, unless you set the hard limits very large, the soft limits small, and the time limits short to prevent users from using `/tmp` as storage.
- Choosing limits. You can choose to set uniform soft and hard limits for most or all users, or you can set limits for each user individually. The recommended method for setting uniform limits is to assign limits for one or more prototype users and apply those limits to actual users.

  You can also set a limit to the time users can exceed the soft limits. Time limits are set for an entire file system and apply to all users of the file system.
- Disk quotas and performance. Disk quotas are designed to have minimal impact on performance. Because the disk quota statistics are resident in memory, the use of disk quotas involves minimal computation and seldom results in the transfer of data to and from a disk. The time required to reboot a system that has crashed will take somewhat longer because of the time required to run `quotacheck`. (See the section, Checking Consistency of File System Usage Data.)

Setting Up Disk Quotas on a File System

To set up disk quotas, use the steps outlined below. Details and examples will follow.

1. Mount the file system for which you will use disk quotas.
2. Edit the file `/etc/checklist` to have disk quotas enabled on the file system the next time you start up the system.

   For an auxiliary file system not listed in the `/etc/checklist` file, you can enable disk quotas for it when you mount it by using the `quotas` option with the `mount` command. However, you must perform the following steps before turning quotas on.

3. Create the empty file `quotas` in the root directory of the file system for which you are enabling quotas.
4. Set user quotas using `edquota` command.

   Set quotas for a prototype user and apply these quotas to all users of that file system, or set individual quotas user by user.

Mount the File System

The file system you want to set up with quotas must be mounted.

Let's suppose you want to want to implement quotas on the HFS file system `/users` that has the device file `/dev/dsk/cEd1s0` . This file system would already be mounted if you have it listed in your `/etc/checklist` file. If it is not mounted, you can mount it by entering:

```
mount /dev/dsk/cEd1s0 /users -t hfs
```

Edit /etc/checklist to Add "quota" Option

For example, if the line in your `/etc/checklist` file for the `/users` file system looks like:

6

```
/dev/dsk/cEd1s0 /users hfs rw,suid 0 1
```

modify that line to include the quota option. Note that options in `/etc/checklist` entries are separated by commas and no spaces. The line should then look like:

```
/dev/dsk/cEd1s0 /users hfs rw,suid,quota  0 1
```

If the entry for a file system listed in `/etc/checklist` contains the option `quota`, the file system will be enabled for disk quotas when the system is started.

Create the "quotas" File in the File System's Root Directory

Each file system using disk quotas must have an initially empty file—named `quotas`—in its root directory. The `quotas` file will contain the limits and usage statistics for each user in the file system in binary form.

To create the quotas file for the /users file system (/users must be mounted), use the cpset command. For example, you might enter,

```
cpset /dev/null /users/quotas 600 root bin
```

In the above command, /dev/null specifies that the file created is empty. /users/quotas specifies that the file quotas is located at the root of the file system mounted on /users. The 600 sets the mode of the file to allow read-write permission to only the owner, in this case root, whose group is bin. See *cpset*(1M) in the *HP-UX Reference*.

Note Assigning user IDs.

The file quotas keeps file system usage information in binary form for users on the basis of their user ID numbers. The quotas file can become large if users on a file system have user IDs that are large (a four-digit number, for example). The quotas file will contain data space for the number of possible users. A high user ID number means the file must create space for a large number of possible users; this could result in wasted space if there are only a few users. So, to control the size of the quotas file, refrain from using large numbers for user IDs. If you are using SAM to create user IDs, you will not have the problem.

While HP-UX supports "sparse" files and does not allocate disk blocks for non-existent users, the act of restoring a backup or of making a copy of the quotas file causes expansion of the sparse file.

6

Establish Quotas for Users of the File System

To establish quotas for the users of a file system, you can use the /etc/edquota command to edit a character representation of the contents of the quotas file for that file system. See the *edquota*(1M) in the *HP-UX Reference*. The editor you will use is the one specified by the EDITOR environment variable. If you have not specified EDITOR, vi will be invoked by default.

Note

The `edquota` utility converts binary data from a `quotas` file into a text representation, creates a temporary file, invokes the editor on that file, and converts the edited text back to binary form before storing the data back to the `quotas` file.

Using edquota -p. Let's assume you want to set uniform limits for users in the `/users` file system. To do this, you can set limits for a prototypical user using the `/etc/edquota` command. Then, using the `/etc/edquota` command with the `-p` option, you can replicate these limits for other users owning files in the file system.

In the following example, a prototypical user in the file system `/users` is assigned a soft limit of 1000 blocks, a hard limit of 1200 blocks, a soft limit of 250 files, and a hard limit of 300 files.

1. Set the limits for a prototype user. Use the `/etc/edquota` command.

   a. Type:

   ```
   /etc/edquota protojoe
   ```

   b. While in the editor, type the following:

   ```
   fs /users blocks (soft = 1000, hard = 1200) inodes (soft = 250, hard = 300)
   ```

   After you save the text file, the `quota` file is updated.

2. Now, run the `/etc/edquota` command with the `-p` option to implement the prototype user's limits for other users of the `/users` file system:

   ```
   /etc/edquota -p protojoe alice george
   ```

   This assigns the prototype limits of the prototypical user, `protojoe`, to the actual users, Alice and George. Notice that you can include more than one user on the command line.

Setting quotas for an individual user. Use the `/etc/edquota` command to set quotas for individuals. For example, suppose you want to set quotas for Ted that would allow him to have higher limits than the prototypical user. Type:

```
/etc/edquota ted
```

When you get into the editor, you would enter a line such as:

```
fs /users blocks (soft = 1200, hard = 1500) inodes (soft = 300, hard = 350)
```

Save the file. Ted now has limits different from the prototypical user.

Note When removing a user from the system, run `/etc/edquota` to set the user's limits to 0. Then, when the user is removed from the system, there will be no entry for that user in the `quotas` file.

Setting Time Limits for a File System's Users

The soft time limits (time limits by which a users must reduce the number of blocks or files to values below soft limits) are set using the `/etc/edquota` command with the `-t` option. The time limits apply to all users of a file system. You can set different time limits for files and file system blocks.

6

For example, you could set the soft time limits of ten days for file system blocks and 15 days for files in the file system `/users`.

To edit the `quotas` file to specify time limits, type:

```
/etc/edquota -t
```

When you are in the editor, type the line:

```
fs /users blocks time limit = 10.00 days, files time limit = 15.00 days
```

Saving the file establishes the specified time soft limits for the file system.

The default time limit for both file system blocks and files is seven days. You can specify the default time limits by entering `0` (zero) in fields where you would specify the limits. For example, to implement default limits for the `root` file system, you could enter the line:

```
fs / blocks time limit = 0, files time limit = 0
```

Turning On Disk Quotas

After you have set up disk quotas on a file system, you need to put quotas into operation.

Turning On Disk Quotas by Mounting the File System

When you mount a file system with the `quota` option, disk quotas are turned on, provided, of course, that the `quotas` file exists in the root directory of the file system.

You can:

1. Include the `quota` option in the file system entry in the `/etc/checklist` file so that the system will enable quotas when the `mount -a` command is issued or when it mounts the file system the next time you start up the system.
2. Mount a file system interactively and include the `quota` option in the mount command line.

   For example,

   ```
   mount /dev/dsk/cEd1s0 /users -o quotas
   ```

Turning On Disk Quotas Using the quotaon Command

1. Check the file system for consistency.

   Having to enable disk quotas with the `quotaon` command implies that the file system has been used with disk quotas off and that the `quotas` file has out-of-date information. The `quotacheck` command should be run on that file system.

   For example, running

   `/etc/quotacheck /dev/dsk/cEd1s0`

   updates the `quotas` file for that file system to reflect any usage while disk quotas was turned off. See the later section "Checking Consistency of File System Usage Data" for a detailed discussion of running `quotacheck` interactively.

2. Use the `quotaon` command.

   Use the `quotaon` command to turn on disk quotas for a mounted file system for which disk quotas is set up but not currently turned on. Remember, the file `quotas` must exist in the root directory of the file system.

   For example, issuing the command

   `/etc/quotaon -v /users`

   will start up quotas on the `/users` file system and print a message that states that quotas are being turned on for the file system.

   You can also use the `/etc/quotaon -v -a` command, in which case the `-a` option turns on disk quotas for each mounted file system with the `quota` options in the file `/etc/checklist`. The `-v` (verbose) option specifies that the affected file systems be listed in a message to the screen.

   If you issue the `/etc/quotaon` command specifying a file system for which quotas are already turned on, there is no effect.

Turning Off Disk Quotas

When you unmount a file system, the system automatically turns off disk quotas. You can turn off disk quotas for a file system without unmounting that file system by using the `/etc/quotaoff` command. However, the use of `/etc/quotaoff` command is not recommended because once quotas are turned off, the actual disk usage will be inconsistent with the usage recorded in the `quotas` file, making the information in the `quotas` file invalid.

If you use the `/etc/quotaoff` command, you must run the `/etc/quotacheck` command to check the consistency between the actual file usage and the `quotas` file before turning on disk quotas for the file system again. See the section "Checking Consistency of File System Usage Data" for a discussion of using the `/etc/quotacheck` command. If `quotaoff` is not used and file systems are not unmounted improperly, `quotacheck` overhead is minimal.

Displaying File System Usage, Soft and Hard Limits

Commands are available to show information about disk usage and quotas.

Reporting File System Usage

You can use `repquota` command to display quota information about file systems. For example,

```
repquota /users
```

shows the usage for each user of the file system `/users`. You might get a report that looks like:

```
/dev/dsk/cEd1s0 (/users):

        Block limits                            File limits
User          used   soft   hard   timeleft    used   soft   hard    timeleft
bill    --      59    100    200                 24     30     40
fred    +-     199    100    200  1.7 weeks      10     30     40
joe     --      63    100    200                  9     30     40
dan     ++     173    100    200  1.4 weeks      32     30     40  1.4 weeks
```

Entering the command,

```
repquota -a
```

displays usage for each user on all file systems listed in the `/etc/checklist` file with the `quota` option. See *repquota*(1M) in *HP-UX Reference*.

6

Reporting a Summary of Ownership

You can use the quot command to display the number of 1024-byte blocks in a file system that are currently owned by each user. For example, for the file system /dev/dsk/cEd3s0, you could issue the command:

```
/etc/quot /dev/rdsk/cEd3s0
```

You would receive the following output:

```
/dev/rdsk/cEd3s0 (/users):
 2843   benny
 2429   fisher
 1102   ariel
  164   #220
   25   anitasz
   15   nanda
```

You could have specified the mount point directory instead of the device file in the command described above and have received the same output.

Reporting Individual Usage

6

A user can display his or her usage by using the quota command. For example, if Joe types quota, he will receive warnings about file systems where his usage exceeds limits:

```
quota -v
```

```
Disk quotas for joe (uid 203):
Filesystem     usage  quota  limit    timeleft  files   quota  limit timeleft
/users           159    110    210    .8 weeks     24      10     25
```

Only a user with superuser privileges can use the *user* option for the quota command to view specific usage and quota information about other users. See *quota*(1).

Using quota -v shows a user all of the quota information on all file systems (including remotely mounted systems) where he or she has limits.

What to Do When Reaching a Hard Limit

When a user on the system reaches a hard limit or fails to reduce usage below soft limits, an error message appears on the terminal. For example, if a user reaches the block limit, the following message appears:

```
DISK LIMIT REACHED -- WRITE FAILED
```

When a user reaches the file limit, the following message appears:

```
FILE LIMIT REACHED -- CREATE FAILED
```

When reaching these limits, a user can no longer create files or use additional file system blocks.

Recovery from this condition requires a sequence of steps, depending on whether or not the user is in an editor when receiving the message.

When Not In an Editor

If a user is *not* in an editor when the limit is reached, the user must:

1. Abort the process or processes that are using the file system.
2. Remove enough files to reduce the number of files and file system blocks well below the soft limits established in the `quotas` file. 6

   The `quota` command reports whether a user is above or below the limit in the specific file system. The `du` command can help in determining the current number of blocks in files and directories. See *du*(1) in *HP-UX Reference*.
3. Rerun the aborted processes.

When In an Editor

When *in* an editor, the user needs to remove files to a level below the quota limits and still preserve the recent changes made to the file being edited. The user can do this by:

1. Writing the file to another file system (such as `/tmp`) where quotas are not exceeded, and getting out of the editor.
2. Removing files until the number remaining is well below the file and file system block quotas, that is, soft limits.

3. Moving the file back into the original file system.

Or, if a job-control shell is being used, the user can do this by:

1. Going to the shell.

   Typing the "susp" character (usually **CTRL-Z**, that is, CTRL and Z at the same time) moves the user to the shell and suspends the editor.

2. Removing files until the number remaining is well below the file and file system block quotas.

3. Typing `fg` at the shell prompt returns the user to the editor.

Checking Consistency of File System Usage Data

You can run the `quotacheck` command

- to check for inconsistencies between the `quotas` file and actual usage
- to update the `quotas` file

The system updates the `quotas` file when users logout and when file systems are unmounted. In this way, the usage information stored in the `quotas` file matches actual usage. But, if disk quotas are turned off for a file system, then, the `quotas` file and the actual usage will become inconsistent when the file system is used.

Checking Quotas When Starting the System

When `quotacheck` runs, the file system being checked must *not* be in use. The best way to run `quotacheck` is from the `/etc/bcheckrc` file during boot up, after file systems are mounted. `quotacheck` can be run with the `-a` option so that it checks all file systems listed `/etc/checklist` with the read-write and disk quotas options.

Running quotacheck Interactively

Before you interactively mount a file system, run `quotacheck` to check that file system for any inconsistencies. Make sure the file system you are checking is unmounted.

You can run `quotacheck -v` to have `quotacheck` report the quotas information for each user in the file system. Otherwise, it reports only the changed quotas.

For example, you might run:

```
quotacheck /dev/dsk/cEd1s0
```

The output might look like:

```
*** Checking quotas for /dev/dsk/cEd1s0 (/users)

/dev/dsk/cEd1s0: dan      fixed    files  12 -> 13     blocks  103 -> 128
```

The columns to the right of Dan's name indicate the `quotas` file for Dan has been fixed, that is, changed to incorporate any changes in the number of files and blocks.

6

Checking File System Consistency

The HP-UX file system can develop inconsistencies over a period of time. For example, turning off the computer without previously shutting down or unmounting the file system will cause some corruption of the system. Except for obvious events, such as a power failure, the causes of file system corruption are difficult to determine.

You should check the file system for consistency periodically and anytime you suspect a problem. Some commands, such as `/etc/update` or `convertfs`, will not function properly unless the file system is free of inconsistencies.

Using the fsck Utility

You can use the `fsck` utility to check file systems for any inconsistencies and to make any necessary repairs. The manual *Solving HP-UX Problems* contains detailed information about using the `fsck` command (see Appendix A, "Using the fsck Command").

Caution When you run `fsck`, make sure the file systems are inactive. The best way to proceed is to:

1. Make sure all users are logged off the system.
2. Issue the command:

   ```
   /etc/shutdown
   ```

   This terminates running processes in an orderly and cautious manner and places the system in single-user mode.
3. Run `fsck` in single-user state. Refer to the manual *Solving HP-UX Problems* when running `fsck`.

7

Managing Swap Space

The **CPU** (Central Processing Unit) divides its time among all **processes** (running programs) that are active at any given time. When a process has received its share of CPU time, or when it reaches a point where the next instruction can't be executed immediately (for example, when the process is waiting for data that has to be retrieved from disk), the process might be **swapped out**, that is, all or part of a process might be moved from main memory to a reserved area that is usually on the `root` (system) disk. This area is known as a **swap area**.

Whether a process actually is swapped out depends on how busy the system is. If the system is not busy (that is, if the active processes are few enough and/or small enough for all of them to fit in main memory), no swapping occurs. There is a daemon that monitors free memory and keeps it to a maximum by cleaning out data that is no longer needed. If it cannot free up enough space to meet demand, it enables swapping.

This chapter explains how to manage your system's swap space. Managing swap space on your system involves determining how much and what type of swap space the system needs, and also involves adding or removing it as the system's needs change.

A complete conceptual discussion of swap space is in the manual *How HP-UX Works: Concepts for the System Administrator*.

Terms Used in this Chapter

The following terms appear frequently in this chapter. You can scan the list now and refer to it later.

device file	A file used by the computer to communicate with a device. Sometimes, a device file is referred to as a "special file" or "device special file." For swapping, the device is usually a disk.
device swap	A disk or area on a disk reserved exclusively for swap space.
dynamically allocatable swap space	Swap space that can be allocated without having to be configured into the kernel. Both device swap and file system swap can be dynamically allocated.
file system	The organization of files on disk into hierarchical directories on a given device.
file system swap	Space within a file system that is used for swapping. File system swap shares disk space with a file system, whereas device swap has exclusive use of a disk space.
interleaved swapping	Swapping where pages are swapped to and from two or more devices on an interleaved basis. This technique reduces the swapping cycle time.
primary swap	The device swap area on the root disk that is available when the system boots.
process	A program running in memory. The image of a process might be temporarily stored on disk, by means of swapping, to free up space in physical memory.
secondary swap	Device swap space used in addition to primary swap. May be configured into the system or added dynamically.
swap in	Reading the process's image from the swap space on the disk into the computer's physical memory.
swap out	Writing the process's image from the computer's physical memory onto the swap space on the disk.
swap space	Space on a disk used for temporarily storing the process image.

Types of Swap Space

HP-UX uses two types of swap space: device swap space and file system swap space. Each type is used differently by the system and each has advantages and disadvantages.

Device Swap

Device swap space occupies a disk or an area on a disk reserved expressly for swapping purposes. At least one device swap area must be available to the system when it boots. This area is known as the **primary** swap area. The primary swap area is configured into the system's kernel at the time of system installation. The system's `dfile` contains the specification for the system's primary swap. You can add **secondary** swap devices by adding other disks.

Device swapping has the advantage of being fast because the system accesses the swap area on the disk directly without going through a file system (as it does in the case of file system swap; see the next section). However, using an area on a disk for device swap only could be an inefficient use of disk space if it goes largely unused.

You can allocate device swap dynamically using either SAM or the `/etc/swapon` command; see the section "Adding, Removing, or Changing Device Swap Space."

File System Swap

7

File system swap space allows a process to use space within an existing file system if it needs more than the allocated device swap space. File system swap space coexists with the device swap space and is used by the system after device swap is used to capacity. When your system only occasionally needs additional swap space, file system swap provides an efficient way to increase it, because it uses unused file system space rather than a dedicated space on a disk that might not be used often. On the other hand, because file system swap requires the system to perform a greater amount of processing and is usually slower than device swap, it is not a good permanent solution.

Calculating How Much Swap Space You Need

Swap space, the disk-based component of virtual memory, must be large enough to hold all the processes that could be running at peak times.

A swap area is configured at the time of system installation; in most cases, the system cannot run without swap space. To take advantage of the memory in your system, at least the equivalent amount of swap space is required.

If system performance is good, and, in particular, if you are not getting swap errors such as

`Sorry pid` *pid number* `was killed due to no swap space`

or,

```
fork: no more space
```

then you do not need additional swap space.

If you know or suspect that you will have to increase (or decrease) your swap space, you can take a two approaches to calculating how much swap space you need:

1. Use the precise but detailed formula in appendix B, "Swap Space Computation."
2. Use a "rule of thumb" method, which is described in the section, "Estimating Swap Space Needs (A Rule of Thumb)."

How Much Swap Do You Have?

To find how much swap space is configured on your system, run the command: *swapinfo*(1M).

```
/etc/swapinfo
```

The output resembles:

```
           Kb       Kb        Kb   PCT  START/        Kb
TYPE    AVAIL     USED      FREE  USED   LIMIT RESERVE  PRI  NAME
dev     75033     3421     71612    5%  222075       -    0 /dev/root
hold        0     5900     -5900
```

The output tells you the type of swap by location, how much of it is available, how much is used, and how much is free.

Under type, in addition to `dev` (device) and `fs` (file system), you might see "`hold`." The operating system can "hold," or reserve, an amount of swap space (from no specific device or file system) based on the possible requirements of currently running processes. This is a means to ensure currently running processes do not run out of swap space. It is possible that a new process will not be able to start until another process terminates.

Until a process terminates, swap space held for it cannot be allocated to or held for new processes.

7

Estimating Swap Space Needs (A Rule of Thumb)

By adding the swap space required by your largest application to the amount of swap space your system has initially configured, you can estimate the total swap space needed.

Use the following to estimate the swap space requirements. Remember, 1 Kbyte = 1024 bytes.

1. Determine the swap space (in Kbytes) required by your largest application (look in the manual supplied with your application or ask the manufacturer). If you will be running several applications concurrently, you should add their swap space requirements together.	___________
2. Add the current amount of swap space on your system based on the output of the `swapinfo` command.	___________
TOTAL swap space needed (in Kbytes); sum of 1 and 2.	___________

7

Swap Space Default

The default maximum amount of swap space you can configure—for both device swap and file system swap combined—is approximately 1,073 Mbytes. The tunable system parameter *maxswapchunks* controls this maximum.

The parameter *maxswapchunks* (default value of 256) limits the number of swap space chunks. The size of each chunk of swap space is the product of *swchunk* (default value of 2048) and `DEV_BSIZE`, the size of a disk sector. Typically, `DEV_BSIZE` (see the file `/etc/disktab`) has a value of 1024 bytes.

For example, when the value of the parameter *maxswapchunks* is 256, the maximum configurable device swap space (*maxswapchunks* x *swchunk* x `DEV_BSIZE`) is:

```
256 x 2048 x 1024 bytes = 537 megabytes
```

If you need to change the limit of configurable swap space from the default, increase the value of the tunable *maxswapchunks* operating system parameter. To change the values of any system parameters, you will need to reconfigure your system's kernel. You can use either SAM or HP-UX commands to change system parameters and regenerate a new kernel. See Chapter 2, "Constructing an HP-UX System", for details about reconfiguring the kernel.

More detailed discussions of the system parameters is located in Appendix A, "System Parameters".

Allocating Swap Areas: Guidelines

After determining how much swap space your system needs, you need next to consider how you are going allocate the swap space.

Guidelines for Selecting Device Swap Areas

When you installed HP-UX on your system disk, you configured a certain amount of space on that disk for swap. You can add device swap space by adding another disk, using it entirely for swap, or partly for device swap and partly for file storage. The maximum number of devices (the default is 10) you can use for swap is controlled by the value of the `nswapdev` parameter. Appendix A, "System Parameters", contains information about the `nswapdev` parameter.

When adding a disk you intend to use for both a file system and device swap, you can use SAM. If you do not plan to use SAM, you will need to build the file system using the `newfs` command. Refer to the file `/etc/disktab` for the disk layout options that can be used with the `newfs` command; the `newfs` command is discussed in Chapter 6, "Managing the File System".

If you want to add a disk that will be used as the root disk, you must consider that an area for a boot program, which you must later install using the `mkboot` command, will use some of the space that would otherwise be used for swapping.

From the performance point of view, two device swap areas, each on a separate disk, are better than one swap area with the equivalent amount of swap space. This allows **interleaved swapping**; that is, where swapping I/O transactions (writes) are alternated or interleaved between the devices. Two memory pages, if they are contiguous, are written to only one device.

Two device swap areas should be of similar size for best performance because, otherwise, when all space in the smaller device swap area is used, the larger swap area is all that is available and interleaving is no longer possible.

When increasing your device swap space,

- If you are limited to only one disk and need to increase device swap space, you will have to reinstall HP-UX, specifying a larger-than-default swap size. See the section titled, "Reinstalling HP-UX to Increase Primary Swap Space." File system swap might provide a better solution.

- If you are adding a new disk for swap space, decide whether you want to use the entire disk for swap or want to use the disk for both a file system and swap.

  Figure 7-1 shows various ways to configure disk space for file system and swap. In each of the example configurations, disk 1 holds the root file system. Figure 7-1a and Figure 7-1b show the best configurations. Figure 7-1d shows the default configuration. The configuration in Figure 7-1c is difficult to achieve because the installation process automatically leaves some swap space on the root disk. You must remake your file system to consume this space that was automatically allocated at installation.

Examples later in this chapter show you how to add device swap space.

```
a.                                      b.
  ----------     ----------               ----------     ----------
 |          |   |          |             |          |   |          |
 |   File   |   |   File   |             |   File   |   |          |
 |  System  |   |  System  |             |  System  |   |          |
 |          |   |          |             |          |   |   Swap   |
 |          |   |          |             |          |   |          |
 ------------   -----------              ------------   |          |
 |   Swap   |   |   Swap   |             |   Swap   |   |          |
 |          |   |          |             |          |   |          |
  ----------     ----------               ----------     ----------
    Disk 1         Disk 2                   Disk 1         Disk 2


c.                                      d.
  ----------     ----------               ----------
 |          |   |          |             |          |
 |          |   |          |             |   File   |
 |   File   |   |          |             |  System  |
 |  System  |   |          |             |          |
 |          |   |   Swap   |             |          |
 |          |   |          |             ------------
 |          |   |          |             |   Swap   |
 |          |   |          |             |          |
  ----------     ----------               ----------
    Disk 1         Disk 2                   Disk 1
```

Figure 7-1. Device Swap Space Configurations

Guidelines for Selecting File System Swap Areas

When you need more swap space and you have no devices available for additional device swap, you can dynamically add file system swap to your system.

Use the following guidelines:

- To keep good system performance, avoid using heavily used file systems. Do not use `root` for file system swap.
- Use the `bdf` command to check file systems for available space. For example,

  ```
  bdf

  Filesystem          kbytes    used    avail capacity    Mounted on
  /dev/dsk/c7d0s0     247308  150363    72214    68%      /
  /dev/dsk/c7d1s0     237810   77532   136497    36%      /users
  ```

  You can also use the `swapinfo` command to show information about file systems for which swap might be already enabled.
- Enabling file system swap allows more processes to run simultaneously and might result in slower system response time.
- The maximum number of file systems you can swap to is controlled by the value of the `nswapfs` parameter (which can range up to ten). Appendix A, "System Parameters", contains information about the `nswapfs` parameter.

7

Guidelines for Using File System Swap in Clusters

File system swap can be configured on the root server's disk and on any client's disk.

- You must be logged in to the node that has the disk (root server or auxiliary server) to enable swap to a file system that physically resides on that disk.

  For example, in the cluster shown in Figure 7-2, `server` cannot enable swapping to `/users/fred` or `/users/joe`.

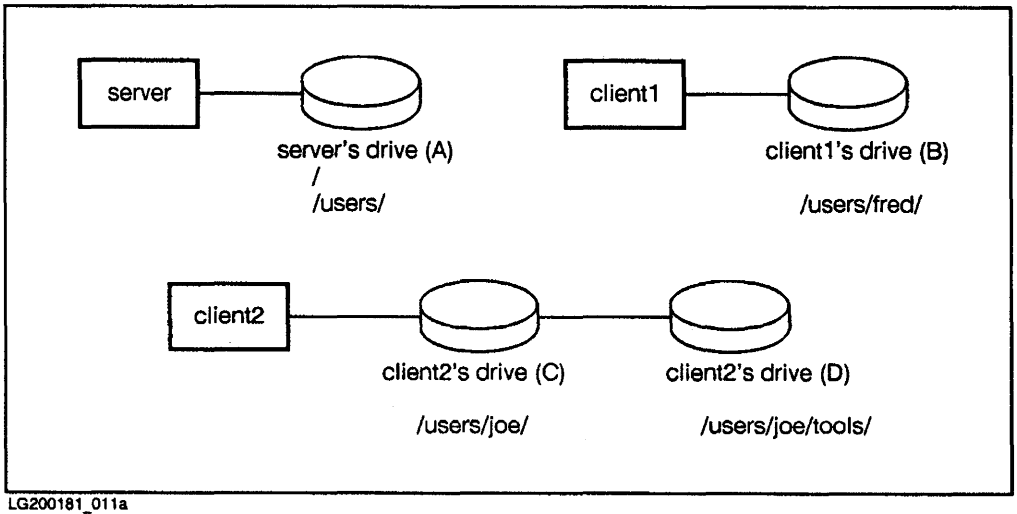
- Once a root server or auxiliary server has enabled swapping to a file system, all nodes swapping to this root or auxiliary server will swap to that file system.

  For example, in the cluster shown in Figure 7-2, if `client1` is a swap server for `client2`, and `client1` enables swapping to the locally mounted file system `/users/fred`, then both `client1` and `client2` will start swapping to `/users/fred`.

  See "Setting up Swap to an Auxiliary Server", under "Local Disks" in Chapter 12, "Adding Peripherals to a Cluster" in *Managing Clusters of HP 9000 Computers* for information on setting up swap to another client's local disk space.

  Directions for setting up file system swap are covered in the sections, "Adding File System Swap Using SAM" or "Adding File System Swap Using `/etc/swapon`" in this chapter.

File system swap in a cluster conforms to the same rules as device swap: each node still swaps to only one node's disk space, and root and auxiliary servers swap to their own disk space.



LG200181_011a

Figure 7-2. Swapping to File Systems in a Cluster

Guidelines for Assigning Swap Priority

Each swap area requires an assigned priority. The system uses the swap areas with higher priority first. If you assign the same priority to two different swap areas, the system uses each of them on an alternating, or interleaved basis. The system gives device swap priority over file system swap when each has the same priority.

7

In general, it's best to assign highest priorities to the swap areas that afford the fastest performance. This means: give device swap areas priority over file system swap areas, give faster devices priority over slower devices, and give lower-use file systems priority over higher-use file systems.

The primary swap area has priority zero (priorities range from 0, the highest, to 10, the lowest). Device and file system swap areas enabled dynamically default to a priority of one if you do not specify a priority.

Adding, Removing, or Changing Device Swap Space

Changing your device swap space means that you will be performing at least one of the following tasks:

- Add another disk, using it in part or entirely for secondary swap. If you use the disk in part for swap, you can use the remaining disk space for file storage.
- Remove a secondary device swap area.
- Change primary swap space. This is most easily done by adding a disk. If you have only the system disk available and need more than the amount of device swap space available after installation of your system, you will have to reinstall your operating system, specifying a larger-than-default swap space. See the section "Reinstalling HP-UX to Increase Primary Swap Space."

Note If you have created a recovery system by using `mkrs` (see "Creating a Recovery System" in chapter 2), you must create a new recovery system whenever you alter the swap space configured on your system. Booting a recovery system that uses an older record of swap space addresses could result in the loss of data.

Changing Primary Swap

You can change the location of the primary swap area, which is the device swap area that is available when you boot your system. Initially, the primary swap area is specified at the time of system installation and is located on the root disk. After installation, you can edit the kernel configuration input file (usually the `dfile`) to respecify the location of the primary swap area, and regenerate a new kernel.

This section describes only the necessary `dfile` entries; Chapter 2, "Constructing an HP-UX System" describes the procedure for reconfiguring the kernel. Refer also to the *config*(1M) entry in the *HP-UX Reference*.

Specifying Primary Swap Devices in the dfile

The first entry in the swap section of the `dfile` specifies the *primary* swap area. Look for the commented line, `* Swap info`. This line introduces the swap section of the `dfile` and is not an actual entry.

By default, the root device swap area is the primary swap area. This is indicated by a blank line or a line that reads `swap auto` following the comment line, `*Swap info`.

For example,

```
* Swap info
swap auto
```

If you want to configure primary swap on a disk other than the root disk, or if you want to configure primary swap with options, you can use the following format for the first swap entry:

`swap` *devname address swap_location* [*nswap*]

devname Device driver name as it appears in the `/etc/master` file.

address Minor device number in hexadecimal (without the preceding `0x`). For example, `e0100` for a disk at select code 14, HP-IB address 1.

swap_location `-1` specifies that the swap space follow a file system on the disk.

7

`0` specifies that the entire disk is to be used for swap; `0` implies there is no file system on the disk.

nswap (Optional.) A number, in decimal format, specifying the maximum number of one-KB disk blocks to be used for swap.

Example. To specify a SCSI disk that will be used entirely for primary swap, add the following swap entry in the `dfile`, assuming the disk is connected to the internal SCSI interface and has its bus address set to 1:

```
* Swap info
swap cs80 e0100 0
```

Specifying Secondary Swap Devices in dfile. Although you can specify secondary swap devices in the `dfile`, it is neither recommended nor necessary because swap devices can be added by using either SAM or the `swapon` command. See the sections "Adding Device Swap Using SAM" and "Adding Device Swap with the /etc/swapon Command."

If you *do* specify other swap devices in the swap section of the `dfile`, their entries must follow the first—or primary—swap entry.

Core Dump Areas

Disk space is required by the system to write, or "dump," an image of the core memory after a system crash. This "core dump" is useful in troubleshooting and restoring the system to working order.

By default, the primary swap area is used for a core dump. The kernel can immediately use the dump area during a crash, and so that the `savecore` command can locate the core dump during boot after a crash.

Reinstalling HP-UX to Increase Primary Swap Space

If you have only one hard disk and must increase device swap space, you must reinstall HP-UX, specifying a larger than default swap size. Remember, if you reinstall with a larger swap area, the space remaining for the file system will be reduced, so consider the size of your file system as a factor.

If you choose to reinstall HP-UX, you can use the following outline of steps:

1. Determine how big you wish your swap space to be using the guidelines in this chapter.
2. Back up the entire file system using the procedures in the chapter titled "Backing Up and Restoring Your System."
3. Reinstall HP-UX, this time specifying the larger swap size in the `File System Parameters` menu. Refer to the *Installing and Updating HP-UX* manual for the instructions on how to install HP-UX.
4. Restore your files from the backup created in step 2.

Using SAM

To use SAM,

- Ensure that you have superuser capabilities.
- Type:

  `/usr/bin/sam`

  Activating the (Help) button from a dialog or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

  Choosing an item from the "Help" menu within a functional area gives you information about:

  - the current functional area
  - keyboard navigation within SAM
  - using the SAM help system
  - displaying the version of SAM you are currently running

Pressing the (f1) key gives you context-sensitive information for the object field at the location of the cursor.

See Chapter 1, "Introduction to System Administration" for additional information about using SAM. If you aren't familiar with SAM, take a moment to look at that overview material. There is a help system in SAM to assist you.

Adding Device Swap Using SAM

To enable device swap, disk space must be available, either an entire disk or a disk with a file system followed by a space reserved for swap.

The reserved space becomes available when you add the disk and specify that you want to use the disk for:

- Both a file system and swap, or
- Only swap.

If you have not yet installed the disk, refer to the *Installing Peripherals* manual for instructions on adding your disk.

Adding Device Swap When Creating a File System on a Disk

When you have added the disk and restarted your computer, you can add swap using SAM as follows:

1. Run SAM.
2. Highlight `Disks and File Systems-->` and activate the (Open) control button.
3. Highlight `CD-ROM, Floppy, and Hard Disks` and activate the (Open) control button.

   SAM displays a list of disks.
4. From "Actions" on the menu bar, choose `Add a Hard Disk Drive...`.
5. Activate the control button `Select a Disk to Add...`. A list of the unused disks will display.

   If the device you are adding does not appear on the list, SAM can provide you help to find it or make it accessible. Activate the `Device Missing...` control button. SAM will direct you through a diagnostic process.

   When you have successfully added your disk, you can resume.
6. Highlight the disk you are adding and activate (OK) to select it.
7. Activate the `Set Disk Usage and Options...` control button.

8. In the menu bar labeled: "Use disk for:," choose `File System and Swap`.
9. Assign a mount directory for the file system.

   Enter the name of a new or an existing empty directory in the field: `Mount Directory:`. This is where the new file system will join the existing file system hierarchy. If the directory you specify does not exist, SAM will create it for you. (See the previous chapter on "Managing File Systems" for more discussion of mount directories.)
10. Choose a priority for the device swap on the "Swap Priority" menu bar. (See "Guidelines for Assigning Swap Priority" if necessary.)
11. Activate the `Create new file system` control button. You must create a file system on a new disk in order to create the reserved swap area following it.
    a. When the file system options appear, you can modify the defaults, if necessary.
    b. Highlight the appropriate combination of "Swap" and "File System" space from the list of choices on the "Disk space allocation" listing. See "Calculating How Much Swap Space You Need" if you don't know what value to use for swap.
12. Activate (OK) to confirm your choices.
13. Skip the `Modify Default Options.......` control button, unless you want to change `When to Mount`, the `Access Permissions`, or the `Set user ID` default settings for the file system you are adding. If you want to modify the default options, SAM's (Help) can provide information.
14. Activate (OK) to confirm your choices.

7

15. Activate OK to have SAM set up both the file system and the device swap space you specified.

    SAM reports its actions as it creates and sets up the file system and swap area.

16. Activate OK to confirm to SAM you have seen the messages. The disk you set up for a file system and swap will now appear in the "Use" column, labeled "`hfs/swap`".

    You have successfully created a file system and added the swap area. They are now ready for use. The `/etc/checklist` file will reflect the additions.

Adding a New Disk For Swap Using SAM

This procedure is very much like the previous one, except the swap area does not share the disk space with a file system.

1. Run SAM.
2. Highlight `Disks and File Systems-->` and activate the Open control button.
3. Highlight `CD-ROM, Floppy, and Hard Disks` and activate the Open control button.

   SAM displays a list of disks. The disk you added will be labeled "`unused`" in the `Use` column.

7

4. Highlight the disk you are adding.
5. From "Actions" on the menu bar, choose `Add a Hard Disk Drive...`.
6. Activate the control button `Select a Disk to Add...`. A list of the unused disks will display.
7. Highlight the disk you are adding and activate OK to select it.
8. Activate the `Set Disk Usage and Options...` control button.
9. In the menu bar labeled: "Use disk for:," choose `Swap Space`.
10. Adjust the priority, if necessary. (See "Guidelines for Assigning Swap Priority" if necessary.)

11. Activate OK to confirm your choices.

12. Skip the `Modify Default Options.......` control button, unless you want to change any defaults. SAM's Help can provide information. Activate OK to confirm your choices.

13. Activate OK to have SAM set up the device swap space you specified.

    SAM reports its actions as it sets up the swap area for use.

14. Activate OK to confirm to SAM you have seen the messages. The disk you set up for swap will now appear in the "Use" column, labeled "**swap**".

    You have successfully added the swap area. It is now ready for use. The `/etc/checklist` file will reflect the addition.

7

Making Changes to Device Swap Using SAM

You can change the characteristics of the existing device swap areas. You can:

- Enable or disable swap areas.

  For example, you might want to set up a swap area that is not automatically enabled when the system boots, but that can be enabled dynamically later.

- Change swapping priority of each swap area.

You can change the characteristics of swap areas in SAM as follows:

1. Run SAM.
2. Highlight `Disks and File Systems->` and activate the (Open) control button.
3. Highlight `Swap` and activate the (Open) control button.
4. Highlight the disk that contains the swap area that you want to modify.
5. From "Actions" on the menu bar, choose `Modify Swap`.
6. On the screen that follows, you can use control buttons to control when swap is enabled.
   a. If the swap is currently enabled, you can disable the swap area by deactivating the `At Every System Boot` control button and rebooting the system. (Device swap cannot be dynamically disabled).
   b. If the swap is currently disabled, you can enable the swap area by activating the `Now` control button. The swap will be enabled immediately.
7. You can also use the `Swap Priority` control button. See "Guidelines for Assigning Swap Priority".
8. Activate (OK) to make the changes.

   SAM reports its actions. Activate (OK) to confirm you have seen the messages.
9. SAM displays the swap device and its changed priority on the "Swap" list. Note, however, that the new priority does not go into effect until the system reboots.

Adding File System Swap Using SAM

When no devices are available to use for swapping, you can use the vacant space within file systems for swapping. When you enable a file system for swap, the operating system can allocate the file system's free space when it needs it, and free up that space for the file system's use when it no longer needs it.

Several file systems (up to ten) can be used for file system swap. The tunable system parameter `nswapfs` determines the maximum number of file systems that can be enabled for swap.

You can add file system swap by using SAM. File system swap is enabled dynamically, that is, while the system is running.

The following outline lists the steps for adding file system swap using SAM:

1. Run SAM.
2. Highlight `Disks and File Systems-->` and activate the Open control button.
3. Highlight `Swap` and activate the Open control button.
4. Highlight the device file for the file system that you want to enable for swap.
5. From "Actions" on the menu bar, choose `Add File System Swap...`.
6. From the list displayed, choose the file system you want to use for swap. (The file systems are listed by their mount directories.)
7. Enter values in the fields for "Minimum Swap (Kbytes)" and "Maximum Swap (Kbytes):" These values specify, respectively:
   a. the minimum amount of the file system space you are designating as usable only for swap. This amount of space within the file system will not be used for file storage.
   b. the maximum amount of file system space you want used for swap. This value lets you keep a specific amount of file system space for file system only.

Note, you must enter values in these fields. SAM will convert the entered value to a value in terms of the file system block size, usually four or eight kilobytes (Kbytes).

However, disk space for swap is a function of the product of *swchunks* (a tunable system parameter, 2048 by default) and the value of `DEV_BSIZE` (defined in `/etc/disktab`, typically 1024 bytes). A typical swap space chunk is 2 megabytes (2048 kilobytes). If you specify 1000 kilobytes as a minimum, for example, the actual minimum chunk of swap space allocated would be 2048 kilobytes.

8. Designate the priority and when you want the swap enabled.
9. Activate [OK] to enable the file system swap.

Changing File System Swap Values Using SAM

The SAM `help` screens provide instructions and suggestions for changing the values currently set for file system swap. Once file system swap is enabled, the `minimum` value cannot be changed; the `maximum` swap value can be increased (but not decreased).

Adding Device Swap with the /etc/swapon Command

To add secondary device swap sections without using SAM, you can use the `/etc/swapon` command. (See the entry for *swapon*(1M) in the *HP-UX Reference*.)

When you're using `/etc/swapon` to add device swap, follow the steps outlined below; details and examples follow.

1. Add the disk you plan to use for device swap following the instructions in the *Installing Peripherals* manual. You can add either a new disk or a disk with an existing file system on it.
2. Determine the *block* device file name for the disk you're adding. The system needs to know this name to send and retrieve data to and from the disk. If the device file does not exist, you will need to create it using the `/etc/mknod` command. This section contains examples, but if you are not familiar with how to create device files, refer to the *Installing Peripherals* manual.
3. Decide whether you want to use the disk you are adding entirely for swapping or for both file storage and swapping.

   If the disk you're adding is new and you plan to use the disk in part for file storage, then you must create the file system by running the `newfs` command, specifying the *disk-type* listed in the `/etc/disktab` file that reserves the appropriate area for swap (and *boot* area, if needed).

   If the disk you are adding already has an existing file system plus space for swap following the file system, you can enable that space for swap by using the `swapon` command with the `-e` option.
4. Determine the priority you want to assign to the secondary swap device. The system uses higher priority swap devices before lower priority devices. If you don't assign a priority, the swap area will receive the default priority of 1.
5. Enable your secondary swap device by running the `/etc/swapon` command. This makes your swap device available for use immediately.
6. Modify the `/etc/checklist` file by adding an entry for your secondary swap device if you want it enabled each time you boot your system.

Add Your Disk

You can add a new disk exclusively for swap or a disk that contains a file system and space for swap on it. In either case, you can add your disk following the instructions in the *Installing Peripherals* manual.

Creating Device Files for Your Disk

You will need both `character` and `block` device files for the disk you are adding. To use the disk for device swap, you need to specify the *block* device file name that corresponds to the disk when you issue the `/etc/swapon` command. Also, if you need to create a file system on the disk, you will need to specify the *character* device file when you issue the `newfs` command.

You can create device files using the `mknod` command. The syntax is described in Chapter 6, "Managing the File System". The following examples show how to use the command to make the device files.

7

Creating the Block Device File

For this example, suppose you are adding an HP-IB disk to the interface card with select code 7 and have set the bus address on the disk to 2 because it is the third disk (the root disk has its bus address set to 0). To make the *block* device file for the disk, use the following command:

```
/etc/mknod /dev/dsk/c7d2s0 b 0 0x070200
```

In the device file name, `/dev/dsk/c7d2s0`, `dsk` is the directory for block device files for disks. The device file, `c7d2s0`, has the following significance:

- `c`*N*`d` - where *N* is a hexadecimal number (uppercase alphabetical characters) that signifies the disk's controller; that is, the select code set on the interface card.
- *n* - where *n* is a hexadecimal number (uppercase alphabetical characters) that signifies the bus address set on the disk drive.
- `s0` - the section number, always `s0`.

There are other conventions for naming device files. For example, you can assign individual device file names for individual platters and sides of platters in the case of optical disk libraries, and you can assign device files to disks in hardware-based disk arrays. See *Installing Peripherals* for details if you are creating device files for these types of disks.

In the next fields, `b` specifies that the device file is for a block device, `0` is the major number for a CS-80 type disk used as a block device. The minor number, `0x070200`, is a hexadecimal number which indicates the device is at select code 7 (`07`) and uses bus address 2 (`02`). (`0x` indicates that the number is hexadecimal, and the final `00` doesn't apply to this example.) More discussion of the significance of minor numbers is included in the manual *How HP-UX Works: Concepts for the System Administrator*. 7

Note Detailed discussions of major and minor numbers are contained in the *Installing Peripherals* manual.

Creating the Character Device File

Continuing the example shown to make the block device file, you can use the following command to make the *character* device file for the disk.

```
/etc/mknod /dev/rdsk/c7d2s0 c 4 0x070200
```

`rdsk` is the directory for character device files for disks. `c` specifies the file is for character devices and `4` specifies the major number for a CS-80 type disk used as a character device. Notice that the minor number is the same in both commands.

Listing the Device Files

You can list device files on your system.

For example, listing the files with the `ll` command in `/dev/dsk` directory might yield the following:

```
total 0
brw-r-----   1 root     sys          0 0x0e0000 Aug  3 13:11 cEd0s0
brw-r-----   1 root     sys          0 0x0e0100 Jul 25 12:53 cEd1s0
brw-r-----   1 root     sys          0 0x070200 Aug 27 11:54 c7d2s0
```

The third line in the listing shows the block device file created in the example command above.

Determine the Overall Usage of the Disk

You can use the disk for swap exclusively, or for both a file system and swap.

If the disk you added already has space for swap beyond an existing file system, or, if you've added a new disk and plan to use it entirely for swap, you can enable device swap using the `/etc/swapon` command; skip the remainder of this sub-section and proceed to the next section, "Determining the Priority for the Secondary Swap Device."

However, if you've added a new disk and plan to use the disk's space for both a file system and for swap, then you will need to run the `newfs` command to create the file system, choosing an optional disk layout specified in the `/etc/disktab` file that reserves an area for device swap.

For example, suppose your new disk is an HP 2213A. When you look in the file `/etc/disktab` by typing,

```
more /etc/disktab
```

you will find the following optional layouts available for your disk:

```
hp7937|hp7937S|HP_7937S:\
 :48 MBytes reserved for swap & boot:ns#25:nt#16:nc#1272:\
       :s0#508800:b0#8192:f0#1024:\
       :se#256:rm#3600:
hp7937_64MB|hp7937S_64MB:\
 :64 MBytes reserved for swap & boot:ns#25:nt#16:nc#1231:\
       :s0#492400:b0#8192:f0#1024:\
       :se#256:rm#3600:
hp7937_80MB|hp7937S_80MB:\
 :80 MBytes reserved for swap & boot:ns#25:nt#16:nc#1190:\
       :s0#476000:b0#8192:f0#1024:\
       :se#256:rm#3600:
hp7937_96MB|hp7937S_96MB:\
 :96 MBytes reserved for swap & boot:ns#25:nt#16:nc#1149:\
       :s0#459600:b0#8192:f0#1024:\
       :se#256:rm#3600:
hp7937_noreserve|hp7937_noswap|hp7937S_noreserve|hp7937S_noswap:\
 :no swap or boot:ns#25:nt#16:nc#1395:\
       :s0#558000:b0#8192:f0#1024:\
       :se#256:rm#3600:
```

Let's suppose that the second option, the option that sets up 64 MBytes of swap, is appropriate for your swap requirements. Also, assuming the default **newfs** file system options are suitable, issue the following **newfs** command:

```
newfs /dev/rdsk/c7d2s0 hp7937_64MB
```

Note the character device file used is the one you created with the **mknod** command.

Note You can find more information and procedures about creating file systems in Chapter 6, "Managing the File System".

Determining the Priority for the Swap Device

You can assign priorities for swap devices (and file system swap areas, too; see "Specifying a Priority for File System Swap"). Priorities range from 0 (highest) to 10 (lowest). Swap spaces with the highest priorities are used first by the system.

For example, you can assign the highest priorities to swap areas on disks that transfer data the fastest, and assign the lower priorities to swap areas on the slower disks.

Enabling Your Swap Device with the /etc/swapon Command

After you have added a disk, determined its block device file name, and determined its priority, you can enable it using the `/etc/swapon` command.

For example, suppose you have added a third disk and intend to use it *entirely* for swap. You want to assign it priority 1. Type the command as follows:

```
/etc/swapon -p 1 /dev/dsk/c7d2s0
```

The priority is assigned with the `-p` option.

Using the -f option

You must use `/etc/swapon -f` to overwrite an obsolete file system on a disk to be used entirely for swap. You will not receive a warning that a file system is being overwritten.

Caution Use the `-f` option with extreme caution. The destruction of the files is permanent unless you have backed them up to other media.

Using the -e option

Suppose you have added a new disk to your system and have created both file system and swap space on the disk. You can enable that swap space using the `/etc/swapon` command with the `-e` option. The `-e` option enables the swap space that was reserved when the file system was created. If you want to assign priority 1 to the device swap area, you would type the command as follows:

```
/etc/swapon -e -p 1 /dev/dsk/c7d2s0
```

Note If you are enabling device swap on a disk that contains a file system, you must use the `-e` option, which sets up swapping in the space beyond the file system.

Enabling Your Swap Device Each Time You Boot the System

7

The device swap area will be enabled each time you boot the system if you include an entry for it in the `/etc/checklist` file (*checklist*(4)). For example, for the device swap you enabled in the example above, add a line in the `/etc/checklist` as follows:

```
/dev/dsk/c7d2s0 /swap swap end,pri=1 0 0 #secondary swap
```

See a detailed discussion of device swap area entries in `/etc/checklist` in the section, "Making Entries for Device Swap in the Checklist File."

The system initialization file `/etc/rc` normally contains the command `/etc/swapon -a` so that all swap areas (both device swap and file system swap) listed in the `/etc/checklist` file become enabled when the system boots.

Making Entries for Device Swap in the Checklist File

Look at the following example entry in an `/etc/checklist` file:

```
/dev/dsk/c7d1s0   /swap    swap  pri=0 0 0 # swap area
```

Entries for device swap in `/etc/checklist` have seven fields separated by blank space. In each field, you need to put either an entry or a placeholder. The following describes making entries for each field.

- First field: Enter the *block device file* corresponding to the disk used for swapping.
- Second field: For device swap, enter a placeholder. For example, you could enter the mount point *directory* for the disk corresponding to the special device file.
- Third field: Enter the *type* of the entry, which for device swap is `swap`.
- Fourth field: Enter *options* here. Priority is indicated by `pri=`*n*, where *n* can range from 0 to 10. The default for priority is 1. If you are adding an entry for a disk that contains a file system, include `end` in the options field to specify that the swap space is in the area between the file system and the end of the disk. If you do not specify any options, use "defaults" as a placeholder.
- Fifth and sixth fields: Enter the placeholder `0` in each of these fields, because they are not necessary for device swap.
- Seventh field (optional): you can enter a comment preceded by the `#` character.

Example, Adding Device Swap Using /etc/swapon

In this example, assume you want to add a new HP7937 disk and use the disk for both a file system and swapping. Following the instructions in the manual *Installing Peripherals*, connect your disk, identify the select code of the interface card, and set the bus address on the disk.

Let's assume you have added the disk to the interface card with select code 7 and set the disk's bus address to 1.

1. Create both the block and character device files for the disk. Run the `/etc/mknod` as follows:

   ```
   mknod /dev/dsk/c7d1s0 b 0 0x070100
   ```

   For the character device file, run:

   ```
   mknod /dev/rdsk/c7d1s0 c 4 0x070100
   ```

2. Use the `newfs` command to create the file system. You want to use the disk in part for both swap and file storage. When you examine the `/etc/disktab` file, you determine that the option `hp7937_80MB`—that is, the option that specifies 80 MBytes swap space—will meet your calculated needs.

   Issue the following command (note: `newfs` requires the character device file):

   ```
   newfs /dev/rdsk/c7d1s0 hp7937_80MB
   ```

3. Run `/etc/swapon` to enable swap. Because the disk now has file system space, you will have to use the `-e` option. The default priority of 1 is suitable. (Note: `/etc/swapon` requires the block device file.)

   ```
   /etc/swapon -e -p 1 /dev/dsk/c7d1s0
   ```

   The new device swap area is now available.

4. Now, edit the `/etc/checklist` file so that the newly added secondary swap areas will be enabled each time you boot the system. To do this, add the following line:

   ```
   /dev/dsk/c7d1s0 /swap swap pri=1 0 0 # secondary device swap
   ```

Removing Device Swap Using HP-UX Commands

You might want to remove device swap you have set up, perhaps because it is no longer needed or large enough.

To remove any device swap you have set up:

1. Edit the `/etc/checklist` file to remove the entry for the specific device swap area you want to remove. Skip this step if you never added an entry in `/etc/checklist` for this device swap area.
2. Reboot your system by running `shutdown -r`. Before issuing this command, make sure no users have either files open or processes running that could be corrupted by the shutdown.

Adding File System Swap Using `/etc/swapon`

When no devices are available to use for swapping, you can use the vacant space within file systems for swapping. When you enable a file system for swap, the operating system can allocate the file system's free space when it needs it, and free up that space for the file system's use when it no longer needs it.

Several file systems (up to ten, by default) can be used for file system swap. The tunable system parameter `nswapfs` determines the maximum number of file systems that can be enabled for swap.

You can add file system swap by using the `/etc/swapon` command. File system swap is enabled dynamically, that is, while the system is running.

You cannot remove file system swap dynamically, although you can edit `/etc/checklist` so that it is not enabled after the next system boot. See "Removing File System Swap Using HP-UX Commands."

Adding File System Swap

If you do not use SAM to add file system swap, use the `/etc/swapon` command.

The following is a summary of the steps to enable file system swap on your system; details and examples are in the following sections.

1. Choose a file system for swap space use.
2. Determine the mount point directory (or the root directory) of the file system.
3. Choose values for the parameters of the `/etc/swapon` command. The parameters, all of which are optional, allow you to customize how your file system swap will work.
4. Run `/etc/swapon` with desired options.
5. Add your file system swap to the `/etc/checklist` file if you want the new file system swap enabled on boot.

Choosing a File System for Swap

Follow the guidelines in the earlier section, "Selecting File System Swap Areas." The file system you designate for swap space use must be mounted. You can designate the file system you want to use for swap by specifying the mount point directory of that file system.

Determine Mount Point Directory of the File System

Specify the absolute path name of the mount point directory for the swap file system in the `/etc/swapon` command line. The mount point directory for the file system can be determined by listing the contents of the file `/etc/mnttab`; the mount directory is listed in the second field.

Choosing Values for /etc/swapon Parameters

The following table discusses the optional parameters you might use for the `/etc/swapon` command when adding file system swap. An example, which makes use of these parameters, is in the following section, "Example, Setting Up File System Swap with /etc/swapon."

/etc/swapon Parameters

Option	What it Does	How you use it
-m	Specifies an initial amount of swap space	Use the `-m` option to specify the number of file system blocks to be initially taken for swap. File system blocks allocated for swap with `-m` option are never returned to the file system. The system allocates swap space in the file system when it requires it and frees it up when it no longer needs it. So, it might be unnecessary to use the `-m` option unless the file system is heavily used. The default amount of initial swap space is 0.
-l	Specifies a limit to file system's swap space.	Specify a limit to how much of the file system space you want to use for file system swap. The default limit is 0, that is, there is no limit to the amount of file system space that the system can use for swap. Use the `-l` option to specify an amount of file system blocks for a limit.
-r	Specifies reserve space for the file system.	Specify that part of the swap file system be reserved exclusively for the file system. The default value is 0, meaning no space is reserved for file system. Use the `-r` option to specify a number of file system blocks to reserve for the file system.
-p	Specifies a priority for file system swap.	The system allocates swap space on devices or in file systems with the highest priority (that is, lowest priority number) first. The default priority value is 1. Use the `-p` option to specify another priority in the range from 0 to 10.

Example, Setting Up File System Swap with /etc/swapon

Let's assume you want to set up swap in the `/extra` file system. You have run the `bdf` command and determined that `/extra`, a file system that is not used often, has ample space available for swap use. You also want to have this file system swap area available for use each time you boot, so you must add an entry in the `/etc/checklist` file. You would do this as follows:

1. Evaluate the values you want to specify for the parameters of the `/etc/swapon` command. For this example, we will make the following assumptions:
   - You are not concerned that file system space will be unavailable initially for swap because the file system has more than enough space for both the file system and swapping. Therefore, you do not need to specify that space be initially enabled for swap. You will let the system take file system space as it needs it.
   - You do want to limit the amount of file system space that can be used by the system to 5,000 file system blocks.
   - You want to reserve 10,000 file system blocks for the file system's exclusive use.
   - You want the file system swap to be accessed after a device swap area that you have previously set up with priority 0, so you decide you will assign the new file system swap priority 1.

Note

The `swapon` parameters for file system swap require values in file system blocks. The size of a file system block is determined when the file system is created, and is variable.

If you are not sure of the block size used by the file system you want to set up swapping to, you can use the command:

`dumpfs` *file_system* `| grep bsize`

In the listing, look at the value to the right of "bsize" to see the current block size used by the file system. The value is in bytes.

Also remember that the operating system will allocate the swap area in chunks, typically 2048 kilobytes in size (see "Swap Space Default"). For reference, a typical 2-megabyte chunk of swap space is 512 4096-byte file system blocks.

2. To activate swapping to this file system immediately, run the `/etc/swapon` command using the parameter values you have chosen:

   `/etc/swapon -l 5000 -r 10000 -p 1 /extra`

3. To verify that you have enabled your new file system, run the command *swapinfo*(1M). You should see a listing similar to the following after entering the command; note the line that begins "fs".

```
swapinfo

Kb      Kb      Kb    PCT  START/      Kb
TYPE    AVAIL   USED    FREE  USED   LIMIT RESERVE  PRI  NAME
.
dev     48560   1888   46672    4%       -       -    0 /dev/dsk/c7d1s0
fs       6144      0    6144    0%    6144       0    1 /sizzle
          .
          .
```

7

4. Add an entry for file system swap in the `/etc/checklist` file if you want your file system swap to be enabled when you boot your system. The command **`swapon -a`** is contained in the `/etc/rc` file and causes all swap areas listed in `/etc/checklist` to be enabled. (Note that because the file system must be mounted before file system swap can be enabled, the file system itself must also have an entry in `/etc/checklist`.)

   An entry in `/etc/checklist` for the file system swap area in the previous example will look like:

   ```
   default /extra swapfs lim=5000,res=10000,pri=1 0 0
   ```

   A detailed discussion of file system swap area entries in `/etc/checklist` is located in the later section, "Making Entries for File System Swap in the Checklist File."

7

Making Entries for File System Swap in the Checklist File

The following example shows an entry in `/etc/checklist` for file system swap.

```
default   /extra swapfs lim=15000,res=20000,pri=1 0 0 #file swap
```

Entries for file system swap in `/etc/checklist` have seven fields separated by blank space. The following describes making entries for each field.

1. First field: For file system swap entries, enter a placeholder, such as "default." (For all other type entries, the first field contains a special device file name, which does not apply for file system swap.)
2. Second field: Enter the name of the mount point *directory* of the file system to be used for swapping. Specify this directory using its absolute path name.
3. Third field: Specify the type of entry, which for file system swap is `swapfs`.
4. Fourth field: Specify the *options* for the file system swap. These options are the same as the parameters used when enabling file system swap with the `/etc/swapon` command. (See the earlier section, "Choosing Values for /etc/swapon Parameters".)

   Briefly, those options are:

   a. min=n, where n is the initial number of file system blocks for swap
   b. lim=n, where n is the limit to the number of file system blocks for swap
   c. res=n, where n is the number of file system blocks reserved for the file system
   d. pri=n, where n, ranging from 0 to 10 (0 is high priority), indicates the swapping priority

   When you specify the options, leave no spaces anywhere in the entry for options and separate the options with commas.
5. Fifth and sixth fields: Enter the placeholder `0` in each of these fields, as these fields are not used for file system swap entries.
6. Seventh field (optional): You can enter a comment preceded by the `#` character.

Removing File System Swap Using HP-UX Commands

To disable swapping to a file system,

1. Edit the `/etc/checklist` file to remove the entry for the specific file system swap area you want to remove. Skip this step if you never added a `swapfs` entry for this file system in the `/etc/checklist` file.
2. Reboot your system by running `shutdown -r`. Before issuing this command, make sure no users have either files open or processes running that could be corrupted by the shutdown.

8

Backing Up and Restoring Your Data

Of all the tasks that system administrators perform, among the most important are creating **system backups**. The most effective way to insure against the loss of your system's data is to copy the data from your system onto storage media (such as magnetic tape, cartridge tape, optical disk, or another hard disk). You should store copies of your data *away from your system* so that you can recover the data should something happen to your primary data. Data can also be backed up over a network to a computer at a different location. The important thing is to have copies of all your important files *somewhere other than on your system*.

This chapter will include the following topics and tasks:

- Terms used in this chapter
- Determining which data to back up
- Determining how often to back up data
- Choosing the type of storage device to use
- Backing up your data
  - using SAM.
  - using HP-UX commands.
- Automating your backup process
  - using SAM.
  - using HP-UX commands.
- Restoring data
  - using SAM.
  - using HP-UX commands.
- Other backup and restore utilities

The most commonly used backup commands for backing up and restoring your data are `fbackup` and `frecover`. SAM also uses these commands. This chapter primarily focuses on SAM and the use of the `fbackup` and `frecover` commands. Other back up and restore commands are listed in "Other Backup and Restore Utilities".

Terms Used in this Chapter

The following terms appear in this chapter. This list of terms appears here so that you can easily locate it. You can scan (or skip over) the list now and, if you need to, refer to it later.

backup levels A mechanism used to distinguish between varying degrees of incremental backup. Each backup level has a date associated with it that indicates when the last backup at that level was created. These dates are stored in the backup database file (`/usr/adm/fbackupfiles/dates` unless the `-d` option to `fbackup` is used to specify a different file). See "Full Backups vs. Incremental Backups".

excluded files A way of specifying *exceptions* in a group of files to be included in a backup (see **included files** below). For example, if you want to back up all of the files in a directory except for one, you can include the directory in your backup and indicate that you want to *exclude* that file.

extraction The process of recovering *specific files* from a group of files in a backup, as opposed to recovering *all* of the files from the backup.

8

full backup A backup that includes *all* of the files in a specified set, *regardless of the date they were created, modified or previously backed up.*

graph file A file that contains instructions about which files and directories to include in a backup, and of those, which files and directories to exclude from a backup.

included files A list of files to be included in a backup.

incremental backups
: A backup that includes only those files *that have been modified* since a previous backup. Backups can be "layered" (for example monthly backups, weekly backups, daily backups) using different backup levels (see **backup levels**, above).

local device
: A backup device that is physically connected to the same computer as the data you are backing up or restoring. The other type of a device is a **remote device**.

recovery
: The process of recovering *all* the files from a backup, as opposed to specific files (see **extraction**, above).

remote device
: A backup device that is physically connected to the a another computer. The other type of a device is a **local device**.

system backups
: The process of storing copies of important files on your system in a safe location not on your system so that you can restore the files if the primary copies on your system are lost or corrupted.

Determining Which Data to Back Up

To determine which data to back up, consider what files you need to recover if your file system becomes corrupt or your disk drive fails. Returning your system to the state just prior to the problem is determined by the information contained on your backups. If your backups include all of the files, you will be able to restore your system. You can only restore your system files as of the date of the most recent backup. Frequency of performing a backup is discussed in "Determining How Often to Back Up Data". If you prepare for the worst case, a total system failure and data corruption, you will be prepared for minor difficulties.

When you back up your system, you must define which files in your directory tree you want to back up. As you read, consider the following directory tree:

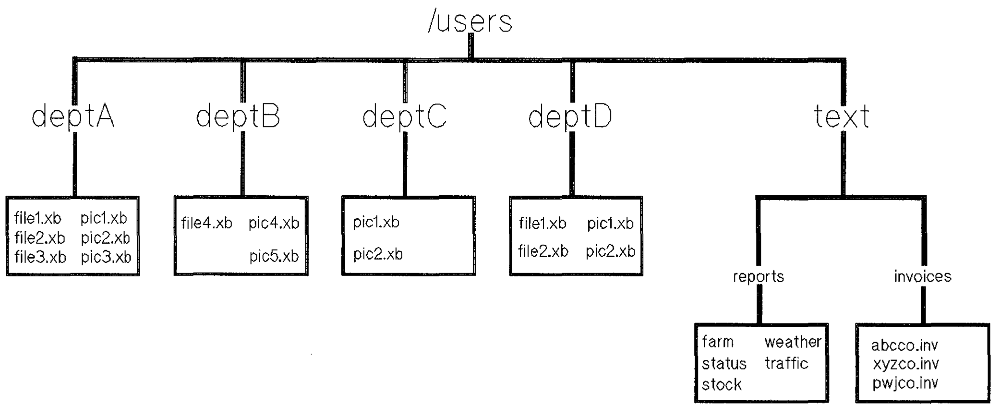


Figure 8-1. An Example Directory Tree

Included Files

Included files are directories and files that you want to include in your backup. When you specify a directory, all of the files and subdirectories are included in the backup.

Suppose you need to back up the files for Departments A, B and C. You explicitly specify that you want the following three directories backed up:

- `/users/deptA`
- `/users/deptB`
- `/users/deptC`

8 Included files are defined with the `-i` option to the `fbackup` and `frecover` commands, or with a graph file. See "Graph Files".

Excluded Files

Excluded files are those files *within your list of included directories and files* that you want to exclude from the backup. In other words, they are the exceptions.

Suppose that you have 100 departments and you need to back up the files for all of the departments *except* one. Entering in each department's directory name would be a lot of work.

In the example from the previous section on "included files," we listed out each directory from the example directory tree *except* for Department D's directory. You can tell the `fbackup` and `frecover` utilities to exclude a subset of the files from a group of files that are to be included in a backup. Another way to accomplish this task is to tell `fbackup` or `frecover` to:

```
INCLUDE:  /users

EXCLUDE:  /users/deptD
```

Excluded files are defined with the `-e` option to the `fbackup` and `frecover` commands, or with a graph file. See "Graph Files".

8

Graph Files

A file containing a list of directories and files to back up is a **graph file**. A graph file determines the scope of the backup. It is common to use different graph files for full and incremental backup schedules. If you use SAM to back up your system, you do not need to create graph files. SAM creates a graph file for you when you specify which files to back up.

When you run the `fbackup` and `frecover` commands, you can specify which files to include by using the `-i` option, and you can specify which files to exclude by using the `-e` option. More than one `-i` option and more than one `-e` option can be specified; however, if you have a long list of entries to specify, this can be a tedious and error prone way of entering the command.

It is possible to enter the information about which files to include/exclude in a file and then tell `fbackup` and `frecover` to look in that file for the list of files to back up or restore. Below are examples of graph files based on the examples in the previous sections "Included Files" and "Excluded Files".

Here is an example of a graph file for the list of files in the previous section, "Included Files":

```
i /users/deptA
i /users/deptB
i /users/deptC
```

Here is an example of a graph file for the example in the previous section, "Excluded Files":

```
i /users
e /users/deptD
```

8

Graph files contain one entry per line. If an entry begins with the two characters `"i "` (i,space), the files or directories represented on that line are *i*ncluded in the backup (or restoration). If an entry begins with the two characters `"e "` (e,space), the files or directories represented on that line are *e*xcluded from the backup (or restoration).

To tell `fbackup` or `frecover` to use a graph file, use the `-g` option followed by the name of the graph file.

Determining How Often to Back Up Data

A question closely related to determining *which* data to back up is determining *how often* to back it up. The critical question is, "*how much data can you afford to lose*?"

Evaluate the applications running on your system and the needs of your users to determine how critical the data on your system is to them. This will give you a guideline as to how often to back up the various files on your system. Consider the following things when determining how frequently to back up a particular file (or type of file):

- How often do the contents of the file change?
- How critical is it that the file's contents be up to date.

Note You can back up different groups of files at different frequencies and you can perform **incremental backups**, that back up *only those files which have changed (or are new) since the last time you performed a backup.* Incremental backups will be discussed later in this chapter.

You should create a backup schedule for your system that describes how often you will perform full backups and incremental backups of the various files on your system.

It is best to back up your system when there are few or no users logged in. Files that are in use when the `fbackup` or `frecover` command encounters them will not be backed up or restored. If you can afford to do so, you should change your system's run-level to the system administration state (single-user mode) before initiating the backup procedure. This will ensure that you are the only one logged in. For information about changing run-levels, see Chapter 4, "Controlling Access to the System".

Full Backups vs. Incremental Backups

Once you have identified the list of files to *include* and *exclude* you need to decide whether you want *all of the files* represented by your list to be backed up (a **full backup**), or *only those files that have changed (or that are new) since the last time you backed up this set of files* (an **incremental backup**).

Note A full backup does *not* mean a backup of every file on your system. It means a backup of every file on your "include list", regardless of when it was last backed up.

Backup Levels

The previous section stated that an incremental backup is a backup that includes *only those files that have changed (or that are new) since the last time you backed up this set of files.* This brings up the question, "how does `fbackup` know when the previous backup was created?" This information is contained in the file `/usr/adm/fbackupfiles/dates`, a file that is updated only when *all* of the following conditions are true:

- The "`-u`" option is used with `fbackup`.
- A graph file is used to indicate which files should be included/excluded when a backup is performed.
- Neither the "`-i`" nor the "`-e`" option is used (graph file used instead)
- The backup completed successfully

Note The `fbackup` command considers different graph files as separate backups. Backing up `graph_file_A` will have no effect on an incremental backup of `graph_file_B`.

Backup levels are a way of specifying varying degrees of incremental backup. For example, suppose you wanted to set up the following backup schedule:

- On the first day of the month, back up an entire set of selected files.
- Every Friday, back up all files in the selected set that have changed since the first of the month.
- Every day except Friday, back up all of the files in the selected set that have changed since the last Friday or first of the month, which ever is most recent.

There are three levels associated with the above schedule (the once per month level, the once per week level, and the once per day level). The once per month level is a *full backup*. The other two are *incremental backups*. The problem is how to distinguish between the two types of incremental backups. This is accomplished with backup levels.

The file `/usr/adm/fbackupfiles/dates` contains information about when the last backup at each backup level was performed. The `dates` file contains:

- the graph file used for the backup
- the level of the backup
- the date of the backup
- the start and end time for the backup

This information is used by `fbackup` to determine which files defined in the graph file are included in the backup. The `fbackup` command uses the following search sequence on the `dates` file to determine the base backup on which to build an incremental backup:

1. matching graph file
2. next lowest level number
3. most recent date

If no lower level is found, a full backup at the specified level is performed. If there are duplicates of a lower level found, the most recent is used as the base for the incremental backup.

You can have up to ten backup levels (0 - 9). Your backup strategy varies based on the level of activity on your system and the capacity of your media.

Recovery Example Using Three Backup Levels

To implement the earlier example of monthly, weekly, and daily backups use following backup levels:

level 0 - full monthly backup

level 1 - weekly backup on Friday

level 2 - daily backup, except Friday

Figure 8-2 illustrates the level numbers for implementing this example.

```
Date of the month: 1  2  3  4  5  6  7  8  9 10 11 12 13 14 15    ... 1
Day of the month: Su  M  T  W Th Fr Sa Su  M  T  W Th  F Sa Su    ...
------------------------------------------------------------------------
backup level       0  2  2  2  2  1  2  2  2  2  2  2  1  2  2    ... 0
```

Figure 8-2. Example of Using Incremental Backups

If your data became corrupt on Thursday the 12th, on Friday the 13th you would follow the following sequence to restore your system to it's Wednesday the 11th state:

1. Restore the monthly full backup from Sunday the 1st.
2. Restore the weekly incremental backup from Friday the 6th.
3. Restore the incremental backup from Wednesday the 11th.

Recovery Example Using Two Backup Levels

The following example illustrates a weekly full backup and daily incremental backup, two backup levels. When implementing your backup strategy using SAM, only two levels of backups are supported. Figure 8-3 illustrates the level numbers supported by SAM:

```
Date of the month: 1  2  3  4  5  6  7  8  9 10 11 12 13 14 15    ... 1
Day of the month: Su  M  T  W Th Fr Sa Su  M  T  W Th  F Sa Su    ...
-----------------------------------------------------------------------
backup level       0  1  1  1  1  1  1  0  1  1  1  1  1  1  0    ... 0
```

Figure 8-3. Example of Using Incremental Backups Supported by SAM

If your data became corrupt on Thursday the 12th, on Friday the 13th you would follow the following sequence to restore your system to it's Wednesday the 11th state:

1. Restore the full backup from Sunday the 8th.
2. Restore the incremental backup from Wednesday the 11th.

Choosing the Type of Storage Device to Use

Once you have determined which files you need to back up, and how often (see the previous two sections for details on how to do this), you need to determine where to copy your files for backup purposes.

When you evaluate where to back up your data, consider the following:

- How much data do you need to back up (rough estimate)?
- How quickly will you need to retrieve the data when you need to?
- What types of storage devices do you have access to?
- How automated do you want the process to be (for example, will you have an operator change tapes when they fill up or will you be using an automatic changing device such as the 35401A cartridge tape changer or one of the optical disk library devices)?
- How quickly will you need to complete a backup?

All backup utilities require some overhead on the media for data structures. The amount of raw data contained on the media is always less than the total capacity of the media.

Use your answers to the above questions along with the following table to help you determine which storage device to use for your backups.

Table 8-1. Determining Which Device to Use for a Backup

Device Type	Holds Lots of Data	Recover Data Quickly	Backup Data Quickly	Unattended Backup?[1]
Reel to Reel Magnetic Tape	Good	Good	Good	No
HP-format Cartridge Tape Single Drive	Fair	Poor	Poor	No
HP Format Cartridge Tape Autochanger[2]	Excellent	Poor	Poor	Yes
DDS Format (DAT) Tape Drive	Excellent	Good	Good	No
Optical Disk Single Drive	Good	Good	Good	No
Optical Disk Multi-disk Library	Excellent	Good	Good	Yes
Hard Disk	Good	Excellent	Excellent	No
Flexible (Floppy) Disk	Poor	Fair	Fair	No
DDS Format or Magnetic Tape over the Network[3]	*see specific device type*	*see specific device type*	*see specific device type*	*see specific device type*

1 You can perform an unattended (automatic) backup for the devices marked "no" in this column IF all of the data will fit on one reel, cartridge, floppy disk etc.

2 Autochanger must be set to "selective" mode (not "sequential" mode) for automatic backup.

3 Only magnetic tape and DDS format (DAT) tape drives are supported for remote backups.

8

When you are planning your backup strategy, it is also necessary to know how much data each media type will hold. Here are several tables containing approximate capacities for commonly used storage media.

Table 8-2. Disk Drive Storage Capacities

Media Type	Storage Capacity (Megabytes)	Comments
Optical Disk	325/side	An optical disk has two surfaces, each side has a capacity of 325 megabytes. For optical disk library devices, multiply 650 megabytes by the number of disks installed in your device. Use section 2 (the entire disk) for backing up. SAM only supports using section 2.
Hard Disk	$\Longrightarrow$	Hard disk capacities vary depending on the model you have.[1]

1 Consult the documentation that came with your disk drive for capacity information.

8

Table 8-3. Magnetic Tape Storage Capacities

Tape Density (bits/inch)	600 foot Reel[1]	1200 foot Reel[1]	2400 foot Reel[1]
800 BPI	5 Mbytes	10 Mbytes	20 Mbytes
1600 BPI	10 Mbytes	20 Mbytes	40 Mbytes
6250 BPI	40 Mbytes	80 Mbytes	140 Mbytes
HP7980/XC Compression Mode[2]	105 Mbytes	210 Mbytes	420 Mbytes

1 Capacities listed are approximations. Actual storage capacities vary with the number of errors encountered on each tape, the number of inter-record gaps on the tape and variations in tape length.

2 The Model HP7980/XC tape drive has a special data compression capability that allows more data to be stored on a given length of tape. The amount of data compression that occurs is data dependent. These values are averages.

Table 8-4. HP Format Cartridge Tape Storage Capacities

Number of Tracks on Tape[1]	150 foot Tape[2]	600 foot Tape[2]
16-Track Tape	16 Mbytes	67 Mbytes
32-Track Tape	32 Mbytes	133 Mbytes

1 Cartridge tapes come in 16-track and 32-track styles. A device (such as a Model 9145 Cartridge Tape drive) that is capable of handling 32-track tapes can read but not write 16-track tapes. 16-track devices cannot use 32-track tapes.

2 Capacities listed are approximations. Actual storage capacities vary with the number of errors encountered on each tape. Capacities are listed in megabytes.

Table 8-5. DDS Format (DAT) Tape Storage Capacities

	60 meter tape (Mbytes)[1]	90 meter tape (Mbytes)[1]
uncompressed mode	1300 (1.3 Gigabytes)	2000 (2 Gigabytes)
compressed mode	1300 to 5200 (1.3 to 5.2 Gigabytes)	2000 to 8000 (2 to 8 Gigabytes)

1 Capacities listed are approximations. Actual storage capacities vary with the type of data and the number of errors encountered on each tape.

Note

- Do not mix compressed and uncompressed data on the same tape.
- Half-height (3.5 inch) tape drives can read and write to 90 meter and 60 meters tapes.
- Full-height (5.25 inch) tape drives can only read and write to 60 meter tapes. They cannot read or write to 90 meter tapes.

Automating the Backup Process

Because of the need to have the activity on the system as low as possible while files are being backed up, many system administrators create their backups during the middle of the night. It is therefore desirable to have a way to automate the process so that the backup can occur unattended. This eliminates the need to have someone manually start the backup in the middle of the night.

For backups to be truly unattended:

- All of the files must fit on one media unit, or
- Several backup devices must be specified, or
- You must use an autochanging device such as an HP35401 cartridge tape changer or an optical disk library device.

If none of the above are true, the backup cannot be automated.

Note SAM does not support multiple devices per automated backup entry. See "Setting Up an Automated Backup Schedule Using SAM".

Restoring Your Data

The primary reason for making backup copies of your data is so you can restore needed files that have been removed (or damaged).

There are two types of situations you are likely to encounter:

1. One or a few files need to be recovered, usually as a result of an accidental deletion or because the file has been overwritten by the wrong data.
2. You need to recover *all* of the files. This is usually part of the system crash recovery process. If you have experienced a file system failure and you suspect that you have corrupt data, refer to Chapter 6, "File System Problems" of the *Solving HP-UX Problems* manual. If your root disk failed and all the data on the disk is lost, you can boot from your recovery tape, see "Recovering From a System Crash Using Your Recovery Tape" in this chapter. To learn how to make a recovery system, see "Creating a Recovery System" in Chapter 2, "Constructing an HP-UX System".

   After you have repaired the file system or replaced the hardware, you can restore your data from your most recent backups.

   Ensure that your system can access the device from which you will restore the files from your backup. This can involve adding a disk or tape drive to your system, refer to the *Installing Peripherals* manual.

If your backup was created by the `fbackup` command (SAM uses the `fbackup` command), you can use SAM or the `frecover` command to restore the files from your backup.

The `frecover` command has several modes of operation and it is important to know the difference between them. The process of recovering *all* files from a backup is called **recovery**. The mode of operation for restoring *individual files* is called **extraction**.

Most of the concepts associated with backing up your system also apply to restoring files. Particularly, "including files", "excluding files", "graph files", and "device files." Refer to "Determining Which Data to Back Up" and "Choosing the Type of Storage Device to Use" for more information.

Backing Up and Restoring Tasks

There are two methods for performing backups and restoring data:

1. SAM (System Administration Manager)
2. HP-UX commands

Generally you should use the SAM method because it is simpler and faster than performing the task with commands. For information about running SAM and navigating within SAM, refer to Chapter 1, "Introduction to System Administration".

SAM allows you to control access to your system through its menu-selection and data-entry screens. By combining multiple "manual commands" into single tasks, SAM can save you time and keystrokes. SAM also eliminates the need to know command names and options.

Although HP-UX commands require you to learn more details than SAM does, you might need or prefer to use HP-UX commands, for the following reasons:

- HP-UX commands give you a greater degree of control.
- SAM might not be configured into your system. You *have* to use HP-UX commands.
- You might be more comfortable using HP-UX commands.

HP-UX has *many* utilities that can be used for creating backups. Each utility has its advantages and disadvantages. The pair of utilities that contain the best mix of features and that give you the greatest flexibility are `fbackup(1M)` and `frecover(1M)`.

The System Administration Manager (SAM) uses the `fbackup` and `frecover` commands to back up your system.

When backing up and restoring files that are NFS mounted to your system, `fbackup` and `frecover` can only backup and restore those files having "other user" read permission. `fbackup` and `frecover` normally operate in user-mode when crossing NFS mount points; not superuser-mode. To ensure that `fbackup` and `frecover` can back up and restore the files exported from the NFS server, login as superuser on the NFS file server and use the `root=` option to the `/usr/etc/exportfs` command to export the correct permissions. Refer to *exportfs*(1M) in the *HP-UX Reference* and the *Installing and Administering NFS Services* manual.

Backing Up Your System To a Local Device Using SAM

Note To backup files on disks physically connected to another computer, enter the `Remote Administration` functional area of SAM and refer to Chapter 1, "Introduction to System Administration", for additional information.

Gather a list of files you want to back up (see "Determining Which Data to Back Up") before you begin.

SAM only supports one level of incremental backups.

If you are setting up your system for performing an unattended backup in the future, see "Setting Up an Automated Backup Schedule Using SAM".

To back up your system right now:

1. Ensure that files you intend to back up are not being accessed.

Note The `fbackup` command will not back up files that are active (open) or locked when it encounters them.

2. Ensure that you have superuser capabilities.
3. Run the `fsck` command to check your file system for inconsistencies before you perform a backup. This ensures that you to do not back up data that is corrupt. Refer to Appendix A, "Using the fsck Command" in the *Solving HP-UX Problems* manual and *fsck*(1M) in the *HP-UX Reference*.

Caution Do not run `fsck` on a file system that is mounted and active. This could introduce data corruption. Run `fsck` in single-user mode when checking the root file system. For file systems other that the root file system, unmount the file system, run `fsck`, and then remount the file system.

4. Run SAM; type:

   `/usr/bin/sam`

   SAM provides an on-line help system to assist you when you need additional information.

   Activating the (Help) button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

   From within a functional area, choosing an item from the "Help" menu gives you information about:

   - the current functional area
   - keyboard navigation within SAM
   - using the SAM help system
   - displaying the version of SAM you are currently running

   From a dialog box (a window displaying fields to be filled in), pressing the (f1) key gives you context-sensitive information for the object at the location of the cursor.

   See Chapter 1, "Introduction to System Administration", for additional information about using SAM.

5. Highlight `Backup and Recovery` and activate the [Open] control button.
6. Highlight `Backup Devices` and activate the [Open] control button.
7. Highlight the backup device from the object list.
8. Choose `Backup Files Interactively` from the "Actions" menu.

   SAM may ask you to provide additional information about:

   - magnetic tape density.
   - DDS format tape with data compression or without data compression.
   - optical disk number in an autochanger library system.
   - HP format cartridge tape number to start with in an autochanger.
9. Activate [Select Backup Scope].
10. Turn on the `Entire System` or `Selected Files` checkbox.

    If you turned on the `Entire System` checkbox, activate the [OK] control button.

    If you turned on the `Selected Files` checkbox, enter each file name in the "Included" and "Excluded" boxes and activate the [Add] control button. If you make a mistake, highlight the entry with the error and use the [Modify] or [Remove] control buttons to correct the mistake.

    When you have completed determining the selecting files to be recovered, activate the [OK] control button.

8

11. To:

    - cancel creating an index log or
    - backup data that is NFS mounted to your system or
    - cancel backing up elements of context-dependent files in an HP-UX cluster,

    activate (Set Additional Parameters...) and turn off and on the appropriate checkboxes.

    Creating an on-line index log is performed by default and is very useful for tracking problems if your backup did not complete successfully. The log files are `/usr/sam/log/br_index.full` for full backups and `/usr/sam/log/br_index.incr` for incremental backups.

    When backing up files that are NFS mounted to your system, `fbackup` can only back up those files having "other user" read permission. `fbackup` normally operates in user-mode when crossing NFS mount points; not superuser-mode. To ensure that `fbackup` can back up the files exported from the NFS server, login as superuser on the NFS file server and use the `root=` option to the `/usr/etc/exportfs` command to export the correct permissions. Refer to *exportfs*(1M) in the *HP-UX Reference* and the *Installing and Administering NFS Services* manual.

    When you have finished setting the additional parameters, activate the (OK) control button.

12. Activate the (OK) control button to begin the backup process.

    If confirmation messages appear, read the message(s) and activate the (OK) control button to proceed in each case. SAM displays a window containing the output of the executed `fbackup` command. If you created an index log, the information displayed will appear in the index log.

Backing Up Your System To a Remote Device Using SAM

Gather the following information before you begin:

- A list of files you want to back up (see "Determining Which Data to Back Up").
- The name of the system to which the backup device is attached.
- The device file, on the remote system, for the backup device.

Note

- To backup files on disks physically connected to another computer, enter the `Remote Administration` functional area of SAM and refer to Chapter 1, "Introduction to System Administration", for additional information.
- SAM only supports backing up remotely to magnetic and DDS format tapes.

SAM only supports one level of incremental backup.

If you are setting up your system for performing an unattended backup in the future, see "Setting Up an Automated Backup Schedule Using SAM".

To back up your system right now:

1. Ensure that files you intend to back up are not being accessed.

Note The `fbackup` command will not back up files that are active (open) or locked when it encounters them.

---

2. Ensure that you have superuser capabilities.

3. Run the `fsck` command to check your file system for inconsistencies before you perform a backup. This ensures that you to do not back up data that is corrupt. Refer to Appendix A, "Using the fsck Command" in the *Solving HP-UX Problems* manual and *fsck*(1M) in the *HP-UX Reference*.

Caution Do not run `fsck` on a file system that is mounted and active. This could introduce data corruption. Run `fsck` in single-user mode when checking the root file system. For file systems other that the root file system, unmount the file system, run `fsck`, and then remount the file system.

---

4. Run SAM; type:

   /usr/bin/sam

   SAM provides an on-line help system to assist you when you need additional information.

   Activating the (Help) button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

   From within a functional area, choosing an item from the "Help" menu gives you information about:

   - the current functional area
   - keyboard navigation within SAM
   - using the SAM help system
   - displaying the version of SAM you are currently running

   From a dialog box (a window displaying fields to be filled in), pressing the (f1) key gives you context-sensitive information for the object at the location of the cursor.

   See Chapter 1, "Introduction to System Administration", for additional information about using SAM.

5. Highlight `Backup and Recovery` and activate the Open control button.
6. Highlight `Backup Devices` and activate the Open control button.
7. Choose `Use Remote Backup Device` and `Backup Files Interactively` from the "Actions" menu.
8. Activate Specify Remote Backup Device...
9. Fill in the hostname (machine name) to which the backup device is attached and the associated device file. Activate the OK control button.
10. Activate Select Backup Scope.
11. Turn on the `Entire System` or `Selected Files` checkbox.

    If you turned on the `Entire System` checkbox, activate the OK control button.

    If you turned on the `Selected Files` checkbox, enter each file name in the "Included" and "Excluded" boxes and activate the Add control button. If you make a mistake, highlight the entry with the error and use the Modify or Remove control buttons to correct the mistake.

    When you are satisfied with the included and excluded lists, activate the OK control button.

8

12. To:

    - cancel creating an index log or
    - backup data that is NFS mounted to your system or
    - cancel backing up context-dependent files in an HP-UX cluster,

    activate (Set Additional Parameters...) and turn off and on the appropriate checkboxes.

    Creating an on-line index file is performed by default and is very useful for tracking problems if your backup did not complete successfully. The log files are `/usr/sam/log/br_index.full` for full backups and `/usr/sam/log/br_index.incr` for incremental backups.

    When backing up files that are NFS mounted to your system, `fbackup` can only back up those files having "other user" read permission. `fbackup` normally operates in user-mode when crossing NFS mount points; not superuser-mode. To ensure that `fbackup` can back up the files exported from the NFS server, login as superuser on the NFS file server and use the `root=` option to the `/usr/etc/exportfs` command to export the correct permissions. Refer to *exportfs*(1M) in the *HP-UX Reference* and the *Installing and Administering NFS Services* manual.

    When you have finished setting the additional parameters, activate the (OK) control button.

13. Activate the (OK) control button to begin the backup process.

    If confirmation messages appear, read the message(s) and activate the (OK) control button to proceed in each case. SAM displays a window containing the output of the executed `fbackup` command. If you created an index log, the information displayed will appear in the index log.

8

Setting Up an Automated Backup Schedule Using SAM

The easiest way to set up an automated backup schedule is to use SAM's "Backup and Recovery" capabilities. SAM allows you to:

- View the entries in the automated backup schedule
- Add an entry to the automated backup schedule
- Remove entries in automated backup schedule
- Override the backup schedule to perform the backup now

You can schedule backups to happen on specific days of the week at a specific time, or you can schedule them to happen on specific days of the month at a specific time.

You can have multiple entries in your automated backup schedule to accommodate combinations of full and incremental backups and to allow you to back up different groups of files at different intervals.

Note

- SAM uses the `fbackup` utility to perform its backups (automated or otherwise). If you use SAM to set up an automated backup schedule, you should be aware that `fbackup` is a highly interactive utility. If it should need attention (tape change, device not on line, etc.), `fbackup` will attempt to prompt for the input it needs. This may cause an automated backup to fail (or not complete).
- SAM supports one full and incremental backup level per graph file.
- SAM does not support multiple backup devices in a single graph file entry. To back up to multiple device, create multiple entries and divide the scope of the backup (file systems) among different backup devices.

If for some reason a particular backup could not proceed, you can override the schedule to perform the backup immediately. For example, if you have a backup scheduled for late at night and you notice that the tape drive was not operational during this time, you can perform the backup immediately. This does not affect the automated backup schedule. Your backups will proceed as scheduled in the future. Refer to "Override the Backup Schedule to Perform the Backup Now".

When backing up files that are NFS mounted to your system, `fbackup` can only back up those files having "other user" read permission. `fbackup` normally operates in user-mode when crossing NFS mount points; not superuser-mode. To ensure that `fbackup` can back up the files exported from the NFS server, login as superuser on the NFS file server and use the `root=` option to the `/usr/etc/exportfs` command to export the correct permissions. Refer to *exportfs*(1M) in the *HP-UX Reference* and the *Installing and Administering NFS Services* manual.

Viewing Entries

To view entries currently defined in your automated backup schedule:

1. Ensure that you have superuser capabilities.
2. Run SAM; type:

   `/usr/bin/sam`

   SAM provides an on-line help system to assist you when you need additional information.

   Activating the (Help) button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

   From within a functional area, choosing an item from the "Help" menu gives you information about:
   - the current functional area
   - keyboard navigation within SAM
   - using the SAM help system
   - displaying the version of SAM you are currently running

   From a dialog box (a window displaying fields to be filled in), pressing the (f1) key gives you context-sensitive information for the object at the location of the cursor.

   See Chapter 1, "Introduction to System Administration", for additional information about using SAM.
3. Highlight `Backup and Recover` and activate the (Open) control button.
4. Highlight `Automated Backups` and activate the (Open) control button.

   The object list displays the following attributes for each automated backup entry:
   - The time of day that the backup will occur.
   - The days of the month *or* week on which the backup will occur.
   - Whether the backup will be a full backup or an incremental backup.
   - Files that are included/excluded in the backup.

   You can view the device files to be used for your automated backups by rearranging the object list attributes. See "Changing the Format of the Object List" in Chapter 1, "Introduction to System Administration".

8

Adding an Entry

To add an entry to your automated backup schedule:

1. Ensure that you have superuser capabilities.
2. Run SAM; type:

   <u>`/usr/bin/sam`</u>

   SAM provides an on-line help system to assist you when you need additional information.

   Activating the (Help) button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

   From within a functional area, choosing an item from the "Help" menu gives you information about:

   - the current functional area
   - keyboard navigation within SAM
   - using the SAM help system
   - displaying the version of SAM you are currently running

   From a dialog box (a window displaying fields to be filled in), pressing the (f1) key gives you context-sensitive information for the object at the location of the cursor.

   See Chapter 1, "Introduction to System Administration", for additional information about using SAM.

3. Highlight `Backup and Recover` and activate the (Open) control button.
4. Highlight `Automated Backups` and activate the (Open) control button.
5. Choose `Add an Automated Backup` and `Local Backup Device` or `Remote Backup Device` from the "Actions" menu.

   To add local device entry:

   a. Activate (Specify Backup Device).
   b. Highlight the backup device and activate the (OK) control button.

      SAM may ask you to provide additional information about:

      i. Magnetic format tape density.
      ii. DDS format tape with data compression or without data compression.
      iii. Optical disk number in an autochanger library system.
      iv. HP format cartridge tape number to start with in an autochanger.

      If there are no local devices detected or the particular device you want is not listed, you will need to add the device to the system. To add the device to the system, exit SAM and refer to the *Installing Peripherals*.

Note If the local backup device does not appear in the object list and you know the device file, you can enter the remote backup device and specify the local hostname and device file. SAM only supports backing up remotely to magnetic and DDS format tapes.

8

   To add a remote device entry:

   a. Activate the (Specify Remote Backup Device).
   b. Fill in the hostname (machine name) to which the backup device is attached and the associated device file.
   c. Activate the (OK) control button.

6. Activate Select Backup Scope... .
7. Turn on the `Entire System` or `Selected Files` checkbox.

   If you turned on the `Entire System` checkbox, activate the OK control button.

   If you turned on the `Selected Files` checkbox, enter each file name in the "Included" and "Excluded" boxes and activate the Add control button. If you make a mistake, highlight the entry with the error and use the Modify or Remove control buttons to correct the mistake.

   When you are satisfied with the included and excluded lists, activate the OK control button.
8. Choose `Select Backup Time...`. Fill in the time of day to perform a full backup. Turn on "Days of the Week" or "Days of the Month" checkboxes to define the date for the backup. Highlight from the list the day(s) or date(s).

   Optionally choose `Enabled` or `Disabled` to schedule an incremental backup. SAM only supports one level of incremental backup.

   For any backup type that is visible, you must specify the time parameter.

   When you are satisfied with the entries, activate the OK control button.

9. To:
   - cancel creating an index log or
   - backup data that is NFS mounted to your system or
   - cancel backing up elements of context-dependent files in an HP-UX cluster,

   activate (Set Additional Parameters...) and turn off and on the appropriate checkboxes.

   Creating an on-line index log is performed by default and is very useful for tracking problems if your backup did not complete successfully. The log files are `/usr/sam/log/br_index.full` for full backups and `/usr/sam/log/br_index.incr` for incremental backups.

   When backing up files that are NFS mounted to your system, `fbackup` can only back up those files having "other user" read permission. `fbackup` normally operates in user-mode when crossing NFS mount points; not superuser-mode. To ensure that `fbackup` can back up the files exported from the NFS server, login as superuser on the NFS file server and use the `root=` option to the `/usr/etc/exportfs` command to export the correct permissions. Refer to *exportfs*(1M) in the *HP-UX Reference* and the *Installing and Administering NFS Services* manual.

   When you have finished setting the additional parameters, activate the (OK) control button.

10. Activate the OK control button to add an entry to the crontab file. If `cron` is not running, SAM will display a message. Refer to *cron*(1M) and *crontab*(1) in the *HP-UX Reference* manual.

    You should see your entry in the object list.

Caution

Prior to the scheduled backup, run the `fsck` command to check your file system for inconsistencies. This ensures that you do not back up data that is corrupt. Refer to Appendix A, "Using the fsck Command" in the *Solving HP-UX Problems* manual and *fsck*(1M) in the *HP-UX Reference*.

Do not run `fsck` on a file system that is mounted and active. This could introduce data corruption. Run `fsck` in single-user mode when checking the root file system. For file systems other that the root file system, unmount the file system, run `fsck`, and then remount the file system.

Removing Entries

To remove an entry from the automated backup schedule:

1. Ensure that you have superuser capabilities.
2. Run SAM; type:

   `/usr/bin/sam`

   SAM provides an on-line help system to assist you when you need additional information.

   Activating the Help button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

   From within a functional area, choosing an item from the "Help" menu gives you information about:

   - the current functional area
   - keyboard navigation within SAM
   - using the SAM help system
   - displaying the version of SAM you are currently running

   From a dialog box (a window displaying fields to be filled in), pressing the f1 key gives you context-sensitive information for the object at the location of the cursor.

   See Chapter 1, "Introduction to System Administration", for additional information about using SAM.
3. Highlight `Backup and Recover` and activate the Open control button.
4. Highlight `Automated Backups` and activate the Open control button.
5. Highlight the entry or entries to be removed.
6. Choose `Remove an Automated Backup...` from the "Actions" menu.

Override the Backup Schedule to Perform the Backup Now

To override the backup schedule to perform the backup now:

1. Ensure that you have superuser capabilities.
2. Run the `fsck` command to check your file system for inconsistencies before you perform a backup. This ensures that you to do not back up data that is corrupt. Refer to Appendix A, "Using the fsck Command" in the *Solving HP-UX Problems* manual and *fsck*(1M) in the *HP-UX Reference*.

Caution Do not run `fsck` on a file system that is mounted and active. This could introduce data corruption. Run `fsck` in single-user mode when checking the root file system. For file systems other that the root file system, unmount the file system, run `fsck`, and then remount the file system.

---

3. Run SAM; type:

   `/usr/bin/sam`

   SAM provides an on-line help system to assist you when you need additional information.

   Activating the (Help) button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

   From within a functional area, choosing an item from the "Help" menu gives you information about:

   - the current functional area
   - keyboard navigation within SAM
   - using the SAM help system
   - displaying the version of SAM you are currently running

   From a dialog box (a window displaying fields to be filled in), pressing the (f1) key gives you context-sensitive information for the object at the location of the cursor.

   See Chapter 1, "Introduction to System Administration", for additional information about using SAM.

4. Highlight `Backup and Recover` and activate the (Open) control button.
5. Highlight `Automated Backups` and activate the (Open) control button.
6. Highlight the backup entry you want to perform now.
7. Choose `Perform Backup Now...` from the "Actions" menu.

Restoring All Files From a Local Device Using SAM

Note To restore data to disks physically connected to another computer, enter the `Remote Administration` functional area of SAM and refer to Chapter 1, "Introduction to System Administration", for additional information.

When restoring files that are NFS mounted to your system, `frecover` can only restore those files having "other user" write permission. `frecover` normally operates in user-mode when crossing NFS mount points; not superuser-mode. To ensure that `frecover` can restore the files exported from the NFS server, login as superuser on the NFS file server and use the `root=` option to the `/usr/etc/exportfs` command to export the correct permissions. Refer to *exportfs*(1M) in the *HP-UX Reference* and the *Installing and Administering NFS Services* manual.

To restore all files using SAM:

1. Ensure that you have superuser capabilities.
2. Run SAM; type:

   /usr/bin/sam

   SAM provides an on-line help system to assist you when you need additional information.

   Activating the (Help) button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

   From within a functional area, choosing an item from the "Help" menu gives you information about:

   - the current functional area
   - keyboard navigation within SAM
   - using the SAM help system
   - displaying the version of SAM you are currently running

   From a dialog box (a window displaying fields to be filled in), pressing the (f1) key gives you context-sensitive information for the object at the location of the cursor.

   See Chapter 1, "Introduction to System Administration", for additional information about using SAM.

8

3. Highlight `Backup and Recover` and activate the [Open] control button.
4. Highlight `Backup Devices` and activate the [Open] control button.
5. Highlight the device in the list from which the data is to be restored.
6. Choose `Recover Files or Directories`
7. Activate [Select Recovery Scope].
8. Turn on the **All Files on Media** checkbox and activate the [OK] control button.
9. To:

   - overwrite new files,
   - maintain original ownership,
   - recover files using full path name,
   - place files in a non-root directory

   activate [Set Additional Parameters] and turn on the appropriate checkbox.

   To restore files relative to a particular directory, fill in the directory.

   Activate the [OK] control button to set the additional parameters.
10. Activate the [OK] control button to start the restore process.

    If confirmation messages appear, read the message(s) and activate the [OK] control button to proceed in each case. SAM displays a window containing the output of the executed `frecover` command.

8

Restoring Individual Files From a Local Device Using SAM

Gather the following information and materials before you begin:

- A list of files you need.
- The media on which the data resides.
- The location on your system to restore the files (original location or relative to some other location).
- The device and device file for restoring the data.

Note To restore data to disks physically connected to another computer, enter the `Remote Administration` functional area of SAM and refer to Chapter 1, "Introduction to System Administration", for additional information.

When restoring files that are NFS mounted to your system, `frecover` can only restore those files having "other user" write permission. The `frecover` command normally operates in user-mode when crossing NFS mount points; not superuser-mode. To ensure that `frecover` can restore the files exported from the NFS server, login as superuser on the NFS file server and use the `root=` option to the `/usr/etc/exportfs` command to export the correct permissions. Refer to *exportfs*(1M) in the *HP-UX Reference* and the *Installing and Administering NFS Services* manual.

To restore individual files:

1. Ensure that you have superuser capabilities.
2. Run SAM; type:

   `/usr/bin/sam`

   SAM provides an on-line help system to assist you when you need additional information.

   Activating the (Help) button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

   From within a functional area, choosing an item from the "Help" menu gives you information about:

   - the current functional area
   - keyboard navigation within SAM
   - using the SAM help system
   - displaying the version of SAM you are currently running

   From a dialog box (a window displaying fields to be filled in), pressing the (f1) key gives you context-sensitive information for the object at the location of the cursor.

   See Chapter 1, "Introduction to System Administration", for additional information about using SAM.
3. Highlight `Backup and Recover` and activate the (Open) control button.
4. Highlight `Backup Devices` and activate the (Open) control button.
5. Highlight the device in the list from which the data is to be restored.
6. Choose `Recover Files or Directories` from the "Actions" menu.

7. Activate (Select Recovery Scope).
8. Turn on the `Selected Files` checkbox.

   - Fill in the filename containing a list of files to restore. The filenames should be full pathnames. This file is *not* a graph file. This file is used to create a graph file. You can use the on-line index file created by a previous backup, but it must be edited to containing only the full pathnames of the files to be restored.

   or

   - Enter each file name in the "Included" and "Excluded" boxes and activate the (Add) control button. If you make a mistake, highlight the entry with the error and use the (Modify) or (Remove) control buttons to correct the mistake.

     You can use both the file and the included/excluded method simultaneously to specify files to be restored.

   When you have completed determining the selecting files to be recovered, activate the (OK) control button.

9. To:

   - overwrite new files,
   - maintain original ownership,
   - recover files using full path name, or
   - place files in a non-root directory

   activate (Set Additional Parameters).

   Turn on the appropriate checkbox.

   To restore files relative to a particular directory, fill in the directory.

   Activate the (OK) control button to set the additional parameters.

10. Activate the (OK) control button to start the restore process.

    If confirmation messages appear, read the message(s) and activate the (OK) control button to proceed in each case. SAM displays a window containing the output of the executed `frecover` command.

Restoring All Files From a Remote Device Using SAM

Note

- To restore files to disks physically connected to another computer, enter the `Remote Administration` functional area of SAM and refer to Chapter 1, "Introduction to System Administration", for additional information.
- SAM only supports restoring data remotely from magnetic and DDS format tapes.

When restoring files that are NFS mounted to your system, `frecover` can only restore those files having "other user" write permission. The `frecover` command normally operates in user-mode when crossing NFS mount points; not superuser-mode. To ensure that `frecover` can restore the files exported from the NFS server, login as superuser on the NFS file server and use the `root=` option to the `/usr/etc/exportfs` command to export the correct permissions. Refer to *exportfs*(1M) in the *HP-UX Reference* and the *Installing and Administering NFS Services* manual.

To restore all files using SAM:

1. Ensure that you have superuser capabilities.
2. Run SAM; type:

   `/usr/bin/sam`

   SAM provides an on-line help system to assist you when you need additional information.

   Activating the (Help) button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

   From within a functional area, choosing an item from the "Help" menu gives you information about:

   - the current functional area
   - keyboard navigation within SAM
   - using the SAM help system
   - displaying the version of SAM you are currently running

   From a dialog box (a window displaying fields to be filled in), pressing the (f1) key gives you context-sensitive information for the object at the location of the cursor.

   See Chapter 1, "Introduction to System Administration", for additional information about using SAM.

8

3. Highlight `Backup and Recover` and activate the Open control button.
4. Highlight `Backup Devices` and activate the Open control button.
5. Choose `Use Remote Backup Device` and `Recover Files or Directories`
6. Activate Specify Remote Backup Device...
7. Fill in the hostname (machine name) to which the backup device is attached and the associated device file. SAM only supports restoring data remotely from magnetic and DDS format tapes.
8. Activate Select Recovery Scope.
9. Choose `All Files on Media` and activate the OK control button.
10. To:
    - overwrite new files,
    - maintain original ownership,
    - recover files using full path name,
    - place files in a non-root directory

    activate Set Additional Parameters and turn on the appropriate checkbox.

    To restore files relative to a particular directory, fill in the directory.

    Activate the OK control button to set the additional parameters.
11. Activate the OK control button to start the restore process.

    If confirmation messages appear, read the message(s) and activate the OK control button to proceed in each case. SAM displays a window containing the output of the executed `frecover` command.

8

Restoring Individual Files From a Remote Device Using SAM

Gather the following information and materials before you begin:

- A list of files you need.
- The media on which the data resides.
- The location on your system to restore the files (original location or relative to some other location).
- The device and device file for restoring the data.

Note

- To restore files to disks physically connected to another computer, enter the `Remote Administration` functional area of SAM and refer to Chapter 1, "Introduction to System Administration", for additional information.
- SAM only supports restoring data remotely from magnetic and DDS format tapes.

When restoring files that are NFS mounted to your system, `frecover` can only restore those files having "other user" write permission. The `frecover` command normally operates in user-mode when crossing NFS mount points; not superuser-mode. To ensure that `frecover` can restore the files exported from the NFS server, login as superuser on the NFS file server and use the `root=` option to the `/usr/etc/exportfs` command to export the correct permissions. Refer to *exportfs*(1M) in the *HP-UX Reference* and the *Installing and Administering NFS Services* manual.

8

To restore individual files:

1. Ensure that you have superuser capabilities.
2. Run SAM; type:

   `/usr/bin/sam`

   SAM provides an on-line help system to assist you when you need additional information.

   Activating the (Help) button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

   From within a functional area, choosing an item from the "Help" menu gives you information about:

   - the current functional area
   - keyboard navigation within SAM
   - using the SAM help system
   - displaying the version of SAM you are currently running

   From a dialog box (a window displaying fields to be filled in), pressing the (f1) key gives you context-sensitive information for the object at the location of the cursor.

   See Chapter 1, "Introduction to System Administration", for additional information about using SAM.

3. Highlight `Backup and Recover` and activate the [Open] control button.
4. Highlight `Backup Devices` and activate the [Open] control button.
5. Choose `Use Remote Backup Device` and `Recover Files or Directories` from the "Actions" menu.
6. Activate [Specify Remote Backup Device].
7. Fill in the hostname (machine name) and the assciated device file and activate the [OK] control button. SAM only supports restoring data remotely from magnetic and DDS format tapes.
8. Activate [Select Recovery Scope].
9. Turn on the `Selected Files` checkbox.
   - Fill in the filename containing a list of files to restore. The filenames should be full pathnames. This file is *not* a graph file. This file is used to create a graph file. You can use the on-line index file created by a previous backup, but it must be edited to containing only the full pathnames of the files to be restored.

     or

   - Enter each file name in the "Included" and "Excluded" boxes and activate the [Add] control button. If you make a mistake, highlight the entry with the error and use the [Modify] or [Remove] control buttons to correct the mistake.

     You can use both the file and the included/excluded method simultaneously to specify files to be restored.

   When you have completed determining the selecting files to be recovered, activate the [OK] control button.

10. To:
    - overwrite new files,
    - maintain original ownership,
    - recover files using full path name, or
    - place files in a non-root directory.

    activate (Set Additional Parameters).

    Turn on the appropriate checkbox.

    To restore files relative to a particular directory, fill in the directory.

    Activate the (OK) control button to set the additional parameters.

11. Activate the (OK) control button to start the restore process.

    If confirmation messages appear, read the message(s) and activate the (OK) control button to proceed in each case. SAM displays a window containing the output of the executed `frecover` command.

Viewing the Index File on the Local Media Using SAM

To view the index stored on the media:

1. Ensure that you have superuser capabilities.
2. Run SAM; type:

   `/usr/bin/sam`

   SAM provides an on-line help system to assist you when you need additional information.

   Activating the (Help) button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

   From within a functional area, choosing an item from the "Help" menu gives you information about:

   - the current functional area
   - keyboard navigation within SAM
   - using the SAM help system
   - displaying the version of SAM you are currently running

   From a dialog box (a window displaying fields to be filled in), pressing the (f1) key gives you context-sensitive information for the object at the location of the cursor.

   See Chapter 1, "Introduction to System Administration", for additional information about using SAM.
3. Highlight `Backup and Recover` and activate the (Open) control button.
4. Highlight `Backup Devices` and activate the (Open) control button.
5. Highlight the device in the list from which the index is to be read and displayed.
6. Choose `Get List of Files on Device` from the "Actions" menu.

7. Fill in the filename to which you want the index file restored and activate the OK control button.

   If the device is an optical autochanger library system or an HP format cartridge tape autochanger, SAM asks you for the disk number or the cartridge tape number. Unless otherwise specified, SAM looks on the media at location one.

   If you backup is contained on multiple media and you specified to create an index, each media has an index file listing the contents of the media itself and all previous media. For example, If your backup is on three (A, B, and C) optical disks, the index file on disk A contains only the files contained on disk A; the index file on disk B contains the files on disk A and B; the index file on disk C contains the files on disk A, disk B, and and disk C.

   SAM will open a window to execute the the `frecover` command to restore the index file.

Important! Although every volume in the backup set has an index, indexes are completely accurate only for the previous volumes in the same set. For example, the index on the last volume may indicate that a file resides on that volume, but it may not have been backed up (it may have been removed after the index was created, but before fbackup attempted to back it up). *The only index guaranteed to be correct in all cases* is the on-line index, that is produced after the last volume has been written. See the next section for information about viewing SAM's on-line index files.

Viewing the Index File on a Remote Device Using SAM

Note

- To restore an index file to disks physically connected to another computer, enter the `Remote Administration` functional area of SAM and refer to Chapter 1, "Introduction to System Administration", for additional information.
- SAM only supports recovering the index file remotely from magnetic and DDS format tapes.

To view the index stored on the media:

1. Ensure that you have superuser capabilities.
2. Run SAM; type:

   `/usr/bin/sam`

   SAM provides an on-line help system to assist you when you need additional information.

   Activating the (Help) button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

   From within a functional area, choosing an item from the "Help" menu gives you information about:

   - the current functional area
   - keyboard navigation within SAM
   - using the SAM help system
   - displaying the version of SAM you are currently running

   From a dialog box (a window displaying fields to be filled in), pressing the (f1) key gives you context-sensitive information for the object at the location of the cursor.

   See Chapter 1, "Introduction to System Administration", for additional information about using SAM.

3. Highlight `Backup and Recover` and activate the (Open) control button.
4. Highlight `Backup Devices` and activate the (Open) control button.
5. Highlight the device in the list from which the index is to be read and displayed.
6. Choose `Use Remote Backup Device` and `Get List of Files on Device` from the "Actions" menu.
7. Fill in the hostname (machine name), device file, and filename to which you want the index file restored and activate the (OK) control button. SAM only supports restoring data remotely from magnetic and DDS format tapes.

   SAM will open a window to execute the the **frecover** command to restore the index file.

Important! Although every volume in the backup set has an index, indexes are completely accurate only for the previous volumes in the same set. For example, the index on the last volume may indicate that a file resides on that volume, but it may not have been backed up (it may have been removed after the index was created, but before fbackup attempted to back it up). *The only index guaranteed to be correct in all cases* is the on-line index, that is produced after the last volume has been written. See the next section for information about viewing SAM's on-line index files.

Viewing the Index Files on Your System Using SAM

Whenever you use SAM to back up your system, the `fbackup` utility creates an on-line index file. SAM keeps a separate index file for each of the following:

- The most recent *full* backup
- The most recent *incremental* backup
- A history log of all operations
- The most recent file recovery operation

To view these on-line index files:

1. Ensure that you have superuser capabilities.
2. Run SAM; type:

   `/usr/bin/sam`

   SAM provides an on-line help system to assist you when you need additional information.

   Activating the (Help) button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

   From within a functional area, choosing an item from the "Help" menu gives you information about:

   - the current functional area
   - keyboard navigation within SAM
   - using the SAM help system
   - displaying the version of SAM you are currently running

   From a dialog box (a window displaying fields to be filled in), pressing the (f1) key gives you context-sensitive information for the object at the location of the cursor.

   See Chapter 1, "Introduction to System Administration", for additional information about using SAM.

3. Highlight `Backup and Recover` and activate the (Open) control button.
4. Highlight `Backup Devices` or `Automated Backups` and activate the (Open) control button.
5. Choose `View Log Files` and one of the following from the "Actions" menu:

   `Full Backup Log...`

   `History Log...`

   `Incremental Backup Log...`

   `Recovery Log...`

   After you have viewed the information, activate the (OK) control button.

Backing Up Your System Using HP-UX Commands

Gather the following information before you begin:

- A list of files you want to back up (see "Determining Which Data to Back Up").
- The type of backup (see "Full Backups vs. Incremental Backups").
- The device file for the device on which to create your backup. All configured HP-UX devices have a *device file* associated with them that tells HP-UX the hardware address of the device and that which driver to use when communicating with the device. For more information about device files, see Chapter 11, "System Configuration" in the *How HP-UX Works: Concepts for the System Administrator* manual or the *Installing Peripherals* manual.

8

When backing up files that are NFS mounted to your system, `fbackup` can only back up those files having "other user" read permission. `fbackup` normally operates in user-mode when crossing NFS mount points; not superuser-mode. To ensure that `fbackup` can back up the files exported from the NFS server, login as superuser on the NFS file server and use the `root=` option to the `/usr/etc/exportfs` command to export the correct permissions. Refer to *exportfs*(1M) in the *HP-UX Reference* and the *Installing and Administering NFS Services* manual.

The `fbackup` Command

To back up files using the `fbackup` command:

1. Ensure that files you intend to back up are not being accessed.

Note The `fbackup` command will not back up files that are active (open) or locked when it encounters them.

2. Verify that the connections to the backup device are correct.
3. Verify that the backup device is turned on.
4. Ensure that the backup device is loaded with media. If the backup requires you to use additional media, the `fbackup` command will prompt you when to load change media.
5. Ensure that you have superuser capabilities.
6. Run the `fsck` command to check your file system for inconsistencies before you perform a backup. This ensures that you to do not back up data that is corrupt. Refer to Appendix A, "Using the fsck Command" in the *Solving HP-UX Problems* manual and *fsck*(1M) in the *HP-UX Reference*.

Caution Do not run `fsck` on a file system that is mounted and active. This could introduce data corruption. Run `fsck` in single-user mode when checking the root file system. For file systems other that the root file system, unmount the file system, run `fsck`, and then remount the file system.

7. Create a backup using the `fbackup` command:

   `/etc/fbackup -f` *device* `[-f` *device*`] ... [-`*level*`] [-uH]`
   `[-i` *path*`] [-e` *path*`] [-g` *graph_file*`] [-I` *index_file*`]`

   The command syntax is shown on two lines because of its length. When you execute an actual `fbackup` command, do *not* enter a carriage return until you have entered the entire command. Let the characters wrap around onto additional lines, if necessary.

   The most frequently used `fbackup` command options are described in Table 8-6. Refer to `fbackup(1M)` in the *HP-UX Reference* manual for details on additional options.

8

Table 8-6. fbackup command options

Option	What it is	Why you need to use it
`-f` *device*	Device File Name	The destination for the information you are backing up. More than one `-f` option can be used. When multiple devices are specified, backups are created on the devices in the order they are specified on the command line. The device access sequence repeats in a cyclical pattern until the backup is finished. If all of the device files have been used and there is still more data to be backed up, `fbackup` will prompt you to load additional media. For creating remote or network backups, the device file format is **machine:device-file**. The **machine** name is restricted to eight characters. Only magnetic tape and DDS format (DAT) tape drives are supported for remote backups. Refer to *fbackup*(1M) in the *HP-UX Reference* for additional information. If you are using an HP format cartridge tape drive (such as a 9144 , 9145 or 35401), you will need to pipe the output of `fbackup` into the `tcio` utility that properly blocks the output for the cartridge tape drive. If you do not do this, the activity of handling the output from `fbackup` will cause excess wear on the cartridge tape drive mechanism which may result in mechanical failure. The `tcio` commadn also optimizes the data transfer rate between certain cartridge tape units and the computer. To send the output of `fbackup` to a HP-UX command like `tcio`, use the -f option and the device file name "-" (dash). This tells `fbackup` to send its output to the standard output device (that can be piped to an HP-UX command).

8

Table 8-6. fbackup command options (continued)

Option	What it is	Why you need to use it
`-0 ... -9`	Backup Level	This option tells **fbackup** the backup level that you want to use for this backup. See the section "Backup Levels" earlier in this chapter for information on how backup levels are used.
`-u`	Update "dates" file	You need to use this option when you want **fbackup** to record information about this backup in the file **/usr/adm/fbackupfiles/dates** so that future incremental backups can be based on the date of this backup.
`-H`	Hidden Files	This option is important ONLY if you are backing up files for an HP-UX cluster. The **-H** option tells **fbackup** to back up *all* elements of context dependent files. Normally, **fbackup** only backs up the files that match the context of the computer it is being executed on. See Chapter 9, "Backing Up Files in a Cluster" in the manual *Managing Clusters of HP 9000 Computers*, HP part number B1864-90015 for more information about this.
`-i` *path*	Include	This option tells **fbackup** which files you want to include in your backup. See "Determining Which Data to Back Up". You can use as many **-i** options as you want.
`-e` *path*	Exclude	This options tells **fbackup** which files (from the list of included files) are to be excluded from the backup (the "exceptions"). See "Determining Which Data to Back Up". You can use as many **-e** options as you want.
`-g` *graph_file*	Graph	If you have a complicated structure of files to back up, or if you want to use the incremental backup features that **fbackup** provides (see "Backup Levels") you should use a "graph file" instead of using the **-i** and **-e** options to specify which directories and files to back up.
`-I` *index_file*	Index File	You can have the **fbackup** utility create an index file for you. This file will contain a complete list of the files that it has just backed up.

8

Table 8-6. fbackup command options (continued)

Option	What it is	Why you need to use it
`-n`	Cross NFS Mount Points	Back up data this is NFS mounted to your system. When backing up files that are NFS mounted to your system, `fbackup` can only back up those files having "other user" read permission. `fbackup` normally operates in user-mode when crossing NFS mount points; not superuser-mode. To ensure that `fbackup` can back up the files exported from the NFS server, login as superuser on the NFS file server and use the `root=` option to the `/usr/etc/exportfs` command to export the correct permissions. Refer to *exportfs*(1M) in the *HP-UX Reference* and the *Installing and Administering NFS Services* manual.

Examples Using the `fbackup` Command

This section contains a series of examples showing a variety of ways to use the `fbackup` command. The examples are based on the directory in Figure 8-4 unless otherwise stated. Figure 8-4 is the same as Figure 8-1, it is repeated for your convenience.

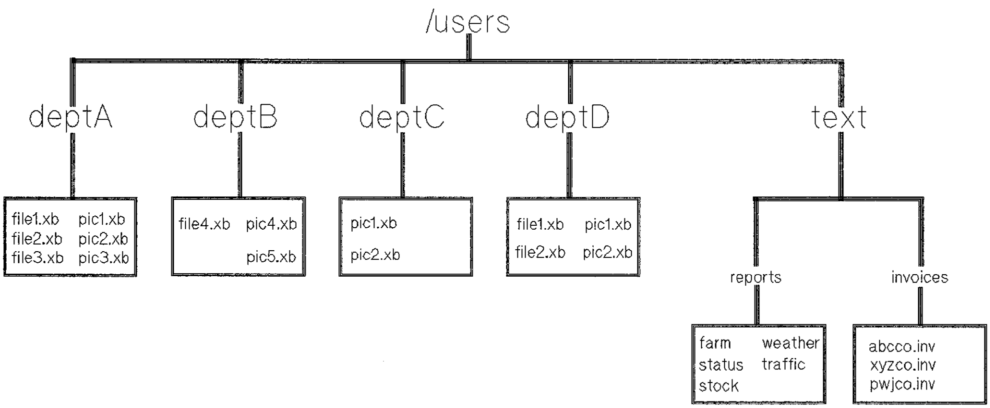


Figure 8-4. An Example Directory Tree

8

The following are example device files:

`/dev/rmt/0m` represents a magnetic tape drive in 1600 bpi mode or a DDS (DAT) tape drive in uncompressed mode.

`/dev/rmt/1h` represents a magnetic tape drive in 6250 bpi mode or a DDS (DAT) tape drive in compressed mode.

`/dev/rct/0s0` represents an HP format HP-IB cartridge tape drive.

`/dev/ac/1a` represents an optical disk in an optical library. This device file represents disk number 1 and surface "a" using section 2 (the entire surface).

For additional information on device files, see Chapter 11, "System Configuration" in *How HP-UX Works: Concepts for the System Administrator* and the *Installing Peripherals* manual.

To back up the entire directory structure in Figure 8-4 with the following criteria:

media:	DDS format (DAT) tape in uncompressed format
device file:	`/dev/rmt/0m`
backup type:	full
index file:	no
graph file:	no
update `dates` file:	no

type:

```
/etc/fbackup -f /dev/rmt/0m -i /users
```

8

To back up the entire structure *except* the /users/text/invoices directory with the following criteria:

media:	magnetic tape drive in 6250bpi mode
device file:	/dev/rmt/0h
backup type:	full
index file:	no
graph file:	yes (/usr/adm/fbackupfiles/graphs/g1)
update dates file:	yes

type:

```
/etc/fbackup -f /dev/rmt/1h -0 -u -g /usr/adm/fbackupfiles/graphs/g1
```

The contents of /usr/adm/fbackupfiles/graphs/g1 is:

```
i /users
e /users/text/invoices
```

To perform an incremental back up (level 5) of the previous example, type:

```
/etc/fbackup -f /dev/rmt/1h -5 -u -g /usr/adm/fbackupfiles/graphs/g1
```

To back up the data as defined in the the previous example over the network to a device connected to remote machine tulip, type:

```
/etc/fbackup -f tulip:/dev/rmt/1h -5 -u -g /usr/adm/fbackupfiles/graphs/g1
```

To back up the entire structure *except* the /users/text/invoices directory with the following criteria:

media:	optical disk library system
device file:	/dev/ac/1a
backup type:	full
index file:	no
graph file:	no
update dates file:	no

type:

```
/etc/fbackup -f /dev/ac/1a -i /users -e /users/text/invoices
```

To back up the entire structure *except* the /users/text/invoices directory with the following criteria:

media:	HP format cartridge tape drive
device file:	/dev/rct/0s0
backup type:	full
index file:	no
graph file:	no
update dates file:	no

type:

```
/etc/fbackup -f - -i /users -e /users/text/invoices | tcio -oe /dev/rct/0s0
```

Caution When you use fbackup to back up files to an HP format cartridge tape drive (such as a Model 9144 Model 9145, or Model 35401/Autochanger), you should always pipe the output from fbackup through the tape blocking utility known as tcio. If you do not do this, the activity of handling the output from fbackup will cause excess wear on the cartridge tape drive mechanism which may result in mechanical failure. The tcio command also optimizes the data transfer rate between certain cartridge tape units and the computer. The tcio command also handles multiple cartridge tapes.

The -f option with the value "-" tells fbackup to send its output to the standard output file. In this example, that output is piped to the utility tcio. The tcio options direct the output to the cartridge tape drive represented by the device file /dev/rct/0s0. For complete information about valid options for tcio, see the tcio(1) manual reference page in the *HP-UX Reference* manual.

8

To back up the entire file system (from /) using two magnetic tape drives in different modes with the following criteria:

media:	two magnetic tape drives (one in 1600bpi mode and the other in 6250bpi mode)
device file:	`/dev/rmt/0m` and `/dev/rmt/0h` respectively
backup type:	full
index file:	yes (`/tmp/index`)
graph file:	no
update `dates` file:	no

type:

```
/etc/fbackup -f /dev/rmt/0m -f /dev/rmt/1h -i / -I /tmp/index
```

This example will shows it is possible to specify more than one device to receive the output from `fbackup`. When more than one device is specified, the second one is used when the media on the first device fills up. This allows for an unattended backup if the media on the second device can hold the remaining data to be backed up.

Also in this example, an index file will be created called `/tmp/index`. An index is written to the beginning of each tape, listing all files in the specified "graph" being backed up. However, if a file is removed *after* the index is written but *before* the file is backed up to tape (or something else happens that prevents the file from being backed up), the index will not be completely accurate. If you tell `fbackup` to make an on-line index file (using the `-I` option), it will create the file *after* the backup is complete. Therefore, the on-line index file will be completely accurate with respect to which files are on each volume of the backup.

8

Backing Up to a Hard Disk Using the `cpio` Command

To back up to a hard disk using `cpio`:

1. Ensure that you have superuser capabilities.
2. Run the `fsck` command to check your file system for inconsistencies before you perform a backup. This ensures that you to do not back up data that is corrupt. Refer to Appendix A, "Using the fsck Command" in the *Solving HP-UX Problems* manual and *fsck*(1M) in the *HP-UX Reference*.

Caution Do not run `fsck` on a file system that is mounted and active. This could introduce data corruption. Run `fsck` in single-user mode when checking the root file system. For file systems other that the root file system, unmount the file system, run `fsck`, and then remount the file system.

---

3. Add a disk to your system. This requires that you:
   - physically connect the disk drive to your system.
   - ensure that the device driver for the disk is part of the kernel.
   - ensure that there is a device file for the disk.

   Refer to the *Installing Peripherals* to add the disk drive to the system.
4. Create a file system on the newly added disk with the `newfs` command, for example:

   `newfs /dev/rdsk/`*disk_device_file* `hp2213A`
5. Mount the newly added disk and file system to your main file system:

   `mount /dev/dsk/`*disk_device_file* `/disk_mount_point`

8

6. Transfer the data from you main file system to the file system on the newly added disk:

```
cd /
find .  -xdev -hidden -print | cpio -padmuvx /disk_mount_point
```

The `-xdev` option to the `find` command that avoids crossing any file system mount points that exist below starting points listed in the pathname list. This avoids a recursive backup of the `disk_mount_point` to the `disk_mount_point`. Refer to *find*(1) in the *HP-UX Reference*.

7. Unmount the disk containing the backed up data:

```
umount /disk_mount_point
```

Note For additional information regarding the `newfs`, `mount`, or `umount` commands, refer to Chapter 6, "Managing the File System".

Backing Up To a Hard Disk or DDS Format Tape Drive Using the dd Command

The recommended utility for quickly backing up your entire file system to a hard disk is the `dd` utility. The `dd` utility is preferred over other utilities because it quickly creates a mirror image of your currently mounted file system. This method of copying your file system is typically used for copying your HP-UX system from one hard disk to another.

It is also important to note that the `dd` utility only performs full backups (complete disk or disk section copies) and a backup log file is not automatically maintained. Using the `dd` command does not allow for individual file recovery. Only the entire disk section containing the file system can be restored.

To perform a full backup using `dd`:

1. Ensure that you have superuser capabilities.
2. Run the `fsck` command to check your file system for inconsistencies before you perform a backup. This ensures that you to do not back up data that is corrupt. Refer to Appendix A, "Using the fsck Command" in the *Solving HP-UX Problems* manual and *fsck*(1M) in the *HP-UX Reference*.

Caution Do not run `fsck` on a file system that is mounted and active. This could introduce data corruption. Run `fsck` in single-user mode when checking the root file system. For file systems other that the root file system, unmount the file system, run `fsck`, and then remount the file system.

---

3. Ensure that your system is configured to recognize the destination hard disk or DDS format tape drive. This requires ensuring the device driver is part of the kernel and that there is an appropriate device file. Refer to the *Installing Peripherals* manual for details.
4. Get your source file system device file with the `bdf` command, for example:

```
bdf
Filesystem        Kbytes    used    avail  capacity  Mounted on
/dev/dsk/6s0      324546  175018   117073       60%      /
```

5. Identify your destination hard disk device file

8

6. Invoke the `dd` command. The command syntax is:

   `/bin/dd if=`*source* `of=`*destination* `bs=`*block_size*

   where:

source	is the device file for the disk drive to be copied.
destination	is the device file for the destination (target) device.
var|block_size|	is the block size for the device as specified by the `/etc/disktab` file.

   For example,

   ```
   dd if=/dev/dsk/6s0 of=/dev/dsk/c1d0s13 bs=1024k
   ```

7. Label the backup hard disk to identify the date, sections used, and their contents. If you do not label the disk with the sections containing your files, you will have to systematically mount every section of the disk to find your files.

Warning

- **The `dd` utility will overwrite data on the destination disk drive. This type of backup is only recommended for use between disks of the same type and size.**
- **Do not interchange the *source* and *destination* parameters! If you do, you will destroy the data you are trying to backup located on your *source* disk.**

It is recommended that you use the same type of backup hard disk as your primary hard disk and use the same section on the destination hard disk to create your backup. Additional hard disk sectioning information is contained in the `/etc/disktab` file and in Chapter 6, "Managing the File System".

Setting Up an Automated Backup Schedule Using HP-UX Commands

Setting up an automated backup schedule using HP-UX commands is more involved than using SAM to do it. This is an area where using SAM is recommended.

You may automate your backup procedure using the `crontab(1)` utility, which interfaces with the HP-UX process scheduling facility, `cron(1M)`. You can find additional information about `cron` and `crontab` in the *HP-UX Reference* manual.

To automate your backup procedure, you need to:

1. Create a file that defines the process you want to automate.
2. Activate the processes that are defined in the file you created.

Note If you schedule `fbackup` via the `crontab` utility you should be aware that `fbackup` is a highly interactive utility. If it should need attention (tape change, device not on line, etc.), `fbackup` will attempt to prompt for the input it needs. This may cause an automated backup to fail (or not complete).

8

Creating an Automated Backup Schedule File

The `crontab` utility allows you to specify an input file containing the date, time, and runstrings of the backup procedures (processes) that you want to automate (see "Examples Using the `fbackup` Command"). This file (the input to the `crontab` utility) contains lines that have six required fields each. The fields are separated by spaces or tabs. Each entry in this file has the following format:

```
minute hour dates months days runstring
```

where:

`minute`	*specifies the minute (0-59)*
`hour`	*specifies the hour (0-23)*
`dates`	*specifies particular dates of the month (1-31)*
`months`	*specifies particular months of the year (1-12)*
`days`	*specifies particular days of the week (0-6 with 0 representing Sunday)*
`runstring`	*specifies the command line or script file to execute*

An entry of "*" in any crontab field represents all legal values.

Therefore, to schedule the `ps(1)` command to execute at 5:10pm (17:10) on every Friday and Monday during June, July, and August, you would make an entry in your crontab file that looks like this:

```
10 17 * 6,7,8 1,5 ps >> psfile 2>&
```

The `2>&` redirects any error messages to the file `psfile`.

Note When scheduling processes with `crontab`, you must redirect any output that is normally sent to the terminal to a file. In the above example, the file containing the output is `psfile`.

An example backup strategy may consist of a full backup (performed once a week on Saturday) and an incremental daily backup (every week day). Assume that the backups are to be performed at 4:03 am and the media is DDS format (DAT) tape. The following crontab file implements the example backup strategy:

```
3 4 * * 1 /usr/adm/incrback  >>  monbackup
3 4 * * 2 /usr/adm/incrback  >>  tuebackup
3 4 * * 3 /usr/adm/incrback  >>  wedbackup
3 4 * * 4 /usr/adm/incrback  >>  thubackup
3 4 * * 5 /usr/adm/incrback  >>  fribackup
3 4 * * 6 /usr/adm/fullback  >>  satbackupfull
```

In the above example "incrback" and "fullback" are shell scripts that contain the `fbackup` commands.

Activating Your Automated Backup Schedule

Once you have created the file defining your time-scheduled backups, you must inform `cron` that it has new jobs to schedule. You do this with the `crontab` utility. For example:

`crontab` *your_crontab_file*

This will activate all of the processes defined in *your_crontab_file*. This cancels any previously scheduled processes not defined in *your_crontab_file*.

Note Before activating a new crontab file, you should view currently scheduled processes. Consider adding these processes to *your_crontab_file*. See "Displaying Your Automated Backup Schedule".

After your cronfile backup has been activated, you must always ensure that:

- Run the `fsck` command to check your file system for inconsistencies before you perform a backup. This ensures that you to do not back up data that is corrupt. Refer to Appendix A, "Using the fsck Command" in the *Solving HP-UX Problems* manual and *fsck*(1M) in the *HP-UX Reference*.

Caution Do not run `fsck` on a file system that is mounted and active. This could introduce data corruption. Run `fsck` in single-user mode when checking the root file system. For file systems other that the root file system, unmount the file system, run `fsck`, and then remount the file system.

8

- The system clock is set properly.
- The backup device is properly connected and the HP-UX I/O system recognizes the device file specified in the `fbackup` runstring.
- Adequate media has been loaded in the backup device.
- The backup device is connected your system and turned on.
- The NFS mounted files you want backed up have the correct permissions

  When backing up files that are NFS mounted to your system, `fbackup` can only back up those files having "other user" read permission. `fbackup` normally operates in user-mode when crossing NFS mount points; not superuser-mode. To ensure that `fbackup` can back up the files exported from the NFS server, login as superuser on the NFS file server and use the `root=` option to the `/usr/etc/exportfs` command to export the correct permissions. Refer to *exportfs*(1M) in the *HP-UX Reference* and the *Installing and Administering NFS Services* manual.

Displaying Your Automated Backup Schedule

To list your currently scheduled processes, execute the command:

```
crontab -l
```

This will display the contents of your activated crontab file. You should always view the currently scheduled processes *before* activating a new crontab file to be sure that you do not cancel processes that need to remain active. If there are such processes, add them to the definitions in your new crontab file before executing the `crontab` command to add new processes.

Deactivating Your Automated Backup Schedule

To deactivate all of your currently scheduled processes, execute the command:

```
crontab -r
```

Changing Your Automated Backup Schedule

To change your currently scheduled processes:

1. Edit your crontab file, which defines the jobs to time schedule to incorporate the changes you want.
2. Activate the edited file as you did the original. See "Activating Your Automated Backup Schedule".

Restoring Files Using HP-UX Commands

Gather the following information and materials before you begin:

- A list of files you need.
- The media on which the data resides.
- The location on your system to restore the files (original location or relative to some other location).
- The device file corresponding to the device being used to for restore the files.

When restoring files that are NFS mounted to your system, `frecover` can only restore those files having "other user" read permission. `frecover` normally operates in user-mode when crossing NFS mount points; not superuser-mode. To ensure that `frecover` can restore the files exported from the NFS server, login as superuser on the NFS file server and use the `root=` option to the `/usr/etc/exportfs` command to export the correct permissions. Refer to
8 *exportfs*(1M) in the *HP-UX Reference* and the *Installing and Administering NFS Services* manual.

The `frecover` Command

The `frecover` command restores backup files made using the `fbackup` utility. If your files on the media did not get created using `fbackup`, refer to "Other Backup and Restore Utilities".

To restore files from backups using `fbackup`:

1. Ensure that files you intend to back up are not being accessed.

Note The `frecover` command will not restore files that are active (open) or locked when it encounters them.

---

2. Verify that the connections to the device are correct.
3. Verify that the device is turned on.
4. Ensure that the device is loaded with media. If the restore process requires you to use additional media, the `frecover` command needs to be executed separately for each media.
5. Ensure that you have superuser capabilities.
6. Restore files using the `frecover` command.
   - The `frecover` command syntax generally used when recovering *all* files from your backup is:

     `/etc/frecover -r -o [-f` *device*`]`

     or

     `/etc/frecover -o [-f` *device*`]`

     where:

`-r`	Recovers all of the files on the media.
`-o`	Recovers the files from the media irrespective of age. Normally `frecover` will not overwrite an existing file with an older version.
`-f`	Specifies the device file from which to recover the data. If not specified the default, `/dev/rmt/0m`, is used. See "The `fbackup` Command".

8

- The `frecover` command syntax generally used when restoring *individual* files to your system is:

  `/etc/frecover -x -o[F | X] [-f` *device*`] [-i` *path*`] [-e` *path*`]`
  `[-g` *graph_file*`]`

  where:

`-x`	Extracts files from the backup.
`-o`	Recovers the files from the media irrespective of age. Normally `frecover` will not overwrite an existing file with an older version.
`-F`	Recovers files without leading directories. Normally `frecover` recovers files to their absolute path name.
`-X`	Recovers files with paths relative to the current directory.
`-f`	Specifies the device file from which to recover the data. If not specified the default, `/dev/rmt/0m`, is used. See "The `fbackup` Command".
`-i`	Defines specific files to include in the recovery.
`-e`	Defines specific files to exclude from the recovery.
`-g`	Specifies the graph file to be used. The lists of files to be included and excluded are with respect to the structure of files represented on the *backup*, not the structure of files currently on your system (although the two may be similar).

  The syntax is presented here on two lines because of page width limitations. When you enter an `frecover` command that is longer than one screen width, do *not* press carriage return until the end of the command. Let the characters wrap around onto the next line if necessary. Items listed in brackets ([ ]) are optional.

`frecover` has other options. For complete details on the options for `frecover`, see *frecover*(1M) in the *HP-UX Reference*.

Caution When you use `frecover` to restore files from a cartridge tape drive (such as a Model 9144 , Model 9145, or Model 35401/Autochanger), you should always pipe the input to `fbackup` through the tape blocking utility known as `tcio`. If you do not do this, the activity of handling the input from the device will cause excess wear on the cartridge tape drive mechanism, which may result in mechanical failure. The `tcio` command also optimizes the data transfer rate between certain cartridge tape units and the computer.

Examples Using the `frecover` Command

The following examples are based on a "full backup" of the directory structure listed in Figure 8-5. Figure 8-5 is the same as Figure 8-4 and Figure 8-1, it is repeated for your convenience.

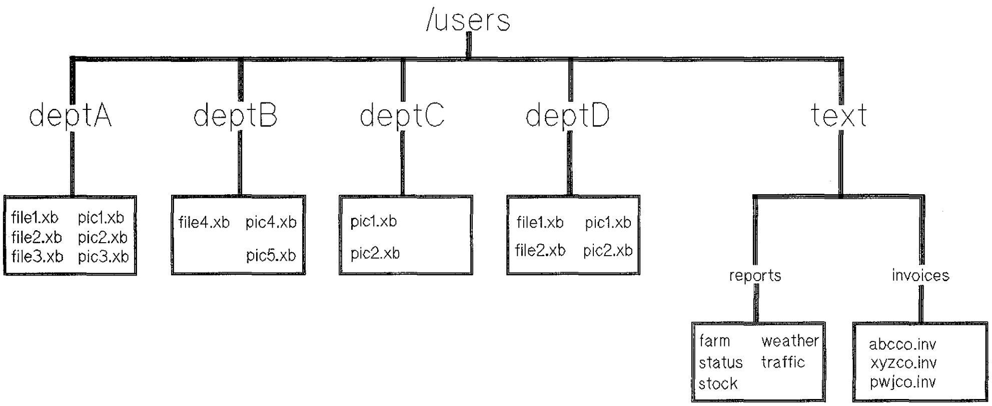


Figure 8-5. An Example Directory Tree

8

The following are example device files:

`/dev/rmt/0m` represents a magnetic tape drive in 1600 bpi mode or a DDS format (DAT) tape drive in uncompressed mode

`/dev/rmt/1h` represents a magnetic tape drive in 6250 bpi mode or a DDS format (DAT) tape drive in compressed mode.

`/dev/rct/0s0` represents an HP format HP-IB cartridge tape drive.

`/dev/ac/1a` represents an optical disk in an optical library. This device file represents disk number 1 and surface "a" using section 2 (the entire surface).

For additional information on device files, see Chapter 11, "System Configuration" in *How HP-UX Works: Concepts for the System Administrator* and the *Installing Peripherals* manual.

To restore the files from all of the directories under `/users/text` from a DDS format (DAT) tape into the `/tmp` directory on the system, type:

```
cd /tmp
/etc/frecover -x -oF -i /users/text
```

First change your working directory to `/tmp`. The `-F` option to `frecover` removes leading path names from all files on the tape. If there are files in the directory `/tmp` whose names match those coming from tape, specifying the `-o` option overwrites the version on disk, even if the copy on disk is newer. The `/tmp` directory now contains all of the files without the leading directories, for example:

```
ls /tmp

./      abcco.inv   pwjco.inv   stock     weather
../     farm        status      traffic   xyzco.inv
```

If there are duplicate filenames found on the tape, files are overwritten with the most recent one extracted from the tape.

To recover all of the files from a full backup using the default device (`/dev/rmt/0m`), type:

```
/etc/frecover
```

You do not need to specify the `-r` option since it is the default. Omitting the `-o` option will not overwrite any newer files on disk.

To recover all of the files from a full backup on an HP format cartridge tape, type:

```
tcio -i /dev/rct/0s0 | /etc/frecover  -f -
```

To restore the files belonging to the directory `/users/deptA` from DDS format (DAT) tape, type:

```
/etc/frecover -x -i /users/deptA
```

If files are currently in that directory (on the disk) that are newer than the corresponding files on the tape, `frecover` will *not* overwrite the newer version on disk because the `-F` option is not specified. Because we are restoring the files from the device represented by device file `/dev/rmt/0m`, we do not need to use the `-f` option.

To restore the files belonging to the directory `/users/deptA` from an HP format cartridge tape, type:

```
tcio -i /dev/rct/0s0 | frecover -x -f - -i /users/deptA
```

If files are currently in that directory on the disk that are newer than the corresponding files on the tape, we will *not* overwrite the newer version on disk. Because we are restoring the files from cartridge, we need to do two things:

1. Use the tape blocking utility, `tcio`, to filter the input from the HP format cartridge tape drive.
2. Use `frecover's` -f option along with the "device" name "-", which indicates that `frecover` is to get its input from the standard input device (the piped output from `tcio`). 8

Restoring Data From a Hard Disk Using the `cpio` Command

1. Add the disk to your system. This requires that the device driver for the disk is part of the kernel and that there is a device file on the system to communicate to the disk. Refer to the *Installing Peripherals* to add the disk drive to the system.

2. Mount the disk to your root file system:

   ```
   mkdir /disk_mount_point
   mount /dev/dsk/disk_device_file /disk_mount_point
   ```

   For additional information refer to Chapter 6, "Managing the File System".

3. Restore data from the file system on the backup disk to your main file system:

   ```
   cd /disk_mount_point
   find /disk_mount_point -hidden -print | cpio -padmuvx /
   ```

8

Restoring Data From a Hard Disk Using the `dd` Command

The recovery steps for restoring a file system from your backup hard disk depends on the file system you want to restore.

For restoring the root(/) file system, HP recommends the following five steps if you created your backup with the `dd` utility:

1. Get your current, destination, root (/) file system device file with the `bdf` command.
2. Get your backup hard disk, source, root(/) file system device file from the label. If you did not label your disk with the sections used for the backup, you must systematically mount all sections of the backup disk to find your files.
3. Reboot your system from the backed up file system on the backup hard disk. Rebooting your system is covered in the "Selecting a System to Boot" section of Chapter 3, "Starting and Stopping HP-UX".
4. Restore the currently mounted, backed up file system to your main disk drive with the `dd` utility.
5. Reboot your system from restored file system on your main hard disk. Rebooting your system is covered in the "Selecting a System to Boot" section of Chapter 3, "Starting and Stopping HP-UX".

For restoring a file system other than your root (/) file system, HP recommends the following five steps if you created your backup with the `dd` command:

1. Get your current, destination, file system device file with the `bdf` command.
2. Get your backup hard disk, source, file system device file from the label. If you did not label your disk with the sections used for the backup, you must systematically mount sections of the backup disk to find your files.
3. Unmount the file system you want to restore from your backup hard disk. See Chapter 6, "Managing the File System", for details on unmounting a file system.
4. Restore the file system from the backup hard disk with the `dd` command. This will overwrite the existing data in the specified destination section of your main hard disk.
5. Remount the recovered file system. See Chapter 6, "Managing the File System", for details on mounting a file system.

Viewing the Index File on the Local Device Using HP-UX Commands

The utility `frecover` has an "index" mode of operation. Using this mode of operation, you can have `fbackup` list the contents of the index at the beginning of a backup volume. To do this, use the `-I` option (instead of either `-r` or `-x`).

The syntax for this is:

`/etc/frecover -I` *path* `-f` *device*

Where:

path	is the file in which to put the directory listing. The default is to print the listing to the standard output (usually the terminal screen).
device	is the device file name for the device containing the backup medium.

Important! Although there is an index at the beginning of each volume in a backup set, indexes are completely accurate only for the previous volumes in the same set. Hence, the index on the last volume may indicate that a file resides on that volume, but it may not have been backed up (for example, if it was removed after the index was created, but before fbackup attempted to back it up). *The only index guaranteed to be correct in all cases* is the on-line index, which is produced after the last volume has been written (the one created using `fbackup's -I` option).

Here are two examples: Assuming that the device file for the magnetic tape drive is `/dev/rmt/0h` and we want to put the listing of the index in the file `/tmp/index2`, we would use the following command:

```
/etc/frecover -I /tmp/index2 -f /dev/rmt/0h
```

Assuming that the device file for the HP format cartridge tape drive is `/dev/rct/0s0` and we wanted to put the listing of the index in the file `/usr/adm/indexlog42`, we would use the following command:

```
tcio -i /dev/rct/0s0 |/etc/frecover -I /usr/adm/indexlog42 -f -
```

Recovering From a System Crash Using Your Recovery Tape

If for some reason you cannot boot your system disk, you can boot a memory-based version of `/hp-ux` (known as a **recovery system**) from a tape cartridge or DDS format (DAT) tape. From the recovery system, you can mount and unmount file systems, run `fsck` to check and repair file systems, copy files back onto your system disk, etc.

Caution Do not run `fsck` on a file system that is mounted and active. This could introduce data corruption. Run `fsck` in single-user mode when checking the root file system. For file systems other that the root file system, unmount the file system, run `fsck`, and then remount the file system.

To learn how to make a recovery system, see "Creating a Recovery System" in Chapter 2, "Constructing an HP-UX System".

If your system disk is unbootable, do the following:

1. Verify that the recovery tape is *not* write protected. HP-UX needs to have write access to your recovery tape when you boot it up.
2. Load the recovery tape in your tape drive and be sure that the drive is turned on.
3. Wait for the drive to become ready (the "busy" light remains off).
4. Reset your computer by turning it off and then back on. Boot the system in *attended mode* by holding down the (space bar) as the computer is performing its self-test.
5. Select the operating system that is on the tape drive as the one you want to boot from (chances are, it will be your only choice).
6. Once your recovery system is up and running you will have a minimum set of commands to use, in order to help you repair and restore your primary (disk-based) operating system.

7. From this point, the specific things you need to do to recover your primary system depend on the nature of what is causing your system not to boot. Here is a list of some of the things that you might need to do. For help in determining what your system's specific problem is, see Chapter 5, "System Boot-Up Problems" in the manual: *Solving HP-UX Problems*, HP part number B2355-90030.

Note If your inability to boot your system is caused by faulty hardware, it will be necessary to have that hardware repaired before you can proceed with the items in this list.

- You might need to run the `fsck` program to repair your root file system.

Caution Run `fsck` in single-user mode when checking the root file system. If you do not, you will introduce data corruption on your root disk.

- You might need to restore `/hp-ux` (if it was corrupted or removed from you disk-based system). This can be done by:
  - Mounting your system disk to an empty directory (make one if necessary) in your memory-based recovery system.
  - Using the `cp` command to copy the `/hp-ux` file from your memory-based system (it is a copy of your *real* `/hp-ux` file) to the directory you used as a mount point for your system disk. The destination file should be called `hp-ux`.
- You might need to restore important system files such as `/etc/inittab`, `/etc/rc`, etc. from your memory-based system to your system disk. The procedure for doing this is almost identical to the procedure for restoring `/hp-ux` that is in the previous item in this list. Only the file names and directories will be different.
- You might need to move, remove, copy, or search for other files.

The important thing to remember is that the memory-based system has limited capabilities. Your primary objective is to restore your disk-based system to a bootable condition and then reboot your computer from your system disk. From that point, you can recover lost files from backup tapes, or whatever else is necessary to restore your system to its normal operational condition.

Other Backup and Restore Utilities

There are other utilities that can be used to back up files from your system. Some of them are listed below. Those mentioned here are *usually* available on other vendors' machines, so these utilities may be useful in transferring files between systems of various vendors.

Run the `fsck` command to check your file system for inconsistencies before you perform a backup. This ensures that you to do not back up data that is corrupt. Refer to Appendix A, "Using the fsck Command" in the *Solving HP-UX Problems* manual and *fsck*(1M) in the *HP-UX Reference*.

Caution Do not run `fsck` on a file system that is mounted and active. This could introduce data corruption. Run `fsck` in single-user mode when checking the root file system. For file systems other that the root file system, unmount the file system, run `fsck`, and then remount the file system.

The other backup utilities available are:

/usr/bin/ftio is designed for 9-track magnetic tape media. The `ftio` utility has increased throughput over `cpio` and `tar` due to multiple processes and a larger blocking factor. The `ftio` **-H** option is required for backing up cluster server context dependent files. You may specify a remote device in the form *host:devfilepath*. This utility is not recommended for backing up secured (trusted) systems.

/bin/cpio The `cpio` utility with piped input from the `find` command can be used to create a backup. The `find` **-hidden** option preserves the context dependent files required to back up a cluster server. You may specify a remote device in the form *host:devfilepath*. This utility is not recommended for backing up secured (trusted) systems.

/bin/dd The `dd` command can be used to create an exact image copy of your disk to DDS format (DAT) tape. The tape can be used to boot from, if your system disk crashes (or its data is erased). See "Backing Up To a Hard Disk or DDS Format Tape Drive Using the `dd` Command".

/usr/bin/tar does not have the same level of error handling as `fbackup` and `frecover`. The `tar` -H modifier is required to back up a cluster server. This utility will include special device files on the backup if the **-N** option is specified. This utility is not recommended for backing up secure (trusted) systems.

9

Managing Printers and Printer Output

What is the Line Printer Spooling System?

The **Line Printer Spooling System** (**lp spooler**) is a set of programs, shell scripts, and directories that control your printers and the flow of data going to them. It:

- helps prevent **intermixed listings**.
- provides control of printout routing.
- allows users to cancel, restart and adjust the priority of print requests.

Once a printer has been added to your system (that is, its driver is in your kernel configuration, and an appropriate device file exists), it can be added to the lp spooler (for example you can redirect the output of a command to the device file associated with the printer). We recommend adding all printers to the lp spooler. If you do not add your printer or plotter to the lp spooler, there is no coordination between multiple users and intermixed listings can occur. Unspooled printing is not recommended. The purpose of the lp spooler is to *automatically* coordinate between multiple users and prevent intermixed listings.

Note The term "printer" can be interchanged with the term "plotter" for the tasks described in this chapter.

This chapter will cover the following topics:

- Components of the lp spooler
- Remote printing
- Controlling data flow through the lp spooler
- Priorities of printers and print requests
- Using plotters with the lp spooler
- Collecting and reporting statistics about data flow through the lp spooler

This chapter describes how to accomplish the tasks associated with these topics using SAM and HP-UX commands. The HP-UX commands method is provided for those who do not have access to SAM or choose not to use it.

If you are already familiar with the basic concepts of the lp spooler you may want to proceed directly to one of the tasks in the "Line Printer Spooler Tasks" section of this chapter.

Note If you are reading this chapter because you have a problem with the lp spooler, you should first refer to Chapter 2, "Line Printer Spooling System Problems" in *Solving HP-UX Problems*, HP part number B2355-90030.

If you are working with the lp spooler for the first time or you want to review key concepts before performing a particular task, you should continue reading the material found in "LP Spooler Overview".

Terms Used in this Chapter

The following terms appear in discussions in this chapter. You can scan the list now and, if you need to, refer to it later.

destination
A print destination is a generic term used to describe a printer or **printer class**. Users can specify a print destination when they print something by using the "`-d`" option to the `lp` command. See **printer class**.

interface script
A shell script, located in the `/usr/spool/lp/interface` directory, that is the final stage of the lp spooler. Each printer that is configured in the **lp spooler** has an interface script that, under the control of the line printer scheduler, sends a print job to the printer.

intermixed listings
Multiple jobs printing on a printer simultaneously that result in printed pages with characters from different print jobs mixed together. The lp spooler is designed to prevent this.

line printer scheduler
The line printer scheduler is the heart of the **lp spooler**. It is the central program that must be running to ensure coordination of requests from users to printers.

lp spooler
The HP-UX software subsystem responsible for controlling output to the printers on your system. Its primary responsibility is to prevent **intermixed listings**. It can also prioritize print jobs and start and stop output to printers.

local printer
A printer, configured into your lp spooler, that is physically connected to your computer. See **remote printer**.

logical printer
Each printer that is defined in your lp spooler is given a name that users will use to refer to it. You can create more than one definition (printer name) for any given printer. The logical printer name refers, not to the printer itself, but to one of the lp spooler definitions used to access the printer.

model script — When a printer is added to the lp spooler, an interface script must be created that can set up the communication to the printer and send data to it. HP supplies models for these interface scripts in the `/usr/spool/lp/model` directory. These models are used by the `lpadmin` command to build the interface script for a printer as it is being defined.

cancel model script — The cancel model script, `/usr/spool/lp/cmodel/rcmodel`, is used to cancel a print request to a printer on a remote system.

status model script — The status model script, `/usr/spool/lp/smodel/rsmodel`, is used to return the status of the remote printer and print requests for the remote

network-based printer or plotter — A printer or plotter that is directly connected to the local area network.

print request — A term used to refer to a specific print job in the lp spooler.

print request identification number — The number the lp spooler uses to identify your print request. This identification number consists of the name of the printer or printer class followed by a sequence number.

print request priority — See **priority**.

printer class — A defined group of printers. A printer class can be used as a print destination instead of a printer name. The first available printer in the printer class will print the next job queued to that printer class.

printer fence priority — See **priority**.

printer name — When a printer is configured into the lp spooler, it is given a name that users can use to specify that printer as a print destination for their printout.

print queues — Also known as request directories, print queues are directories used by the lp spooler to hold print jobs for each print destination until they can be printed.

priority
A value associated with each printer and print request. Priorities are used to control which print requests can print on a given printer. Priorities can be adjusted and must have a range from 0 to 7. See "Priorities of Printers and Print Requests".

remote print requests
A print request issued via the lp spooler on your system to be printed on a printer that is attached to a remote computer.

remote printer
A printer that is defined in your lp spooler but is physically connected to another computer (and accessed over a network).

remote spooling
The process used to allow printing to printers that are defined as part of your lp spooler but physically connected to another computer.

remote spooling daemon
A "behind the scenes" (background) program that runs on a remote computer. The remote spooling daemon receives print requests via a network and submits the print requests to its local lp spooler on the network user's behalf.

request directories
See **print queues**.

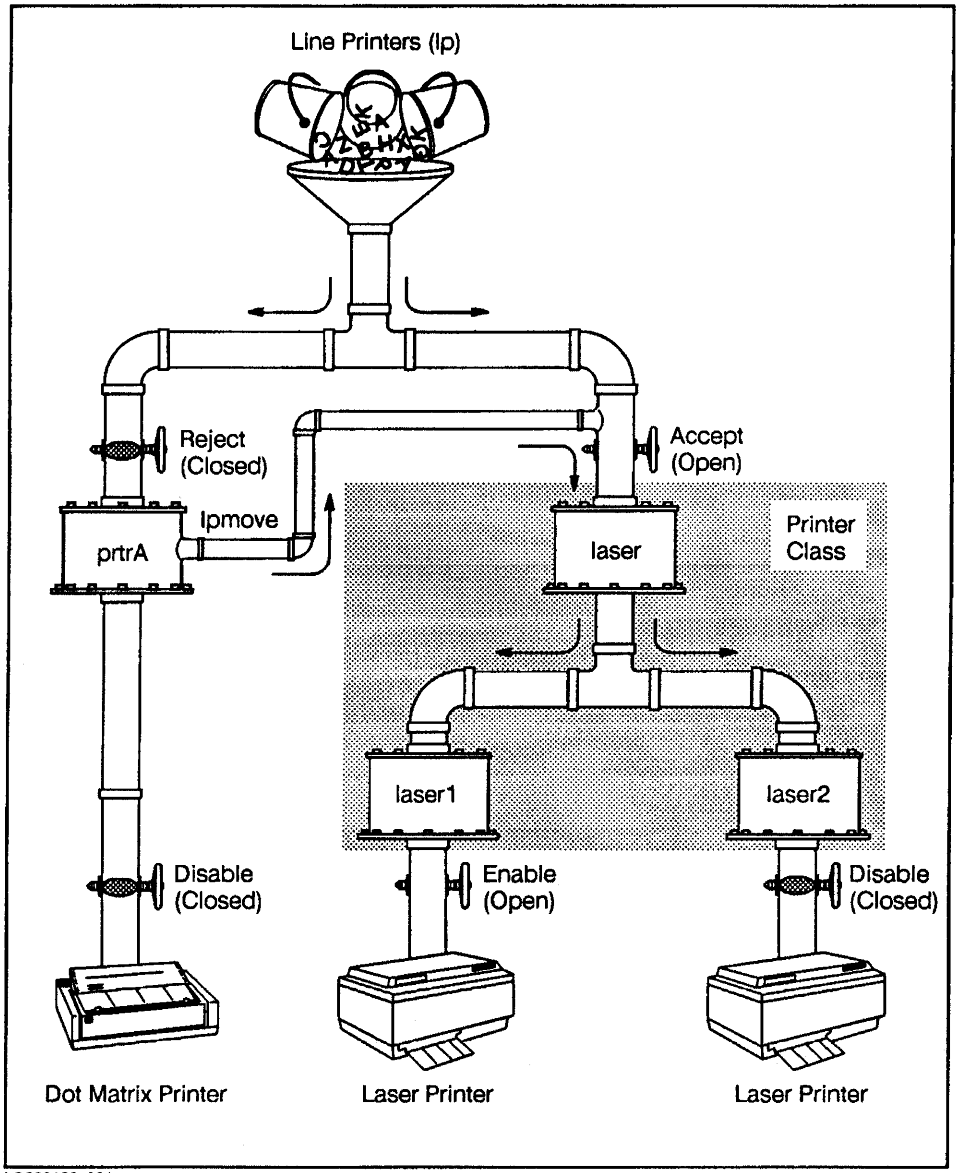
system default printer
When a user issues a print request, the user can specify a print destination. A system default printer can be defined so that, if a print destination is not specified, the lp spooler will use the system default printer.

LP Spooler Overview

You can think of the lp spooler as if it were a plumbing system. Figure 9-1 shows how this "plumbing system" might look. The data to be printed represents the "water" in this system. There are various request directories, sometimes referred to as printer queues, which serve as temporary holding tanks for print requests until they are sent to a printer to be printed. The flow of print requests is controlled at the request directory and printer level. The terms *accept* and *reject* refer to controlling the flow of print requests to the request directories while the terms *enable* and *disable* refer to controlling the flow of print requests to the printers. Accepting, rejecting, enabling, and disabling print requests control the data through the lp spooler as valves would control the flow of water in a real plumbing system. Shell scripts (called interface scripts) near the end of the data flow serve as pumps which "pump" an orderly flow of data to the printers.

The line printer scheduler controls the routing of print requests from the request directories to the printers. It functions as an automated flow controller in the "plumbing system" to prevent **intermixed listings** and to provide efficient use of the printers on your system. Intermixed listings are multiple print requests printing on a printer simultaneously that result in printed pages with characters from different print requests mixed together.

You can add a printer to, or remove it from your system. If the "drain gets clogged" for one printer, you can re-route the print requests for that printer to another printer and you can "flush" unwanted print requests from the spooling system. You can also sent a print requests to another computer to printed. Sending print requests to another computer to be printed is called **remote spooling** and the other computer is referred to as a remote system. When you use remote spooling, a special shell script ("pump") is used to send the data to a remote system. A program on the remote system receives the data and directs it into the remote system's LP spooler.



LG200139_001a

Figure 9-1. Line Printer Spooler "Plumbing Diagram."

The Components of the LP Spooler

The components of the lp spooler are:

- printer names
- printer classes
- print destinations
- system default printer
- printer interfaces
- printer models
- device files
- line printer scheduler
- local printer
- remote printer
- print request identification number

Printer Names

When you configure a printer into the lp spooler, you assign it a name that you will use to refer to it when you later submit print requests. This name is referred to as the **printer name**. Printer names can contain up to 14 characters, which can be alpha-numeric or underscores. The name may or may not be the same as the device file name. Some correspondence between the printer name and device file name is suggested. The printer name is the name of the printer that shows up when you request the status of the printer queue with the `lpstat` command.

A hypothetical system "hypo1" has the following printers defined in its lp spooler. The printers have the following names:

- laser1
- laser2
- phred
- letterhead
- invoices
- check_printer

Printer Classes

You can treat a *group of printers* as if they were one printer. A **printer class** is a name that you can use to refer to the *group of printers*. When submitting a print request you can specify a particular printer name or a printer class name. When submitting a print request to a printer class, the print requests will print on the first available printer in the group rather than on a specific printer. Printers that are members of a printer class can still be referenced individually. Creating a printer class is optional.

On the hypothetical system "hypo1," three of the printers are grouped into a printer class called "laser".

printer class: laser

- laser1
- laser2
- phred

- Printer class names can contain up to 14 characters, which can be alpha-numeric or underscores.
- Printer class names and printer names on the same system cannot be the same name. Printer names and class names must all be unique.
- Printer classes cannot include remote printers.
- A printer class must contain at least one printer.
- A printer can only belong to one printer class at a time.
- To remove a printer from a printer class, you must remove the printer from the lp spooler and re-add without specifying a printer class.

LP Spooler Overview

Print Destinations

Several of the commands for the lp spooler require you to specify a print **destination**. A destination is the name of a printer or printer class.

For our example system "hypo1", possible destinations are:

- printer class: laser
- laser1
- laser2
- phred
- invoices
- check_printer
- letterhead

System Default Printer (Destination)

You can appoint one of the print destinations in your lp spooler to be the system default printer. It is not necessary to have a system default printer, but it is recommended. A system default printer receives any print requests that are not sent to a specific print destination. You can have only one *system* default printer.

In addition to, or instead of, a *system* default printer, you can assign each *user* a default printer to use. To do this, simply set the user's LPDEST shell environment variable to the name of the system default printer.

- If LPDEST *is* set and a user does not specify a different printer to use, the printer referenced by LPDEST will be used.
- If LPDEST *is not* set for a user, and the user does not specify a printer, the system default printer (if one is set) will be used.
- If neither LPDEST or the system default printer is set, a user must specify a printer (or printer class).

Printer Interfaces

A printer interface, also known as an **interface script**, is the final stage of the lp spooler. It is the part of the lp spooler that is responsible for sending data to a printer. Each printer that you have defined for use by the lp spooler has its own interface script (shell script) that resides in the `/usr/spool/lp/interface` directory. When printers are added to the lp spooler, an interface script is copied from `/usr/spool/lp/model` to `/usr/spool/lp/interface` and given the printer name.

If we were to list the directory `/usr/spool/lp/interface` on our hypothetical system "hypol," it would contain the printer interface files `laser1`, `laser2`, `phred`, `letterhead`, `invoices`, and `check_printer`.

The entry for the class name `laser` would be located in the directory `/usr/spool/lp/class`; it would not be found in the interface directory.

Printer Models

There are printer interface script "models" you can choose from that have been created for you in the `/usr/spool/lp/model` directory. Many of them have names that match the model numbers of Hewlett Packard printers and plotters.

When you configure your printer into the lp spooler, you must specify which printer model interface script you want to use. The model will be automatically copied from the `/usr/spool/lp/model` directory into the `/usr/spool/lp/interface` directory and given the name that you specified as your printer name (see "Printer Names").

If you list the `/usr/spool/lp/model` directory, it should look similar to this:

```
HPGL1         draftpro   hp2560       hp2932a    hp7596a
HPGL2         dumb       hp2563a      hp2934a    laserjet
PCL1          dumbplot   hp2564b      hp33440a   laserjetIIISi
PCL2          fonts      hp2565a      hp33447a   paintjet
PCL3          hp2225a    hp2566b      hp3630a    quietjet
PCL4          hp2225d    hp2567b      hp7440a    rmodel
PRINT3K.model hp2227a    hp2631g      hp7475a    rmttroff
bf_remote     hp2228a    hp2684a      hp7550a    ruggedwriter
colorpro      hp2235a    hp2686a      hp7570a    thinkjet
deskjet       hp2276a    hp2686a.pif  hp7595a
```

If you have an HP printer, you will probably find a model script that matches its model number or name. Those interface model scripts that match your printers typically do not need to be changed. If you know how to do shell programming, you can customize printer interface model scripts to meet your specific printing needs (see *Shells: User's Guide* for information on shell programming).

Caution The `update` program described in the *Installing and Updating HP-UX* manual can replace or remove model scripts in the process of updating your system. If you create your own printer interface scripts, keep the file names unique and keep a backup copy somewhere on the system.

If you *do not* have an HP printer, try using the `dumb` interface model. You might have to modify it to be able to use all of the features of your non-HP printer, but "dumb" should work for basic ASCII text printing. If the `dumb` printer interface model script does not work, contact your printer supplier for a UNIX$_{TM}$ line printer spooler interface script or try the script that most closely matches your non-HP printer type.

Device Files

Device files are *not* part of the lp spooler; they are special files that define the necessary device driver and hardware address needed to communicate with a particular physical device (in this case a printer). The printer name referred to by the lp spooler and the name of the device file for a printer are not required to be the same, but a correspondence is recommended.

You can create printer device files using SAM or HP-UX commands when you add a printer to the lp spooler. SAM creates a device file for you. If necessary, SAM can override the default device file naming convention. For information and specific instruction about how to make device files for your printers, see *How HP-UX Works: Concepts for the System Administrator*, HP part number B2355-90029 manual, Chapter 12, "HP-UX Peripherals" or the *Installing Peripherals* manual.

When you configure a printer into your lp spooler, you must supply the name of your printer's device file.

Note In an HP-UX cluster, device files are context-dependent files (CDFs). When adding or removing a printer or plotter from your system, ensure that you are logged on to the computer to which the printer or plotter is physically attached.

Line Printer Scheduler

The line printer scheduler is the heart of the lp spooler. It is the part of the lp spooler that prevents intermixed listings (output from more than one print request mixed together on a printed page) and controls flow of print requests to the printers. Its duties also include monitoring printer and print request priorities, monitoring/adjusting printer status, and logging lp spooler activities. The `lpsched` command starts the LP spooler. Because of the central role it plays, starting `lpsched` is referred to as "starting the LP spooler", and stopping `lpsched` is often referred to as "stopping the LP spooler." You can use the `lpsched` command directly or through SAM (see "Starting and Stopping the LP Spooler Using HP-UX Commands" and "Starting and Stopping the LP Spooler Using SAM").

LP Spooler Overview

Local Printer

A **local printer** is a printer that is physically connected to your system. In an HP-UX cluster, a printer connected to any member of the cluster is considered to be a local printer.

Remote Printer

A **remote printer** is a printer that is not physically connected to your system, but can be accessed by your system through a local area network (LAN). To configure a remote printer into your local lp spooler, you must be able to access the remote system via a LAN. The process of adding a remote printer is similar to that of adding a local printer, though you will need to supply some slightly different information. See "Adding a Remote Printer Using SAM" and "Adding a Remote Printer Using HP-UX Commands".

Network-Based Printer/Plotter

A network-based printer or plotter is connected directly to the local area network (LAN). A network-based printer or plotter is *not* physically connected to any system. This chapter provides instructions for setting up a network-based printer by means of SAM (see "Adding a Network-Based Printer Using SAM"). If you do not prefer to use SAM, consult the instructions shipped with the printer or printer interface card product.

Print Request Identification Number

When you submit a print request by means of the `lp` command, `lp` responds with a **print request identification number** consisting of the name of the printer (or printer class) followed by a number. Here are some examples of typical print request identification numbers:

```
laser-3456
phred-2152
letterhead-1547
```

Remote Spooling

If you have several systems connected to a Local Area Network (LAN) and would like the systems to share the use of a printer, you can set up the lp spoolers of the systems that are not physically connected to the printer to automatically send their print requests (via the LAN) to the lp spooler of the system that does have the printer. The systems without printers act as though they were *a user* on the system with the printer, submitting print requests to that system's lp spooler. This is accomplished by a special program known as the **Remote Spooling Daemon** (`rlpdaemon`).

The `rlpdaemon` program runs in the background (on the system with the printer) monitoring the incoming LAN traffic for any remote print requests from other systems. When these requests arrive, the `rlpdaemon` program submits them to its local lp spooler on behalf of the remote user. In addition to remote print requests, the remote spooling daemon must also handle "cancel" and "status" requests from remote systems.

There are special "interface scripts" on the remote systems that issue cancel and status requests. These special interface scripts have a lot in common with printer interface scripts. They have a model directory that can hold sample versions of these scripts, and they have an interface directory where the scripts currently in use reside. The cancel and status models are copied into their respective interface directories automatically when adding a remote printer.

Note If your system and the system with the printer are members of the same HP-UX cluster, the printer is considered to be a *local printer* even though it is not physically connected to your computer. See *Managing Clusters of HP 9000 Computers*, HP part number B1864-90015.

LP Spooler Overview

The directory /usr/spool/lp/cmodel contains a sample interface script, rcmodel, that sends a remote cancel command to the system with the printer. When you configure a remote printer into your lp spooler, the **cancel model script** is copied into the /usr/spool/lp/cinterface directory and is given the same name as the printer.

The directory /usr/spool/lp/smodel contains a sample of an interface script, called rsmodel, which sends a remote status command to the system with the printer. When you configure a remote printer into your lp spooler, the **status model script** is copied into the /usr/spool/lp/sinterface directory and is given the same name as the printer.

It is unlikely that you will need to customize the remote cancel and status model scripts. If you do customize these "remote control" scripts, you must copy them to a different file name to avoid destroying your changes when updating the system with the update utility.

Configuring a remote printer into your lp spooler requires additional information beyond what is needed to configure a local printer. In addition to the information you normally supply when configuring a local printer into your lp spooler, you will need to tell your system:

- The name of the system with the printer
- The interface script to use when it issues a remote cancel request
- The interface script to use when it issues a remote status request
- The name of the printer (as it is defined in the lp spooler of the *remote system*) where you want your printouts to be printed.

See "Adding a Remote Printer Using SAM" and "Adding a Remote Printer Using HP-UX Commands".

Priorities of Printers and Print Requests

To control the order of printed requests, you can assign priority values to printers and to specific print requests. Assigning priorities is *NOT* required.

- Priority values must be in the range of 0 to 7.
- Priority 7 is the highest priority.
- A value assigned to each printer, known as a **printer fence priority**, determines the minimum priority that a print request must have in order to be able to print. A print request having a priority equal to or greater than the fence priority of its printer will print. HP-UX assigns a printer fence priority value of zero (0) when you add a printer to the lp spooler. You can change printer fence priorities dynamically with SAM or the `lpfence` command. See "Changing A Printer Fence Priority Using SAM" or "Setting a Printer Priority Fence Using HP-UX Commands".
- A value assigned to each print request, known as a **print request priority**, is associated with the destination printer. The print request priority for each printer can be determined when each printer is added to the line printer spooling system. If the printer print request priority is changed after a print request has been put in the print queue, the print request's priority does not change.
- Print request priorities *lower* than the printer priority will not print. If a print request's priority is lower than its printer's priority, it will remain in the request directory ("printer queue") for that printer. It will remain there until its priority is raised or its printer's priority is lowered to allow it to print (or until the request is canceled).
- You cannot directly set a printer class priority. See "Printer Classes" for an example of a printer class. The class priority is the same as the highest priority of any printer in the class.
- If multiple print requests are waiting to be printed on a specific printer and all have priorities high enough to print:
  - The lp spooler will print next the print request with the highest priority.
  - If more than one print request has the highest priority, all print requests with that priority will print in the order they were received by the lp spooler.

Using Plotters with the LP Spooler

Because the lp spooler is nothing more than a data routing mechanism, it can be used with other output devices. Apart from printers, the devices most commonly used with the lp spooler are plotters. The following model scripts are supplied so that you can use your lp spooler with Hewlett Packard plotters:

Table 9-1. LP Spooler Models for Plotters

Script Name	Plotters it can be used with
HPGL1:	HP7440A, HP7475A
HPGL2:	HP7550A, HP7595A, HP7596A, HP7570A
colorpro:	HP7440A, HP7475A
draftpro:	HP7550A, HP7595A, HP7596A, HP7570A
dumbplot:	miscellaneous
hp7440a:	HP7440A, HP7475A
hp7475a:	HP7440A, HP7475A
hp7550a:	HP7550A, HP7595A, HP7596A, HP7570A
hp7570a:	HP7550A, HP7595A, HP7596A, HP7570A
hp7595a:	HP7550A, HP7595A, HP7596A, HP7570A
hp7596a:	HP7550A, HP7595A, HP7596A, HP7570A

Controlling Data Flow Through the LP Spooler

There are three points in the lp spooler where you can control the flow of data:

1. You can start or stop the LP spooler. This has a global effect. If you stop the LP spooler, printing for *all printers* stops.
2. You can tell the lp spooler to accept or reject any new print requests for a printer. If you instruct the lp spooler to reject print requests for a printer class, users will be given a message telling them that the printer class that they requested is not accepting requests when they attempt to print something to that destination. Rejecting print requests should be used when a printer or a class of printers is being taken off the system for a extended period of time. Rejecting print requests is not recommended for making the printer unavailable for a short time. For example, rejecting print requests is not recommended for adding paper or changing the toner cartridge. A minor delay due to these short term services is usually acceptable.
3. You can tell the lp spooler to enable or disable a printer for printing. Print requests continue to be accepted for the disabled printer unless you have explicitly rejected print requests. Disable a printer should to make the printer temporarily unavailable for a short time, for example, disabling the printer to add paper or change toner. Do not disable a printer for a long time without also rejecting requests for that printer; otherwise users' print requests will keep accumulating in the print queue and they will not get any notice that their requests will not print. Once you reject print requests for a printer, a user submitting a print request to that printer will get a message stating that the printer is not accepting requests.

   To print, a printer must be accepting and enabled.

Note When you use SAM to "enable" or "disable" a printer, SAM performs *both* the accept/reject operation *and* the enable/disable operation listed above. If you wish to "disable" a printer but still accept requests for that printer (letting them accumulate in the request directory for the printer), you must use the HP-UX commands method.

Logging and Analyzing Printer Activity

Analyzing printer activity can help you determine if there are bottlenecks in your lp spooler. It can also help you determine/justify the need to add additional printers to your lp spooler. There are facilities to help you analyze the flow of data through your lp spooler.

There are two phases to analyzing lp spooler activity: a *data collection* phase and a *data reporting* phase. The data collection phase begins when the lp spooler starts. The `-a` option to the `lpsched` command turns on the data collection processes when you start the LP spooler (see "Starting and Stopping the LP Spooler Using HP-UX Commands"). The data reporting phase can occur any time after the lp spooler has been started. The following statistics are calculated:

- average waiting time from when a print request is submitted to the start of printing
- standard deviation for waiting time
- average printing time from start to end of print request
- standard deviation of printing time
- average number of bytes (characters) printed per request
- standard deviation for number of bytes
- sum of bytes printed for all requests in Kbytes
- total number of requests since logging started

See "Displaying Statistics about Printer Activity Using HP-UX Commands".

Initial LP Spooler Set Up

Initial LP spooler setup consists of the following tasks:

1. Add at least one printer to the lp spooler.
2. Tell the lp spooler to accept print requests for this printer.
3. Tell the lp spooler to enable the printer for printing.
4. Turn on the LP spooler.

When you use SAM to add a printer, SAM:

- tells the lp spooler to accept print requests for the printer.
- enables the printer.
- starts the lp spooler.

If you are not using SAM, you must do these tasks yourself; refer to "Setting Up the LP Spooler Using HP-UX Commands".

Line Printer Spooler Tasks

The two methods of controlling the lp spooler are:

1. The System Administration Manager (SAM)
2. HP-UX commands

SAM allows you to control the lp spooler through its menu-selection and data-entry screens. By combining multiple "manual commands" into single tasks, SAM can save you time and keystrokes. SAM also eliminates the need to know command names and options for the lp spooler.

Although HP-UX commands require you to learn more details than SAM does, you might need or prefer to use HP-UX commands, for the following reasons:

- HP-UX commands give you a greater degree of control over the lp spooler.
- SAM might not be configured into your system. You *have* to use HP-UX commands to control the lp spooler.
- You might be more comfortable using HP-UX commands.
- You may need to use the data collection facility. If you want to start data collection, you must use the `lpsched -a` command, not SAM, to start the lp spooler. See "Starting and Stopping the LP Spooler Using HP-UX Commands".

See Chapter 1, "Introduction to System Administration" for additional information about using SAM.

Viewing Printers and Print Request Status Using SAM

To view printers:

1. Run SAM; type:

   `/usr/bin/sam`

   See Chapter 1, "Introduction to System Administration" for additional information about using SAM.
2. Highlight `Printers and Plotters` and activate the (Open) control button.
3. Highlight `Printers/Plotters` and activate the (Open) control button.

To view print requests:

1. Run SAM; type:

   `/usr/bin/sam`

   See Chapter 1, "Introduction to System Administration" for additional information about using SAM.
2. Highlight `Printers and Plotters` and activate the (Open) control button.
3. Highlight `Print Requests` and activate the (Open) control button.

You can also view print requests by choosing `Print Requests` from the "List" menu within the "Printer/Plotter Manager" Window.

Additional Task Information

SAM provides an on line help system to assist you when you need additional information.

Activating the (Help) button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

From within a functional area, choosing an item from the "Help" menu gives you information about:

- the current functional area
- keyboard navigation within SAM
- using the SAM help system
- displaying the version of SAM you are currently running

From a dialog box (a window displaying fields to be filled in), pressing the (f1) key gives you context-sensitive information for the object at the location of the cursor.

Note The print request queue can change rapidly. To ensure that you are viewing the current data, choose `Refresh List` from the "Options" menu to view the current state of the print request queue.

The "Printer/Plotter Manager" object list displays the following information about the printers in the lp spooler:

- system default printer
- status of LP spooler (RUNNING or STOPPED)
- the printer name
- printer status (`enabled`, `disabled`, `idle`, `busy`)
- priority for each printer and printer class
- the printer type (`local`, `remote`, or `network`)
- the location of each printer (the device file for local printers; printer name and system for remote printers; no entry for network-based printers)

Adding a Local Printer Using SAM

To add a local printer:

1. Physically connect the printer(s) to your system. Refer to the instructions shipped with your printer. You should always shut down your system and turn off the power when you are changing hardware configuration of your system. For additional configuration information refer to the *Installing Peripherals* manual.
2. Gather the following information:
   - The name you are giving to this printer or plotter. Printer names can be up to 14 characters in length, and the characters must be alphanumeric (A-Z, a-z, 0-9) or an underscore (_).
   - The name of the device file that the printer or plotter will use. SAM creates the device file for you. SAM uses the default device file named `lp_`*printer-name*. You can override the default device file name by specifying your device file name when filling in the printer information.
   - The model script from the `/usr/spool/lp/model` directory, for example, `laserjetIIISi` for an HP LaserJet IIISi.
   - The print request priority for this printer. The default is zero (0).
   - The class to which the printer or plotter will be added (optional). Printer class names can be up to 14 characters in length, and the characters must be from the set (A-Z, a-z, 0-9). The underscore (_) character is allowed in printer class names.

   In addition, decide whether or not to make this device your system's default printer.

3. Run SAM; type:

   `/usr/bin/sam`

   See Chapter 1, "Introduction to System Administration" for additional information about using SAM.

Note

- In an HP-UX cluster, run SAM from the machine to which the printer is physically attached, client or server. See *Managing Clusters of HP 9000 Computers*, HP part number B1864-90015 for additional cluster information.
- During the process of adding and removing printers, SAM stops the lp spooler. Print requests being printed at the time the lp spooler stopped might not complete successfully. It is best to add a printer when there are no requests currently printing.

---

4. Highlight `Peripheral Devices` and activate the (Open) control button.
5. Highlight `Printers and Plotters` and activate the (Open) control button.
6. Highlight `Printers/Plotters` and activate the (Open) control button.
7. Choose `Add a Local Printer/Plotter >` and the menu item associated with the printer interface type from the "Actions" menu.

Note

The printer printer driver must be part of the kernel to add the printer to the lp spooler. If the printer driver is not currently configured into the kernel, SAM prompts you to add the driver(s) and reboot the system.

If you are creating a new kernel for a cluster client, SAM does not create a backup copy of your kernel. If you tell SAM to "Move the Kernel into Place", SAM generates a new kernel and overwrites `/hp-ux`. *Do not do this*; instead:

a. Exit SAM without moving the new kernel into place.

b. Create a backup of your current kernel (copy it to some name other than `/SYSBCKUP`).

c. Move the new kernel (`/etc/conf/hp-ux`) to `/hp-ux`.

d. Reboot your system

e. Re-enter SAM to continue adding the printer to your system.

You should be aware of the effects on other users before rebooting your system. Note especially the following situations:

- If anyone else is logged into your system, rebooting will interrupt their work.
- If your system is a cluster server, or a swap server for other clients in a cluster, rebooting your system brings down the associated clients. See Chapter 10, "Booting and Shutting Down Clusters and Cluster Nodes" in *Managing Clusters of HP 9000 Computers* for details.
- If your system is a file server in a cluster, rebooting it makes any mounted file systems unavailable to clients until the system is running again. See Chapter 10, "Booting and Shutting Down Clusters and Cluster Nodes" in *Managing Clusters of HP 9000 Computers*.
- If your system is an Internet Protocol router, rebooting it affects any IP traffic routed through your system.

8. Highlight the interface to which you connected the printer and fill in and additional information (port number or bus address) and activate the (OK) control button.

   If an interface entry is not listed, activate the (Diagnose Missing Card) control button.

9. Fill in the printer interface dialog box fields, choose from the menu button values, and turn on and off check box values.

   Activating the (Help) button from a dialog or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

   Pressing the (f1) key gives you context-sensitive information for the object field at the location of the cursor.

10. Activate the (OK) control button.

Additional Task Information

SAM provides an on line help system to assist you when you need additional information.

Activating the (Help) button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

From within a functional area, choosing an item from the "Help" menu gives you information about:

- the current functional area
- keyboard navigation within SAM
- using the SAM help system
- displaying the version of SAM you are currently running

From a dialog box (a window displaying fields to be filled in), pressing the (f1) key gives you context-sensitive information for the object at the location of the cursor.

In an HP-UX cluster, a printer connected to any node in the cluster is considered to be a local printer.

The printer driver names, major number, and interface types are as follows:

Table 9-2. Series 300/400 Printer Drivers

Printer Driver Name	Major Number	Printer Driver Description
`hpib`	21	HP-IB (AMIGO and raw protocol) driver
`ciper`	26	HP-IB CIPER protocol driver
`printer`	7	HP-IB raw protocol driver
`parallel`	21	Parallel driver (requires the `hpib` driver)
`pci`	1	Serial driver for the Series 300 built in RS-232 port
`apci`	1	Serial driver for the Series 400 built in RS-232 port
`98626`	1	Serial driver for the built in RS-232 port and the HP 98626 interface
`98628`	1	Serial driver for the HP 98628 datacomm interface
`98642`	1	Serial driver for the HP 98642 4-channel multiplexer and the HP 98638 8-channel multiplexer interfaces

Refer to the *Managing Clusters of HP 9000 Computers* manual and the Chapter 2, "Constructing an HP-UX System" chapter of this manual for details on configuring the kernel using SAM.

Adding a Remote Printer Using SAM

1. Ensure that the remote system has the printer installed and configured into the remote system's line printer spooler system.
2. If you are adding a remote printer to an HP-UX cluster, ensure you are logged onto the cluster server.
3. Gather the following information:
   - The name you are giving to this printer or plotter. See "Printer Names".
   - Whether or not you wish to make this device your system's default printer. See "System Default Printer (Destination)".
   - The name of the remote system to which the printer or plotter is attached.
   - The name of the remote printer or plotter.
   - The "cancel" model on the remote system (optional). See "Remote Spooling".
   - The "status" model on the remote system (optional). See "Remote Spooling".
   - Whether or not you wish to allow any user to cancel any printing request.
   - Whether or not the remote printer is on a system using BSD (Berkeley Software Distribution) UNIX. Using BSD disables any `lp -o`*parm* options. BSD systems do not understand the `-o` option.

4. Run SAM; type:

   `/usr/bin/sam`

   See Chapter 1, "Introduction to System Administration" for additional information about using SAM.

Note During the process of adding and removing printers, SAM stops the lp spooler Print requests being printed at the time the lp spooler stopped might not complete successfully. It is best to add a printer when there are no requests currently printing.

---

5. Highlight `Peripheral Devices` and activate the (Open) control button.
6. Highlight `Printers and Plotters` and activate the (Open) control button.
7. Highlight `Printers/Plotters` and activate the (Open) control button.
8. Choose `Add a remote printer/plotter >` and the menu item associated with the printer interface type from the "Actions" menu.
9. Fill in the printer interface dialog box fields and turn on off check box values.

   Activating the (Help) button from a dialog or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

   Pressing the (f1) key gives you context-sensitive information for the object field at the location of the cursor.
10. Activate the (OK) control button.

Additional Task Information

SAM provides an on line help system to assist you when you need additional information.

Activating the (Help) button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

From within a functional area, choosing an item from the "Help" menu gives you information about:

- the current functional area
- keyboard navigation within SAM
- using the SAM help system
- displaying the version of SAM you are currently running

From a dialog box (a window displaying fields to be filled in), pressing the (f1) key gives you context-sensitive information for the object at the location of the cursor.

To configure a remote printer into your lp spooler, you must be able to access the system with the printer via a local area network (LAN). The process of adding a remote printer is similar to that of adding a local printer, though you will need to supply SAM with some slightly different information.

Remote printers cannot be members of a printer class.

Adding a Network-Based Printer Using SAM

To add a network-based printer or plotter using SAM:

1. Ensure that the printer is connected to the network according to the installation instructions shipped with the network-based printer or the network interface card for the printer.
2. Gather the following information:
   - The name you are giving to this printer or plotter. See "Printer Names".
   - The printer node name.
   - The model or interface that the printer will use. See "Printer Models".
   - The link-level address of the network card installed in the printer.
   - The TCP-IP protocol printer requires an Internet Protocol (IP) address.
   - The priority for this printer. See "Priorities of Printers and Print Requests".
   - The class to which the printer or plotter will be added (optional). See "Printer Classes".

   In addition, decide whether or not you wish to make this device your system's default printer. See "System Default Printer (Destination)".
3. Run SAM; type:

   ```
   /usr/bin/sam
   ```

   See Chapter 1, "Introduction to System Administration" for additional information about using SAM.
4. Highlight `Peripheral Devices` and activate the (Open) control button.
5. Highlight `Printers and Plotters` and activate the (Open) control button.
6. Highlight `Printers/Plotters` and activate the (Open) control button.
7. Choose `Add a network-based printer` then `Add TCP-IP protocol printer...` from the "Actions" menu.

9

8. Fill in the printer interface dialog box fields and turn on and off check box values.

   Activating the (Help) button from a dialog or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

   Pressing the (f1) key gives you context-sensitive information for the object field at the location of the cursor.

9. Activate the (OK) control button.

Additional Task Information

SAM provides an on line help system to assist you when you need additional information.

Activating the (Help) button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

From within a functional area, choosing an item from the "Help" menu gives you information about:

- the current functional area
- keyboard navigation within SAM
- using the SAM help system
- displaying the version of SAM you are currently running

From a dialog box (a window displaying fields to be filled in), pressing the (f1) key gives you context-sensitive information for the object at the location of the cursor.

The software SAM needs to configure your network-based printer is shipped separately. Follow the instruction shipped with your printer to load the software.

In an HP-UX cluster, you can run SAM from a cluster client or the cluster server to add a network-based printer, in either case the printer will be available to all computers in the cluster.

Removing a Printer Using SAM

1. Run SAM; type:

    `/usr/bin/sam`

    See Chapter 1, "Introduction to System Administration" for additional information about using SAM.
2. Highlight `Peripheral Devices` and activate the (Open) control button.
3. Highlight `Printers and Plotters` and activate the (Open) control button.
4. Highlight `Printers/Plotters` and activate the (Open) control button.
5. Highlight the printer you want to remove in the object list.
6. Choose `Remove a printer/plotter >` from the "Actions" menu.

Additional Task Information

SAM provides an on line help system to assist you when you need additional information.

Activating the (Help) button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

From within a functional area, choosing an item from the "Help" menu gives you information about:

- the current functional area
- keyboard navigation within SAM
- using the SAM help system
- displaying the version of SAM you are currently running

From a dialog box (a window displaying fields to be filled in), pressing the (f1) key gives you context-sensitive information for the object at the location of the cursor.

Removing a Printer Using SAM

If you are in an HP-UX cluster, you can remove a printer with SAM while logged into the cluster client or server.

Note

- During the process of adding and removing printers, SAM stops the lp spooler. Print requests being printed at the time the lp spooler is stopped might not complete successfully. It is best to stop the lp spooler when there are no requests currently printing.
- SAM cancels all print requests in the request directory for the printer you are removing.

SAM does not remove the device file for the printer removed from the lp spooler.

Starting and Stopping the LP Spooler Using SAM

To *start* the LP spooler:

1. Run SAM; type:

   `/usr/bin/sam`

   See Chapter 1, "Introduction to System Administration" for additional information about using SAM.
2. Highlight `Peripheral Devices` and activate the (Open) control button.
3. Highlight `Printers and Plotters` and activate the (Open) control button.
4. Highlight `Printers/Plotters` and activate the (Open) control button.
5. Choose `Start up printer spooler` from the "Actions" menu.

To *stop* the LP spooler:

1. Run SAM; type:

   `/usr/bin/sam`

   See Chapter 1, "Introduction to System Administration" for additional information about using SAM.
2. Highlight `Peripheral Devices` and activate the (Open) control button.
3. Highlight `Printers and Plotters` and activate the (Open) control button.
4. Highlight `Printers/Plotters` and activate the (Open) control button.
5. Choose `Shut down printer spooler` from the "Actions" menu.

Additional Task Information

SAM provides an on line help system to assist you when you need additional information.

Activating the (Help) button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

From within a functional area, choosing an item from the "Help" menu gives you information about:

- the current functional area
- keyboard navigation within SAM
- using the SAM help system
- displaying the version of SAM you are currently running

From a dialog box (a window displaying fields to be filled in), pressing the (f1) key gives you context-sensitive information for the object at the location of the cursor.

If you are in an HP-UX cluster, you can start and stop the lp spooler with SAM while logged into the cluster client or server.

Note

- Printing on all printers stops.
- When SAM stops the lp spooler there is no guarantee that print requests being printed at the time will complete successfully. It is best to stop the lp spooler when there are no requests currently printing.

To turn on the data collection processes, refer to "Starting and Stopping the LP Spooler Using HP-UX Commands".

Determining the Status of the LP Spooler Using SAM

To determine the status of the lp spooler:

1. Run SAM; type:

   `/usr/bin/sam`

   See Chapter 1, "Introduction to System Administration" for additional information about using SAM.
2. Highlight `Peripheral Devices` and activate the (Open) control button.
3. Highlight `Printers and Plotters` and activate the (Open) control button.
4. Highlight `Printers/Plotters` and activate the (Open) control button.

The status area of the object list will display the status of the scheduler as "`Scheduler: RUNNING`" or "`Scheduler: STOPPED`".

Additional Task Information

SAM provides an on line help system to assist you when you need additional information.

Activating the (Help) button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

From within a functional area, choosing an item from the "Help" menu gives you information about:

- the current functional area
- keyboard navigation within SAM
- using the SAM help system
- displaying the version of SAM you are currently running

From a dialog box (a window displaying fields to be filled in), pressing the (f1) key gives you context-sensitive information for the object at the location of the cursor.

Disabling a Printer Using SAM

1. Run SAM; type:

   /usr/bin/sam

   See Chapter 1, "Introduction to System Administration" for additional information about using SAM.
2. Highlight `Peripheral Devices` and activate the (Open) control button.
3. Highlight `Printers and Plotters` and activate the (Open) control button.
4. Highlight `Printers/Plotters` and activate the (Open) control button.
5. Highlight the printer you want to disable in the object list.
6. Choose `Disable printer` from the "Actions" menu.

Additional Task Information

SAM provides an on line help system to assist you when you need additional information.

Activating the (Help) button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

From within a functional area, choosing an item from the "Help" menu gives you information about:

- the current functional area
- keyboard navigation within SAM
- using the SAM help system
- displaying the version of SAM you are currently running

From a dialog box (a window displaying fields to be filled in), pressing the (f1) key gives you context-sensitive information for the object at the location of the cursor.

- It is best to disable printer when there are no requests currently printing.
- If you are in an HP-UX cluster, you can disable a printer with SAM while logged into the cluster client or server.

Note When you use SAM to "enable" or "disable" a printer, SAM performs *both* the accept/reject operation *and* the enable/disable operation. If you wish to "disable" a printer but still accept requests for that printer (letting them accumulate in the request directory for the printer), you must use the HP-UX commands method to disable the printer (see "Enabling or Disabling a Printer Using HP-UX Commands").

Enabling a Printer Using SAM

To enable a printer using SAM:

1. Run SAM; type:

   /usr/bin/sam

   See Chapter 1, "Introduction to System Administration" for additional information about using SAM.
2. Highlight `Peripheral Devices` and activate the (Open) control button.
3. Highlight `Printers and Plotters` and activate the (Open) control button.
4. Highlight `Printers/Plotters` and activate the (Open) control button.
5. Highlight the printer you want to enable in the object list.
6. Choose `Enable printer` from the "Actions" menu.

Additional Task Information

SAM provides an on line help system to assist you when you need additional information.

Activating the (Help) button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

From within a functional area, choosing an item from the "Help" menu gives you information about:

- the current functional area
- keyboard navigation within SAM
- using the SAM help system
- displaying the version of SAM you are currently running

9

From a dialog box (a window displaying fields to be filled in), pressing the (f1) key gives you context-sensitive information for the object at the location of the cursor.

If you are in an HP-UX cluster, you can enable a printer with SAM while logged into the cluster client or server.

Note When you use SAM to "enable" or "disable" a printer, SAM performs *both* the accept/reject operation *and* the enable/disable operation. If you wish to "disable" a printer but still accept requests for that printer (letting them accumulate in the request directory for the printer), you must use the HP-UX commands method to disable the printer (see "Enabling or Disabling a Printer Using HP-UX Commands").

Changing A Printer Fence Priority Using SAM

To change a printer priority using SAM:

1. Run SAM; type:

   <u>`/usr/bin/sam`</u>

   See Chapter 1, "Introduction to System Administration" for additional information about using SAM.
2. Highlight `Peripheral Devices` and activate the (Open) control button.
3. Highlight `Printers and Plotters` and activate the (Open) control button.
4. Highlight `Printers/Plotters` and activate the (Open) control button.
5. Highlight the printer for which you want to change the priority.
6. Choose `Modify fence priority` from the "Actions" menu.
7. Choose the new priority value from the **`Printer priority`** menu button.
8. Activate the (OK) control button.

Additional Task Information

SAM provides an on line help system to assist you when you need additional information.

Activating the (Help) button from the SAM main window, a dialog box, or message box gives you information about the attributes and tasks you can perform from the currently displayed window.

From within a functional area, choosing an item from the "Help" menu gives you information about:

- the current functional area
- keyboard navigation within SAM
- using the SAM help system
- displaying the version of SAM you are currently running

From a dialog box (a window displaying fields to be filled in), pressing the (f1) key gives you context-sensitive information for the object at the location of the cursor.

See "Priorities of Printers and Print Requests" for additional information.

Setting Up the LP Spooler Using HP-UX Commands

1. Add at least one printer to the lp spooler (see "Adding a Local Printer Using HP-UX Commands" or "Adding a Remote Printer Using HP-UX Commands").
2. Tell the lp spooler to accept print requests for this printer (see "Accepting and Rejecting Print Requests for a Printer Using HP-UX Commands").
3. Tell the lp spooler to enable the printer for printing (see "Enabling or Disabling a Printer Using HP-UX Commands").
4. Start the LP spooler (see "Starting and Stopping the LP Spooler Using HP-UX Commands").

Ensuring the Printer Driver is in the Kernel Using HP-UX Commands

In the following instructions, the term "standalone machine" refers to a machine that is *not* part of an HP-UX cluster. Instructions differ when reconfiguring a standalone machine, cluster server, or cluster client kernel.

Reconfiguring the kernel requires that you reboot your system. Note the following impact on other users *before* you shut down and reboot your system:

- If others are logged into your system, rebooting it interrupts their work. If you have a small number of users or cluster clients on your system, it is best to notify your users in person of the impending system shutdown. It is possible that users can be using an application and not be aware of the message sent by the `shutdown` command.
- If your system is a cluster server, or a swap server for other clients in a cluster, rebooting your system brings down the associated clients. See the Chapter 10, "Booting and Shutting Down Clusters and Cluster Nodes" chapter of *Managing Clusters of HP 9000 Computers* for details.
- If your system is a file server in a cluster, rebooting it makes any file systems mounted to the file server unavailable to clients until the system is running again. See the Chapter 10, "Booting and Shutting Down Clusters and Cluster Nodes" chapter of *Managing Clusters of HP 9000 Computers* for details.
- If your system is an Internet Protocol router, rebooting it affects any IP traffic routed through your system.

Ensuring the Printer Driver is in the Kernel Using HP-UX Commands

To ensure the printer driver is part of the kernel using HP-UX commands:

1. Ensure that you have superuser capabilities.
2. In an HP-UX cluster, ensure you are logged onto the machine for which a new kernel is being generated. You can log in at the cluster node console or remotely log in to the cluster node from another location by using the `rlogin` command. See *Managing Clusters of HP 9000 Computers* for additional cluster information.
3. Change your directory to `/etc/conf`:

   ```
   cd /etc/conf
   ```

Caution You *must* get out of the root directory if you will be creating a new kernel. Otherwise you will overwrite the current kernel.

Ensuring the Printer Driver is in the Kernel Using HP-UX Commands

4. Look at the entries in the kernel configuration description file to determine if the printer driver is part of your current kernel configuration. The `dfile` is the configuration description file that generally reflects your system.

   If the printer driver *is* part of the current kernel configuration, exit this task module; otherwise, complete the steps detailed in the Chapter 2, "Constructing an HP-UX System" to add the printer driver to the kernel. During this process you will need to refer to Table 9-3.

   The printer driver names are described in Table 9-3.

Table 9-3. Series 300/400 Printer Drivers

Printer Driver Name	Printer Driver Description
`hpib`	HP-IB (AMIGO and raw protocol) driver
`ciper`	HP-IB CIPER protocol driver
`printer`	HP-IB raw protocol driver
`parallel`	Parallel driver (requires the `hpib` driver)
`pci`	Serial driver for the Series 300 built in RS-232 port
`apci`	Serial driver for the Series 400 built in RS-232 port
`98626`	Serial driver for the built in RS-232 port and the HP 98626 interface
`98628`	Serial driver for the HP 98628 datacomm interface
`98642`	Serial driver for the HP 98642 4-channel multiplexer and the HP 98638 8-channel multiplexer interfaces

Determining if a Device File Exists for your Printer Using HP-UX Commands

1. Use the *Installing Peripherals* manual to help you determine what the minor numbers for your printer should be (based on the printer's interface and hardware address). The printer driver names, major number, and interface types are as follows:

Table 9-4. Series 300/400 Printer Drivers

Printer Driver Name	Major Number	Printer Driver Description
`hpib`	21	HP-IB (AMIGO and raw protocol) driver
`ciper`	26	HP-IB CIPER protocol driver
`printer`	7	HP-IB raw protocol driver
`parallel`	21	Parallel driver (requires the `hpib` driver)
`pci`	1	Serial driver for the Series 300 built in RS-232 port
`apci`	1	Serial driver for the Series 400 built in RS-232 port
`98626`	1	Serial driver for the built in RS-232 port and the HP 98626 interface
`98628`	1	Serial driver for the HP 98628 datacomm interface
`98642`	1	Serial driver for the HP 98642 4-channel multiplexer and the HP 98638 8-channel multiplexer interfaces

2. Use the `ll` command to list the directory `/dev`. Look through the entries for one that matches the major *and* minor numbers. The fifth column of information (immediately to the right of the group ownership) represents the major number for the corresponding device file. The sixth column (immediately to the left of the date) represents the minor number for the device file.

3. If you find one that matches, note its device file name (last column of information in the `ll` listing) for use with the HP-UX commands to add a printer to your spooling system (later in this chapter).

   If you do *not* find one with major *and* minor numbers that match, you will need to create a device file for your printer. See the *Installing Peripherals* for the procedure on how to do this.

Additional Task Information

A device file is the mechanism that HP-UX uses to determine which of the devices attached to your computer it should use for an I/O operation. The major number of the device file tells HP-UX which drivers to use; the minor number tell HP-UX the hardware address of the device. Device files are usually located in the `/dev` directory.

Note In an HP-UX cluster, device files are context-dependent files (CDFs). When adding or removing a printer or plotter from your system, ensure that you are logged on to the computer to which the printer or plotter is physically attached.

Adding a Local Printer Using HP-UX Commands

To add a local printer using HP-UX commands:

1. If you are adding a printer to an HP-UX cluster, ensure you are logged onto the machine to which the printer is physically attached. See *Managing Clusters of HP 9000 Computers*, HP part number B1864-90015 for additional cluster information.
2. Ensure that you have superuser capabilities.
3. Ensure the appropriate printer driver is in your kernel (see "Ensuring the Printer Driver is in the Kernel Using HP-UX Commands").
4. Ensure a device file exists for the printer (see "Determining if a Device File Exists for your Printer Using HP-UX Commands").
5. Stop the LP spooler with the `lpshut` command:

   ```
   /usr/lib/lpshut
   ```

Note When the lp spooler is stopped there is no guarantee that print requests currently printing will complete successfully. It is best to stop the lp spooler when there are no requests currently printing.

6. Add the printer to the lp spooler with the `lpadmin` command. There is an example later in this section. The command has the following syntax:

   `/usr/lib/lpadmin -p`*pname* `-v`*devfile* `-m`*model* [`-d`] [`-g`*priority*] [`-c`*class*] [`-a`*client*]

   where:

   pname is the name that you use to refer to this printer when using the various lp spooler commands (required). Printer names can be up to 14 characters in length, and the characters must either be alphanumeric (A-Z, a-z, 0-9) or an underscore (_).

   devfile is the name of the device file to be used to communicate with this printer (required).

model — is the script you would like to "model" your printer's interface script after. The `lpadmin` command will make a copy of this model script and place it in the directory `/usr/spool/lp/interface`, with the name you specified in the `-p` option described above (required).

`-d` — specifies that you want this printer to be the system default printer.

priority — The minimum priority a print request will need in order to print on this printer (optional). The default value is zero (0), which permits any print request to print on this printer. See "Priorities of Printers and Print Requests".

class — The name of the group of printers that this printer is a member (optional). Printer class names can be up to 14 characters in length, and the characters must either be alphanumeric (A-Z, a-z, 0-9) or an underscore (_).

client — Indicates that the printer specified with the `p` option is attached to the specified cluster client (optional). If this parameter is omitted in an HP-UX cluster, the `lpadmin` command assumes that the printer is attached to the cluster server.

When using the `lpadmin` command, *do not* put any spaces between the options and their respective values. For example:

TYPE THIS:

`-p`*invoices*

NOT THIS:

`-p` *invoices*

7. Allow print requests to enter the request directory for the newly added printer with the `accept` command:

   `/usr/lib/accept` *pname*

   where:

   pname is the name you gave to this printer in the `lpadmin` command.

   See "Accepting and Rejecting Print Requests for a Printer Using HP-UX Commands".

8. Enable the newly added printer to process print requests with the `enable` command:

   `/usr/bin/enable` *pname*

   where:

   pname is the name given to refer to this printer.

   See "Enabling or Disabling a Printer Using HP-UX Commands".

9. Start the line printer scheduler with the `lpsched` command:

   `/usr/lib/lpsched`

   See "Starting and Stopping the LP Spooler Using HP-UX Commands".

Additional Task Information

A **local printer** is a printer that is physically connected to your system. In an HP-UX cluster, a printer connected to any node in the cluster is considered to be a local printer.

Adding a printer to the lp spooler is not the same thing as adding a printer to your system. The first involves connecting the printer to your computer and configuring HP-UX to communicate with the printer. The second involves configuring the software subsystem (known as the LP spooler) that manages printer requests.

Because `lpadmin` is constructing and modifying files that are used by the line printer scheduler, it is important that the scheduler is stopped when you use the `lpadmin` command to add a new printer. Therefore, you should be sure that `lpsched` is stopped *before* using the `lpadmin` command.

Examples

To determine the status of the lp spooler:

```
/usr/bin/lpstat -r
scheduler is running
```

To stop the lp spooler:

```
/usr/lib/lpshut
```

To two add printers named `invoices` and `check_printer` to the lp spooler:

```
/usr/lib/lpadmin -pinvoices -v/dev/ivprint -mhp2934a
/usr/lib/lpadmin -pcheck_printer -v/dev/ckprint -mhp2564b -g7
```

To enable the print request directories to accept printer requests:

```
/usr/lib/accept invoices
/usr/lib/accept check_printer
/usr/lib/accept newclass
```

`accept` *applies to printer classes also*

To permit the printers to process print requests:

```
/usr/bin/enable invoices
/usr/bin/enable check_printer
```

To restart the lp spooler:

```
/usr/lib/lpsched
```

Adding a Remote Printer Using HP-UX Commands

To add a remote printer using HP-UX commands:

1. If you are adding a remote printer to an HP-UX cluster, ensure you are logged onto the cluster server.
2. Ensure that you have superuser capabilities.
3. Stop the LP spooler with the `lpshut` command:

   ```
   /usr/lib/lpshut
   ```

Note It is best to stop the LP spooler when there are no requests currently printing.

4. Add the printer to the lp spooler using the `lpadmin` command:

   `/usr/lib/lpadmin -p`*pname* `-v`*devfile* `-m`*model* `[-d]` `[-g`*priority*`]` `[-ocm`*cmodel*`]` `\`
   `[-osm`*smodel*`]` `[-orm`*remsys*`]` `[-orp`*rpname*`]` `[-ob3]` `[-orc]`

   where:

   pname This is the name that you will use to send print requests to this printer. Printer names can be up to 14 characters in length, and the characters must either be alphanumeric (A-Z, a-z, 0-9) or an underscore (_).

   devfile Since the printer is not physically connected to your local system, use the `/dev/null` device file.

   model The remote model script is the `/usr/spool/lp/model/rmodel`. A copy of this file will be put in the `/usr/spool/interface` directory with the name you specified in *pname*.

   `-d` specifies that you want this printer to be the system default printer.

   priority You only need to use this option if you want your printer to have a priority other than zero (optional). See "Changing the Priority of Print Requests Using HP-UX Commands".

cmodel
: The cancel model script `/usr/spool/lp/cmodel/rcmodel` is used to forward a "cancel" request over to the remote system's lp spooler. The lp spooler copies "/usr/spool/lp/cmodel/rcmodel" to the "/usr/spool/lp/cinterface" directory with the name you specified in *pname*. See "Remote Spooling".

smodel
: The status model script `/usr/spool/lp/smodel/rsmodel` is used to forward a "status" request over to the remote system's lp spooler. The lp spooler copies "/usr/spool/lp/smodel/rsmodel" to the "/usr/spool/lp/sinterface" directory with the name you specified in *pname*. See "Remote Spooling".

remsys
: The name of the remote system to which the printer is physically connected. You can get the remote system name by entering the command `hostname` (with no options) on the system with the printer. The name of the remote system must be available to the local system, either from a name server or in the `/etc/hosts` file on the local system (required).

rpname
: This is the printer name *as it is defined on the remote system.*

When using the `lpadmin` command, *do not* put any spaces between the options and their respective values. `lpadmin` will not interpret your input correctly if you do. For example:

TYPE THIS:

`-p`*invoices*

NOT THIS:

`-p` *invoices*

9

5. Allow print requests to enter the request directory for the newly added remote printer with the `accept` command:

   `/usr/lib/accept` *pname*

   where:

   pname is the local name given to this remote printer.

   See "Accepting and Rejecting Print Requests for a Printer Using HP-UX Commands".

6. Enable the newly added remote printer to process print requests with the `enable` command:

   `/usr/bin/enable` *pname*

   where:

   pname is the local name given to refer to this remote printer.

   See "Enabling or Disabling a Printer Using HP-UX Commands".

7. Start the line printer scheduler with the `lpsched` command:

   `/usr/lib/lpsched`

   See "Starting and Stopping the LP Spooler Using HP-UX Commands"

Additional Task Information

A **remote printer** is a printer that is not physically connected to your system, but can be accessed by your system through a local area network (LAN). To configure a remote printer into your local lp spooler, you must be able to access the remote system via a LAN. The process of adding a remote printer is similar to that of adding a local printer, though you will need to supply some slightly different information.

Remote printers cannot be members of a printer class.

Adding a printer to the lp spooler is not the same thing as adding a printer to your system. The first involves connecting the printer to your computer and configuring HP-UX to communicate with the printer. The second involves configuring the software subsystem (known as the Line Printer Spooling System) that manages printer output.

Because the `lpadmin` is constructing and modifying files that are used by the line printer scheduler, it is important that the scheduler is stopped when you use the `lpadmin` command to add a new printer.

You only need to use the `-ob3` option if your print request will be printed on or pass through a system that uses the Berkeley Software Distribution (BSD) style lp spooler. BSD systems use three-digit (rather than four-digit) print request-ID numbers (these are the numbers returned when you send something to print). The `-ob3` option disables any `lp -o`*parm* options. BSD systems do not understand the `-o` option to the `lp` command.

Use the `-orc` if you want to restrict users to cancelling only their own print requests.

Examples

To determine the lp spooler status:

```
/usr/bin/lpstat -r
scheduler is stopped
```

To add a remote printer, referred to locally as `letterhead`, physically connected to the system `hypo2` that uses the BSD style print request-ID numbers, and is known on the remote system as "*memos*":

```
/usr/lib/lpadmin -pletterhead -v/dev/null -mrmodel -ocmrcmodel \
   -osmrsmodel -ormhypo2 -ob3 -orpmemos
```

Note Because there are so many options to the commands, these examples use a backslash (\) to represent a line continuation. When you type these commands, you can enter the backslash as shown or you can omit the backslash and type the entire command before pressing (Return).

To add a remote printer, referred to locally as *remote_drafts*, physically connect to the system `system13`, known on the remote system as `old_reliable`, and requires a printer priority of 3:

```
/usr/lib/lpadmin -premote_drafts -v/dev/null -mrmodel -ocmrcmodel \
    -osmrsmodel -ormsystem13 -g3 -orpold_reliable
```

To allow print requests to enter the request directory for the newly added remote printers:

```
/usr/lib/accept letterhead
/usr/lib/accept remote_drafts
```

To enable the newly added remote printers:

```
/usr/bin/enable letterhead
/usr/bin/enable remote_drafts
```

To start the line printer scheduler, type:

```
/usr/lib/lpsched
```

Adding a Network-Based Printer Using HP-UX Commands

To add a network-based printer or plotter using HP-UX commands, follow the instructions shipped with the network-based printer or the network interface card for the printer.

Additional Task Information

The software needed to configure your network-based printer is shipped separately. Follow the instruction shipped with your printer to load the software and configure the printer.

In an HP-UX cluster, once the printer is added to the server, the printer will be available to all computers in the cluster.

Creating a Printer Class Using HP-UX Commands

To create a class of printers, use the `-c` option to the `lpadmin` command when you add a printer to the lp spooler or after you have added several printers to the lp spooler. A printer class must contain at least one printer. See "Adding a Local Printer Using HP-UX Commands" for instructions on creating a printer class as you add a printer to the lp spooler.

To create a printer class after several printers have been added to the lp spooler:

1. Ensure that you have superuser capabilities.
2. Stop the lp spooler (see "Starting and Stopping the LP Spooler Using HP-UX Commands").

Note It is best to stop the LP spooler when there are no requests currently printing.

3. Create the printer class by entering the `lpadmin` command, specifying the `-c` option, for every printer you wish to add to a class of printers. There is an example at the end of this section.
4. Start the lp spooler (see "Starting and Stopping the LP Spooler Using HP-UX Commands").
5. Allow print requests to enter the request directory for the newly added printer class with the `accept` command:

   `/usr/lib/accept` *pname*

   where:

   pname is the name given to this printer class.

   See "Accepting and Rejecting Print Requests for a Printer Using HP-UX Commands".

Additional Task Information

Printer classes cannot include remote printers.

A printer can only belong to one printer class at a time. To remove a printer from a printer class, remove the printer from the lp spooler and re-add the printer omitting the `-c` option of the `lpadmin` command.

It is not necessary to specify the model and device file options because the printers have already been defined for the lp spooler.

Printer class names can be up to 14 characters in length, and the characters must either be alphanumeric (A-Z, a-z, 0-9) or an underscore (_). Note that class names and printer names on the same system cannot be the same name. Class and printer names must be unique. A printer can only belong to one printer class at a time.

Examples

To create a `laser` class of printers consisting of printers *laser1*, *laser2* and *phred*:

```
/usr/lib/lpadmin -plaser1 -claser
/usr/lib/lpadmin -plaser2 -claser
/usr/lib/lpadmin -pphred -claser
```

To remove a printer from a printer class, remove the printer from the lp spooler and re-add the printer without the printer class (see "Adding a Local Printer Using HP-UX Commands" and "Adding a Local Printer Using SAM").

Removing a Printer or Printer Class Using HP-UX Commands

To remove a printer or printer class using HP-UX commands:

1. Ensure that you have superuser capabilities.
2. Deny any further print requests for the printer with the `reject` command:

   `/usr/lib/reject` [`-r` "*message*"] *name* [*name*]

   where:

   message is a message to be displayed when users obtain status information about the printer(s) and/or printer classes.

   name is the name of the printer or printer class.

   See “Accepting and Rejecting Print Requests for a Printer Using HP-UX Commands”.
3. *(If you are removing a printer class, skip this step and continue with step 4.)*

   Disable the printer to be removed with the `disable` command:

   `/usr/bin/disable` [`-r` "*message*"] [`-c`] *pname* [*pname*]

   where:

   message is a message to be displayed when users obtain status information about the printer(s).

   pname is the name of the printer to be disabled.

Note When you disable a printer, any print requests waiting to be printed for that printer will remain in the printer's request directory. If you wish to cancel all print requests for a printer at the time you disable it, use the `-c` option with the `disable` command:

```
/usr/bin/disable -c letterhead
```

9

See “Enabling or Disabling a Printer Using HP-UX Commands”.

4. Stop the lp spooler:

   ```
   /usr/lib/lpshut
   ```

   Before you stop the line printer scheduler (spooling system), beware of the following:

   a. *All* printing will stop until you restart the scheduler.

   b. Any print requests that are currently printing will be completely reprinted when you restart the scheduler. This includes the print requests that were printing page 9,999 of a 10,000 page printout.

5. To preserve the print requests in the request directory, move all print requests in the request directory for the printer or printer class to another printer or printer class request directory (see "Moving *All* Requests Using HP-UX Commands").

6. Remove the printer or printer class from lp spooler with the `lpadmin` command:

   `/usr/lib/lpadmin -x`*name*

   where:

   name is the name of the printer or printer class to be removed.

7. *If you have just removed your only printer, omit this step.*

   Start the lp spooler (see "Starting and Stopping the LP Spooler Using HP-UX Commands"):

   ```
   /usr/lib/lpsched
   ```

Additional Task Information

Because the `lpadmin` is deleting and modifying files that are being examined by the line printer scheduler, it is important that the scheduler is stopped when you use the `lpadmin` command to remove the printer from the lp spooler.

When you remove a printer class, the printers in it are *not* removed. You can still use them as individual printers. If the only printer in a printer class is removed, the printer class is removed also.

Examples

To remove the `laser1` printer:

```
/usr/lib/lpadmin -xlaser1
```

To remove the `laser` printer class:

```
/usr/lib/lpadmin -xlaser
```

Accepting and Rejecting Print Requests for a Printer Using HP-UX Commands

To *accept* print requests for a printer or printer class, use the `accept` command:

`/usr/lib/accept` *name* [*name*]

where:

name is the name of the printer class whose request directory is to be enabled to receive print requests.

You can issue individual commands for each printer class or you can combine the printer classes in one command.

To *reject* print requests for a printer or printer class, use the `reject` command:

`/usr/lib/reject [-r"`*message*`"]` *name* `[-r"`*message*`"] [`*name*`]`

where:

message is a message to be displayed when users obtain status information about the printer or printer class.

name is the name of the printer or printer class whose request directory is being prohibited from receiving print requests.

You can issue individual commands for each printer class or you can combine the printer classes in one command separated by spaces. If you combine them, you can also specify different reasons for rejecting printer requests for different printers (and printer classes).

Additional Task Information

Even if all printers that are members of a class are accepting requests, the class can still reject requests. If that were the case, users would need to specify *a specific printer*, not the class, in later print requests.

If all printers in a class are *rejecting* requests but the class itself is accepting requests, the print requests will remain in the request directory until at least one of the printers in the class begins to process print requests.

If you do not specify a reason, the status requests will get the response, "Printer <*printer_name*> is NOT ACCEPTING requests: Reason is unknown."

Examples

To accept print requests for the `laser1`, `laser2`, `phred`, `invoices`, `check_printer` printers and the `laser` printer class:

```
/usr/lib/accept laser1
/usr/lib/accept phred
/usr/lib/accept invoices laser2 check_printer laser
```

To reject print requests for the `laser1`, `laser2`, `phred`, `invoices`, `check_printer` printers and the `laser` printer class:

```
/usr/lib/reject -r"Printer on loan to seismology lab." laser1
/usr/lib/reject -r"Printers being serviced" laser1 check_printer
/usr/lib/reject -r"Invoice forms on order" invoices\
   -r "printers are being serviced" laser1 laser2 phred laser
```

Note A backslash (\) is used to represent a line continuation. When you type these commands, you can enter the backslash as shown or you can omit the backslash and type the entire command before pressing (Return).

Enabling or Disabling a Printer Using HP-UX Commands

To *enable* a printer to process print requests, use the `enable` command:

`/usr/bin/enable` *pname* [*pname*]

where:

pname is the name of the printer to be enabled to process print requests.

You can issue individual commands for each printer or you can combine the printers in one command separated by spaces.

To *disable* a printer to process print requests, use the `disable` command:

`/usr/bin/disable [-r"`*message*`"]` *pname* `[-r"`*message*`"] [`*pname*`]`

where:

message is a message to be displayed when users obtain status information about the printer(s).

pname is the name of the printer to be disabled to process print requests.

You can issue individual commands for each printer class or you can combine the printer classes in one command separated by spaces. If you combine them, you can also specify different reasons for disabling printer requests for different printers (and printer classes).

Additional Task Information

Note When you disable a printer, any print requests waiting to be printed for that printer will remain in the printer's request directory. When the printer is enabled again, the print requests will print. Any print request that are printing at the time the `disable` command is issued will be completely reprinted when the printer is enabled. If you wish to cancel all print requests for a printer at the time you disable it, use the `-c` option with the `disable` command:

```
/usr/bin/disable -c letterhead
```

Examples

To enable the `check_printer`, `laser1`, `laser2`, and `phred` printers:

```
/usr/bin/enable check_printer
/usr/bin/enable laser1 laser2 phred
```

To disable the `check_printer`, `invoices`, `phred`, `letterhead`, and `laser` printers:

```
/usr/bin/disable check_printer
/usr/bin/disable invoices phred letterhead
/usr/bin/disable -r "printer disabled to change paper" laser1
```

Setting a Printer Priority Fence Using HP-UX Commands

To set or change a printer priority:

1. Ensure that you have superuser capabilities.
2. Stop the lp spooler (see "Starting and Stopping the LP Spooler Using HP-UX Commands").

Note It is best to stop the LP spooler when there are no requests currently printing.

3. Use the `lpfence` command to set priority for a particular printer:

   `/usr/lib/lpfence` *pname priority*

   where:

   pname is the printer name.

   priority is the minimum required priority a print request must have in order to be printed on printer *pname*. Fence value range is 0 (lowest) to 7 (highest).

4. Restart the lp spooler (see "Starting and Stopping the LP Spooler Using HP-UX Commands"):

   ```
   /usr/lib/lpsched
   ```

Additional Task Information

When a printer is added to the lp spooler, the default priority is set to 0 (see "Priorities of Printers and Print Requests").

Starting and Stopping the LP Spooler Using HP-UX Commands

To *start* the lp spooler, use the `lpsched` command:

```
/usr/lib/lpsched
```

To *stop* the lp spooler, use the `lpshut` command:

```
/usr/lib/lpshut
```

Additional Task Information

Before you stop the line printer scheduler (spooling system), beware of the following:

- *All* printing will stop until you restart the scheduler.
- Any print requests that are currently printing will be completely reprinted when you restart the scheduler. This includes the print requests that were printing page 9,999 of a 10,000 page printout.

In order to report statistics about data flow through your lp spooler, you must tell the lp spooler that you want it to keep track of these statistics by specifying the `-a` option when starting the lp spooler with the `lpsched` command. The `-a` option tells the lp spooler to log statistical information about its activities to the file "`/usr/spool/lp/lpana.log`", a file which will be used by the `lpana` command to report the statistics.

Examples

To find out lp spooler status:

```
/usr/bin/lpstat -r
scheduler is stopped
```

To collect statistics about the data flow through the lp spooler, start the lp spooler with the `-a` option:

```
/usr/lib/lpsched -a
```

Canceling Print Requests Using HP-UX Commands

To cancel print requests, use the `cancel` command:

`/usr/bin/cancel` *req-ID* [*printer*]

where:

req-ID	is the print request identification number.
printer	is the printer name.

You can issue individual commands for each print request or you can combine the print requests in one command separated by spaces.

You do not need superuser capabilities to use the `cancel` command.

Additional Task Information

To list print request identification numbers, use the `lpstat` command (see "Viewing the Status of Printers and Print Requests Using HP-UX Commands").

The `cancel` command has several useful options that allow you to do things such as cancel all print requests that *you* have submitted or cancel all requests associated with a particular printer or printer class. Here are a few helpful `cancel` options and their descriptions:

`-a`	Remove all requests a user owns on the specified *printer*. The owner is determined by the user's login name and host name on the machine where the `lp` command was invoked
`-e`	Empty the spool queue of all requests for the specified *printer*. Only users with superuser capabilities can use the `-e` option
`-i`	Cancel only local requests.
`-u`*user*	Remove any requests queued belonging to *user*. Multiple `-u` options are allowed. Only users with superuser capabilities can use the `-u` option.

Examples

```
cancel laser-3456
cancel phred-2152
cancel letterhead-1547
```

or

```
cancel laser-3456 phred-2152 letterhead-1547
```

Moving *All* Requests Using HP-UX Commands

To move *all* print requests to another request directory using HP-UX commands:

1. Ensure your have superuser capabilities.
2. Prohibit any further requests from entering the request directory with the `reject` command:

   `/usr/lib/reject` *name* [*name*]

   where:

   name — is the name of the printer or printer class request directory to be enabled to receive print requests.

   You can issue individual commands for each printer class or you can combine the printer classes in one command separated by spaces. If you combine them, you can also specify different reasons for rejecting printer requests for different printers (and printer classes). See "Accepting and Rejecting Print Requests for a Printer Using HP-UX Commands".
3. Disable the printer with the `disable` command:

   `/usr/bin/disable [-r"`*message*`"]` *pname* `[-r"`*message*`"] [`*pname*`]`

   where:

   message — is a message to be displayed when users obtain status information about the printer(s).

   pname — is the name of the printer to be disabled to process print requests.

   You can issue individual commands for each printer class or you can combine the printer classes in one command separated by spaces. If you combine them, you can also specify different reasons for disabling printer requests for different printers (and printer classes). See "Enabling or Disabling a Printer Using HP-UX Commands".
4. Stop the lp spooler with the `lpshut` command:

   `/usr/lib/lpshut`

Moving *All* Requests Using HP-UX Commands

5. Relocate all of the print requests in the request directory to another request directory with the `lpmove` command:

   `/usr/lib/lpmove` *source dest*

   where:

   source — is the printer or printer class request directory that you want to move to the *dest* request directory.

   dest — is the printer or printer class request directory to receive the print requests from the *source* request directory.

6. Restart the line printer scheduler with the `lpsched` command:

   `/usr/lib/lpsched`

7. If the *source* printer or printer class is to be made available to receive print requests:

   a. Re-enable the printer(s) to process print requests with the `enable` command:

      `/usr/bin/enable` *pname* [*pname*]

      where:

      pname — is the name of the printer to be enabled to process print requests.

      You can issue individual commands for each printer or you can combine the printers in one command separated by spaces.

   b. Re-enable the printer or printer class request directory to accept print requests with the `accept` command:

      `/usr/lib/accept` *name* [*name*]

      where:

      name — is the name of the printer or printer class request directory to be enabled to receive print requests.

      9

      You can issue individual commands for each printer class or you can combine the printer classes in one command.

Examples

To move all print requests from `laser1` request directory to `phred` request directory:

```
/usr/lib/reject laser1
/usr/bin/disable laser1
/usr/lib/lpshut
/usr/lib/lpmove laser1 phred
/user/lib/sched
/usr/bin/enable laser1
/usr/lib/accept laser1
```

Moving Selected Print Requests Using HP-UX Commands

To move selected print requests to another request directory using HP-UX commands:

1. Ensure that the lp spooler is running.
2. Move selected print requests using the `lpalt` command:

   `/usr/bin/lpalt` *source* `-d`*dest*

   where:

source	is the identification number of the print request to be moved.
dest	is the printer or printer class request directory to receive the print request specified by *source*.

Additional Task Information

The `lpalt` command cannot be used to alter a print request that is currently printing.

The `lpalt` command will alter a print request from a *remote* printer *only* if the print request is owned by the user who is issuing the `lpalt` command and, again, this alteration will only take place if the print request is not currently printing.

Examples

To move print request laser-6610 to phred request directory:

```
lpalt laser-6610 -dphred
new request id is phred-6613
```

Viewing the Status of Printers and Print Requests Using HP-UX Commands

To view the status of printers and print requests, use the `lpstat` command:

```
/usr/bin/lpstat [-t]
```

If no options are given, `lpstat` displays the status of all requests made by the user. The `-t` option lists the following additional information:

- status of the lp spooler.
- system default printer.
- list of class names and their members.
- list of printers and associated device files.
- status of each print request directory (accepting or rejecting). If a reason was specified when the requests were rejected the reason is displayed.
- status of each printer (enabled or disabled). If a reason was specified when the printer was disabled, the reason is displayed.
- priority for each printer.
- list of print requests for each printer that includes the following attributes for each print request:
  - print request identification number
  - name of user that submitted the print request
  - priority
  - date and time submitted
  - file name
  - size

Additional Task Information

The `-t` option of the `lpstat` command is very detailed. For information on other options of this command, refer to *lpstat*(1) in the *HP-UX Reference*, HP part number B2355-90033.

Examples

To display a summary status of the lp spooler:

```
lpstat -t

scheduler is running
system default destination: laser
members of class laser:
      laser1
      laser2
      phred
device for letterhead: /dev/null
device for check_printer: /dev/null
device for laser1: /dev/lj1
    remote to: shasta on mountian
device for laser2: /dev/lj2
    remote to: hood on mountian
device for phred: /dev/lj3
device for invoices: /dev/invoices
laser1 accepting requests since Apr 18 14:46
laser2 accepting requests since May 13 14:08
phred accepting requests since Apr 18 14:46
laser accepting requests since Apr 18 14:46
letterhead accepting requests since Apr 18 14:46
invoices accepting requests since Apr 18 14:56
check_printer accepting requests since May 3 14:57
printer laser1 now printing laser1-1807.  enabled since Apr 23 13:47
 fence priority : 0
printer laser2 now printing laser2-1809.  enabled since Apr 23 13:47
 fence priority : 0
printer phred is idle.  enabled since Apr 18 14:46
 fence priority : 3
printer letterhead now printing letterhead-1810.  enabled since Apr 23 13:47
 fence priority : 4
printer invoices is idle.  enabled since Apr 19 10:24
 fence priority : 0
printer check_printer is idle.  enabled since Apr 18 14:56
 fence priority : 0
laser1-1808          susanl          priority 0  Jun 14 10:05 on laser1
 disktab                                    5808 bytes
laser1-1809          susanl          priority 0  Jun 14 10:05
 report1                                    17301 bytes
laser2-1810          kimj            priority 0  Jun 14 10:07 on laser2
 memokmj                                     947 bytes
letterhead-1811      johnc           priority 4  Jun 14 10:09 on letterhead
 salaries                                   2999 bytes
```

Changing the Priority of Print Requests Using HP-UX Commands

To change the priority of a print request, use the `lpalt` command:

`/usr/bin/lpalt` *preq-ID* `-p`*new_priority*

where:

preq-ID — is the print request identification number for the print request targeted for a new priority.

new_priority — is the new priority. Valid values are 0 to 7.

Additional Task Information

There are two primary reasons for changing a print request priority:

1. To move the print request ahead of other requests within the request directory.

   For example, you can change the priority of your print request to be higher than that of the large print request that is ahead of yours. When the line printer scheduler selects the next print request to send to the printer, it will take the one with the highest priority (which is now yours because you changed the priority).

Note Once a print request is *printing*, it will not yield to a print request of higher priority. In this case, you can move your print request to another printer if possible. See "Moving Selected Print Requests Using HP-UX Commands" for details.

2. To match or exceed the printer's priority, enabling the print request to be processed (see "Priorities of Printers and Print Requests").

Unless you tell it otherwise, the `lp` command (used to print things) will assign your print request a priority equal to that of its printer's printer priority setting. If your print request is assigned to a printer class, the highest printer priority setting among all the printers in the class will be used.

Examples

To find the following print request information:

- The *print request-ID* for the print request you want to change
- The *current priority of the print request*
- The *priorities of the other print requests* on the same printer
- The *priority of the printer*

use the `lpstat` command:

```
lpstat
phred-1827     stevenm     priority 0  Jun 14 10:05 on phred
   proglisting                          1708 bytes
phred-1828     paulv       priority 2  Jun 14 10:05
   LONGproglist                         6900714 bytes
phred-1829     chrisn      priority 1  Jun 14 10:05
   urgentmemo                           311 bytes
```

To move print request phred-1829 ahead in the request directory:

`lpalt phred-1829 -p3`   *changes phred-1829's priority to 3*

Displaying Statistics about Printer Activity Using HP-UX Commands

Note Prior to displaying statistics about printer activity, the lp spooler must have been started with the `/usr/lib/lpsched -a` command to create a log of activity in the `/usr/spool/lp/lpana.log` file. See "Starting and Stopping the LP Spooler Using HP-UX Commands".

To display statistics about printer activity, use the `lpana` command:

`/usr/lib/lpana` [`-d`*dest*]

where:

dest defines the printer or printer class for which statistics are displayed. By default, `lpana` will report statistics for *all* printers and printer classes (optional).

Additional Task Information

Table 9-5. Interpreting `lpana's` Output

<table>
<tr><th>Column Name</th><th>How to Interpret the Results</th></tr>
<tr><td>wait [AV]</td><td>This is the average length of time (in minutes and seconds) that print requests spent in their printer's queue before they began to print.

If this number is low, that's good! It means that print requests assigned to this printer begin printing quickly. This might be a good printer to "take the load off" of other printers that have longer <code>wait</code> times.

If this number is high, check the following things:
Is there a lot of traffic going through this printer? See the columns called <code>sum KB</code> and <code>num_of requests</code> (later in this table) for information on how to determine this. You might want to route some of the print requests to another printer.
Has the printer been taken offline frequently or for an extended period of time?
Has this print destination been disabled (but the lp spooler continued to accept requests for it). This can happen if you <code>disable</code> a printer but do not also <code>reject</code> the print destination.</td></tr>
</table>

Table 9-5. Interpreting `lpana`'s Output (continued)

Column Name	How to Interpret the Results
wait [SD]	This is the standard deviation from the "average wait time." This number can help you determine how typical the "average wait time" (reported in the `wait [AV]` column) is. If this number is *small*, it means that the number in the `wait [AV]` column is fairly representative of a "typical" print request. It makes sense to interpret the `wait [AV]` as explained in the description of that column, above.
wait [SD] (cont.)	If this number is *large* it indicates that the number in the `wait [AV]` column is not representative of a "typical" print request. This could indicate that a small number of print requests had to wait an unusually long (or short) time and their wait times are skewing the data reported as the "average wait time." It might be wise to monitor the statistics for a longer period of time before making changes to your lp spooler as a result of this data.
print [AV]	This is the average amount of time print requests took to actually print (the elapsed time from the time a print request begins to print until it has finished printing). If this number is *small*, print requests for this print destination are not taking long to print. It probably indicates that the "typical" print request for this print destination is small. Fast printers and fast communication lines can also help keep this number down. If this number is *large*, print requests for the corresponding print destination are taking a long time to print. This may be due to their size (perhaps they contain a lot of graphic data) or this may be due to a slow printer or communications line.

Table 9-5. Interpreting `lpana's` Output (continued)

Column Name	How to Interpret the Results
print [SD]	This is the standard deviation from the "average print time." Similar to the standard deviation for the "average wait time" this number lets you know how typical the "print [AV]" number is. If this number is *small*, the "print [AV]" number is representative of the print time for typical print request. Essentially it means that all of the print requests for this print destination take about the same amount of time to print. If this number is *large*, the "print [AV]" time is not too representative of a typical print request. This means that there is a wide variation in how long print requests take to print (for this print destination).
bytes [AV]	This is the average size (in bytes) for print requests going to this print destination.
bytes [SD]	This is the standard deviation from the "average size." It tells you how typical the "bytes [AV]" number is. If this number is *small*, print requests for this print destination do not vary in size much. If this number is *large*, print requests for this print destination vary a lot in size.
sum [KB]	This is the number of kilobytes (# of bytes x 1024) of data sent to this print destination during the reporting period.
num_of requests	This is the number of print requests sent to this print destination during the reporting period.

Examples

To display statistics for all printers:

```
/usr/lib/lpana
```

```
performance analysis is done from Jun.22 '90 14:02 through Jun.27 '90 15:29
---printers      ----wait----    ---print---     ---bytes---    -sum- num_of
    /classes--      AV     SD      AV     SD       AV      SD      KB requests
letterhead        0'00      0    0'49      2    59565       0     116        2
phred             0'00      0    0'45     22    14202       0     166       12
check_printer     0'09     31    0'51     73    12378       0     302       25
laser1            0'02      5    0'04      1    36686       0    2400       67
laser2            3'45      0    1'45      0      783       0       1        1
```

To display statistics for the `laser` printer class:

```
/usr/lib/lpana -d laser
```

```
performance analysis is done from Jun.22 '90 14:02 through Jun.27 '90 15:29
---printers      ----wait----    ---print---     ---bytes---    -sum- num_of
    /classes--      AV     SD      AV     SD       AV      SD      KB requests
laser1            0'02      5    0'04      1    36686       0    2400       67
laser2            3'45      0    1'45      0      783       0       1        1
```

9

10
Communicating With the Users on Your System

HP-UX provides you with several utilities to communicate with your system users. These include the following commands, which will be explained in this chapter:

- *news*(1M)
- *write*(1)
- *wall*(1M)
- *uucp*(1)
- *mail*(1), *mailx*(1), *elm*(1).

Taking advantage of these utilities will make your job as system administrator easier, and will enhance communications between you and your users and among individual users.

Terms Used in this Chapter

The following terms are explained in this chapter:

elm An electronic mailer that is more flexible than `mail` or `mailx`.

mail A basic electronic mailer that is the base for both `mailx` and `elm`. It only supports command-line input, and does not provide for editing of outgoing messages. However, you can use `mail` to send a file that was written outside of the mail program.

mailx An enhanced version of `mail`. `mailx` provides commands for saving, deleting, and responding to messages that you have received, and for editing and reviewing messages that you wish to send.

mesg A command, when issued by an individual user, that permits or denies other users from writing to the user's terminal.

motd A file displayed on the terminal whenever a user logs in. This file can contain a "message of the day" that you want your users to read when they log in.

news A command that enables you to leave messages and other news items for your users. Each user can automatically receive the news items upon logging in to the system, or upon invoking the `news` command.

UUCP A utility that allows users on one HP-UX system to send files to users on another HP-UX system.

wall A command that allows you to send, or broadcast, messages to all users, or to users identified in a distribution list.

write A command that allows a user to send a message directly to another user's terminal on the same system.

Displaying Messages to Users Logging into Your System

HP-UX provides two methods by which you can keep your users informed about your system. The first is a file `/etc/motd` (message of the day). The contents of this file is displayed on a user's terminal each time the user logs into the system. The second method uses the HP-UX **news** command.

motd

You can place a message in the `/etc/motd` file, and this file will be read to a user's terminal each time that the user logs into the system. The process of reading the file is handled automatically by `login`. This is an easy way to inform your users about such information as the system backup schedule or scheduled maintenance.

Another `motd` file is automatically read by the printer spooler, which, in turn, prints a message at the top of each user's printout. This file is in `/usr/spool/lp/motd`. This file can be used to keep your user's informed about such information as the printer name and status.

news

The **news** command allows users to read announcements which have been left on the system. Information for system users can be placed in files under the `/usr/news` directory. Any user may create a file in this directory for other users to read. A user can access these files by typing **news**. There are several options:

- `news -a` displays all files in the `/usr/news` directory. This includes both new files and files the user has read.
- `news -n` displays the names of the files in the `/usr/news` directory without displaying their content.
- `news -s` lists the names of the files in the `/usr/news` directory that the user has not yet read.

You can abort the reading of one **news** item and begin the reading of the next **news** item by typing your interrupt key sequence. You can terminate the **news** program by typing a second interrupt sequence within one second of the first. You can determine your interrupt key sequence by typing **stty -a**.

Users can put the command `news` in their `.profile` or `.login` file, and they will automatically receive the system news when they log in.

Communicating With a User Who is Logged into Your System

The *write*(1) command allows one user to send a message directly to another user's terminal, and permits that person to directly respond to the originator. This provides for true two-way communication.

The originator of the session types: `write` *user*, where *user* is the login name of the receiver of the communication. The receiver will see `Message from` *yourname* on the terminal, where *yourname* is the originator's login name.

The receiver may then follow the same procedure to send a message back to the originator, and two-way communication is established. The bell on the originator's terminal will sound twice to indicate that two-way communication is possible.

To end the communication session, type your interrupt key sequence. You can determine your interrupt key sequence by typing the command: `stty -a`.

Permission to write to a user's terminal may by granted or denied by the user typing the `mesg` command. If the user types `mesg y`, (the default) write permission is granted. If the user types `mesg n`, write permission is denied.

Broadcasting a Message to All Users Logged into Your System

The `wall` (write to all) command allows the system administrator to send a message to all users logged into the system. It can be used to notify users of items of immediate concern, such as the need to shut down the system.

If the `wall` command is used without arguments, the standard input from your terminal is read until an end-of-file (ctrl-d) is received. Then the message is sent to all logged-in users preceded by: **Broadcast Message from** ... .

If the `wall -g`*groupname* command is used, the standard input from your terminal is sent to all logged-in users whose names are listed in the file *groupname* in the directory `/etc/group`. The message is preceded by: **Broadcast Message from ... to group** *groupname.*

If the `wall` command is followed by a file name, the content of the specified file is used for the message, rather than input from your terminal.

When in a HP cluster environment, use the command `cwall` to write to all logged-in users of the cluster.

Communicating With Users on Other Systems Using UUCP

HP-UX provides a utility called UUCP that allows users to send files between different computer systems. The computer systems must be connected directly together (hardwired), or connected to the telephone system by modems. After the hardware is properly connected and the software is configured, users can transfer files using the `uucp` command.

The `uucp` command provides users a number of options in designating the source and destination files for the transfer. Other commands associated with `uucp` are `uulog` and `uuname`.

While UUCP is easy for individual users to use, the process of setting up the hardware and software is complex. This process is described in detail in the manual *Remote Access: User's Guide* (HP part number B2355-90037). Refer to this manual for additional information on UUCP.

Using Electronic Mail Systems

Several utilities are available that permit users to communicate through electronic mail. These are `mail`, `mailx`, and `elm`.

The preferred HP-UX electronic mail program is `elm`, which provides many advantages over `mail` and `mailx`, including an interactive screen-oriented processing system, a command menu, and help. Using `elm`, users can customize their e-mail environment.

Information on using electronic mail is presented in detail in the manual *Mail Systems: User's Guide* (HP part number B1862-90012).

11

System Accounting Concepts and Tasks

Multiuser HP-UX allows concurrent sharing of computer resources among multiple users: several users can be logged in, all sharing disk space, memory, and the CPU. On multiuser systems, HP-UX System Accounting provides the means to:

- Monitor disk space usage for individual users.
- Record connect session data (logins/logouts).
- Collect resource utilization data (such as memory usage and execution times) for individual processes.
- Charge fees to specific users.
- Generate summary files and reports that can be used to analyze system performance and bill users for resource consumption.

Note Much of the material in this chapter assumes greater knowledge of HP-UX than is required of the "average" user. In particular, System Accounting borrows many concepts from from most of the previous chapters. If you are unfamiliar with the concepts and terminology in those chapters, then you should review them.

What Is in This Chapter?

HP-UX System Accounting allows you to accomplish accounting tasks through a number of versatile commands. This chapter illustrates the use of these commands and contains the following sections:

- "Installation and Daily Usage" shows the routine daily usage of System Accounting and shows you how to install it.
- "Overview of System Accounting" provides the background information necessary to understand how to use System Accounting.
- "Disk Space Usage Accounting" illustrates the use of the accounting commands that monitor disk space utilization on a per-user basis.
- "Connect Session Accounting" describes the commands that record and report connect session accounting information.
- "Process Accounting" shows how to generate per-process accounting data and reports.
- "Charging Fees to Users" is the section where you learn how to charge fees to users.
- "Summarizing and Reporting Accounting Information" shows how to generate the main daily and monthly accounting reports that are used to monitor system performance and bill users.
- "Updating the Holidays File" describes how to set up the file describing your holidays.
- "Fixing Corrupted Files" is useful when System Accounting files become inconsistent or messed up. This section discusses how to fix these files.
- "Sample Accounting Shell Scripts" provides listings of shell scripts that you might find useful on your system.
- "System Accounting Files" contains brief definitions of the files used by System Accounting.

Installation and Daily Usage

The purpose of this section is to show you:

- What you must do to get System Accounting running on your system.
- How System Accounting automatically creates daily and monthly accounting data and reports.

After reading this section, you should be able to install System Accounting on your system. Once properly installed, System Accounting will automatically generate daily and monthly accounting data and reports.

How to Install System Accounting

Not all users require accounting services on their systems. For this reason, HP-UX System Accounting is provided as an option: if you want to use System Accounting, you must install it yourself. The installation procedure is covered here.

There are three steps in the installation process:

1. Update `/etc/rc`
2. Create `crontab` entries
3. Set PATH for accounting commands

Each of these steps must be carried out to insure that System Accounting automatically creates daily and monthly accounting information. Detailed descriptions of each step follow.

Update /etc/rc

The system initialization shell script `rc` must be updated to automatically start System Accounting when the system is switched into multiuser mode. This requires adding the following entry in the `localrc` section of `/etc/rc`:

```
/bin/su - adm -c /usr/lib/acct/startup
```

Create crontab Entries

To automate the daily and monthly creation of accounting data, you should create a `crontab` file that `cron` can use to automatically run certain accounting commands. This process entails the following steps:

1. Log in to System Accounting as the user `adm`.
2. Use an editor to create the `crontab` file containing the accounting commands that are to be run automatically by `cron`. (The actual entries to make in this file are shown after these steps.)
3. Execute the `crontab` command, specifying the file created in step 2 as input. This step insures that the `crontab` file created in step 2 will be scanned by `cron` every minute. After invoking this command, the step 2 file will be stored in the file:

   ```
   /usr/spool/cron/crontabs/adm
   ```

4. At this point, you are finished creating `crontab` entries. If you ever want to change the entries, simply re-edit the file created in step 2 and use the `crontab` command again. Refer to the *crontab(1)* entry in the *HP-UX Reference* for more information.

The following entries, accompanied by a description of each, should be made in the `crontab` file created in above:

```
0 4 * * 1-6 /usr/lib/acct/runacct 2> /usr/adm/acct/nite/fd2log
```

`runacct`, the main accounting shell script, should be executed daily (during non-prime hours) to generate daily accounting reports. The above entry executes `runacct` at 4:00am every Monday through Saturday. Error messages will be redirected to the file `/usr/adm/acct/nite/fd2log`, if any errors occur while `runacct` executes.

```
0 2 * * 4 /usr/lib/acct/dodisk
```

`dodisk` creates total accounting records that summarize disk space usage for individual users. This entry runs `dodisk` at 2:00am every Thursday morning.

```
5 * * * * /usr/lib/acct/ckpacct
```

To insure that the process accounting file, pacct, doesn't get too large, the command ckpacct should be executed hourly. This entry invokes ckpacct at five minutes into every hour.

```
15 5 1 * * /usr/lib/acct/monacct
```

The monthly merging of accounting data is facilitated through the monacct command. This entry allows monacct to generate a monthly total report and total accounting file. monacct will be executed at 5:15am on the first day of every month.

Note The dates and times shown in the crontab entries above are only suggestions; you can tailor crontab entries to suit your needs. However, if you use different entries than those shown here, be sure that monacct is run at such a time as to allow runacct sufficient time to finish.

Set PATH for Accounting Commands

Finally, you should set the PATH shell variable in /usr/adm/.profile so that System Accounting knows where to look for commands. Path should be set as follows:

```
PATH=/usr/lib/acct:/bin:/usr/bin:/etc:/usr/adm
```

Summary of Daily Operation

The daily operation of System Accounting is summarized by the following steps:

1. When HP-UX is switched into multiuser mode, the system initialization shell script rc executes the accounting command startup. The purpose of startup is to start System Accounting, and it performs the following functions:
   a. Calls acctwtmp to add a boot record to wtmp. This record is marked by storing "acctg on" in the device name field of the wtmp record.
   b. Turns process accounting on via turnacct on. turnacct on executes accton with the filename argument /usr/adm/pacct.
   c. Removes work files left in the sum directory by runacct.

2. A report of the previous day's accounting information can be created by running `prdaily`. Obviously, this step is omitted the first day that System Accounting is installed, because the previous day's accounting information doesn't exist yet. However, after `runacct` has been executed, `prdaily` will generate valid reports.
3. The `ckpacct` command is executed every hour via `cron` to insure that the process accounting file `pacct` doesn't become too large. If `pacct` grows past a set maximum number of blocks, `turnacct switch` is invoked, which creates a new `pacct` file. (Other conditions may also limit the size of the process accounting file or turn process accounting off; for more details, refer to the discussion of `ckpacct` in the "Process Accounting" section of this chapter.) The advantage of having several smaller `pacct` files is that `runacct` can be restarted faster if a failure occurs while processing these records.
4. The `chargefee` program can be used to charge fees to users. It adds records to the file `fee`. These records are processed during the next execution of `runacct` and merged in with total accounting records.
5. `runacct` is executed via `cron` each night. It processes the active fee file and the process, connect session, and disk total accounting files. It produces command and resource-usage summaries by login name.
6. When the system is turned off using `shutdown`, the `shutacct` command is executed. The purpose of `shutacct` is to stop System Accounting, and it performs the following functions:
   a. Writes a termination record to `wtmp` via the command `acctwtmp`. This record is marked by having "acctg off" in the device name field.
   b. Turns process accounting off by calling `turnacct off`.

Overview of System Accounting

In this section, the intrinsics of System Accounting are examined. Key terms are defined, commands are introduced, system data flow is described, and finally, you are shown the login and directory structure of System Accounting.

Definitions

The following terms are specific to System Accounting.

prime/non-prime connect time

Prime time is the time during the day when the computer system is most heavily used—for example, from 9:00am to 5:00pm. Non-prime time is the remaining time during the day when the system is less heavily used—from 5:00pm to 9:00am in this example.

When reporting computer time usage, System Accounting distinguishes between prime and non-prime time usage. You can specify prime and non-prime time on your system by editing the file `/usr/lib/acct/holidays`. (For details on the `holidays` file, refer to the section "Updating the Holidays File" in this chapter.

Note Prime time is in effect only on weekdays (Monday through Friday); non-prime time is in effect during the weekends (Saturdays and Sundays) and on any holidays specified in the `holidays` file.

process accounting records

Once System Accounting is installed and turned on, the following occurs: whenever a process terminates, the kernel writes a process accounting record for the terminating process into the current process accounting file, `/usr/adm/pacct` by default. (You can specify that a file other than `pacct` be used as the process accounting file, if desired.)

A process accounting record contains resource-usage data for a single process; it summarizes *how much* of the various resources the process used during its lifetime. Examples of information contained in process accounting records are:

- the user ID of the process's owner
- the name of the command that spawned the process
- the amount of time it took the process to execute

For greater detail on the contents and format of process accounting records, refer to *acct(4)* in the *HP-UX Reference*.

total accounting records

These records, created by various accounting commands, contain summary accounting information for individual users. These records provide the basic information for many reports generated by System Accounting. Some examples of information contained in these records are:

- the ID and user name of the user for whom the total accounting record was created
- the total number of processes that the user has spawned during the accounting period for which the total accounting record was created
- fees for special services rendered to this user

The exact contents and format of total accounting records can be found in *acct(4)*. In addition, commands covered in later sections of this chapter show how these records are created and used by System Accounting.

Introduction to Commands

System Accounting provides many versatile commands to accomplish numerous, varied tasks. There are commands that create data, commands that display data, commands that remove data, commands that merge data, and commands that summarize and report data. In addition, the output of one command may become the input to other commands.

System Accounting commands can be logically categorized into six basic command groups:

- installation
- disk usage accounting
- connect session accounting
- process accounting
- charging fees
- summarizing and reporting accounting information

Descriptions of these command groups, along with a brief synopsis of each command, follow.

Installation

These commands insure that System Accounting is properly installed. They are used to turn accounting on when HP-UX is powered up and turn accounting off when the system is shut down. They may also do some file cleanups. Two such commands exist:

- `startup`—starts accounting when HP-UX is switched to multiuser mode. `startup` is invoked from `/etc/rc`.
- `shutacct`—turns off accounting when HP-UX is turned off via the `/etc/shutdown` shell.

Disk Space Usage Accounting

In general, these commands produce disk usage accounting information: they show disk space usage (in blocks) for individual users. They also produce total accounting records. There are four commands:

- `acctdusg` and `diskusg`—both commands show how many blocks of disk space users are consuming. They differ in command options, and the manner in which they produce the information—`acctdusg` takes its input from a list of path names created by `find`, and `diskusg` looks at the inodes of the file system to create its output.
- `acctdisk`—produces total accounting records. Its input is supplied (either directly or indirectly) from `acctdusg` or `diskusg`.
- `dodisk`—produces total accounting records by using the `diskusg` and `acctdisk` commands. `dodisk` is normally invoked by `cron`.

Connect Session Accounting

Independently of System Accounting, the programs `login` and `init` record connect sessions by writing records into `/etc/wtmp`. System Accounting commands can display or fix this file, and can produce total accounting records for this file. There are six commands:

- `acctwtmp`—writes records to `wtmp`.
- `fwtmp`—displays the information contained in `wtmp`.
- `wtmpfix`—normalizes connect session records that span date changes (refer to *date(1)*). Also validates login names in connect session records.
- `acctcon1`—summarizes `wtmp` in ASCII readable format, producing one line per connect session.
- `acctcon2`—takes input of the format produced by `acctcon1` and produces total accounting records as output.
- `prctmp`—displays the session record file, normally called:

  `/usr/adm/acct/nite/ctmp`

Process Accounting

When process accounting is turned on, the kernel writes a process accounting record to pacct whenever a process terminates. A number of accounting commands exist that summarize and report this accounting information. In addition, certain commands turn process accounting on or off and insure that pacct doesn't become too large. The process accounting commands are:

- accton—turns process accounting on or off, depending on whether or not a filename argument is supplied with the command. If no filename is given, then process accounting is turned off; the kernel stops writing process accounting records to pacct. If a filename is specified, then the kernel starts writing process accounting records to the specified filename.

  accton uses the system call acct to turn process accounting on or off. Only the superuser can execute accton.

- ckpacct—checks the size of the process accounting file pacct. If pacct becomes too large, then a new pacct file is created via turnacct switch. *If disk space becomes critically short, then process accounting is turned off until sufficient space is available.* This command is normally invoked by cron.
- turnacct on || off || switch—performs one of three functions, depending on which argument (on, off, or switch) is specified. turnacct on turns process accounting on by calling accton with the default filename argument /usr/adm/pacct; turnacct off turns process accounting off by calling accton with no filename argument; turnacct switch renames the current pacct file (so that it is no longer the current process accounting file) and creates a new, empty pacct file.
- acctcom—displays process accounting records contained in pacct (or any specified file).
- acctcms—takes pacct as input, and produces summary accounting information by command, as opposed to by process.
- acctprc1—produces readable process accounting information, mainly for input into acctprc2.
- acctprc2—takes input of the form produced by acctprc1 and produces total accounting records.

Charging Fees

Occasionally, you may want to charge a user for something. For example, you might charge fees to users for fixing any damaged files that they have. The `chargefee` command allows you to charge fees to specific users.

Summarizing and Reporting Accounting Information

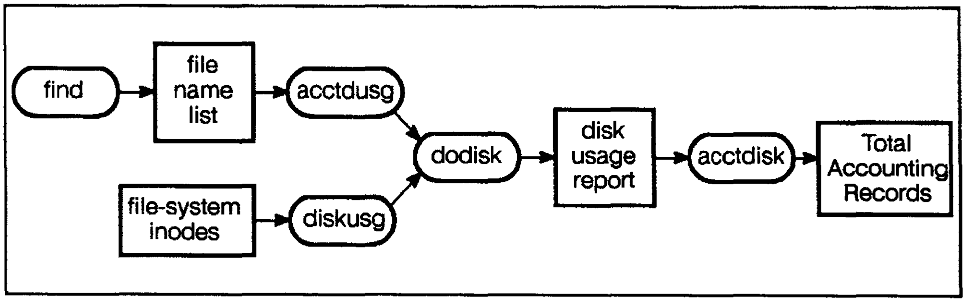
This group of commands summarizes and reports the data created through the command groups described above. These are the commands that are probably used most frequently; they represent the highest level of accounting commands. Five such commands exist:

- `prtacct`—takes as input total accounting records and displays the records in ASCII readable format.
- `acctmerg`—combines the contents of separate total accounting files into a single total accounting file. This command allows the merging of disk, process, and connect session total accounting records.
- `runacct`—is the main accounting shell script. Normally invoked daily by `cron`, this command processes disk, connect session, process, and fee accounting information and produces summary files and reports. It accomplishes its task by proceeding through various states. In each successive state it invokes accounting commands to perform a specific task. For example, in one state, total accounting records for connect sessions are created; in another, disk, connect session, process, and fee total accounting records are merged to create one total accounting file.
- `prdaily`—invoked by `runacct` to format a report of the previous day's accounting data; the report is in the file `/user/adm/acct/sum/rpt`*mmdd* where *mmdd* is the month and day of the report. `runacct` may also be used to display a report of the current day's accounting information.
- `monacct`—invoked once a month (or accounting period), this command summarizes daily accounting files and produces a summary files for the accounting period.

System Data Flow

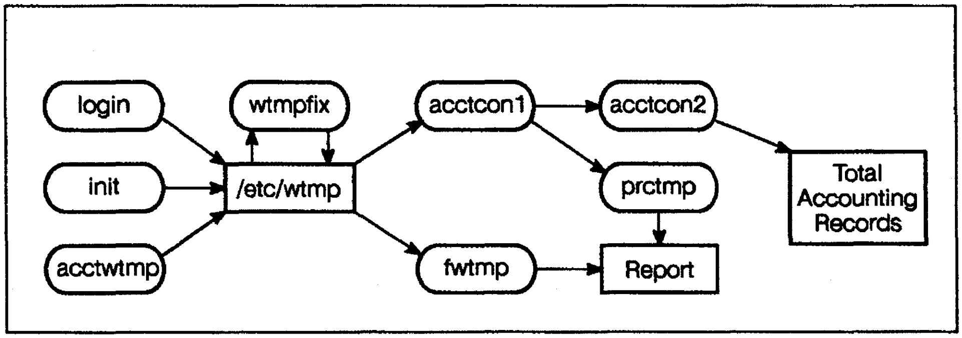
At this point, you have the rudimentary knowledge necessary to understand how System Accounting works; you know some important definitions and should basically know what the various commands do. The purpose of this section is to help you visualize how the different commands work together to create accounting data.

The following figures illustrate, through the use of diagrams, how accounting data is created. Each diagram represents the data flow for a given command group.



LG200172_003

Figure 11-1. Disk Usage Accounting



LG200172_004

Figure 11-2. Connect Session Accounting

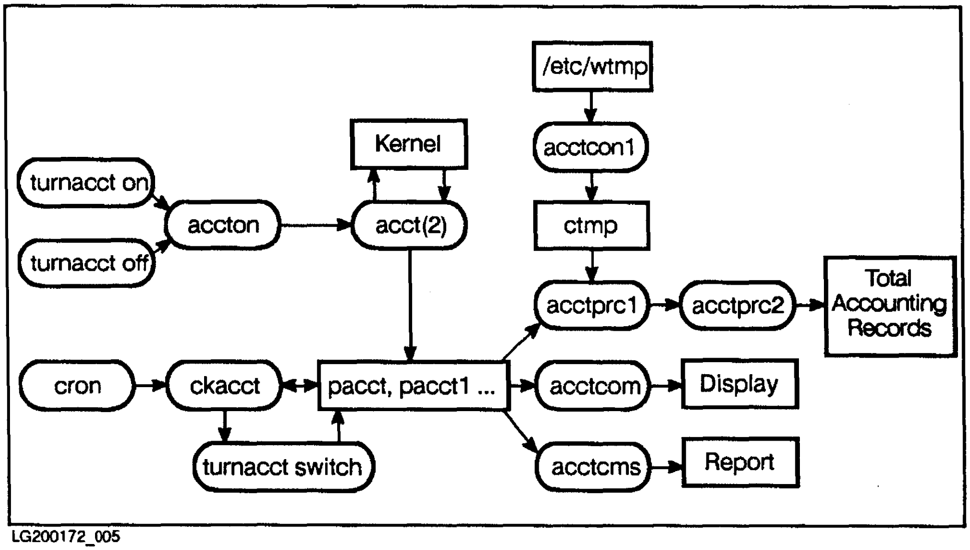


Figure 11-3. Process Accounting

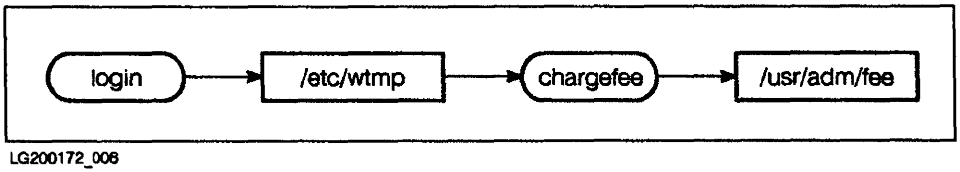


Figure 11-4. Charging Fees

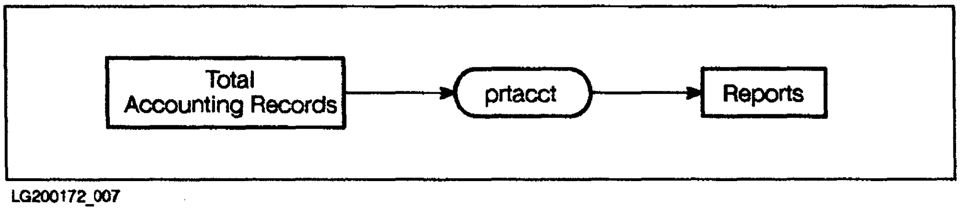


Figure 11-5. Summarizing and Reporting

Login and Directory Structure

You now know the basics, but you still can't begin learning the day-to-day usage of accounting commands until you know where to log in. In addition, you should know the accounting directory structure—where the various commands, directories, and files are located. These two topics are discussed here.

Logging In

The login name for System Accounting is `adm`; the user ID for `adm` is 4. The `adm` login is a member of the *group* `adm`, and the group `adm` has a group ID of 4, also.

The home directory for the `adm` login is `/usr/adm`. You log in to System Accounting the same way you do for any account—simply supply the login name to the HP-UX login prompt:

```
login: adm
```

Note The integrity of accounting data files must be maintained if System Accounting is to generate accurate reports. For this reason, it is highly recommended that a password be used with the `adm` login.

Directory Structure

System Accounting uses a multi-level directory structure to organize its many accounting files. Each directory in this structure stores related groups of files, commands, or other directories. (Refer to the section "System Accounting Files" in this chapter for definitions of the accounting data files.)

Figure 11-6 illustrates this structure, and descriptions of each directory follow:

- `/usr/adm`—contains all active data-collection files, such as `pacct` and `fee`.
- `/usr/adm/acct`—contains the `nite`, `sum`, and `fiscal` directories described below.
- `/usr/adm/acct/nite`—stores data files that are processed daily by `runacct`.

- `/usr/adm/acct/sum`—cumulative summary files updated by `runacct` are kept here.
- `/usr/adm/acct/fiscal`—periodic (monthly) summary files created by `monacct` are stored here.
- `/usr/lib/acct`—System Accounting commands reside here.
- `/etc`—contains `wtmp`, and shell scripts `rc` and `shutdown`.

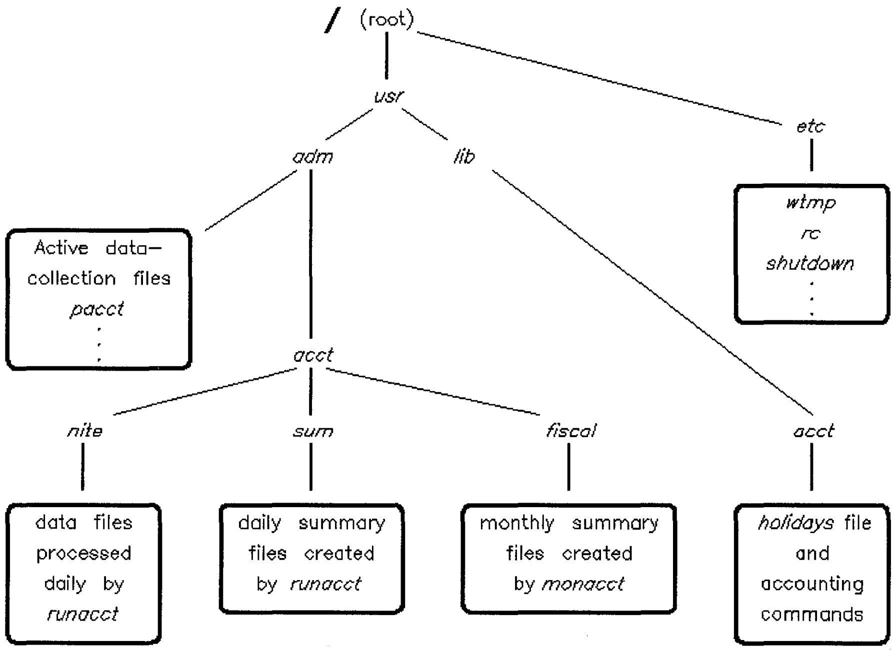


Figure 11-6. System Accounting Directory Structure

Disk Space Usage Accounting

System Accounting provides the means to monitor disk space utilization for individual users. In this section, disk space usage accounting commands are explained. Before reading this discussion, you may want to review the "File System Implementation" chapter of this manual.

Disk usage commands provide two main functions: they report disk usage (in blocks) for individual users and create disk total accounting records (supplied as inputs to commands such as `prtacct` or `runacct`).

Reporting Disk Space Usage

Two commands—`acctdusg` and `diskusg`—report disk usage for individual users; both commands show the number of disk blocks allocated to specific users. However, each command has slightly different options. In addition, each differs in the manner in which it produces accounting information.

acctdusg

`acctdusg` takes from standard input a list of path names, usually created by the `find` command. For each file in the list, `acctdusg` identifies the owner of the file, computes the number of blocks allocated to the file, and adds this amount to a running total for the file's owner. When finished looking through the list, `acctdusg` displays the information accumulated for each user: user ID, user name, and number of blocks used.

This command is useful for reporting disk usage information for specific users or files. For example, suppose you want to know how many blocks of disk space you are using: your user ID is `351`, user name is `bill`, and your home directory is `/users/pseudo/bill`. The following illustrates how you would use the `find` and `acctdusg` commands to show this information.

```
find /users/pseudo/bill  -hidden -print > bills.files
acctdusg < bills.files
00351   bill                30
rm bills.files
```

In the above example, `bill` is using 30 blocks of disk space. The series of commands shown could easily have been combined into one line, such as:

```
find $HOME  -hidden -print | acctdusg
00351   bill                30
```

The next example shows how to use `acctdusg` to generate disk usage information for all files in the system:

```
find /  -hidden -print | acctdusg
00350   fred                11
00351   bill                30
00352   mike                17
00353   sarah               13
00354   molly               18
00000   root                 3
00004   adm                 36
00001   bin               2434
```

Two options are included with `acctdusg`:

`-u` *no_owners* — If `-u` is given, then path names of the files for which no owner is found are written into the file *no_owners*. This option could potentially find users who are trying to avoid disk charges.

`-p` *p_file* — The password file `/etc/passwd` is the default file used by `acctdusg` to determine ownership of files. If the `-p` option is used, then `acctdusg` will use *p_file* instead. This option is not needed if your password file is `/etc/passwd`.

The shell script **grpdusg**, provided in the section "Sample Accounting Shell Scripts" later in this chapter, displays disk accounting information for users in a given group. It illustrates the use of the **-u** option with **acctdusg**.

diskusg

This command reports disk usage information in the same format as acctdusg—user ID, user name, and total disk blocks used. However, **diskusg** generates disk accounting information by looking through the *inodes* of a specified special file. (Refer to *inode(4)* and Chapter 8, "HFS File System" in the manual *How HP-UX Works: Concepts for the System Administrator* for more information on inodes and special files.) Therefore, **diskusg** is faster and more accurate than **acctdusg**.

The syntax of the **diskusg** command is:

diskusg [*options*] [*files*]

It generates a disk usage report from data in *files*, if specified; otherwise standard input is used. **diskusg** is normally invoked with the *files* argument. When specified, *files* are the special file names of the devices containing the inode information used by **diskusg** to generate its report. *files* is normally a special file from the **/dev** directory.

The following options may be used with **diskusg**:

- **-s** This tells **diskusg** that: (1) input is in **diskusg** output format, and (2) that all lines for a single user should be combined into a single line. This option is used to merge data from separate files, each containing the output from using **diskusg** on different devices.
- **-v** This option is useful for finding users who are trying to avoid disk space accounting charges. When this option is specified, **diskusg** writes records to **stderr** (standard error output) showing the special file name, inode number, and user ID of files that apparently have no owner.
- **-i** *fnmlist* Causes **diskusg** to ignore the data on those file systems whose file system name is in *fnmlist*. *fnmlist* is a list of file systems separated by commas or enclosed within quotes.
- **-p** *p_file* This is the same as the **-p** option of **acctdusg**.
- **-u** *u_file* This option produces *exactly* the same output as the **-v** option. The difference between the two options is that **-v** writes its output to **stderr**; this option writes its output to the file *u_file*.

The output of **diskusg** is normally used by **acctdisk** to create disk total accounting records. In addition, **diskusg** is normally called by **dodisk**.

The following example creates disk usage information for all users whose files reside on the disk whose device file is /dev/rdsk/1s0. *Note that the file system used in this example is the same as was used in the previous* acctdusg *example.*

```
diskusg /dev/rdsk/1s0
0       root     10616
1       bin      778
4       adm      96
350     fred     14
351     bill     32
352     mike     20
353     sarah    16
354     molly    22
355     julie    2
501     guest    2
```

The differences between **diskusg** and **acctdusg** are best illustrated by comparing their outputs. Note that:

1. **acctdusg** places leading zeros on user IDs; **diskusg** doesn't.
2. **acctdusg** counts files *only under each users* $HOME *directory*. Files that users own in directories other than their home directory (for example, files in the /tmp directory) are counted as files with no owner.
3. Two extra users—**julie** and **guest**—show up in the output of **diskusg** when compared with the output from **acctdusg**. This occurred because the directories of these two users were empty; therefore, no disk usage totals were generated by **acctdusg**. However, **diskusg** looked at inodes and saw that **julie** and **guest** were actually using two blocks for the directories themselves.
4. If two or more users have links to a particular file, then **acctdusg** will prorate disk space usage for the file between each user. For example, if three users had a link to a 300-block file called **skurbnich.dat**, each user would be charged for 100 blocks of this file.

Creating Total Accounting Records

Two commands are used to create total accounting records: `acctdisk`, and `dodisk`.

acctdisk

`acctdisk` uses standard input records of the format produced by `acctdusg` and `diskusg`. From these records, `acctdisk` produces disk total accounting records that may be inputs to `prtacct` or `runacct`.

The following would write disk total accounting records to the file `disktacct` for all users in the group `pseudo`:

```
find / -group pseudo -print | acctdusg | acctdisk > disktacct
```

The next example would generate disk total accounting records for all users who have files on the disk `/dev/rdsk/1s0`. The total accounting records are written to the file `disktacct`.

```
diskusg /dev/rdsk/1s0 | acctdisk > disktacct
```

`acctdisk` has no options and is normally invoked by `dodisk`.

dodisk

`dodisk` is normally invoked by `cron` to create disk total accounting records for daily usage by System Accounting. The syntax for `dodisk` is:

`dodisk` [`-o`] [*files* ...]

In the default case, `dodisk` creates disk total accounting records on the special files whose names are stored in `/etc/checklist`; the special file names are supplied as input to `diskusg`, which pipes its output to `acctdisk`, which in turn creates total accounting records.

If the `-o` option is used, `dodisk` creates total accounting records more slowly by using `acctdusg` instead of `diskusg`.

If *files* are used, disk accounting will be done on these file systems only. When the `-o` option is used, *files* should be mount points of mounted file systems; if omitted, *files* should be the special file names of mountable file systems.

Note Refer to the "Installation and Daily Usage" section of this chapter for more information on how `dodisk` should be invoked by `cron`.

It is possible for malicious users to defeat disk space accounting by giving their files away to other users with *chown(2)* or *chown(1)* (by default, all users can execute them). To avoid this, take away the ability to use these commands from some or all users with the *setprivgrp(1M)* command. To let only the superuser use the change-ownership abilities, add the following line to `/etc/rc`:

```
setprivgrp -n CHOWN
```

To let one or more groups of users use the change-ownership abilities, add a line for each group to `/etc/rc`, similar to the following:

`setprivgrp` *group_name* `CHOWN`

Note Taking away the change-ownership ability may cause problems when running some commands or applications.

Connect Session Accounting

Whenever a user logs in or out of HP-UX, the program `login` records the connect session in the file `/etc/wtmp`. Records in `wtmp` contain the following information:

- the terminal name on which the connect session occurred
- the login name of the user
- the current time/date at login or logout
- other status information (refer to *utmp(4)* for details)

System Accounting provides commands that allow you to write records to `wtmp`, to display and manipulate `wtmp`, and to create total accounting records from `wtmp`. These commands are covered in this section.

Writing Records to wtmp - acctwtmp

The command `acctwtmp` allows you to write records to `wtmp` for whatever reason you might have. `acctwtmp` is normally invoked by `startup` and `shutacct` to record when System Accounting was turned on and off, respectively. The format of the command is:

```
acctwtmp "reason"
```

where *reason* is a string describing the reason for writing the record to `wtmp`. Note that `acctwtmp` does not directly write records to `wtmp`: it writes a record containing the terminal name, current time, and reason string to standard output. To actually write the record to `wtmp` you must append the output from `acctwtmp` to the `wtmp` file as follows:

```
acctwtmp "reason" >>/etc/wtmp
```

The *reason* string may be any combination of letters, numbers, spaces, and the dollar sign ($), but may not exceed 11 characters in length. (*reason* must be enclosed in double quotes as shown.)

Displaying Connect Session Records - fwtmp

To display the contents of `wtmp`, you can use the command `fwtmp`. When no options are used, `fwtmp` uses standard input records of the format contained in `wtmp`; it writes to standard output the ASCII readable equivalent of the input records. Two alternatives exist for the output from this command:

- The output of this command can be edited, via an HP-UX editor such as `vi`, and then rewritten to `wtmp` using special `fwtmp` options described below.
- The output can be supplied as input to commands which convert the information to total accounting records.

The syntax of `fwtmp` is:

```
fwtmp [-ic]
```

If no option is specified for the `fwtmp` command, then input is in binary format and is to be converted to ASCII readable format. The various combinations of the options *i* and *C* provide other combinations of input and output formats. The possible options are described below:

Option	Description
`-ic`	Input is in ASCII readable form and is to be converted to binary form. This is essentially the opposite of using `fwtmp` without any options.
`-i`	Both input and output are in ASCII readable format. This is the same as performing an ASCII to ASCII copy.
`-c`	Both input and output are in binary format—a binary to binary copy.

The following example shows the output produced by `fwtmp`. It is followed by a description of each column in the report:

```
fwtmp < /etc/wtmp
                  system boot    0  2 0000 0000 479472540 Mar 12 03:49:00 1985
root        co console           0  7 0000 0000 479475173 Mar 12 04:32:53 1985
                  acctg on       0  9 0000 0000 479493135 Mar 12 09:32:15 1985
mike        a1 ttya1           352  7 0000 0000 479493590 Mar 12 09:40:00 1985
mike        a1 ttya1           352  8 0011 0000 479496000 Mar 12 10:20:00 1985
sarah       07 tty07           353  7 0000 0000 479518335 Mar 12 16:32:15 1985
bill        10 tty10           351  7 0000 0000 479521475 Mar 12 17:24:35 1985
sarah       07 tty07           353  8 0011 0000 479522478 Mar 12 17:41:18 1985
bill        10 tty10           351  8 0011 0000 479526487 Mar 12 18:48:07 1985
            co console           0  8 0011 0000 479526488 Mar 12 18:48:08 1985
                  acctg off      0  9 0000 0000 479526493 Mar 12 18:48:13 1985
                  system boot    0  2 0000 0000 479389800 Mar 12 05:00:00 1985
```

Column	Description
1	The login name of the user who logged in or out.
2	`/etc/inittab` ID (this is usually the number of the line on which the connect session took place).
3	The name of the device on which the connect session occurred.
4	Process ID of the user who logged in or out.
5	Entry type. This field contains information on the type of record—for example, it shows whether the record is a login record (entry type=7), logout record (entry type=8), or if the record was written by `acctwtmp` (entry type=9). Refer to *utmp(4)* for more details on this field.
6-7	Exit status for connect session. Refer to *login(1)* and *utmp(4)* for details.
8	Time that entry was made (in elapsed seconds since January 1, 1970).
9-12	The equivalent of column 8 in date/time format showing month, day, time of day (in 24-hour format), and year.

Fixing wtmp Errors - wtmpfix

When a user logs into HP-UX, the `login` program stores the value seven (7) in the entry type field of the connect session record. When the same user logs out, an entry type of eight (8) is recorded. You can see this by examining the sample output created by `fwtmp` in the previous section. Note that in the example, login records precede their corresponding logout records in chronological order.

Occasionally, this time-stamped ordering becomes inconsistent: logout records might precede login records. (This occurs when the date and time are reset while users are still logged in.) When this happens, the commands that create connect session total accounting records will not work properly.

Fortunately, the command `wtmpfix` fixes corrupted `wtmp` files. `wtmpfix` takes `wtmp` binary records as input and corrects the time/date stamps to be consistent; its standard output is also binary `wtmp` records. The syntax for `wtmpfix` us:

`wtmpfix` [*files*]

If *files* is given, then input is taken from *files*. A dash (-) can be used in place of *files* to indicate standard input. *Note that if you specify* `wtmp` *as both input to and output from this command,* `wtmp` *will be destroyed.* Therefore, take care not to destroy `wtmp`. The following shows how to properly fix `wtmp` using `wtmpfix`:

```
wtmpfix /etc/wtmp > wtmp.temp
fwtmp -c < wtmp.temp > /etc/wtmp
rm wtmp.temp
```

Creating Total Accounting Records

This final set of connect session accounting commands is used to create connect session total accounting records. Before reading any further, you may want to review Figure 11-5 (in the "System Data Flow" section of this chapter).

acctcon1

`acctcon1` converts a sequence of login/logoff records (of the format contained in `wtmp`) read from its standard input to a sequence of records, one per login session. Its input is normally redirected from `wtmp`; its output is columnar ASCII and can be supplied as input to `prctmp` or `acctcon2`.

The use of `acctcon1` is illustrated below by first displaying the contents of `wtmp` with `fwtmp`, and then using `acctcon1` to create a connect session summary file. `acctcon1`'s columnar data `acctcon1` is described following the report:

```
fwtmp < /etc/wtmp
               system boot    0  2 0000 0000 479472540 Mar 12 03:49:00 1985
root        co console        0  7 0000 0000 479475173 Mar 12 04:32:53 1985
               acctg on       0  9 0000 0000 479493135 Mar 12 09:32:15 1985
mike        a1 ttya1        352  7 0000 0000 479493590 Mar 12 09:40:00 1985
mike        a1 ttya1        352  8 0011 0000 479496000 Mar 12 10:20:00 1985
sarah       07 tty07        353  7 0000 0000 479518335 Mar 12 16:32:15 1985
bill        10 tty10        351  7 0000 0000 479521475 Mar 12 17:24:35 1985
sarah       07 tty07        353  8 0011 0000 479522478 Mar 12 17:41:18 1985
bill        10 tty10        351  8 0011 0000 479526487 Mar 12 18:48:07 1985
            co console        0  8 0011 0000 479526488 Mar 12 18:48:08 1985
               acctg off      0  9 0000 0000 479526493 Mar 12 18:48:13 1985
acctcon1 < /etc/wtmp
20095488    353    sarah   1665    2478    479518335   Tue Mar 12 16:32:15 1985
521012224   352    mike                    479493590   Tue Mar 12 09:40:00 1985
520095488   351    bill    0       5012    479521475   Tue Mar 12 17:24:35 1985
521011712   0      root    41047   6488    479475173   Tue Mar 12 04:32:53 1985
```

Column	Description
1	Shows the device address (in decimal equivalent of major/minor device address) at which the connect session occurred.
2	Gives the user ID for the connect session record.
3	Displays the login name for the user.
4	Shows the number of prime connect time seconds that were used during the connect session.
5	Shows non-prime connect seconds.
6	Displays the connect session starting time (in seconds elapsed since January 1, 1970).
7-11	Shows the conversion of column six to date/time format showing month, day time of day (in 24-hour format), and year.

In addition to its normal usage, `acctcon1` has four options:

Option	Description
`-p`	This option tells **`acctcon1`** not to produce one record per connect session. Instead, `acctcon1` simply echoes its input—one line per **`wtmp`** record—showing line name, login name, and time (in both seconds and day/time format). Using this option is similar to using **`fwtmp`**, except that this option doesn't show status information, whereas **`fwtmp`** does.
`-t`	**`acctcon1`** maintains a list of lines on which users are logged in. When it reaches the end of its input, it emits a session record for each line that still appears to be active. It normally assumes that its input is a current file, so that it uses the current time as the ending time for each session in progress. The `-t` flag causes it to use, instead, the last time found in its input, thus assuring reasonable and repeatable numbers for non-current files.
`-l` *file*	This option causes a line usage summary report to be placed in *file*. This report shows each line's name, number of minutes used, percentage of total elapsed time used, number of sessions charged, number of logins, and number of logins and logoffs. This report can be used to keep track of line usage, identify bad lines, and find software/hardware oddities. *Note that hang-up, termination of* `login`*, and termination of the login shell each generate logoff records; therefore, the number of logoffs is often three to four times the number of connect sessions.*
`-o` *file*	Using the `-o` option (for example, `acctcon1 -o f_overall`) causes *file* to be filled with an overall record for the accounting period, giving starting time, ending time, number of reboots, and number of date changes.

The following example of the line use file (`line_use`) is created from the same `wtmp` file used in the previous `acctcon1` example; the standard output of `acctcon1` has been redirected into the file `ctmp`:

```
acctcon1 -t -l line_use < /etc/wtmp > ctmp
cat line_use
TOTAL DURATION IS 899 MINUTES
LINE    MINUTES PERCENT # SESS  # ON    # OFF
console 856     95      1       1       1
tty07   69      8       1       1       1
ttya1   40      4       1       1       1
tty10   84      9       1       1       1
TOTALS  1049    --      4       4       4
```

prctmp

The `prctmp` command is simple. Its only function is to put headings on the output created by `acctcon1`. `prctmp` makes a readable report from the output of `acctcon1`.

`prctmp` takes its input from standard input; therefore, to create a `prctmp` report from `acctcon1` information, you can simply pipe the output from `acctcon1` into `prctmp` as follows:

```
acctcon1 < /etc/wtmp | prctmp
```

`prctmp` will respond by generating a report with appropriate headings over the columns of output from `acctcon1`.

acctcon2

`acctcon2` creates connect session total accounting records from standard input of the format created by `acctcon1`. In other words, to create connect session total accounting records, simply send the output from `acctcon1` into the input of `acctcon2`.

The total accounting records created by acctcon2 are sent to standard output. So if you want to store these records, you must redirect standard output. The following command line shows how to write total accounting records from the connect session record file (wtmp) into the file ctacct:

```
acctcon1 < /etc/wtmp | acctcon2 > ctacct
```

Process Accounting

Process accounting commands provide the means to accumulate execution statistics—such as memory usage, CPU time, number of input/output transfers—for individual processes. This section describes how to:

1. Turn process accounting on.
2. Turn process accounting off.
3. Make sure that the process accounting file (`pacct`) doesn't become too large.
4. Display process accounting records.
5. Generate a command summary report.
6. Create total accounting records from the process accounting file.

You might find it helpful to look at the System Data Flow Diagram Figure 11-3 before reading this section.

Turning Process Accounting On

Before System Accounting can generate process accounting data, process accounting must be turned on. Two commands can be used to accomplish this task: `turnacct on` and `accton`. After process accounting has been turned on, the kernel will write a process accounting record for every terminating process. The record will be written into the current process accounting file (`pacct` by default).

Note

The `startup` command, placed in the system initialization shell script `/etc/rc`, automatically turns process accounting on. Therefore, if you have updated `/etc/rc` for System Accounting (as described in the section "How to Install System Accounting" in this chapter), process accounting will automatically be activated, and you should seldom need to use the commands described here.

These commands are described for your benefit in case you ever need to manually turn process accounting on or off.

turnacct on

The command used most often to activate accounting is `turnacct on`; only the superuser and the `adm` login can execute this command. `turnacct on` assumes that the process accounting file is the default file `pacct`. The action of `turnacct on` can be summarized as follows:

1. Check to see if the process accounting file `pacct` exists.
2. If `pacct` doesn't exist, then create a new `pacct` file.
3. Turn process accounting on by invoking `accton` with the filename argument `pacct`.

To execute this command, simply enter `turnacct on` at the HP-UX prompt.

accton

Again, only the superuser and the `adm` login can execute `accton`. When invoked with a filename argument, `accton` turns on process accounting and makes the specified filename the current process accounting file. For example,

```
accton /usr/adm/pacct
```

tells the kernel to start writing process accounting records to the file called `/usr/adm/pacct`. The next example would activate process accounting and make the current process accounting file `/usr/adm/XX107`:

```
accton /usr/adm/XX107
```

Note The filename you specify must be an existing file; otherwise, `accton` will fail.

Note that in the Figure 11-3, `accton` is shown calling another routine, `acct`. `acct` is the system call that actually tells the kernel to start writing process accounting records. Refer to the *HP-UX Reference* for more details on *acct(2)*.

Turning Process Accounting Off

Two commands are used to turn process accounting off: `turnacct off` and `accton` (with no filename argument). These commands tell the kernel to stop writing records to the current process accounting file.

Note If you have updated the `/etc/shutdown` shell script as described in the section "How to Install System Accounting" in this chapter, you will seldom, if ever, use these commands. The reason is that the `shutacct` command, added to `/etc/shutdown`, automatically turns process accounting off.

---

turnacct off

`turnacct off` can be executed only by the superuser and the `adm` login. `turnacct off` turns process accounting off by invoking the `accton` command without the optional filename argument. You execute this command by typing:

```
turnacct off
```

accton

When `accton` is invoked without the optional filename argument, process accounting is turned off. You would enter this command as:

```
accton
```

As shown in Figure 11-3, `accton` tells the kernel to stop writing process accounting records by using the system call `acct`.

Checking the Size of pacct

On a multiuser system, many processes can execute during a single hour. Therefore, process accounting files have the potential to become quite large. System Accounting has built-in mechanisms that insure that the default process accounting file `pacct` doesn't become too large. The two commands used for this purpose are: `turnacct switch` and `ckpacct`.

Note The commands described here work only on the default process accounting file, `pacct`.

ckpacct

The command `ckpacct` is normally invoked by `cron` every hour to insure that the current process accounting file `pacct` hasn't become to large. The format of `ckpacct` is:

`ckpacct` [*blocks*]

If the size of `pacct` exceeds the *blocks* argument, 1 000 by default if *blocks* is not specified, then `turnacct switch` is executed. `turnacct switch` renames the current `pacct` file and creates a new `pacct` file.

Note If the amount of free space falls below a certain threshold, `ckpacct` will automatically turn off process accounting via `turnacct off`. With 5.0 HP-UX, accounting was turned off when free space fell below 2%, and back on when it went above 4%. Beginning with 5.1 HP-UX, these percentages are configured using the `acctresume` and `acctsuspend` system parameters (Refer to "Operating System Parameters"). These percentages are in addition to the `minfree` attribute. When free space goes over the specified percentage, process accounting will be reactivated.

The kernel may also enforce a size limit on the size of `pacct`. This will take precedence over the limit set by `ckpacct`. Refer to *acctsh(1M)* and *acct(2)* in the *HP-UX Reference* for more details.

turnacct switch

`turnacct switch` is used to create a new `pacct` file when the current `pacct` file is too large. The action of `turnacct switch` can be summarized as follows:

1. Process accounting is temporarily turned off.
2. The current `pacct` file is renamed to `pacct`*incr*, where *incr* is a number starting at *1* and incrementing by one for each additional `pacct` file that is created via `turnacct switch`.
3. After the old `pacct` file is renamed to `pacctincr`, a new, current `pacct` file is created.
4. Process accounting is restarted; the kernel starts writing records to the newly created `pacct` file.

The example below illustrates the effect of using the `turnacct switch` command. In the example, `turnacct switch` is executed from the `adm` home directory `/usr/adm`. Comment lines begin with a cross-hatch (#) and are included in the example only as explanatory material:

```
$ #
$ # First, list all the process accounting files
$ # (at this point, there is only one).
$ #
ll pacct*
-rw-rw-r--    1 adm     adm      2196 Mar 21 12:44 pacct
$ #
$ # Now execute turnacct switch, which will rename the current
$ # pacct file to pacct1 and will create a new pacct file.
$ #
turnacct switch
$ #
$ # Now verify this by listing all process accounting
$ # files again.
$ #
ll pacct*
-rw-rw-r--    1 adm     adm        72 Mar 21 12:46 pacct
-rw-rw-r--    1 adm     adm      2196 Mar 21 12:44 pacct1
$ #
$ # The current process accounting file is pacct.  The previous
$ # process accounting file is now named pacct1.
$ #
```

Displaying Process Accounting Records - acctcom

The `acctcom` command allows you to display records from any file containing process accounting records. Normally you would use this command to display records from the `pacct` files (`pacct`, `pacct1`, `pacct2` ...).

`acctcom` is a very versatile command; its syntax follows:

`acctcom` [[*options*] [*file*]] ...

If no *file* is specified, `acctcom` uses the current `pacct` file as input. Input can also be taken from standard input. Some of `acctcom`'s options allow you to select only the records that you want to see; other options control the format of the report.

The information contained in this section is organized as follows:

- First, definitions are given for the columnar data produced by `acctcom`.
- Command options that control the format of the report are discussed.
- Options that allow you to select particular records are described.
- Finally, to help you understand how to use `acctcom`'s options, sample `acctcom` reports are shown.

Definitions of Information Produced by acctcom

`acctcom` generates a columnar report with descriptive headings on each column. Each line of the report represents the execution statistics that a particular process accumulated during its lifetime. The standard columns in the report—that is, the columns that are displayed when none of `acctcom`'s options are specified—are shown below:

Column Header	Definition
COMMAND NAME	The name of the command or program that spawned the process is shown here. Whenever you enter a command, you are spawning a process. For example, if you enter the command `ll /usr/lib/acct` you are creating a process with the command name `ll`. If a command requiring superuser privileges is executed, a # appears before the command name.
USER	The login name of the user who created the process is displayed here.
TTYNAME	This is the name of the terminal from which the process was executed. If the process was not executed from a known terminal (for example, if it was executed via `cron`), then a question mark(?) appears in this column.

Column Header	Definition
`START TIME`	The time that the process began executing (in *hh:mm:ss* format) is displayed here.
`END TIME`	This is the time (*hh:mm:ss*) that the process finished executing.
`REAL (SECS)`	The number of seconds that elapsed from `START TIME` to `END TIME` is shown in this column.
`CPU (SECS)`	This column shows how much of the CPU's time a process used during its execution.
`MEAN SIZE(K)`	This is a rough estimate (in kilobytes) of the amount of memory that a process used during execution. This estimate is determined from the current process's memory usage at each system clock interrupt. It is, therefore, subject to statistical sampling errors. Only the memory resident pages of a process are counted; no pages in the swap space are counted. Shared code and data is divided among the processes using it. The size is divided by the number of processes sharing the code or data.

Listed below are the columns that are not displayed on the standard report, but which can be displayed by using `acctcom` options:

Column Header	Definition
`F`	For a process created by **`fork`** which does not do an **`exec`**, this column takes the value *1*; commands which require superuser privileges show a *2*; superuser commands which do a **`fork`** without an **`exec`** show a *3*; otherwise, this column shows a *0*.
`STAT`	This column displays the system exit status. (This is *not* the status returned by **`exit`** to a parent process during **`wait`**). When a process terminates normally, this field shows a *0*. If a command terminates abnormally, then a value other than zero is shown. For example, if you interrupt a command with the DEL key, this column will contain a *2*.
`HOG FACTOR`	The hog factor is computed as the `CPU` time divided by `REAL` time; it provides a relative measure of the available CPU time used by the process during its execution. For example, a hog factor of less than 0.50 indicates that the process spent less than half of its time using the CPU. A hog factor of 0.75 indicates that a process spent 75% of its time using the CPU.
`KCORE MIN`	This calculation provides a combined measurement of the amount of memory used (in kilobytes) and the length of time it was used (in minutes). It is computed as follows: `KCORE MIN = CPU (SECS) * MEAN SIZE(K) / 60`
`CPU SYS`	This is the portion of total CPU time that was spent executing operating system code, such as system calls (for example, writing to disk).
`USER (SECS)`	This is the remaining portion of CPU time. User CPU time is the amount of time actually spent executing a process's code (rather than system code).

Column Header	Definition

`CPU FACTOR`	Whenever you execute a command, the CPU spends part of its time actually executing the command's code (user CPU time) and spends the rest of its time performing system functions, such as writing to the disk or terminal (system CPU time). That is, total CPU time is comprised of both `CPU SYS` and `USER` CPU time:
	`CPU (SECS) = CPU SYS + USER (SECS)`
	The CPU factor shows the ratio of user CPU time to total CPU time:
	`CPU FACTOR = USER (SECS) / (CPU SYS + USER (SECS))`
	For example, if a command has a CPU factor of 0.35, that means that the CPU spent 35% of its time executing user code and 65% performing system functions.

`CHARS TRNSFD`	The number of characters (bytes) read and/or written by the command is displayed in this column.
`BLOCKS R/W`	This column shows the number of file system blocks read and/or written as a result of executing this command. *This number is not directly related to* `CHARS TRNSFD` *and may vary each time the command is executed*, because `BLOCKS R/W` is affected by directory searches made before opening files, other processes accessing the same files, and general file system activity.

Report Format Options

When no report format options are specified, `acctcom` will produce a report containing only the default information. Optional information can be displayed only by using the report format options. Definitions of the report format options follow:

Option	Description
`-a`	Cause average statistics to be displayed at the end of the report. The following information is shown: total number of commands processed (`cmds=xxx`) ■ average real time per process (`Real=x.xx`) ■ average CPU time per process (`CPU=x.xx`) ■ average USER CPU time per process (`USER=x.xx`) ■ average SYS CPU time per process (`SYS=x.xx`) ■ average characters transferred (`CHARS=x.xx`) ■ average blocks transferred (`BLK=x.xx`) ■ average CPU factor (`USR/TOT=x.xx`) ■ average HOG factor (`HOG=x.xx`)
`-b`	Display the process records in reverse order: most recently executed commands will be shown first.
`-f`	Print the `fork/exec` flag (`F` column) and process exit status (`STAT` column) on the report.
`-h`	Cause the optional `HOG FACTOR` column to be displayed, instead of the standard mean memory size column `MEAN SIZE(K)`.
`-i`	Replace the standard `MEAN SIZE(K)` column in the report with the optional I/O counts—`CHARS TRNSFD` and `BLOCKS R/W`.
`-k`	Replace the standard `MEAN SIZE(K)` column with `KCORE MIN`.

Option	Description
-m	Show the default column MEAN SIZE(K) on the report. This option is used to include MEAN SIZE(K) when it has been bumped off by another option. The following example: produces a report showing both KCORE MIN and MEAN SIZE(K). acctcom -km
-r	Include the optional CPU FACTOR column in the report.
-t	Show separate system and user CPU times (CPU SYS and USER (SECS), respectively).
-v	Suppress the printing of column headings at the top of the report.
-q	This option is the same as the -a option, except that individual process accounting records are not displayed—only the averages are displayed.
-o *ofile*	Copy the input process accounting records to *ofile*.

Record Selection Options

The options described here allow you to select the records that are included in the report produced by `acctcom`. For each option, descriptions and examples are provided:

Option	Description
`-l` *line*	Display only the processes that were executed from the user terminal `/dev/`*line*. For example: `acctcom console` would display records only for the processes that were created from the terminal **console**.
`-u` *user*	Show only the processes belonging to *user*. *user* can be any of the following: ■ a user ID (for example, `acctcom -u 355`) ■ user name (`acctcom -u julie`) ■ a cross-hatch # (`acctcom -u#`) ■ a question mark *?* (`acctcom -u?`) If # is specified as the user name, then only the commands that require superuser privileges will be displayed by acctcom. If *?* is given as the user, then only the processes with unknown process IDs will be displayed. As an example, the following two commands are equivalent: `acctcom -u 0` `acctcom -u root`
`-g` *group*	Show only the processes belonging to *group*. *group* may be specified as either a group name or group ID. For example, suppose the group **pseudo** with group ID **300** is defined in **/etc/group**; then the following two commands are equivalent: `acctcom -g 300` `acctcom -g pseudo`

Option	Description
`-s` *time*	Select processes existing *at or after time*. Time is given in 24-hour format—*hr*[:*min*[:*sec*]]. The following example would display all the processes that existed at or after 3:30pm: `acctcom -s 15:30`
`-e` *time*	Select processes that existed *at or before time*. Time is supplied in 24-hour format *hr*[:*min*[:*sec*]]. The next example would display all the processes that existed between midnight and 12:15am: `acctcom -e 0:15`
`-S` *time*	Select processes *starting* at or after time where *time* is in 24-hour format. The following example would display all the processes that *started* at 1:30:42pm or after: `acctcom -S 13:30:42`
`-E` *time*	Display only the processes that *terminated* at or before *time*, where time is in 24-hour format *hr*:[*min*[:*sec*]]. Note both the `-S` and `-E` options with the same *time* argument will cause **acctcom** to display only the processes that existed at the specified *time*. For example, to see all the processes that existed at exactly 30 minutes past noon, you would enter: `acctcom -S 12:30 -E 12:30`
`-n` *pattern*	Show only the commands matching *pattern*. *pattern* can be a regular expression as described in *ed(1)*, except that + means one or more occurrences. For example, to display all processes that were created by executing the `ls` command, you would enter: `acctcom -n ls` To display all the commands that start with **acct**, enter: `acctcom -n acct` To see all the commands that contain the letter *m* in their spelling you can use the wild card character *. Type: `acctcom -n .*m.*`

Option	Description
`-H` *factor*	Display only those processes whose hog factor exceeds *factor*. For example, `acctcom -H 0.85` would display all the processes that spent over 85% of their execution time in the CPU. You can use this option to find greedy processes—processes that are hogging the CPU.
`-O` *time*	Show only those processes whose system CPU time exceeds *time*, specified in seconds. The following example would be used to determine which processes took more than 8.25 seconds of operating system CPU time to execute: `acctcom -O 8.25` This option could be used to determine which processes are making heavy use of the operating system calls.
`-C` *sec*	Show only the processes whose total CPU time (`SYS + USER`) exceeds *sec* seconds. The next example would display all the processes that used over 5.28 seconds of CPU time to execute: `acctcom -C 5.28`
`-I` *chars*	Display only the processes transferring more characters than the limit given by *chars*. For example, `acctcom -I 10240` will display all the processes that transferred over ten kilobytes of characters (10 240 = 10 × 1 024 bytes).

Sample Reports

The following sample report illustrates the use of `acctcom` without any options. The report generated is the standard report produced when no options are specified:

```
acctcom
ACCOUNTING RECORDS FROM:  Thu Mar 21 12:52:26 1985
COMMAND                          START    END           REAL     CPU    MEAN
NAME       USER      TTYNAME   TIME     TIME         (SECS)  (SECS) SIZE(K)
#accton    root      console   12:52:26 12:52:26       0.12     0.10   19.00
ls         sarah     tty07     14:04:08 14:04:08       0.28     0.23   16.50
ckpacct    adm       ?         14:30:00 14:30:05       5.13     1.45   24.00
pwd        bill      tty10     15:09:07 15:09:07       0.48     0.22   22.50
find       sarah     tty07     18:51:37 18:51:39       2.73     0.15   26.50
tabs       root      console   19:10:18 19:10:18       0.92     0.13   23.50
stty       root      console   19:10:19 19:10:19       0.88     0.08   26.00
mail       bill      tty10     19:10:21 19:10:22       1.78     0.23   28.50
news       root      console   19:10:23 19:10:23       0.73     0.12   23.00
acctcom    adm       ttya0     19:53:16 19:53:38      22.58     2.55   28.50
```

The next example displays all the processes created between 7:00pm and 7:30pm by the user `root`. In addition, the optional CPU factor and average statistics are included in the output:

```
acctcom -S 19:00 -E 19:30 -u root -ah
START AFT: Thu Mar 21 19:00:00 1985
END BEFOR: Thu Mar 21 19:30:00 1985
COMMAND                          START    END           REAL     CPU     HOG
NAME       USER      TTYNAME   TIME     TIME         (SECS)  (SECS)  FACTOR
tabs       root      console   19:10:18 19:10:18       0.92     0.13    0.14
stty       root      console   19:10:19 19:10:19       0.88     0.08    0.09
news       root      console   19:10:23 19:10:23       0.73     0.12    0.16
cmds=3 Real=0.84   CPU=0.11   USER=0.02    SYS=0.09    CHAR=26.12    BLK=11.50
USR/TOT=0.19 HOG=0.13
```

Sample reports are helpful, but the best way to learn the various `acctcom` options is to use them. Take a few minutes to experiment with this command; it is very powerful and can provide you with much useful information if used properly.

Command Summary Report - acctcms

The `acctcms` command takes process accounting records as input; but instead of reporting on the individual processes, `acctcms` generates a report on the commands that generated the process accounting records. The action of `acctcms` can be summarized as follows:

1. `acctcms` looks through the input process accounting records and accumulates execution statistics for each unique command name. This information is stored in internal summary format—one record per command name.
2. Depending on the `acctcms` options used, the command summary records created in step 1 are sorted.
3. The command summary records are written to standard output in the internal summary format mentioned in step 1. This format is not readable.

The syntax of the `acctcms` command is:

`acctcms` [*options*]`files`

where *files* is a list of the input process accounting files for which the command summary report is to be generated. The *options* are discussed in the following sections.

Producing a Readable Report - the -a option

By default, the output of `acctcms` is in internal summary record format; if you display it to your terminal, all you see is gibberish. To get a ASCII, readable report, use the `-a` option.

The `-a` option causes `acctcms` to produce a report with descriptive column headings. Total and average (mean) execution statistics for each command are displayed—one line per command—along with total and average statistics over all commands in the report. Descriptions of the columnar data produced by `acctcms` are shown in the following table.

Column Header	Description
COMMAND NAME	The name of the command for which execution statistics are summarized. Unfortunately, all shell procedures are lumped together under the name **sh**, because only object modules are reported by the process accounting system.
NUMBER CMDS	The total number of times that the command was invoked.
TOTAL KCOREMIN	The total amount of kcore minutes accumulated for the command. (Refer to the section "Definitions of Information Produced by acctcom" in this chapter for a more complete description of kcore minutes.)
TOTAL CPU-MIN	The total CPU time that the named command has accumulated.
TOTAL REAL-MIN	Total accumulated real time minutes are displayed in this column.
MEAN SIZE-K	The average amount of memory (in kilobytes) consumed by the command.
MEAN CPU-MIN	The average CPU time consumed per command invocation is shown here; the following equation shows how it is computed: `MEAN CPU-MIN = TOTAL CPU-MIN / NUMBER CMDS`
HOG FACTOR	The average hog factor over all invocations of the command. It is computed as: `HOG FACTOR = TOTAL CPU-MIN / TOTAL REAL-MIN`
CHARS TRNSFD	The total number of characters transferred by the command. Note that this number may sometimes be negative.
BLOCKS READ	A total count of the physical blocks read and written by the given command. (Refer to the section "Displaying Process Accounting Records—acctcom" in this chapter for details on the significance of this total.)

Note When only the `-a` option is specified, the report is sorted in descending order on the `TOTAL KCOREMIN` column: commands using more `TOTAL KCOREMIN` are shown before those using fewer `TOTAL KCOREMIN`. This report gives a relative measure of the amount of memory used over time by the various commands: commands toward the start of the report are making more use of memory resources than are commands toward the end of the report.

Other Options

In addition to the `-a` option, several other options can be used to control the format of the report generated by `acctcms`. Some options specify which field to sort the report on; other options control the printing of prime/non-prime time usage. The options and a description of their use follow:

Option	Description
`-c`	Sort the commands in descending order on `TOTAL CPU-MIN`, rather than the default `TOTAL KCOREMIN`. This report can be used to determine which commands are using most of the computer's CPU time.
`-n`	Cause the report to be sorted in descending order on the column named `NUMBER CMDS`. Commands toward the start of this report are the ones used most frequently; commands toward the end are used least often.
`-j`	Combine all commands invoked only once on one line of the report. This line is denoted by having "`***other`" in the `COMMAND NAME` column. This option is useful for shortening a report that has many one-invocation commands.
`-o`	*Used only with the* `-a` *option*, `-o` causes the report to be generated only for commands that were executed during non-prime time (as specified in the `holidays` file). You can use this option to get a non-prime time command summary report.
`-p`	*Also used only with the* `-a` *option*, `-p` elicits a report generated only for commands that were executed during prime time (as specified in `holidays`). This option is used to get a prime time command summary report.

Option	Description
-apo	When the options -o and -p are used together with -a, a combination prime and non-prime time report is produced. The output of this report is same as that produced by -a alone, except that the NUMBER CMDS, TOTAL CPU-MIN, and TOTAL REAL-MIN columns are divided into two columns—one for prime time totals, the other for non-prime time. (Prime time columns have a (P) header, while non-prime time columns are headed by (NP).)

-s [*files*]	Specifies that any named input *files* following the -s on the command line are already in internal summary format. This option is useful for merging previous acctcms reports with current reports. The following example uses -s to create a command summary report from previous process accounting files (pacct?) and the current process accounting file (pacct). The final ASCII report is stored in the file ascii_summary.
	`acctcms pacct? > old_summary`
	`acctcms pacct > new_summary`
	`acctcms -as old_summary new_summary > ascii_summary`

Sample Report

The ASCII reports produced by acctcms contain more than 80 characters per line. When these reports are displayed at an 80-column terminal, the lines wrap around on the screen. In addition, if the report is printed on an 80-column printer, some of the rightmost columns will be lost. Therefore, be sure to do one of the following:

- Use a printer with compressed print capabilities, so that all of the report will fit on standard computer paper.
- Use a printer with enough columns to display all the information—for example, a 132-column printer.

The following example generates a command summary report for the current process accounting file (no file is specified, so the current `pacct` file is assumed). By giving the `-j` option, all the commands that were executed only once are grouped under the command name `***other`. Note also that total execution statistics for all commands are grouped under the command name `TOTALS`.

```
acctcms -aj
                                TOTAL COMMAND SUMMARY
COMMAND NUMBER    TOTAL    TOTAL      TOTAL  MEAN      MEAN     HOG    CHARS BLOCKS
NAME      CMDS KCOREMIN  CPU-MIN REAL-MIN SIZE-K   CPU-MIN   FACTOR TRNSFD   READ

TOTALS      61    17.63   0.38       164.49  46.25     0.01     0.00 104553   1027

acctcms     17    12.13   0.16         0.35  76.72     0.01     0.45  49192    306
sh           8     2.43   0.09       152.86  26.79     0.01     0.00   9043    163
more         3     0.73   0.02        10.50  31.00     0.01     0.00  21618     83
ll           6     0.61   0.04         0.11  16.50     0.01     0.33   5715     95
acctcom      4     0.58   0.02         0.07  28.50     0.01     0.30  15319     42
***other     9     0.54   0.02         0.14  25.26     0.00     0.16    459    161
cat          4     0.19   0.01         0.35  22.97     0.00     0.02   3112     52
rm           2     0.11   0.00         0.02  22.22     0.00     0.29      0     29
chmod        2     0.10   0.00         0.01  22.00     0.00     0.35      0     15
accton       2     0.08   0.00         0.02  19.00     0.00     0.29      0     22
sed          2     0.08   0.01         0.04  14.50     0.00     0.13     73     38
echo         2     0.05   0.00         0.02  20.00     0.00     0.16     22     21
```

Creating Total Accounting Records

Two commands—`acctprc1` and `acctprc2`—are used to create total accounting records from the process accounting files. The output from `acctprc1` is supplied as input to `acctprc2` which produces the total accounting records. These commands are normally invoked by `runacct` to produce daily accounting information.

acctprc1

This command reads process accounting records from standard input, adds login names corresponding to the user ID of each record, and then writes for each process an ASCII line showing:

- the ID of the user that created the process
- the user's login name
- prime CPU time in ticks (a "tick" is one fiftieth of a second)
- non-prime CPU time, also in ticks
- mean memory size (in pages—4 Kbytes per page)

The format of `acctprc1` is:

`acctprc1` [*ctmp*]

where `ctmp` contains a list of login sessions of the form created by `acctcon1`, sorted by user ID and login name.

Note The number of sessions should be 1000 or less. If there are more than 1000 sessions, the accounting system "hangs"—i.e., suspends indefinitely—and must be killed manually (via the `kill` command) and restarted.

To use `acctprc1`, input must be redirected from a process accounting file. The following example creates a file, `ascii_ptacct`, containing ASCII process accounting information that can be used to create process total accounting records. This file is created from the current process accounting file `pacct`.

```
acctprc1 <pacct >ascii_ptacct
```

Normally, `acctprc1` gets login names from the password file `/etc/passwd`, which is sufficient on systems where each user has a unique user ID. However, on systems where different users share the same user ID, the `ctmp` file should be specified; it helps `acctprc1` distinguish different login names that share the same user ID.

acctprc2

This command reads from standard input records of the form created by acctprc1; it then summarizes the records by user ID and name, and writes the sorted summaries to standard output as total accounting records. The following example creates total accounting records for all processes in the current process accounting file pacct; the total accounting records are stored in the file ptacct.

```
acctprc1 <pacct |acctprc2 >ptacct
```

Charging Fees to Users – chargefee

System Accounting provides the capability to charge fees to specific users; the `chargefee` command is used to accomplish this task. `chargefee` allows you to charge generic *units* to a specific login name. The syntax of this command is:

`chargefee` *login_name number*

where *number* is the number of units to be charged to a particular user, and *login_name* is the login name of the user to whom *number* units are to be charged.

Note *number* can be any whole number in the range -32 768 to 32 767; when charging fees, keep in mind that the sum of each user's fees must also be within this range.

`chargefee` accumulates fee charge records in the file `/usr/adm/fee`. These records are then merged with other accounting records via `runacct`.

The following example charges 25 units to the user whose login name is `julie`:

```
chargefee julie 25
```

Suppose you inadvertently charged 247 units to the user named `zimblits`, and you want to return his charges to their original value. You would enter the following:

```
chargefee zimblits -247
```

Summarizing and Reporting Accounting Information

This final group of commands summarizes and reports accounting information. Certain commands display and merge total accounting files, while others generate the daily and monthly reports used to analyze system performance and bill users for resource usage. The following commands are discussed in this section:

- `prtacct`—displays total accounting records
- `acctmerg`—merges total accounting files
- `runacct`—generates daily summary files and reports
- `prdaily`—displays the daily summary files and reports created by `runacct`
- `monacct`—creates monthly summary files and reports

Displaying Total Accounting Records - prtacct

The `prtacct` command allows you to display the contents of a process accounting file. Its format is

`prtacct` *file* "*heading*"

where:

- *file* is the name of the total accounting file to be displayed.
- "*heading*" is a comment to be included in the standard report header produced by `prtacct`.

The format of the `prtacct` report is described next and is followed by an example.

Report Format

`prtacct` produces a columnar report with one line per total accounting record. Descriptive column headings are included in the report. Definitions of each column follow:

Column Header	Description
`UID`	This column shows the user ID of the owner of the total accounting record—that is, the ID of the user for whom the total accounting record was created.
`LOGIN NAME`	The login name of the owner of the total accounting record is displayed here.
`CPU (MINS)`	This column shows the total amount of CPU time (in minutes) that the user has consumed. This column is divided into prime and non-prime columns (`PRIME` and `NPRIME`, respectively). Information in these columns is created through process accounting commands.
`KCORE-MINS`	This represents a cumulative measure of memory and CPU time that a user consumed (refer to the section "Definitions of Information Produced by acctcom" in this chapter for a more precise definition). Information in this column is also divided into `PRIME` and `NPRIME` columns. This information is created through process accounting commands.
`CONNECT (MINS)`	This identifies the real time used (in minutes). In essence, what this column identifies is the amount of time that the user was logged in to the system. This column is also subdivided into `PRIME` and `NPRIME` columns. The connect session accounting commands are the source of this information.
`DISK BLOCKS`	The total number of disk blocks allocated to the user is shown here. This information is created via disk space accounting commands.
`# OF PROCS`	The total number of processes spawned by the user is displayed here. This information is created via the process accounting commands.

Column Header	Description
# OF SESS	This column shows how many times the user logged in. Connect session accounting commands create this data.
# DISK SAMPLES	This column indicates how many times the disk accounting was run to obtain the average number of disk blocks listed in the DISK BLOCKS column.
FEE	The number of fee units charged via **chargefee** is displayed here.

Example

The following example displays disk total accounting records. First, the total accounting records are created via disk space accounting commands; then, they are displayed using `prtacct`. When examining this report, take note of the following:

- There are many similarities between this and the sample report produced by `diskusg` (refer to the section "Disk Space Usage Accounting" in this chapter).
- Only the columns relating to disk space usage have non-zero values, because the total accounting records were created only from disk space usage accounting commands.

The example report produced by `prtacct` follows:

```
for file_system in 'cat /etc/checklist'
> do
> diskusg $file_system >dtmp.'basename $file_system'
> done
diskusg -s dtmp.* |sort +0n +1 |acctdisk >disktacct
prtacct disktacct "DISC TOTAL ACCOUNTING RECORDS"

Mar 26 17:01 1985  DISC TOTAL ACCOUNTING RECORDS Page 1

    LOGIN   CPU (MINS)   KCORE-MINS   CONNECT (MINS) DISK   # OF  # OF # DISK FEE
UID NAME   PRIME NPRIME PRIME NPRIME PRIME   NPRIME BLOCKS PROCS SESS SAMPLES
0   TOTAL  0     0      0     0      0       0      11598  0     0    10       0
0   root   0     0      0     0      0       0      10616  0     0    1        0
1   bin    0     0      0     0      0       0      778    0     0    1        0
4   adm    0     0      0     0      0       0      96     0     0    1        0
350 fred   0     0      0     0      0       0      14     0     0    1        0
351 bill   0     0      0     0      0       0      32     0     0    1        0
352 mike   0     0      0     0      0       0      20     0     0    1        0
353 sarah  0     0      0     0      0       0      16     0     0    1        0
354 molly  0     0      0     0      0       0      22     0     0    1        0
355 julie  0     0      0     0      0       0      2      0     0    1        0
501 guest  0     0      0     0      0       0      2      0     0    1        0
```

Merging Total Accounting Files - acctmerg

Normally executed by `runacct`, the `acctmerg` command merges separate total accounting files into a single total accounting file. All the total accounting records for a particular user name and ID are merged together to form one total accounting record for the given user name and ID. This command is useful for merging disk, connect session, and process total accounting files together to form a single, comprehensive total accounting file.

`acctmerg` reads standard input and up to nine additional files, all in total accounting record format. Its syntax is:

`acctmerg` [*options*] [*file*] ...

where:

- *options* control the report format and the manner in which records are merged.
- *file* is one of up to nine files (in addition to standard input) that are to be merged into a single total accounting file, written to standard output.

Command Options

The following options may be used with **acctmerg** to control the report format and the manner in which the total accounting records are merged:

Option	Description
-a	**acctmerg** normally produces output as total accounting records. The **-a** option causes **acctmerg** to produce output in ASCII. Note that the output generated by using this option is the same as the report produced by **prtacct**, except that no report headings or totals are displayed—only the columnar data is shown.
-i	In the default case, **acctmerg** assumes that its input files contain total accounting records. If **-i** is specified, then **acctmerg** will expect input files to be in the ASCII format created by the **-a** option.
-p	This option simply echoes input records—no merging or processing is done. The output is displayed in the format produced by the **-a** option.
-t	This option produces a single total accounting record that summarizes all input records. To see the ASCII version of this record, you must use the **-t** and **-a** options together:

```
acctmerg -t -a <tot_acct_recs
```

Note that **-t** *and* **-a** *can be specified in any order, but they must be specified separately as shown.*

Option	Description
-u	Normally, **acctmerg** merges records that have the same user ID and user name. Using **-u** causes **acctmerg** to merge records on the basis of same user ID only—that is, the user name is disregarded as a key on which to merge records.
-v	This option causes **acctmerg** to produce output in verbose ASCII format. The same report is produced as the **-a** option, except that floating point numbers are displayed in more precise notation:

<mantissa>e<exponent>

Use the `-a`, `-v`, and `-i` options to edit total accounting records. For example, if you created a total accounting file (`ptacct`) containing process total accounting records, and you want to make some adjustments to these records, use the following sequence to "repair" this file:

```
acctmerg -v -a <ptacct >ptacct.ascii
```
edit ptacct.ascii as desired ...

```
acctmerg -i <ptacct.ascii >ptacct
```
then copy the changes back to ptacct

Example

The following example creates disk, process, and connect session total accounting records, merges them together, and stores the merged file in the file `merged_file`:

```
for fs in `cat /etc/checklist`
> do
> diskusg $fs >dtmp.`basename $fs`
> done
diskusg -s dtmp.* |sort +0n +1 |acctdisk >dtacct
```
First, create disk space usage total accounting records (dtacct)

```
acctcon1 </etc/wtmp |acctcon2 >ctacct
```
Now create the connect session total accounting records (ctacct)

```
ptacct
for p_file in pacct*
> do
> acctprc1 <$p_file |acctprc2 >>ptacct
> done
```
Create process total accounting records (ptacct)

```
acctmerg dtacct ctacct <ptacct >tacct
$
```

Now merge all the total accounting files into a single total accounting file (tacct)

Creating Daily Accounting Information - runacct

runacct is the main daily accounting shell procedure. Start runacct via cron during non-prime hours, when users are logged off. This is because it does not correctly log time for users that log on before running runacct.

runacct processes disk, connect session, process, and fee accounting files. It prepares cumulative summary files for use by prdaily and for billing purposes. This section discusses the following aspects of runacct:

- files processed by runacct
- the states that runacct progresses through while executing
- recovery from runacct failure
- restarting runacct
- reports produced by runacct

Files Processed by runacct

The following files, processed by runacct, are of particular interest to the reader. (Filenames are given relative to the directory /usr/adm/acct.)

- nite/lineuse contains usage statistics for each terminal line on the system. This report is especially useful for detecting bad lines. If the ratio of logoffs to logins on a particular line exceeds 3 to 1, then there is a good possibility that the line is failing.
- nite/daytacct contains total accounting records from the previous day.
- sum/tacct contains accumulated total accounting records for each day's total accounting records (nite/daytacct) and can be used for billing purposes. It is restarted each month or fiscal period by the monacct shell script.
- sum/daycms is produced by acctcms. It contains the daily command summary. The ASCII version of this file is in nite/daycms.
- sum/cms holds the accumulation of each day's command summaries (sum/daycms). A new sum/cms file is created each month by monacct. The ASCII version of this file is in nite/cms.
- sum/loginlog maintains a record of the last time each user logged in.

- `sum/rprt`*mmdd* is the main daily accounting report created by `runacct`. The name for this report is created automatically by the system with *mm* being the month and *dd* the day of the report. This report can be printed via `prdaily`.

`runacct` takes care not to damage files in the event of errors. A series of protection mechanisms are used that attempt to recognize errors, provide intelligent diagnostics, and terminate processing in such a way that `runacct` can be restarted with minimal intervention. To accomplish these goals, the following actions are performed by `runacct`:

- `runacct`'s progress is recorded by writing descriptive messages to the `nite/active` file.
- All diagnostics output during the execution of `runacct` are redirected to the file `nite/fd2log`.
- If the files `lock` and `lock1` exist when `runacct` is invoked, an error message will be displayed, and execution will terminate.
- The `lastdate` file contains the month and day that `runacct` was last run and is used to prevent more than one execution per day.
- If `runacct` detects an error, a message is written to `/dev/console`, mail is sent to `root` and `adm`, locks are removed, diagnostics files are saved, and execution is terminated.

The States of runacct

In order to allow `runacct` to be restartable, processing is broken down into separate re-entrant *states*. As `runacct` executes, it records its progress by writing the name of the most recently completed state into the file called `/usr/adm/statefile`. After processing for a state is complete, `runacct` examines `statefile` to determine which state to enter next. When `runacct` reaches the final state (`CLEANUP`), the `lock` and `lock1` files are removed, and execution terminates. `runacct`'s states are described in the next table.

State	Action
SETUP	The command **turnacct switch** is executed. The process accounting files, **pacct?**, are moved to **Spacct?.***mmdd*. The **/etc/wtmp** file is moved to **nite/wtmp.***mmdd* with the current time added on the end.
WTMPFIX	**nite/wtmp.***mmdd* is checked for correctness by **wtmpfix**. Some date changes will cause **acctcon1** to fail, so **wtmpfix** attempts to adjust the time stamps in the **nite/wtmp.***mmdd* file if a date change record appears.
CONNECT1	Connect session records are written to **ctmp**. The **lineuse** file is created, and the **reboots** file, showing all of the boot records found in **nite/wtmp.***mmdd*, is created.
CONNECT2	**ctmp** is converted to connect session total accounting records in the file **ctacct.***mmdd*.
PROCESS	The **acctprc1** and **acctprc2** programs are used to convert the process accounting files, **Spacct?.***mmdd*, to the total accounting records in **ptacct?.***mmdd*. The **Spacct** and **ptacct** files are correlated by number so that if **runacct** fails, the unnecessary reprocessing of **Spacct** files will not occur. One precaution should be noted: *when restarting* **runacct** *in this state, remove the last* **ptacct** *file; if you don't,* **runacct** *will not finish.*
MERGE	Merge the process and connect session total accounting records to form **nite/daytacct**.
FEES	Merge in any ASCII **tacct** records from the file **fee** into **nite/daytacct**.
DISK	On the day after the **dodisk** shell script runs, merge **nite/disktacct** with **nite/daytacct**.
MERGETACCT	Merge **nite/daytacct** with **sum/tacct**, the cumulative total accounting file. Each day, **nite/daytacct** is saved in **sum/tacct***mmdd*, so that **sum/tacct** can be recreated in the event it becomes corrupted or lost.
CMS	Merge in today's command summary with the cumulative summary file **sum/cms**. Produce ASCII and internal format command summary files.

State	Action
USEREXIT	Any installation-dependent (local) accounting programs can be run in this state. For example, you might want to execute commands that generate daily billing data for individual users (the shell script acct_bill in the section "Sample System Accounting Shell Scripts" could be used for this purpose). To have local accounting programs executed by runacct, simply enter the commands in runacct in the code for the USEREXIT state of runacct.
CLEANUP	Clean up the temporary files, run prdaily and save its output in the file sum/rprt*mmdd*, remove the locks, then exit.

Recovering from Failure

It is possible that runacct might fail and terminate abnormally. The primary reasons for runacct failure are:

- a system "crash"
- not enough disk space remaining in /usr
- a corrupted wtmp file

If the nite/active*mmdd* file exists, check it first for error messages. If the nite/active file and lock files exist, check fd2log for any mysterious messages. The following are error messages produced by runacct and the recommended recovery actions:

```
ERROR: locks found, run aborted
```

The files lock and lock1 were found. These files must be removed before runacct can be restarted.

ERROR: acctg already run for *date*: check /usr/adm/acct/nite/lastdate

The date in lastdate and today's date are the same. Remove lastdate before restarting runacct.

ERROR: turnacct switch returned rc=*?*

Check the integrity of turnacct and accton. The accton program must be owned by root and have the setuid bit set.

ERROR: Spacct?.*mmdd* already exists

File setups have probably already run. Check the status of files, then run setups manually.

ERROR: `/usr/adm/acct/nite/wtmp.`*mmdd* `already exists, run setup manually`

You must perform the `SETUP` step manually, because the daily `wtmp` file already exists.

```
ERROR: wtmpfix errors see /usr/adm/acct/nite/wtmperror
```

`wtmpfix` detected a corrupted `wtmp` file. Refer to the section "Fixing Corrupted Files" in this chapter for details on fixing `wtmp` errors.

```
ERROR: connect acctg failed: check /usr/adm/acct/nite/log
```

`acctcon1` encountered a bad `wtmp` file. Again, refer to the section "Fixing Corrupted Files" in this chapter for information on how to fix the file.

```
ERROR: Invalid state, check /usr/adm/acct/nite/active
```

the file `statefile` is probably corrupted. Check `statefile` and read `active` before restarting.

Restarting runacct

`runacct` is normally run via `cron` only once per day. However, if an error occurs while executing `runacct` (as described above), it may be necessary to restart `runacct`. `runacct` has the following syntax:

`runacct` [*state*]

`runacct` assumes that it is being invoked for the first time on the current day. The entry point for processing is based on the contents of `statefile`. To override `statefile`, include the desired entry *state* on the command line.

For example, to start `runacct`, you would enter:

```
nohup runacct 2> /usr/adm/acct/nite/fd2log &
```

To restart `runacct` at state `WTMPFIX`:

```
nohup runacct WTMPFIX 2>/usr/adm/acct/nite/fd2log &
```

All the above examples were run in the background (`&`) and use the `nohup` command so the process continues running even though you may log out.

Daily Reports

`runacct` generates five basic reports upon each invocation. Brief descriptions of each report follow. Detailed descriptions of the reports are found in the following section, "Displaying runacct Reports—prdaily."

- **Daily Line Usage Report**—summarizes connect session accounting since the last invocation of `runacct`. It provides a log of system reboots, power failure recoveries, and any other records dumped into `/etc/wtmp` via `acctwtmp`. In addition, it provides a breakdown of line utilization.
- **Daily Resource Usage Report**—gives a summary of resource usage per individual user: it basically merges all the total accounting records for individual users and displays the records, one per user.
- **Daily Command Summary**—summarizes resource usage data for individual commands since the last invocation of `runacct`. The data included in this report is useful in determining the most heavily used commands; you can use these commands' characteristics of resource utilization when "tuning" your system.

  This report is sorted by `TOTAL KCOREMIN`, an arbitrary but useful yardstick for calculating "drain" on a system.
- **Monthly Total Command Summary**—This report is exactly the same as the Daily Command Summary, except that the Daily Command Summary contains command summary information accumulated only since the last invocation of `runacct`, while the Monthly Total Command Summary summarizes commands from the start of the fiscal period to the current date. In other words, the monthly report reflects the data accumulated since the last invocation of `monacct`.
- **Last Login**—simply gives the date each user last logged in to the system. This could be a good source for finding likely candidates for the archives, or getting rid of unused login directories.

Displaying runacct Reports - prdaily

As `runacct` finishes executing, it deposits a report of the current day's accounting in the file `/usr/adm/acct/sum/rptmmdd`, where *mmdd* is the month and day that the report was generated. The `prdaily` command is used to display the contents of any daily report file created by `runacct`. Its syntax is:

`prdaily` [`-l`][`-c`][*mmdd*]

where:

- *mmdd* is an optional report date. If no date is specified, `prdaily` produces a report of the current day's accounting information. Previous days' accounting reports can be displayed by using the *mmdd* option and specifying the exact report date desired.
- The `-l` option prints a report of exceptional usage by login name for the specified date. This option is used to determine which users are consuming excessive amounts of system resources. The limits for exceptional usage are kept in the file `/usr/lib/acct/ptelus.awk` and can be edited to reflect your installation's requirements.
- Valid only for the current day's accounting, the `-c` option is used to get a report of exceptional resource usage by command. This option is used to determine which commands are using excessive amounts of system resources. The limits for exceptional usage are maintained in the file `/usr/lib/acct/ptecms.awk` and can be edited to reflect your system's needs.

The reports produced by `runacct` were described briefly in the previous sub-section. Now the reports are discussed in more detail.

Daily Line Usage Report

In the first part of this report, the `FROM/TO` banner should alert you to which period is being reported. The times are the date-time that the last report was generated by `runacct`, and the date-time that the current report was generated. It is followed by a log of system reboots, shutdowns, power failure recoveries, and any other records dumped into `wtmp` by the `acctwtmp` command.

The second part of the report is a breakdown of line utilization. The `TOTAL DURATION` shows how long the system was in a multiuser state. The columns of the report are defined as follows:

Column	Description
`LINE`	The terminal line or access port being reported on.
`MINUTES`	The total number of minutes that the line was in use during the accounting period.
`PERCENT`	The percentage of `TOTAL DURATION` that the line was in use: `PERCENT = (MINUTES / TOTAL DURATION) * 100`
`# SESS`	The number of times that this port was accessed for a `login` session.
`# ON`	Historically, this column displayed the number of times that the port was used to log a user on; but since `login` can no longer be executed explicitly to log in a new user, this column should be identical to `# SESS`.
`# OFF`	This column reflects not only the number of times a user logged off, but also any interrupts that occurred on the line. Interrupts occur on a port when `getty` is first invoked. A `getty` is invoked when the system is brought to run-level 2. This column comes into play when `# OFF` exceeds `# ON` by a large factor. This usually indicates that the multiplexer, modem, or cable is going bad, or that there is a bad connection somewhere. The most common cause of this is an unconnected cable dangling from the multiplexer.

During real time, `wtmp` should be monitored as this is the file from which connect session accounting is taken. If it grows rapidly, execute `acctcon1` to determine which line is the noisiest. If the interrupting is occurring at a high rate, general system performance will be affected.

Daily Resource Usage Report

This report gives a by-user breakdown of system resource usage. The format of this report is the same as that produced by the `prtacct` command. (For definitions of the data and format of this report, refer to the discussion of `prtacct` in the "Displaying Total Account Records – prtacct" section of this chapter.)

Daily and Monthly Command Summary

These two reports are the same, except that the Daily Command Summary reports information only for commands executed since the last invocation of `runacct`; the Monthly Command Summary contains information on commands executed since the last invocation of `monacct`.

The output of this report is identical to that produced by `acctcms`. For definitions of the data found in this report, refer to the discussion of `acctcms` in the "Process Accounting" section of this chapter.

Last Login

This report simply shows the last date and time that each user logged in. The longer it has been since a particular user logged in, the more likely it is that the user's files could be archived, or maybe even that the user could be removed from the system.

Creating Monthly Accounting Reports - monacct

`monacct` creates monthly summary files and reports; the resulting output is stored in the directory `/usr/adm/acct/fiscal`. After creating its monthly reports, it removes the old daily accounting files from the directory `/usr/adm/acct/sum` and replaces them with new summary accounting files.

`monacct` should be invoked once each month or accounting period. Its syntax is

`monacct` *number*

where *number* indicates which month or period it is (01=January, 12=December). If *number* is not specified, `monacct` assumes that it is being invoked for the current month; this default is useful if `monacct` is executed via `cron` on the first day of each month (as described in the "Daily Usage and Installation" section of this chapter).

Descriptions of the files created in the `acct/fiscal` directory follow:

- `cms`*?*—contains the total command summary file for the accounting period denoted by *?*. The file is stored in internal summary format. Therefore, to display this file, you must use the `acctcms` command. The following example shows how to display this file for the month of June:

  ```
  acctcms -a -s /usr/adm/acct/nite/fiscal/cms06
  ```

- `fiscrpt`*?*—contains a report similar to that produced by `prdaily`. The report shows line and resource usage for the month represented by *?*. The following would display the fiscal accounting file for the month of November:

  ```
  cat /usr/adm/acct/nite/fiscal/fiscrpt11
  ```

- `tacct`*?*—is the total accounting file for the month represented by *?*. To display this file, you must use the `prtacct` command. The following would display the total accounting summary file for the month of January:

  ```
  prtacct /usr/adm/acct/fiscal/tacct01 "JANUARY TOTAL ACCOUNTING"
  ```

Updating the Holidays File

The file `/usr/lib/acct/holidays` contains the information that System Accounting needs to distinguish between prime and non-prime time. It contains the following information:

- **Comment Lines**—Comment lines are entered by placing an asterisk (*) as the first character in the line; they may appear anywhere in the file.
- **Year Designation Line**—This line should be the first non-comment line in the file and must appear only once. The line consists of three four-digit numbers (leading blanks and tabs are ignored). The first number designates the year; the second denotes the time (in 24-hour format) that prime time starts; the third gives the time that prime time ends and non-prime time starts.

  For example, to specify the year as 1985, prime time at 9:00 a.m., and non-prime time at 4:30 p.m., the following entry would be appropriate:

  ```
  1985    0900    1630
  ```

  A special condition allowed for in the time field is that `2400` is automatically converted to `0000`.
- **Company Holiday Lines**—These entries follow the year designation line. Company holidays are days when few people should be using the computer. Therefore, System Accounting assumes that non-prime time is in effect during the entire 24 hours of a specified holiday.

  Company holiday lines have the following format:

  day_of_year   *Month*   *Day*   *Description of Holiday*

  The *day_of_year* field is a number in the range 1 through 366, corresponding to the day of the year for the particular holiday (leading blanks and tabs are ignored). The remaining fields are simply commentary and are not used by other programs.

Note As delivered, the `holidays` file contains valid entries for Hewlett-Packard's prime/non-prime time, and holidays. You should check this file and edit it as necessary to reflect your organization's requirements.

Fixing Corrupted Files

System Accounting files may become corrupted or lost. Some of these files can simply be ignored or restored from the files saved through backup procedures. However, certain files must be fixed in order to maintain the integrity of System Accounting. Two of the files that must be fixed are `/etc/wtmp` and `/usr/adm/acct/sum/tacct`.

Fixing wtmp Errors

The `wtmp` files seem to cause the most problems in the daily operation of System Accounting. When the date is changed and HP-UX is switched into multiuser mode, a set of date change records is written into `/etc/wtmp`. The `wtmpfix` command is designed to adjust the time stamps in the `wtmp` records when a date change is encountered. However, some combinations of date changes and reboots won't be caught by `wtmpfix` and cause `acctcon1` to fail. The following steps show how to "patch" a damaged `wtmp` file.

```
cd /usr/adm/acct/nite
fwtmp <wtmp.mmdd>wtmp.temp
        Using an editor, delete corrupted records or
        delete all records from beginning up to the date change
fwtmp -ic <wtmp.temp >wtmp.mmdd
rm wtmp.temp
```

If the `wtmp` file is beyond repair, create a null `wtmp` file. This will prevent any charging of connect time. `acctprc1` will not be able to determine which login owned a particular process, but it will be charged to the login that is first in the password file for that user ID.

Fixing tacct Errors

If your installation is using System Accounting to charge users for system resource usage, the integrity of `sum/tacct` is quite important. If `sum/tacct` ever becomes corrupted, then check the contents of `sum/tacctprev` with the command `prtacct`. If it looks correct, then the latest `sum/tacct.`*mmdd* should be patched up, and `sum/tacct` should then be recreated. A simple patch procedure would be:

```
cd /usr/adm/acct/sum
acctmerg -a -v <tacct.mmdd>tacct.temp
      Using an editor, remove the bad records and
      write duplicate UID records to another file
acctmerg -i <tacct.temp >tacct.mmdd
acctmerg tacctprev <tacct.mmdd>tacct
rm tacct.temp
```

Remember that `monacct` removes all the `tacct.`*mmdd* files; therefore, `sum/tacct` can be recreated by merging these files together.

Sample Accounting Shell Scripts

grpdusg

This shell script displays disk space usage totals for the users who are members of a specified group. The syntax of this command is:

grpdusg *group_name*

where *group_name* is the name of the group for which disk space accounting information is to be generated.

For example,

grpdusg pseudo

generates disk space usage information for all the users in the group pseudo.

The Shell Script

```
# Check for the group-name parameter.
#
if      [ $# -ne 1 ]
then    echo "\nUsage:  grpdusg group-name\n"
        exit 1
fi
echo    "\nOne moment please...\n"
#
# Use the find command to find all the files whose owners are members of
# group-name.  Pipe the output from find into acctdusg which will accumulate
# disk space usage information for the users in group-name.
# NOTE:
#       - accounting data is temporarily stored in _${1}_tmp
#       - error messages are stored temporarily in _${1}_err
#       - if files exist that have no owners, then the names of
#         these files are stored in _no_owners
#
fn=_${1}_
find / -group $1 - hidden -print 2>${fn}err |acctdusg -u _no_owners >${fn}tmp
#
# Remove the _no_owners file if its size is not greater than zero.
#
if      [ -s _no_owners ]
then    echo "\nFiles having no owners exist--check _no_owners\n"
else    rm _no_owners
        echo "\nAll files have owners-- _no_owners not created\n"
fi
#
# Use echo and awk to display disk usage totals for this group.
#
echo "\nDisk space usage information (group is ${1}):\n"
awk 'BEGIN {print "\n_UID____USER
NAME________BLOCKS"}
     { sum += $3 ;              # add up total disk blocks used
       print $0                 # display information for user
     }
     END { print "\nTOTAL DISC SPACE USAGE= ", sum, "blocks" }' ${fn}tmp
#
# Remove temporary files, then exit.
#
rm ${fn}*
```

acct_bill

acct_bill takes as input a total accounting file and produces as output billing totals for all users found in the input file. The syntax of acct_bill is:

acct_bill [*mmdd*]

If the optional *mmdd* is not specified, then acct_bill takes as input the current day's total accounting file (acct/nite/daytacct); if *mmdd* is given, then input is taken from the total accounting file for the date specified by *mmdd* (acct/sum/tacct*mmdd*). Output is written to the file bills*mmdd*, where *mmdd* is the date given with the command, or the current date if *mmdd* was not specified with the command.

Examples

To generate billing information for the current day, simply enter:

acct_bill

and the billing information will be stored in the file acct/sum/bills*mmdd*, where *mmdd* is the current date.

To create billing information for January 23rd, you would enter:

acct_bill 0123

after which the billing information would be stored in the file named acct/sum/bills0123.

To automatically generate daily billing totals for all users, you should call acct_bill without the date argument from the USEREXIT state of runacct.

Output Produced by acct_bill

The output of acct_bill contains one line per user and has the following format:

user_ID   *user_name*   *billing_amount*

where *user_ID* and *user_name* identify the user who is being billed, and *billing_amount* shows the total amount that the user is to be charged.

billing_amount is computed by multiplying *accounting coefficients* (found in the shell script) by columns of the report generated by prtacct. Assuming that billing amounts are in dollars, the coefficients (as they are shown in the shell script that follows) produce the following billing amounts:

- ten cents for every minute of prime CPU time consumed
- five cents for every minute of non-prime CPU time consumed
- a half cent for every prime kcore minute used
- two-tenths of a cent for every non-prime kcore minute
- a half cent for every prime connect time minute
- two-tenths of a cent for every non-prime connect minute
- two-and-a-half cents for every block of disk space used
- two-and-a-half cents for every process spawned by the user
- ten cents for every connect session
- each fee unit charged via chargefee counts as one cent

You should experiment with this command by altering the coefficients to see how *billing_amount* is affected. After gaining confidence with this shell script, you can alter the coefficients to suit your installation's needs.

The Shell Script

```
_date=`date +%m%d`
_outfile=/usr/adm/acct/sum/bills
_infile=/usr/adm/acct
#
# Set _infile and _outfile, based on whether or not mmdd was given
#
if      [ $# -eq 0 ]
then                    # Generate billing data for current day.
        _infile=${_infile}/nite/daytacct
        _outfile=${_outfile}${_date}
else                    # Create billing data for date given (mmdd).
        _infile=${_infile}/sum/tacct${1}
        _outfile=${_outfile}${1}
```

```
fi
#
# Create a file containing the ASCII equivalent of the input total
# accounting file (tacct_ASC.tmp_).  The file can then be supplied as input
# to awk, which will generate billing data for each user.
#
acctmerg -a -t <$_infile >tacct_ASC.tmp  # output TOTAL amount first
acctmerg -a <$_infile >>tacct_ASC.tmp # append users' total accounting records
#
# Using awk, compute billing totals for each user in the total accounting file.
#
awk 'BEGIN {
             # ***************************************************
             #   A C C O U N T I N G   C O E F F I C I E N T S
             # ***************************************************
             cpu_P =0.10  # 0.10 monetary units per minute of prime CPU time
             cpu_NP=0.05  # 0.05 monetary units per non-prime CPU minute used
             kcm_P =0.005 # for prime kcore minutes consumed
             kcm_NP=0.002 # for non-prime kcore minutes used
             con_P =0.005 # prime connect (real) time
             con_NP=0.002 # non-prime connect time used
             blk =  0.025 # number of blocks used
             prc =  0.025 # number of processes spawned
             ses =  0.10  # number of connect sessions
             fee =  0.01  # 100 charge units per monetary unit
             # ***************************************************
           }
     # Start computing billing amounts for each user.
     { _sum = cpu_P*$3 + kcm_P*$5 + con_P*$7        # compute prime usage
       _sum+= cpu_NP*$4+ kcm_NP*$6+ con_NP*$8       # add non-prime usage
       _sum+= blk*$9 + prc*$10 + ses*$11 + fee*$13  # add remaining amounts
       printf "%-8s %-10s %10.3f\n", $1, $2, _sum   # display user total
     }' tacct_ASC.tmp_ >$_outfile  # write output from awk to appropriate file
rm tacct_ASC.tmp_                  # remove the temporary ASCII file
```

System Accounting Files

This section contains descriptions of the different files processed by HP-UX System Accounting. The files are grouped according to the directory in which they are found.

Files in the /usr/adm Directory

Filename	Contents
`diskdiag`	Diagnostic output from the execution of disk space accounting commands.
`dtmp`	Output from the **acctdusg** program.
`fee`	Output from the **fchargefee** command (ASCII total accounting records).
`pacct`	The current active process accounting file.
`pacct?`	Process accounting files switched via **turnacct switch**.

Files in the /usr/adm/acct/nite Directory

Filename	Contents
`active`	Used by **`runacct`** to record progress. It contains warning and error messages. `active`*mmdd* is the same as `active` after `runacct` detects an error.
`ctacct.`*mmdd*	Total accounting records created from connect session accounting where *mmdd* is the month and day the file was created.
`ctmp`	Output of `acctcon1`—connect session records.
`daycms`	ASCII daily command summary used by `prdaily`.
`daytacct`	Total accounting records for current day.
`disktacct`	Total accounting records created by the `dodisk` command.
`fd2log`	Diagnostic output from the execution of `runacct` (refer to `crontab` entry).
`lastdate`	The last day that `runacct` was executed, in `date|#`*+%m%d* format. (Refer to *date(1)* for a description of *+%m%d* date format.)
`lock` and `lock1`	Used to control serial use of `runacct`.
`lineuse`	Terminal (`tty`) line usage report used by `prdaily`.
`log`	Diagnostics output from `acctcon1`.
`log`*mmdd*	Same as `log` after `runacct` detects an error.
`reboots`	Contains beginning and ending dates from `wtmp`, and a listing of reboots.
`statefile`	Used to record the current state being executed by `runacct`.
`tmpwtmp`	`wtmp` file, corrected by `wtmpfix`.
`wtmperror`	Error messages, if any, from `wtmpfix`.
`wtmperror`*mmdd*	Same as `wtmperror` after `runacct` detects an error.
`wtmp.`*mmdd*	The previous day's `wtmp` file.

Files in the /usr/adm/acct/sum Directory

Filename	Contents
`cms`	Total command summary file for current month in internal summary format.
`cmsprev`	Command summary file without latest update.
`daycms`	Command summary file for previous day in internal summary format.
`loginlog`	Shows the last login date for each user.
`rpt`*mmdd*	Daily accounting report for date *mmdd*.
`tacct`	Cumulative total accounting file for current month.
`tacctprev`	Same as `tacct` without latest update.
`tacct`*mmdd*	Total accounting file for date *mmdd*.
`wtmp.`*mmdd*	Saved copy of wtmp file for date *mmdd*. Removed after reboot.

Files in the /usr/adm/acct/fiscal Directory

Filename	Contents
`cms`*?*	Total command summary for month *?* in internal summary format.
`fiscrpt`*?*	Report similar to `prdaily` for the month *?*.
`tacct`*?*	Total accounting file for the month *?*.

A

System Parameters

This appendix describes the tunable system parameters and also shows their Backus Naur Forms. The information in this appendix is Series 300/400 specific.

If necessary, you can change the value of these tunable parameters with SAM or the `config` command to customize the HP-UX kernel.

Logical Groups of Parameters

This reference is organized alphabetically. However, many parameters tend to fall into logical groups. Table A-1 illustrates these logical groups.

Table A-1.

Group	Parameters
Accounting	acctresume, acctsuspend, timeslice
Cluster	check_alive_period, dskless_fsbufs, dskless_node, maxswapchunks, minswapchunks, ngcsp, num_cnodes, selftest_period, server_node, serving_array_size, reboot_option, retry_alive_period, using_array_size
File System	fs_async, maxfiles, maxfiles_lim, nbuf, nfile, nflocks, ninode
Hardware	fpa, num_lan_cards, parity_option
Message	mesg, msgmap, msgmax, msgmnb, msgmni, msgseg, msgssz, msgtql
Miscellaneous	dst, maxusers, ncallout, ndilbuffers, npty, scroll_lines, timezone, unlockable_mem
MS-DOS	dos_mem_byte
Networking	netisr_priority
Obsolete[1]	ntext
Process	maxdsiz, maxssiz, maxtsiz, maxuprc, nproc
Semaphore	sema, semaem, semmap, semmni, semmns, semmnu, semume, semvmx
Shared Memory	shmem, shmmax, shmmin, shmmni, shmseg
Streams[2]	NSTREVENT NSTRPUSH STRCTLSZ STRMSGSZ
Swap	nswapdev, nswapfs, swchunk

1 This parameter is no longer used by any supported funcionality within the current release of HP-UX. Do not modify this parameter.

2 Consult the documentation for the optional Streams product to learn more about these parameters

Using SAM to Check or Change HP-UX Kernel Parameters

To check HP-UX kernel parameters with SAM:

1. Log on as `root`.
2. Run SAM:

   ```
   # /usr/bin/sam
   ```

3. Highlight `Kernel Configuration->` and activate [Open].
4. Highlight `Configurable Parameters` and activate [Open].
5. If you are presented with a window entitled "Kernel Configuration," go on to the next step.

   If you are presented with a window entitled "Select New Template File," activate [Template path name...]. A window entitled "Template Files on the System" appears. Choose `/hp-ux` from the list in this window and activate [OK].
6. Look in the upper-left corner of the "Kernel Configuration" window. If you see a line that reads `Template file: /hp-ux`, continue. If not, choose `Select New Template File...` from the "Actions" menu and go to the previous step.

   Examine the list of drivers in the "Kernel Configuration" window. (You may have to scroll through the list to see them all.) When you find the parameter your wish to change, examine its entry in the column labled `Current Value`. If it is *not* the value you need, change it with the next procedure. If it is the value you need, exit the "Kernel Configuration" window, then exit SAM.

To change HP-UX kernel parameters with SAM:

1. If you are not currently logged onto the system, log on as `root`.
2. Run SAM:

   ```
   # /usr/bin/sam
   ```

3. Highlight `Kernel Configuration->` and activate [Open].
4. Highlight `Configurable Parameters` and activate [Open].

A

5. Highlight the parameter you wish to change. (You may have to scroll through the list to find it.)

Note If you wish to change more than one parameter, you may do so by highlighting several of them.

---

6. From the "Actions" menu, choose `Modify Configurable Parameter...` .
7. On the "Modify Configurable Parameter" screen, highlight and turn on one of the methods for parameter modification, then fill in the associated fields and activate [OK].

   You will receive a series of messages indicating the progress of the task. If the task is successful, the entry under the column labeled `Pending Value` will change to the new value you have chosen.
8. From the "Actions" menu, choose `Create a New Kernel` .

Note Creation of a new kernel requires that the system be rebooted.

---

9. You will be presented with a confirmation message. Take one of the following actions:

   - If you want to create a new kernel now, activate (Yes). After the new kernel is built the system will reboot. You will be given an opportunity to take one of three actions:

     - Move the new kernel into place and reboot the system.
     - Move the new kernel into place *without* rebooting the system.
     - Exit without moving the new kernel into place.

     Turn on the radio button for the action you wish to take and activate (OK). If you chose the option to reboot, the system will reboot itself.

   - If you do *not* want to create a new kernel now, activate (No). You may create the new kernel at any time. Exit the "Kernel Configuration" window. You will be given an opportunity to take one of three actions:

     - Create a new kernel.
     - Defer creation of a new kernel.
     - Cancel the kernel modifications you have specified.

     Turn on the radio button for the action you wish to take and activate (OK).

10. Exit SAM by returning to the "System Administration Manager" window and activating (Exit SAM).

A

Parameter Descriptions

Note You can damage your system by changing these parameters improperly. Be sure you know the implications before you change them. Never set system parameters outside the given range. These parameters interact and should be changed in a balanced way.

A

Parameter descriptions include:

Name	The parameter name.
Range	The range of the parameter. Due to interactions with other parameters, sometimes the full range of a parameter cannot be attained.
Default	The default value of the parameter. This value may be specified as a formula that depends on other system parameters. If these other system parameters change, the default value changes correspondingly.
Use	A description of how the system uses the parameter.
Space Utilization	A formula for the allocation of dependent space. Not every parameter description has this field. Usually, dependent space is not an issue for most systems. If you have to calculate dependent space, use the *size*(1) command (refer to the *HP-UX Reference*).
Dependencies	The interaction of the parameter with other system parameters, or how changing it affects system performance, or a formula showing relationships with other parameters.
BNF Format	The Backus Naur Form (BNF) format for the parameter. The BNF format for the tunable system parameters is:

parameter (integer `or formula)`
anychars_except_whitespace

acctresume

Name acctresume - resume accounting due to disk usage

Range -100 -> 101

Default 4

Use

The system disables process accounting when the available space on the file system where the accounting file resides falls below a certain threshold. The threshold is described under acctsuspend. The system re-enables process accounting when sufficient space becomes available. The parameter, acctresume, is the threshold (percentage of free space) that the system must have to re-enable process accounting. This percentage is added to minimum free percentage (minfree) for the file system.

A value of zero re-enables accounting when the free space reaches minfree. A value less than zero allows process accounting to use the space which is reserved for superuser use. A value greater than 100 prevents the the system from re-enabling process accounting when space is available.

When accounting is re-enabled in this way, the system issues this message:

```
Accounting resumed
```

The parameter acctresume is relevant only to systems that use process accounting.

Dependencies (interactions with other system values)

acctsuspend < acctresume

BNF Format

```
acctresume 4

BNF:
    <acctresume-stmt>  ::= acctresume <integer>
                         |  acctresume <anychars_except_whitespace>
```

A

acctsuspend

Name acctsuspend - suspend accounting due to disk usage

Range -100 -> 100

Default 2

Use

The system disables process accounting when the available space on the file system where the accounting file resides falls below a certain threshold. The parameter, **acctsuspend** (specified as a percentage of free space), is the threshold. This percentage is added to minimum free percentage (minfree) for the file system.

A value of zero disables process accounting when the free space falls below minfree. A value less than zero allows process accounting to use the space which is reserved for superuser use. If the sum of **acctsuspend** and minfree is less than zero, process accounting will remain enabled.

When accounting is disabled in this way, the system will issue this message:

```
Accounting suspended
```

The parameter **acctsuspend** is only relevant to systems that use process accounting.

Dependencies (interactions with other system values)

`acctsuspend < acctresume`

BNF Format

```
acctsuspend 2

 BNF:

    <acctsuspend-stmt> ::= acctsuspend <integer>
                         |  acctsuspend <anychars_except_whitespace>
```

A

bufpages

Name `bufpages` - number of buffer pages

Range 0, 64 -> memory limited

Default nbuf * 2

If `bufpages` is equal to zero when the system boots, then two pages are allocated for every buffer header defined by `nbuf`. If `nbuf` is also zero, then 10 percent of available memory is used.

Use

The parameter `bufpages` defines the number of pages in the file system buffer cache. Each page is allocated 4096 bytes of memory.

These buffers are used for all file system I/O operations, plus all other block I/O operations in the system (exec, mount, inode reading and some device drivers.)

Note If you set `bufpages` to a number less than 64, or greater than the maximum supported by the system, the number will be increased or decreased as appropriate, and a message is printed at boot time.

Dependencies (interactions with other system values)

`bufpages <= (nbuf*2)`

This variable may override the value specified for `nbuf`.

The maximum memory allocated to the buffer pool will be limited based on the memory allocated to the system for other purposes. Thus, modifying parameters that affect system memory may affect the maximum memory allocatable to the buffer pool.

BNF Format

```
bufpages 0

BNF:

<bufpages-stmt>  ::= bufpages <integer>
                   |  bufpages <anychars_except_whitespace>
```

check_alive_period

Name check_alive_period - sets the time period, in seconds, that a cluster node—server or client—will wait before sending status-checking messages in the event no communication is received from another cluster node.

Range 1 to no limit

Default 4

Use

When communication ceases between a server and a client in a cluster, the state is said to go from "active" to "alive". The check_alive_period parameter specifies the time period that a cluster node allows another node to remain in the "alive" state before sending status-checking messages to the other node. If no response from the other cluster node is received during the check_alive_period, status-checking messages are sent—by the cluster server to all cluster clients and by each client to the cluster server—at one-second intervals for the time specified by retry_alive_period.

Caution Do not change the default value of this parameter unless you are certain of the effects of the changes.

Note This parameter cannot be changed by using SAM; refer to Chapter 2, "Constructing an HP-UX System" for information about changing system parameters.

See the discussion for the retry_alive_period system parameter.

Dependencies (interactions with other system values)

check_alive_period > 1

BNF Format

```
check_alive_period 4

BNF:

<check_alive_period-stmt>  ::= check_alive_period <integer>
```

dos_mem_byte

Name dos_mem_byte—Reserves memory for the HP 98286 DOS Coprocessor

Range 0 to memory limited

Default 0

Use

The HP 98286 DOS Coprocessor uses system memory. This memory must be reserved on Series 300 systems with more than 6 Mbytes of main memory. The reserved memory is not available to HP-UX regardless of whether the DOS Coprocessor is running.

On Series 300 with 6 Mbytes or less, reserved memory is not required. The DOS Coprocessor shares system memory with HP-UX.

The amount of reserved memory depends upon the memory configuration of the DOS Coprocessor. 1 Mbyte of reserved memory is sufficient for DOS configured with 640 Kbytes of main memory and 64 Kbytes of expanded memory. Use of more DOS expanded or DOS extended memory requires correspondingly more reserved memory.

Cost

The amount of memory specified is reserved only for use by the DOS Coprocessor and is unavailable for other use.

Dependencies

none

dskless_fsbufs

A

Name dskless_fsbufs - specifies the size of the file system buffers that can be allocated under interrupt

Range 0 -> 200 (200 is the maximum value of serving_array_size)

Default 0 (if the cluster code is not configured into the kernel)\

serving_array_size (if the cluster code is configured into the kernel)\

The cluster code is configured into the kernel if the kernel description file you used contains the driver called dskless. Refer to the section on kernel configuration for more information.

Use

This parameter directly sizes the cluster fsbuf page pool. The fsbuf pool is a collection of file system buffers that are utilized for inbound cluster traffic. The value should be <= serving_array_size. If you configure it to be > serving_array_size, it will be reset to be equal to serving_array_size. Diskless cnodes receive much less traffic than the root server, so this parameter should be smaller on the cluster cnode than on the root server.

If an inbound cluster message is large enough to require one of these buffers and none are available, the cluster protocol correctly handles retries.

On the root server the fsbuf pool is allocated when the root server issues the cluster command. On a cluster cnode, the netbuf pool is allocated at kernel initialization time.

Space Utilization pagesize × dskless_fsbufs

On Series 300 and Series 700, pagesize is 4 KB. Pages used for fsbufs are unavailable for general use.

Dependencies (interactions with other system values)

By default, dskless_fsbufs equals serving_array_size. It should always be <= the serving_array_size parameter.

BNF Format

```
diskless_fsbufs 80

BNF:

<dskless_fsbufs-stmt>  ::= dskless_fsbufs <integer>
                        |  dskless_fsbufs <anychars_except_whitespace>
```

A

dskless_node

Name `dskless_node` - identifies the system as a cluster server or a cluster client

A

Range 1 (If 1, this system is a cluster client)

0 (If 0, this system is a cluster server)

Default 0

Use

If you are configuring the root server node, `dskless_node` should be 0 (default) and `server_node` should be set to 1. If you are configuring a standalone system, both `dskless_node` and `server_node` should be 0 (the default).

Dependencies (interactions with other system values)

None.

BNF Format

```
dskless_node 0
dskless_node 1

BNF:

<dskless_node-stmt>  ::= dskless_node <integer>
                       | dskless_node <anychars_except_whitespace>
```

dst

Name dst - daylight savings time

Range 0 -> 5

Default 1

Use

This parameter specifies whether to convert to daylight savings time.

These definitions of the parameter values are from the file `usr/include/sys/time.h`:

```
#define DST_NONE        0        /* not on dst */
#define DST_USA         1        /* USA style dst */
#define DST_AUST        2        /* Australian style dst */
#define DST_WET         3        /* Western European dst */
#define DST_MET         4        /* Middle European dst */
#define DST_EET         5        /* Eastern European dst */
```

Dependencies (interactions with other system values)

It is used with time zone.

BNF Format

```
dst 0
dst 1

BNF:

    <dst-stmt> ::= dst <integer>
```

A

fpa

Name `fpa`—HP 98248A Floating Point Accelerator enable/disable

Range 0,1

Default 1

Use

`fpa` determines whether the code for the HP 98248A Floating Point Accelerator is included in the kernel. If `fpa` = 1 the the code is included, if `fpa` = 0 it is not.

If you wish to use the floating point capabilities, you must:

- set `fpa` to 1 (the default)
- create a device file for the card (described in the HP 98248A installation note)
- download the floating point microcode (described in the HP 98248A installation note)

Cost

Approximately 5 Kbytes.

Dependencies

None.

fs_async

Name `fs_async` - select asynchronous writes to disk

Range 0, 1

Default 0 (disk writes are synchronous)

Use

A non-zero value specifies asynchronous writes to disk. If no value is specified for `fs_async`, writes of the file system data structures to disk are performed synchronously.

Synchronous writes to disk help insure system integrity.

Asynchronous writes to disk can improve file system performance significantly. However, with asynchronous writes, file system data structures might be left in an inconsistent state in the event of a system crash; system administrator intervention to run `fsck` might be required.

If asynchronous writes are selected, HP-UX file system semantics for NFS and HP-UX cluster environments are preserved. In addition, files opened with the `O_SYNC` flag (synchronous writing) will continue to be written synchronously when the asynchronous writes feature has been configured into the kernel.

Dependencies (interactions with other system values)

None.

BNF Format

```
fs_async 0
fs_async 1

BNF:

     <fs_async-stmt> ::= fs_async <integer>
```

maxdsiz

Name `maxdsiz` - maximum data size

Range 0x40000 -> 0xF0E00000

Default 0x1000000

A

Use

This value is entered in bytes.

The parameter **maxdsiz** defines the maximum size of the data segment of an executing process.

The default value is large enough for most processes. The **maxdsiz** parameter should be increased only if you have one or more processes that use large amounts of data.

Each time the system loads a process, or an executing process attempts to expand its data segment, the system checks the size of the process's data segment.

If **maxdsiz** is exceeded, the system will terminate the process or issue an error message.

Dependencies (interactions with other system values)

process text + process data + process stack <= 4,094 MB

BNF Format

```
maxdsiz 0x1000000

BNF:

    <maxdsize-stmt>  ::= maxdsize <integer>
                      |  maxdsize <anychars_except_whitespace>
```

maxfiles

Name `maxfiles` - soft limit to the number of files a process can have open

Range 0 - 2048

Default 60

Use

The parameter represents the system default soft limit to the number of open files a process may have. It is possible for a process to increase its soft limit and therefore open more than `maxfiles` files.

Non-superuser processes can increase their soft limit until their hard limit (`maxfiles_lim`) is reached.

Dependencies (interactions with other system values)

`maxfiles` is limited by `nfile` and the inode table.

BNF Format

```
maxfiles  1024

BNF:

<maxfiles-stmt>  ::= maxfiles <integer>
                   |  maxfiles <anychars_except_whitespace>
```

maxfiles_lim

Name maxfiles_lim - hard limit for the number of files a process can have open

A

Range 0 - 2048

Default 1024

Use

The parameter represents the system default hard limit to the number of open files a process may have. It is possible for a non-superuser process to increase its soft limit (maxfiles) up to the hard limit.

Dependencies (interactions with other system values)

maxfiles_lim is limited by nfile, ninode.

BNF Format

```
maxfiles_lim  2048

BNF:

<maxfiles_lim-stmt>  ::= maxfiles <integer>
                    |  maxfiles_lim <anychars_except_whitespace>
```

maxssiz

Name maxssiz - maximum stack size

Range 0x40000 -> 0xF0E00000

Default 0x200000

Use

This value is entered in bytes. The parameter **maxssiz** defines the maximum size of the stack segment of an executing process.

The default is large enough for the stack of most processes. The parameter **maxssiz** should only be increased if you have one or more processes that need a large stack.

The stack grows dynamically. As it grows, the system checks the size of the process's stack segment. If the **maxssiz** is exceeded, the process is killed.

Dependencies (interactions with other system values)

process text + process data + process stack <= 4,094 MB

BNF Format

```
maxssiz 0x200000

BNF:

    <maxssiz-stmt>  ::= maxssiz <integer>
                      |  maxssiz <anychars_except_whitespace>
```

maxswapchunks

Name `maxswapchunks` - maximum amount of swap space allocated to the system

A

Range 1 -> 2^{14}

Default 512

Use

This parameter defines the maximum amount of system swap space.

This parameter should be used for a cluster client that uses a large amount of the cluster server's swap space. You do not have to limit the amount of swap space if the cluster client has its own swap.

On a standalone system or on a cluster client with local swap space, this parameter should have a larger value than the total swap space. Using the default values of **maxswapchunks** and **swchunk** results in 537 MB of swap space.

Dependencies (interactions with other system values)

The total swap space is limited by:

```
maxswapchunks * swchunk * 1024 bytes
```

Total swap space cannot exceed 2 gigabytes.

BNF Format

```
maxswapchunks 512

BNF:
    <maxswapchunks-stmt>  ::= maxswapchunks <integer>
       |  maxswapchunks <anychars_except_whitespace>
```

maxtsiz

Name `maxtsiz` - maximum text size

Range 0x40000 -> 0xF0E00000

Default 0x1000000 (64 MB)

Use

This value is entered in bytes. The parameter **maxtsiz** defines the maximum size of the shared text segment of an executing process.

The current default accommodates the text segments of most processes. Unless you plan to execute a process with a text segment larger than 64 MB, **maxtsiz** should not be modified.

Dependencies (interactions with other system values)

Each time the system loads a process with shared text, the system checks the size of its shared text segment. The system issues an error message and aborts the process if the text segment is larger than **maxtsiz**.

BNF Format

```
maxtsiz 0x1000000

BNF:

    <maxtsiz-stmt>  ::= maxtsiz <integer>
                      |  maxtsiz <anychars_except_whitespace>
```

maxuprc

Name maxuprc - maximum number of user processes

Range 3 -> (nproc - 4)

Default 50 processes

Use

The parameter **maxuprc** defines (for each user) the maximum number of simultaneous processes. A user is identified by the user ID number, not by the number of login instances. Each user will need at least one process for the shell, and other processes for work purposes (the default is usually adequate).

The superuser is exempt from this limit.

Pipelines need at least one simultaneous process for each side of a '|'. Some commands, such as cc, fc, and pc, use more than one process per invocation.

If a user tries to start a new process when the total number of processes for the user is larger than **maxuprc**, the system will issue this message to the user:

```
no more processes
```

If a user is doing a fork ( ) system call to create a new process and the total number of processes for the user exceeds maxuprc, fork ( ) will return -1 and set the errno to EAGAIN.

Dependencies (interactions with other system values)

If **maxuprc** is set to a value greater than or equal to nproc (maximum number of processes in the system) then **maxuprc** is no longer a limit, a single user could monopolize system resources.

BNF Format

```
maxuprc 50

BNF:

    <maxuprc-stmt>  ::= maxuprc <integer>
                      | maxuprc <anychars_except_whitespace>
```

maxusers

Name `maxusers` - limiter for system resource allocation

Range 0 -> memory-limited

Default 8

Use

The parameter **maxusers** limits system resource allocation, not the actual number of users on the system. By itself, **maxusers** does not determine the size of any structures in the system. The default value of other global system parameters depend on maxusers. If you tune the parameters that use **maxusers**, then the effect of **maxusers** on kernel size is proportionately smaller.

The **maxusers** parameter defines the macro MAXUSERS (for example, "#define MAXUSERS 8"). It determines the size of system tables. The actual limit of the number of users depends on the license version of HP-UX purchased. You can examine the license version using the **uname** command.

Rather than varying each configurable parameter individually, it is easier to specify certain parameters using a formula based on the maximum number of expected users (for example, `nproc (20+8*MAXUSERS)`). Thus, if you increase the maximum number of users on your system, you only need to change the `maxusers` statement.

Dependencies (interactions with other system values)

The default values of `nproc`, `ncallout`, `ninode`, `nfile`, and `serving_array_size` depend on `maxusers`. Refer to the file `/etc/master` for the descriptions of those interactions.

BNF Format

```
maxusers 8
maxusers 32

BNF:

    <maxusers> ::= maxusers <integer>
```

mesg

Name mesg - System V message parameters

Range 0 -> 1

Default 1

A

Use

mesg determines whether the code for System V IPC message parameters will be included in the kernel.

If mesg = 1, the code is included;
if mesg = 0, then the code is not included.

All message parameters depend on the value of mesg.

minswapchunks

Name `minswapchunks` - minimum amount of swap space allocated to the system

Range 1 < = `minswapchunks` < = `maxswapchunks`

Default 4

Use

This parameter sets the minimum amount of swap space allocated for a system. The minimum amount of swap space is:

```
minswapchunks * swchunk * 1024 bytes
```

A cluster client that swaps to the cluster server will always reserve at least `minswapchunks` of swap space from the cluster server.

Dependencies (interactions with other system values)

```
minswapchunks < maxswapchunks
```

Total swap space must be at least:

```
minswapchunks * swchunk * 1024 bytes
```

BNF Format

```
minswapchunks 1
minswapchunks 3

BNF:

    <minswapchunks-stmt>  ::= minswapchunks <integer>
       | minswapchunks <anychars_except_whitespace>
```

msgmap

Name msgmap - message map

Range 3 -> memory limited

Default msgtql + 2

Use

Each set of messages allocated per identifier occupies one or more contiguous slots in the msg array. As messages are allocated and deallocated the msg array may become fragmented.

The parameter **msgmap** dimensions the resource map used to allocate the buffer space for messages. This map shows the free holes in the msg array. An entry in the map is used to point to each set of contiguous unallocated slots; the entry consists of a pointer to the set, plus the size of the set.

If a message set request cannot be accommodated, the system issues the message:

```
DANGER: mfree map overflow
```

If you get this error message, regenerate the kernel with a larger value for msgmap.

There is less fragmentation of the msg array if all message identifiers have the same number of messages. Then, **msgmap** can be smaller.

Dependencies (interactions with other system values)

msgmap <= (msgtql + 2)

msgmap <= (msgseg + 2)

If msgmap is greater than msgtql + 2, then part of the space allocated for msgmap will not be used.

BNF Format

```
msgmap 100

BNF:

     <msgmap-stmt>  ::= msgmap <integer>
                     |  msgmap <anychars_except_whitespace>
```

A

msgmax

Name `msgmax` - message maximum size

Range 0 -> 64 KB

Default 8192 bytes

Use

The parameter **msgmax** limits the size, in bytes, of a single message.

Increase the value of **msgmax** only if you plan to execute applications that require larger messages. This parameter keeps malicious or poorly written programs from using all of the message buffer space.

A **msgsnd** system call which attempts to send a message larger than **msgmax** bytes returns an error.

Dependencies (interactions with other system values)

msgmax <= msgmnb

msgmax <= (msgssz*msgseg)

BNF Format

```
msgmax 8192

BNF:

    <msgmax-stmt>  ::= msgmax <integer>
                     |  msgmax <anychars_except_whitespace>
```

msgmnb

Name `msgmnb` - maximum number of bytes on the message queue

Range 0 -> 64 KB

Default 16384 bytes

Use

The parameter **msgmnb** is the maximum total size, in bytes, of all messages that can be queued on a message queue at the same time.

A **msgsnd** system call which attempts to exceed this limit returns either:

- an EAGAIN error if IPC_NOWAIT is set.
- an EINTR error if IPC_NOWAIT is not set.

Dependencies (interactions with other system values)

`msgmnb >= msgmax`

`msgmnb <= (msgssz*msgseg)`

BNF Format

```
msgmnb 16384

BNF:

    <msgmnb-stmt>  ::= msgmnb <integer>
                     | msgmnb <anychars_except_whitespace>
```

A

msgmni

Name `msgmni` - number of message queue identifiers

Range 1 -> memory limited

Default 50

Use

The parameter **msgmni** dimensions the array of message queue identifiers.

A message queue identifier is needed for each message queue in the system.

An attempt to allocate a new message queue with the **msgget** system call when **msgmni** message queues already exist returns a ENOSPC error.

If a message queue remains allocated, it is on the system even after the process(es) using it have stopped. Deallocate message queues using *ipcrm*(1).

Users should deallocate messages when processes are complete.

Dependencies (interactions with other system values)

None.

BNF Format

```
msgmni 50

BNF:

    <msgmni-stmt>  ::= msgmni <integer>
                     | msgmni <anychars_except_whitespace>
```

msgseg

Name msgseg - message segments

Range 1 -> 32767

Default 16384

Use

The parameter **msgseg**, together with **msgssz**, determines the size of the buffer available for queuing messages.

The parameter **msgssz** determines the size, in bytes, of the units in which messages are allocated space. When a message is allocated, its size is rounded up to the nearest multiple of **msgssz**.

The parameter **msgseg** is the number of these units available.

In most cases, the product of **msgseg * msgssz** is important because it determines the total amount of space available for messages. Different **msgseg:msgssz** ratios that yield the same product will just cause this space to be fragmented differently for the same usage.

Space Utilization

msgseg * msgssz bytes

Dependencies (interactions with other system values)

(msgseg * msgssz) >= msgmax

BNF Format

```
msgseg 1024

BNF:

    <msgseg-stmt>  ::= msgseg <integer>
                     | msgseg <anychars_except_whitespace>
```

A

msgssz

Name msgssz - message segment size

Range 1 -> memory limited

Default 1 byte

Use

The parameter **msgssz**, together with **msgseg**, determines the size of the buffer available for queuing messages.

The parameter **msgssz** determines the size, in bytes, of the units in which messages are allocated space. When a message is allocated, its size is rounded up to the nearest multiple of **msgssz**.

The parameter **msgseg** is the number of these units available.

In most cases, the product of **msgseg * msgssz** is important because it determines the total amount of space available for messages. Different **msgseg:msgssz** ratios that yield the same product will just cause this space to be fragmented differently for the same usage.

Space Utilization

msgseg * msgssz bytes

Dependencies (interactions with other system values)

(msgseg * msgssz) >= msgmax

BNF Format

```
msgssz 8

BNF:

     <msgssz-stmt>  ::= msgssz <integer>
                      | msgssz <anychars_except_whitespace>
```

msgtql

Name msgtql - number of message headers

Range 1 -> memory limited

Default 40

Use

The parameter **msgtql** dimensions an array of message headers. A message header is used for each message queued in the system.

A **msgsnd** system call which attempts to exceed this limit either:

- blocks waiting for a free header or,
- returns EAGAIN error

depending on whether the IPC_NOWAIT flag is set with the call.

Dependencies (interactions with other system values)

msgmap <= msgtql + 2

If msgmap is greater than **msgtql** + 2, then some allocated space will be wasted.

BNF Format

```
msgtql 40

BNF:

    <msgtql-stmt>  ::= msgtql <integer>
                     | msgtql <anychars_except_whitespace>
```

nbuf

Name nbuf - number of buffer headers

Range 0, 16 -> memory limited

Default 0 (configured dynamically)

If at boot time `nbuf` is = 0, then one buffer header is allocated for every two pages of buffer memory defined by the `bufpages` parameter. If `bufpages` is also zero, 10% of available memory is used.

Use

The parameter `nbuf` defines the number of file system buffer-cache buffer headers. Each buffer is allocated 4096 bytes of memory unless overridden by a conflicting value for `bufpages`.

These buffers are used for all file system I/O operations, plus all other block I/O operations in the system (such as exec, mount, inode reading, and some device drivers).

While `nbuf` is available for compatibility with previous releases, it is recommended that the size of the buffer pool be configured with the `bufpages` parameter.

Note If you set `nbuf` to a number less than 16, greater than the maximum supported by the system, or to a value that is inconsistent with the value of `bufpages`, the number will be increased or decreased as appropriate, and a message printed at boot time.

Dependencies (interactions with other system values)

`bufpages <= nbuf*2`

bufpages controls the actual memory allocated to the buffer pool. If both **bufpages** and **nbuf** are set and the values conflict so that it is impossible to configure a system using both of them, **bufpages** overrides.

BNF Format

```
nbuf 0

BNF:

    <nbuf-stmt>  ::= nbuf <integer>
                   | nbuf <anychars_except_whitespace>
```

ncallout

Name ncallout - number of timeouts

Range 6 -> memory limited

Default 16 + NPROC + USING_ARRAY_SIZE + SERVING_ARRAY_SIZE

Use

The parameter **ncallout** is the maximum number of timeouts that can be scheduled by the kernel at any one time. Timeouts are used by:

- alarm (system call)
- setitimer (system call)
- select (system call)
- drivers
- uucp processes
- process scheduling

When the system runs out of timeouts, it prints the following fatal error to the

```
panic: timeout table overflow
```

Dependencies (interactions with other system values)

The larger **nproc** is, the larger **ncallout** should be. A guideline of 1 callout per process should be used unless you have processes that use many of the callouts.

BNF Format

```
ncallout (64+NPROC)

BNF:

    <ncallout-stmt>  ::= ncallout <integer>
                       | ncallout <anychars_except_whitespace>
```

ndilbuffers

Name `ndilbuffers` - number of DIL buffers

Range 1 -> memory limited

Default 30

Use

`ndilbuffers` defines the maximum number of DIL open device files at any one time in the system.

`ndilbuffers` is used exclusively by the Device I/O Library. If DIL is not used, no DIL buffers are necessary.

Dependencies (interactions with other system values)

None.

BNF Format

```
ndilbuffers 30

BNF:

    <ndilbuffers-stmt>  ::= ndilbuffers <integer>
```

netisr_priority

Name `netisr_priority` - a realtime process priority for networking

Range -1, 0 -> 127

Default -1

Use

The `netisr_priority` parameter specifies the realtime process priority of the netisr process. The netisr daemon executes on systems with networking—ARPA/BSD, X.25/9000, and HP-UX clusters—processing the packets for these networking services.

A value of -1 specifies that networking packets are handled on an interrupt basis. This yields the fastest possible packet handling rate.

A value between 0 and 127 (zero being highest priority) specifies the priority at which the process scheduler handles networking packets.

Refer to *rtprio*(1) in *HP-UX Reference*; also refer to the *HP-UX Real-Time Programming Manual* for more information.

Dependencies (interactions with other system values).

None.

BNF Format

```
netisr_priority 0

BNF:

    <netisr_priority-stmt>  ::= netisr_priority  <integer>
```

nfile

Name `nfile` - number of files

Range 14 -> memory-limited

Default (16 * (NPROC + 16 + MAXUSERS) / 10 + 32 + 2 * NPTY)

Use

The parameter **nfile** defines the maximum number of open files at any one time in the system.

It is the number of slots in the file descriptor table. Be generous with this number since the cost is low, and not having enough slots would cut down on the amount of work that can be done simultaneously in the system.

Dependencies (interactions with other system values)

`nfile` depends on `nproc`, `maxusers`, and `npty`.

Processes At least three file descriptors per process (stdin, stdout, stderr).

Pipes 2 per pipe (1 per side).

BNF Format

```
nfile (16*(NPROC+16+MAXUSERS)/10+32+2*NPTY)

BNF:

    <nfile-stmt>  ::= nfile <integer>
                   |  nfile <anychars_except_whitespace>
```

nflocks

Name `nflocks` - number of file locks

Range 2 -> memory-limited

Default 200

Use

The parameter **nflocks** gives the possible number of file/record locks in the system. When choosing this number, note that one file may have several locks and databases may need an exceptionally large number of locks (if they use `lockf`).

Dependencies (interactions with other system values)

None.

BNF Format

```
nflocks 200

BNF:

    <nflocks-stmt>  ::= nflocks <integer>
                      | nflocks <anychars_except_whitespace>
```

ngcsp

Name ngcsp - number of general cluster server processes

Range 1 -> memory limited

Default 8 * num_cnodes

In an HP-UX cluster, the default values for num_cnodes are 1 for clients and 5 for servers; this parameter does not apply to standalone systems.

Use

The parameter ngcsp specifies the maximum number of general cluster server processes (GCSPs) that can exist simultaneously in the system. Values for ngcsp are needed for the server and all client machines in a cluster; values for ngcsp are ignored on standalone systems.

Space Utilization 20 bytes * ngcsp

Dependencies

```
ngcsp = 8 * num_cnodes

nproc = 20 + (8*maxusers) + ngcsp
```

Each GCSP needs one process slot, so ngcsp should be less than (nproc - 5).

Each GCSP used needs a serving array entry (like some other requests), so ngcsp must be less than serving_array_size.

BNF Format

```
ngcsp  (8*num_cnodes)

BNF:

    <ngcsp-stmt>  ::= ngcsp <integer>
                    | ngcsp <anychars_except_whitespace>
```

A

ninode

Name ninode - number of inodes

Range 14 -> memory-limited

Default NPROC + 48 + MAXUSERS + (2 * NPTY) + (SERVER_NODE * 18 * NUM_CNODES)

Use

The parameter ninode defines the maximum number of open inodes which can be in-core.

It is the number of slots in the inode table. The inode table is used as a cache memory. For efficiency reasons, the last ninode (number of) open inodes is kept in main memory. The table is hashed.

Dependencies (interactions with other system values)

Each unique open file has an open inode associated with it. Therefore, the larger the number of unique open files, the larger ninode should be.

The default value of ninode depends on nproc, maxusers, num_cnodes, npty, and server_node.

BNF Format

```
ninode (NPROC+16+MAXUSERS+32)

BNF:

    <ninode-stmt>  ::= ninode <integer>
                     | ninode <anychars_except_whitespace>
```

nproc

Name nproc - number of processes

Range 6 -> memory limited

Default 20 + (8 * MAXUSERS) + NGCSP

Use

The parameter `nproc` specifies the maximum total number of processes that can exist simultaneously in the system.

There are at least four system overhead processes at all times, and one entry is always reserved for the superuser.

When the total number of processes in the system is larger than nproc, the system issues these messages:

At the system console:

```
proc: table is full
```

Also, if a user tries to start a new process from a shell, the following message prints on their terminal:

```
no more processes
```

If a user is executing `fork( )` to create a new process, `fork( )` will return -1 and set the errno to EAGAIN.

Dependencies (interactions with other system values)

The default values of `ninode`, `nfile`, `using_array_size`, and `ncallout` depend on `nproc`.

`maxuprc <= (nproc - 4)`

BNF Format

```
nproc (20+86*MAXUSERS)

BNF:

    <nproc-stmt>  ::= nproc <integer>
                    | nproc <anychars_except_whitespace>
```

A

npty

Name npty - number of pseudo-teletypes

Range 1 -> memory limited

Default 82

Use

The parameter **npty** limits the number of the following structures that can be used by the pseudo-teletype driver:

struct tty	pt_tty[npty];
struct tty	*pt_line[npty];
struct pty_info	pty_info[npty];

Dependencies (interactions with other system values)

None.

BNF Format

```
npty 60

BNF:

    <npty-stmt>  ::= npty <integer>
                   | npty <anychars_except_whitespace>
```

nswapdev

Name nswapdev - number of file systems that you can enable for dynamic swap

Range 1-25

Default 10

Use

The parameter **nswapdev** defines the maximum number of devices that you can use for device swap.

Dependencies (interactions with other system values)

None.

BNF Format

```
nswapdev 10

BNF:

    <nswapdev-stmt>  ::= nswapdev <integer>
                       | nswapdev <anychars_except_whitespace>
```

A

nswapfs

Name `nswapfs` - number of file systems that you can enable for dynamic swap

Range 1-25

Default 10

Use

The parameter **nswapfs** defines the maximum number of file systems that you can use for file system swap.

Dependencies (interactions with other system values)

None.

BNF Format

```
nswapfs 10

BNF:

    <nswapfs-stmt>  ::= nswapfs <integer>
                      | nswapfs <anychars_except_whitespace>
```

num_cnodes

Name num_cnodes - limiters for cluster system resource allocation

Range 0 -> 255

Default (5 * SERVER_NODE) + DSKLESS_NODE
(5 for cluster server, 1 for cluster client)

Use

This parameter is a limiter for cluster resource allocation; the value of other global system parameters depends on num_cnodes. Alone, it does not determine the size of any structure in the system.

This parameter indicates the number of cluster clients that a server can expect to serve simultaneously. It does not place an actual, absolute limit on the number of clients supported by a cluster server.

Suggested values are:

5 if 0-5 clients
10 if 6-10 clients
15 if 11-15 clients
20 if 16-20 clients
25 if 21-25 clients

Space Utilization

Increasing the value of num_cnodes indirectly results in increased kernel data structure and buffers. Thus, there is less memory available for user processes.

Dependencies (interactions with other system values)

```
serving_array_size = (server_node * num_cnodes * maxusers
+ 2 * maxusers)

ninode = (nproc + 16 + maxusers) + 32 + 2 (2 * npty) +
(server_node * 18 * num_cnodes)

ngcsp = 8 * num_cnodes
```

BNF Format

```
num_cnodes  25

BNF:

    <num_cnodes-stmt>  ::= num_cnodes <integer>
                     |  num_cnodes <anychars_except_whitespace>
```

num_lan_cards

Name num_lan_cards—maximum number of LAN interface cards the system will support

Range 0 to 5

Default 2

Use

num_lan_cards defines the maximum number of LAN interface cards the system will support. This number should be greater than or equal to the number of LAN interface cards actually present.

Cost

Approximately 1200 bytes per LAN interface card.

Dependencies (interactions with other system values)

None.

A

parity_option

Name `parity_option`—used to handle parity errors

Range 0 to 2

Default 2

Use

`parity_option` selects the kind of action that the system takes if it encounters a parity error.

The actions are as follows:

0 Print a 'Parity error' message to the console.

1 Print a 'Parity error' message to console, plus:

- if user state, it kills the current process (which may not always be the process which caused the error, as with a DMA card) and prints an error message to its tty.
- if supervisor state, it panics with a 'parity error' message to the console.

2 Always panics with a 'parity error' message to console.

Caution Values other than 2 could result in data corruption depending on where the RAM parity error occurs.

Cost

None.

Dependencies

None.

reboot_option

Name `reboot_option` - specifies how a cluster node will reboot itself after it has determined that the root server or its swap server has gone down

Range 0 - Halt; same as `/etc/reboot -h`

1 - Reboot; same as `/etc/reboot`

Default 1

Use

Once a cluster node determines that it is no longer able to communicate with its root server or a swap server, it will reboot itself. The `reboot_option` specifies how it will reboot.

Caution Do not change the default value of this parameter unless you are certain of the effects of the changes.

Note This parameter cannot be changed by using SAM; refer to Chapter 2, "Constructing an HP-UX System" for information about changing system parameters.

Dependencies (interactions with other system values)

None.

BNF Format

```
reboot_option 0

BNF:

    <reboot_option-stmt>  ::= reboot_option <integer>
```

retry_alive_period

A

Name retry_alive_period—sets the time period, in seconds, that status-checking messages will be sent by one cluster node to another cluster node that is still not responding at the end of the check_alive_period

Range 4 to no limit

Default 21

Use

When communication ceases between a server and a client in a cluster, the state is said to go from "active" to "alive". The check_alive_period parameter specifies the time period that a cluster node allows another node to remain in the "alive" state before sending status-checking messages to the other node. If no response from the other cluster node is received during the check_alive_period, status-checking messages are sent—by the cluster server to all cluster clients and by each client to the cluster server—at one-second intervals for the time specified by retry_alive_period.

A higher value for retry_alive_period makes it less likely that a cluster client will panic during a local power failure on a server; however, if a cluster node fails, it will take longer for the other cluster nodes that need the resources of the failed node to detect and recover from the failure.

Caution Do not change the default value of this parameter unless you are certain of the effects of the changes.

Note This parameter cannot be changed by using SAM; refer to Chapter 2, "Constructing an HP-UX System" for information about changing system parameters.

See the related discussions for the check_alive_period and the reboot_option parameters.

Dependencies (interactions with other system values)

retry_alive_period > 4

BNF Format

```
retry_alive_period 21
```

BNF:

```
<retry_alive_period-stmt>  ::= retry_alive_period <integer>
```

A

scroll_lines

Name `scroll_lines` - ITE buffer lines

Range 100 -> 999

Default 100

Use

The parameter **`scroll_lines`** defines the scrolling area (the number of lines of emulated terminal screen memory on each Internal Terminal Emulator (ITE) port configured into the system).

For each configured graphics interface in the system, the graphics driver uses 2 * line_length * scroll_lines bytes of data. For example, a 98720 graphics display has an ITE line length of 128 characters. Setting **`scroll_lines`** to 100 causes 2 * 128 * 100 = 25600 bytes of kernel space to be used for each graphics terminal's screen memory.

Dependencies (interactions with other system values)

None.

BNF Format

```
scroll_lines 100

BNF:

    <scroll_lines-stmt>  ::= scroll_lines <integer>
```

selftest_period

Name selftest_period - Interval between kernel self tests.

Range 0, 90 -> 3600 seconds

Default 0 (If the cluster code is not configured into the kernel; that is, if the dfile does not include the subsystem dskless).

120 seconds (If the cluster code is configured into the kernel; that is, if the dfile includes the subsystem dskless).

A

Use

The parameter selftest_period is used by the cluster kernel self test code to determine how often to execute a self test. The self test checks the availability of kernel resources needed for clusters. A zero value indicates that the self test should not be executed.

Dependencies (interactions with other system values)

None.

BNF Format

```
selftest_period  120

BNF:

    <selftest_period-stmt>  ::= selftest_period <integer>
                          |  selftest_period <anychars_except_whitespace>
```

sema

Name `sema` - System V semaphores

Range 0 -> 1

Default 1

Use

`sema` determines whether the code for System V IPC semaphores will be included in the kernel.

If `sema = 1`, the code is included;
if `sema = 0`, then the code is not included.

HP Windows/9000 and the Starbase graphics library both require the semaphore code.

If `sema`=0, and you have programs which use the *semget*(2) or *semop*(2) system calls, you will receive a SIGSYS signal.

Dependencies (interactions with other system values)

All semaphore parameters depend on the value of `sema`.

semaem

Name semaem - "adjust on exit" maximum value for semaphores

Range 0 -> min (semvmx, 32767)

Default 16384

Use

An *undo* is an optional flag in a semaphore operation which causes that operation to be undone if the process which invoked it dies.

The parameter **semaem** is the maximum value by which a semaphore can be undone.

This value is cumulative per process, so if one process has more than one undo operation on a semaphore, the value of each undo operation is added up in the variable semadj. The parameter semadj is the number by which the semaphore will be incremented or decremented if the process dies.

Read the manual page for *semop*(2) for more detailed information on semaphore undos.

Any semop calls which attempts to set |semadj| > semaem results in an ERANGE error.

Dependencies (interactions with other system values)

```
semaem <= semvmx
```

BNF Format

```
semaem 16384

BNF:

    <semaem-stmt>  ::= semaem <integer>
                    |  semaem <anychars_except_whitespace>
```

semmap

Name semmap - semaphore map

Range 4 -> memory limited

Default (semmni + 2)

Use

Each set of semaphores allocated per identifier occupies 1 or more contiguous slots in the sem array. As semaphores are allocated and deallocated, the sem array might become fragmented.

The parameter **semmap** dimensions the resource map which shows the free holes in the sem array. An entry in this map is used to point to each set of contiguous unallocated slots; the entry consists of a pointer to the set, plus the size of the set.

If semaphore usage is heavy and a request for a semaphore set cannot be accommodated, the following message appears:

```
danger: mfree map overflow
```

You should then configure a new kernel with a larger value for **semmap**.

Fragmentation of the sem array is reduced if all semaphore identifiers have the same number of semaphores; **semmap** can then be somewhat smaller.

Four is the lower limit: 1 slot is overhead for the map and the second slot is always needed at system initialization to show that the sem array is free.

Dependencies (interactions with other system values)

(semmap-2) = the maximum number of contiguous unallocated pieces of the sem array.

semmap<=(semmni+2)

If semmap is greater, then some allocated space will be wasted.

BNF Format

```
semmap 10

BNF:

    <semmap-stmt>  ::= semmap <integer>
                     |  semmap <anychars_except_whitespace>
```

A

semmni

Name `semmni` - number of semaphore identifiers

Range 2 -> memory limited

Default 64

Use

The parameter **semmni** defines the number of sets (identifiers) of semaphores available to the users.

When the system runs out of semaphore sets, the **semget** system call will return a ENOSPC error message.

Dependencies (interactions with other system values)

```
semmni <= semmns
semmns <= (semmni * semmsl)
semmap <= (semmni+2)
```

semmsl is the value of the maximum number of semaphores that can be associated with a semaphore ID. The value of **semmsl** is set at 500 and is *not* tunable.

BNF Format

```
semmni 64

BNF:

     <semmni-stmt>  ::= semmni <integer>
                      | semmni <anychars_except_whitespace>
```

semmns

Name `semmns` - total number of semaphores in system

Range 2 -> memory limited

Default 128

Use

The parameter **semmns** defines the total number of semaphores available to the users of the system.

When the system does not have enough contiguous semaphores in the sem array to satisfy a **semget** request, the call returns a ENOSPC error. This error may occur even though there may be enough free semaphores, but they are not contiguous.

Dependencies (interactions with other system values)

```
semmni <= semmns
semmns <= (semmni * semmsl)
```

`semmsl` is the value of the maximum number of semaphores that can be associated with a semaphore ID. The value of **semmsl** is set at 500 and is *not* tunable.

BNF Format

```
semmns 128

BNF:

    <semmns-stmt>  ::= semmns <integer>
                    |  semmns <anychars_except_whitespace>
```

A

semmnu

Name semmnu - number of semaphore **undo** structures

Range 1 -> (nproc - 4)

Default 30

Use

An *undo* is a special, optional, flag in a semaphore operation which causes that operation to be undone if the process which invoked it terminates.

The parameter **semmnu** is the number of processes which can have undo's pending on a given semaphore. It determines the size of the sem_undo structure.

Refer to the *semop*(2) in the *HP-UX Reference* for more information.

You should increase **semume** if the user gets ENOSPC errors on semop calls using the SEM_UNDO flag.

Dependencies (interactions with other system values)

- **semmnu** determines the size of the structure sem_undo, which in turn contains the substructure dimensioned by **semume**.
- There is no point in having **semmnu** = (nproc -4) because it is the largest number of processes in the system that could use semaphores simultaneously.

BNF Format

```
semmnu 30

BNF:

    <semmnu-stmt>  ::= semmnu <integer>
                    |  semmnu <anychars_except_whitespace>
```

semume

Name `semume` - semaphore **undo** entries per process

Range 1 -> `semmns`

Default 10

Use

An *undo* is an optional flag in a semaphore operation that causes that operation to be undone if the process that invoked it dies.

The parameter `semume` limits the number of semaphores that each process can have undos pending on.

Read the manual page for *semop*(2) for a more detailed explanation of undo.

`semop` is the value of the maximum number of semaphores you can change with one system call. Check the file `/usr/include/sys/sem.h` for this value.

When you get EINVAL errors on `semop` calls with the SEM_UNDO flag, then increase the value of `semume`.

Dependencies (interactions with other system values)

`semume <= semmns`

The parameter `semume` is the size of the substructure undo, which is part of the sem_undo structure. The size of sem_undo is determined by `semume`.

BNF Format

```
semume 10

BNF:

    <semume-stmt>  ::= semume <integer>
                    |  semume <anychars_except_whitespace>
```

semvmx

Name semvmx - semaphore maximum value

Range 1 -> 65535

Default 32767

Use

The parameter **semvmx** is the maximum value that a semaphore is allowed to reach. This limit is imposed by the largest number that can be stored in a 16-bit unsigned integer (65,535).

A **semop** system call that tries to increment a semaphore value to greater than **semvmx** will cause an ERANGE error. If **semvmx** exceeds 65,535, then semaphore values can overflow and these errors will not be caught.

semop is the value of the maximum number of semaphores you can change with one system call. Check the file `/usr/include/sys/sem.h` for this value.

Dependencies (interactions with other system values)

semaem <= semvmx

BNF Format

```
semvmx 32767

BNF:

    <semvmx-stmt>  ::= semvmx <integer>
                     | semvmx <anychars_except_whitespace>
```

server_node

Name server_node - flag used to size an array for the root server's inbound requests

Range 1 (If 1, serving_array[ ], num_cnodes, and ninode are sized for a cluster server)

0 (If 0, serving_array[ ], num_cnodes, and ninode are sized for a cluster client)

Default 0

A

Use

This parameter is the flag used to determine the size of serving_array[ ] and ninode. serving_array[ ] is an array of kernel structures used by a cluster client for inbound requests. If this parameter is set (server_node=1), serving_array[ ] will be sized appropriately for a root server node. The cluster's root server should have this parameter set to 1, and should have the dskless_node parameter set to 0 (default).

If you are configuring a cluster client, server_node should be 0 (default) and dskless_node should be set to 1. If you are configuring a standalone system, both dskless_node and server_node should be 0 (the default).

Refer to the descriptions of serving_array_size and ninode system parameters for information on these resources.

Dependencies (interactions with other system values)

```
num_cnodes = (5 * server_node) + dskless_node
```

```
serving_array_size = (server_node * num_cnodes * maxusers + 2 *
maxusers)
```

```
ninode = (nproc + 16 + maxusers) + 34 + (2 * npty) + (server_node * 18 *
num_cnodes)
```

A

BNF Format

```
server_node  0
server_node  1

BNF:
    <server_node-stmt>  ::= server_node 0
                         |  server_node 1
```

serving_array_size

Name serving_array_size - size of the cluster request serving array

Range 0 -> 200 (200 is MAX_SERVING_ARRAY)

Default 0 (If the cluster code is not configured into the kernel; that is, if the dfile does not include the dskless subsystem)

server_node * num_cnodes * maxusers + (2 * maxusers) (if the cluster code is configured into the kernel; that is, if the dfile file includes the dskless subsystem)

A

Use

This parameter defines the size of the kernel's serving array. serving_array[ ] is an array of kernel structures that holds information about inbound cluster network requests:

Each inbound request requires a single serving_array[ ] entry.

If both configurable parameters, dskless_node and server_node, are equal to 0, the system is treated as standalone. For a standalone system, serving_array_size is 0 and serving_array[ ] is not compiled into the kernel.

Space Utilization

20 bytes * serving_array_size

Dependencies (interactions with other system values)

```
serving_array_size = (server_node * num_cnodes
* maxusers + 2 * maxusers)

dskless_fsbufs = serving_array_size

ncallout = (16 + nproc + using_array_size
+ serving_array_size)
```

Each GCSP requires a serving array entry (refer to ngcsp).

BNF Format

```
serving_array_size  0
serving_array_size  (server_node*num_cnodes*maxusers+2*maxusers)

BNF:

    <serving_array_size-stmt>  ::= serving_array_size <integer>
          |    server_node <anychars_except_whitespace>
```

A

shmem

Name `shmem` - shared memory disable/enable

Range 0, 1

Default 1

Use

`shmem` determines whether the code for System V IPC shared memory is included in the kernel. If `shmem` = 0 the code is not included, if `shmem` = 1 then it is included.

Dependencies (interactions with other system values)

HP Windows/9000 and the Starbase graphics library both require the presence of shared memory code.

shmmax

Name shmmax - shared memory maximum

Range 0x200000 -> 0x2FFFFFFF

A

This is a system-wide limit.

Default 0x600000

Use

The parameter **shmmax** defines the maximum shared memory segment size in bytes.

Dependencies (interactions with other system values)

None.

BNF Format

```
shmmax 0x4000000

BNF:

    <shmmax-stmt>  ::= shmmax <integer>
                     |  shmmax <anychars_except_whitespace>
```

shmmin

Name `shmmin`—shared memory minimum

Range positive integers

Default 1 byte

Use

`shmmin` defines the minimum shared memory segment size.

Cost

None.

Dependencies

`shmmin` < `shmmax`

If `shmem` = 0, then the code for shared memory is not included in the kernel and the value of `shmmin` is irrelevant.

If `shmem` = 1, then the code for shared memory is included and `shmmin` is tunable.

If it is reconfigured other subsystems (such as Windows/9000) may not work.

shmmni

Name `shmmni` - shared memory maximum number of identifiers

Range 1 -> 1024

A

Default 30 identifiers

Use

The parameter **shmmni** defines the maximum number of shared memory segments systemwide. Make it large enough to hold as many shared memory segments as will be used simultaneously.

The data structure associated with each shared memory segment is 104 bytes per identifier. The maximum cost is 104 * `shmmni`.

Dependencies (interactions with other system values)

None.

BNF Format

```
shmmni 100

BNF:

    <shmmni-stmt>  ::= shmmni <integer>
                     |  shmmni <anychars_except_whitespace>
```

shmseg

Name shmseg - shared memory segments

Range 1 -> shmmni

Default 10

Use

The parameter **shmseg** defines the maximum number of shared memory segments that can be attached to a process at any given time.

Dependencies (interactions with other system values)

None.

BNF Format

```
shmseg 12

BNF:

    <shmseg-stmt>  ::= shmseg <integer>
                     | shmseg <anychars_except_whitespace>
```

A

A

swchunk

Name swchunk - chunk size for swap

Range 0x800 -> 0x4000

Default 2048

Use

This parameter defines the chunk size for swap. This value must be a power of two. This parameter cannot be configured with SAM.

Dependencies (interactions with other system values)

Total swap space is limited by:

```
swchunk * maxswapchunk * DEV_BSIZE
```

where DEV_BSIZE is 1024 bytes.

Total swap space cannot exceed 2 gigabytes.

BNF Format

```
swchunk 2048
swchunk 4096

BNF:

<swchunk-stmt>  ::= swchunk<integer>
       |  swchunk <anychars_except_whitespace>
```

timeslice

Name `timeslice` - scheduling timeslice interval

Range -1 -> 2^{31}

Default HZ/10

Use

The `timeslice` interval is the amount of time one process is allowed to run before the CPU is given to the next process at the same priority. The value of `timeslice` is specified in units of (10 millisecond) clock ticks. There are two special values:

0 Use the system default value (currently 10 ticks, or 100 milliseconds)

-1 Disable round-robin scheduling completely

Impact on System

This parameter will cause a process to check for pending signals when the time specified expires. This guarantees that a process which does not make any system calls (including a runaway process in an infinite loop) can be terminated. Thus setting `timeslice` to a very large value, or to -1, can prevent such processes from getting signals.

Change this parameter only on systems dedicated to applications with specific realtime needs.

No memory allocation relates to this parameter. Some CPU time is spent at each timeslice interval, but this time has not been precisely measured.

Dependencies (interactions with other system values)

None.

BNF Format

```
timeslice  (HZ/10)

BNF:
    <timeslice-stmt>  ::= timeslice <integer>
                    |  timeslice <anychars_except_whitespace>
```

timezone

Name `timezone` - minutes west of the Greenwich meridian

Range 0 -> 1440

Default 420

Use

The `timezone` parameter indicates the minutes west of the Greenwich meridian:

```
struct  timezone tz = { TIMEZONE, DST };
struct timezone {
int tz_minuteswest; /* minutes west of Greenwich */
int tz_dsttime;     /* type of dst correction */
};
#define DST_NONE      0     /* not on dst */
#define DST_USA       1     /* USA style dst */
#define DST_AUST      2     /* Australian style dst */
#define DST_WET       3     /* Western European dst */
#define DST_MET       4     /* Middle European dst */
#define DST_EET       5     /* Eastern European dst */
```

Dependencies (interactions with other system values)

It is used with `dst` (daylight savings time). This should be made consistent with the TZ environment variable (see *environ*(MISC) and *login*(1) in the *HP-UX Reference*).

BNF Format

```
timezone 480

BNF:

    <timezone-stmt>  ::= timezone <integer>
```

unlockable_mem

Name unlockable_mem - unlockable memory

Range 0 -> (the available memory indicated at power-up)

Default 102400

Use

The parameter **unlockable_mem** defines the minimum amount of memory that will always be available for virtual memory and/or system overhead.

It limits the amount of memory that can be locked (lockable memory) to **unlockable_mem** (the available memory indicated at power up).

If **unlockable_mem** is greater than available memory, the system sets **unlockable_mem** to available memory.

Lockable memory is used for:

- Process images and overhead locked with *plock*(2)
- Shared memory segments locked with the SHM_LOC command of the *shmctl*(2) system call
- Miscellaneous dynamic kernel data structures used by the shared memory system and some drivers.

Any call that needs lockable memory may fail if the value is too small. Note that lockable memory limits the amount of memory that can be locked, but that this memory is available for virtual memory except when it is locked.

Dependencies (interactions with other system values)

unlockable_mem <= physical memory

BNF Format

```
unlockable_mem 0

BNF:

    <unlockable_mem-stmt>  ::= unlockable_mem <integer>
        |  unlockable_mem <anychars_except_whitespace>
```

using_array_size

Name `using_array_size` - size of the cluster client's request using array

Range 0 -> (function of `maxusers`)

Default 0 (if the cluster code is not configured into the kernel; that is, if the `dfile` file does not include the `dskless` subsystem)

`nproc` (if the cluster code is configured into the kernel; that is; if the `dfile` includes the `dskless` subsystem)

Use

The parameter `using_array_size` defines the size of the kernel's using array. The using array is an array of kernel structures that hold information on outbound cluster network requests. `using_array_size` has the same value as the `nproc` parameter.

Each active outbound request requires one `using_array[ ]` entry. Outbound requests are not discarded if all `using_array[ ]` slots are used; these requests are delayed until the required resource is available.

If both of the parameters, `dskless_node` and `server_node` are equal to zero, the system is treated as standalone. For a standalone system, `using_array_size` is zero and `using_array[ ]` is not compiled into the kernel.

Dependencies (interactions with other system values)

`ncallout = (16 + nproc + using_array_size + serving_array_size)` The `size of the using array is dependent on the nproc` configurable parameter.

BNF Format

```
using_array_size  (nproc)

BNF:

    <using_array_size-stmt>  ::= using_array_size <integer>
       |  using_array_size <anychars_except_whitespace>
```

B

Swap Space Computation

Swap Space Computation

A. SUM (all shared code sizes) of all running processes as shown by `ps -el`.

   Do not count the page daemon, swapper, or statdaemon processes. The `file` command will show you if a file contains shared text, and you can find the size of the text by means of the `size` command.

B. SUM (all data and stack sizes) of all processes. By using the `size` command, you can calculate the size of initialized data and uninitialized data (BSS). This represents only part of the total swap space requirements of the process. In addition, you must calculate the amount of dynamic heap and stack space that the program might require. If you are familiar with the program's runtime logic, you might be able to calculate this by looking at requests made to `sbrk` or `malloc`.

   You can approximate by running the program with a typical input stream, and determine the total virtual memory size in number of pages. The virtual memory size can be obtained by running `ps -el` and looking in the SZ (size in 512-byte blocks) field for the program you are interested in.

   Subtract the code size calculated in step A from this to get the total data and stack size.

C. SUM (sticky code sizes) for all **sticky code** files that will be executed, but are not currently being used by any processes. Typically editors fall into this category. (See the discussion under "The Sticky Bit" in *How HP-UX Works: Concepts for the System Administrator*.)

D. SUM (all existing shared memory segment sizes) for shared memory segments created by users via `shmget`. `Ipcs` can be used to show active shared memory segments.

E. Size of the scratch area used by **exec** to hold arguments. The default size of this area is 256 Kbytes; it can be changed by using **uxgen**.

F. Fragmentation and overhead.

   Fragmentation is the difference between the swap space needed at any given time and the actual amount allocated. The parameter **swchunk** controls swap space allocation—see Appendix A for details.

   Overhead is additional disk space needed to store system-related information when a process is swapped out.

   There is no easy way to figure out an an accurate value for fragmentation and overhead. We suggest you take an arbitrary value such as 6Mb.

Swap space = A + B + C + D + E + F.

Swap Space Computation Worksheet

A. For shared code, fill out the code space needed by the process.

```
Process ID                Code size.


-----------------       ------------------

-----------------       ------------------

-----------------       ------------------

-----------------       ------------------

-----------------       ------------------
```

B. For each shared process listed above, fill out the data and stack space needed by the process. For each nonshared process, add the process's code size to its data size and enter the amount (that is, total from executing size).

```
Process ID                Data size.
                          (minimum data space = dmmin x 1Kb
                          block default = 32Kb)


-----------------       ------------------

-----------------       ------------------

-----------------       ------------------

-----------------       ------------------

-----------------       ------------------
```

B

C. For each sticky bit file that was executed since power-up, but not currently used, fill out the code space.

```
Process ID                  Code size.

-----------------      ------------------

-----------------      ------------------

-----------------      ------------------

-----------------      ------------------

-----------------      ------------------
```

D. For each shared memory segment, give the shared segment size.

```
Shared Memory               Segment Size.

-----------------      ------------------

-----------------      ------------------

-----------------      ------------------

-----------------      ------------------

-----------------      ------------------
```

E. Scratch area used for arguments during **exec**. Default is 256 Kb:

```
-----------------

-----------------
```

F. Fragmentation and overhead.

We suggest using an estimate such as 6 Mb.

```
-----------------------------

TOTAL AMOUNT OF SWAP SPACE NEEDED IS:

A   + B + C + D + E + F =  Total swap space

____+____+____+____+____+____=  -------------------------------
```

Example

Let's assume that you are going to run four FORTRAN compiles with optimization. This example shows how to calculate the additional swap space that might be required to handle this. Let's start with one compile and gather some statistics.

Note The following example may not be indicative of how much swap space your compiles would use, because the amount of swap space required by HP-UX compilers depends on the size of the program being compiled. Further, compiling with optimization may consume almost twice as much swap space.

```
% fc -o test.f >& out &
[1] 3663
ps\ -l)
F S   UID   PID  PPID  C PRI NI   ADDR  SZ   WCHAN TTY      TIME COMD
1 S   867 22055     1  1 168 20 a0a308 121 1515308 ttyd3p4  0:07 csh
1 S   867  3663 22055  0 158 20 5f3900  28  4c8024 ttyd3p4  0:00 fc
1 R   867  3664  3663204 229 20 d2ae306963         ttyd3p4  0:25 f77comp
1 R   867  3680 22055 49 190 20 f9d260 182         ttyd3p4  0:00 ps

% file /usr/lib/f77comp
/usr/lib/f77comp:       S800 shared executable

% size /usr/lib/f77comp
5720($MILLICODE$) + 141600($LIT$) + 1726120($CODE$) + 8($CODE20$) +
576($UNWIND$MILLICODE$) + 47152($UNWIND$) + 1824($UNWIND$) + 16($UNWIND20$) +
132($RECOVER$) + 164192($GLOBAL$) + 93032($DATA$) + 9424($DATA$) +
8($PFACOUNTER$) + 24400($BSS$) = 2214204
```

From the above information, you can determine that

- The code size for /usr/lib/f77comp is 5720+1726120+8= 1731848 bytes
- The data size for /usr/bin/f77comp is 93032+9424= 102456 bytes
- The BSS size for /usr/bin/f77comp is 24400
- (BSS and initialized data = 102456 + 24400 = 126856 bytes)

The `ps` command tells you that this FORTRAN compile uses 6963 pages or 14260224 bytes. Subtracting the code size from this and leaves 12528376 bytes for the total data, heap, and stack. The difference between this data size and the fixed (obtained from `size` above), is the amount of dynamic space used by the FORTRAN compiler for this program.

A.)Process ID Code Size

3664 1731848

B.)Process ID Data size

3664 12528376

Therefore, you need 1.7 Mb of swap space for the compiler text (of which there will be only one copy) and 12.5 Mbyte of swap space for the per process data. This would mean that the system would need approximately 1.7+4 * 12.5 (or 51.7 Mb) of additional swap space for the four compiles to execute in parallel.

C

Federal Information Processing Standard

The U.S. Government has published the Federal Information Processing Standard (FIPS 151-1, hereafter called FIPS). Based on the POSIX standard IEEE Std 1003.1-1988, FIPS specifies the behavior of a system in areas where the POSIX standard permits divergent behavior. In three areas, HP-UX permits a wider range of behavior than allowed by FIPS. These areas are:

- Changing file ownership
- Group ID of new files
- Truncation of filenames

Based on the announcement of the FIPS published in the *Federal Register, Volume 54, no. 70, April 13, 1989*, the following sections explain the configuration of HP-UX so it conforms to the FIPS, pending its approval.

C

Restricting the chown(1) Function

The POSIX standard permits an implementation to allow users to change the ownership of their own files (as does System V) or restricts this action to privileged users (as does 4.3BSD). You can control this with the privileged group facility (see *getprivgrp*(2) in the *HP-UX Reference*). The FIPS makes the following statement, which requires the 4.3BSD behavior:

```
The implementation shall support the option
_POSIX_CHOWN_RESTRICTED.
```

Configure HP-UX to behave this way by removing users from groups with the privilege PRIV_CHOWN. By default, HP-UX grants this privilege to all users, so you must revoke the privilege each time you start up the system, or add this line to the file /etc/rc:

```
setprivgrp -n CHOWN
```

Note The use of some commands—those associated with backup and recovery operations, for example—may be affected by restricting users' access privileges.

Controlling the Group ID of New Files

The POSIX standard permits an implementation either to set the group ID of a newly created file either to the effective group ID of the creating process (as does System V) or to the group ID of the parent directory of the new file (as does 4.3BSD). HP-UX follows the 4.3BSD semantics if the set-group-ID bit of the parent directory is set, and follows System V semantics otherwise. The FIPS makes the following statement, which effectively requires the 4.3BSD behavior:

```
The implementation shall support the setting of the
group ID of a file (when it is created) to that of its
parent directory.
```

An HP-UX system can be configured to behave this way by setting the set-group-ID bit of all directories in the system. When HP-UX is installed, this bit is not set on directories, so this requires setting it once for all directories where the FIPS behavior is desired. Executing the following command as superuser will do this for the entire system; the command should be executed with no NFS mounts or RFA netunams in effect:

```
find / -type d -exec chmod g+s \;
```

You may choose to leave the setgid bit off for some directories which are not associated with any group, because the effective group ID of the creating process may be more meaningful for files in those directories. Examples of such directories include `/tmp` and `/usr/tmp`. This can be done by constructing a more complex `find` command, or by turning the set-group-ID bit off for those files after the `find` command, with a command such as:

```
chmod g-s /tmp /usr/tmp
```

This practice may not conform strictly to the FIPS.

Truncating Filenames During Pathname Resolution

When a filename specified by a user is longer than the maximum supported by the file system, the POSIX standard permits an implementation either to truncate the name to the supported maximum (as does System V) or to give an `ENAMETOOLONG` error (as does 4.3BSD). HP-UX follows the 4.3BSD semantics for file systems that support long filenames, and follows System V semantics for other file systems. The FIPS makes the following statement, which effectively requires the 4.3BSD behavior:

```
The implementation shall support the functionality
associated with the feature {_POSIX_NO_TRUNC}.
```

To conform with the FIPS, convert all file systems to support long filenames (see Chapter 6, "Managing the File System").

Index

A

access control lists, 4-11
  creating entries, 4-43
  removing entries, 4-48, 4-50, 4-63, 4-66, 4-76, 4-78
  replacing entries, 4-71
accessing **setuid** and **setgid** system calls, 4-8, 4-80
access permissions, 4-2
accounting, 2-27. *See also* system accounting
acctresume parameter, A-7
acctsuspend parameter, A-8
ACLs (access control lists), 4-11
adding
  a local printer, 9-25, 9-51
  an automated backup schedule using HP-UX commands, 8-69–74
  an automated backup schedule using SAM, 8-28–38
  a network-based printer, 9-33, 9-61
  a remote printer, 9-30, 9-56
  a user group, 4-30, 4-58
  device drivers to kernel using SAM, 2-46
  peripherals, 2-6, 5-4
  subsystems, 2-56
  subsystems using SAM, 2-59
  users, 4-16, 4-34
  users and groups, 2-21
  users to groups, 4-33, 4-72
adding a disk
  using SAM, 6-14
adding device swap
  using **swapon**, 7-25
adding file systems
  CD-ROM file system, 6-36
  NFS file system, 6-42
  using **mount**, 6-34
  using SAM, 6-29
adding file system swap
  using SAM, 7-23
  using **swapon**, 7-36
after installing HP-UX, 2-7
alias
  setting up, 2-34
assessing users' needs, 2-1, 2-2
assigning special group privileges, 4-79
assigning swap priority, 7-12, 7-30
automating backups, 8-17
  using HP-UX commands, 8-69–74
  using SAM, 8-28–38

B

backup index file
  viewing using **frecover**, 8-83
  viewing using SAM, 8-51, 8-53, 8-55
backup kernel
  booting, 2-54
  creating, 2-42
  for a cluster client, 2-42
  for a cluster server, 2-43
  restoring and booting, 2-55
backup levels, 8-2, 8-8–11

backup media capacities, 8-13–16
backups
  automating, 8-17, 8-28–38, 8-69–74
  automating using HP-UX commands, 8-69–74
  automating using SAM, 8-28–38
  cartridge tape data blocking, 8-58, 8-62
  cartridge tapes, 8-63, 8-77
  choosing storage device, 8-12–13
  determining how often, 8-7
  determining which data, 8-3
  excluded files, 8-2, 8-5, 8-6
  fbackup, 8-18, 8-19, 8-57–64
  file extraction, 8-2
  full, 8-2, 8-8–11, 8-61, 8-63, 8-67
  graph file, 8-2, 8-6
  included files, 8-2, 8-4, 8-6
  incremental, 8-3, 8-7, 8-8–11, 8-62
  index files, 8-52, 8-54, 8-59, 8-63, 8-83
  initial backup, 2-38
  magnetic tapes, 8-61, 8-62
  media capacity, 8-13–16
  other utilities, 8-86
  over the network using **fbackup**, 8-58, 8-62
  over the network using SAM, 8-24
  recovery, 8-3
  restoring data, 8-18, 8-41, 8-47, 8-75
  system, 8-3
  tcio, 8-63, 8-77
  to a hard disk, 8-67
  using HP-UX commands, 8-19, 8-56–74
  using SAM, 8-20–56
  utilities, 8-19
backup storage devices, 8-13
bdf, 6-61
block device file
  definition, 6-2
block size file system parameter, 6-25
booting the backup kernel using the Boot ROM, 2-54
boot-up
  customizing system startup scripts, 2-30
  problems, 2-7
bootup problems, 4-85
Bourne shell
  login files, 2-29, 2-34
bufpages parameter, A-9
bytes-per-inode file system parameter, 6-25

C

cancel model script (printer), 9-4
cartridge tape backup example, 8-63
cartridge tape data blocking (**tcio**), 8-58, 8-62, 8-77
cartridge tape (HP format) capacity, 8-15
catman, 2-19
CD-ROM file system, 6-9
  adding using **mount**, 6-36
changing file ownership, 4-8, 4-80
changing run-levels, 4-86
character device file
  definition, 6-2
charging fees, 11-12, 11-55
check_alive_period parameter, A-11
checking
  file system consistency, 6-78
checking **quotas** consistencies, **quotacheck**, 6-77
chown
  restricting, 6-64
cluster
  adding users and groups, 2-21
  backing up context dependent files, 8-59, 8-86, 8-87
  backup kernel for a client, 2-42

backup kernel for a cluster server, 2-43
booting client from backup kernel, 2-55
booting server from backup kernel, 2-54
configuring kernel, 2-43
customizing the login prompt, 2-33
dfile requirement, 2-41
/etc/inittab, 2-31
/etc/issue, 2-33
installing and updating optional software, 2-5
installing HP-UX, 2-5
local printers, 9-15
Managing Clusters of HP 9000 Computers, 2-5
updating HP-UX, 2-5
command
lpana, 9-85, 9-86
accept, 9-6, 9-55, 9-67, 9-76
bdf, 6-61, 8-67
cancel, 9-73
catman, 2-19
chacl, 4-11, 4-43, 4-48, 4-50, 4-63, 4-66, 4-71, 4-76, 4-78
chfn, 4-42, 4-57
chgrp, 4-40, 4-45
chmod, 4-45
chown, 4-40, 4-45, 4-49, 4-65
convertfs, 6-58
cpio, 8-86
cpset, 6-67
crontab, 8-70, 8-72, 8-74
csh, 4-38
cwall, 10-5
date, 2-16, 2-17
dd, 8-67, 8-81
df, 6-61
disable, 9-6, 9-64, 9-69, 9-75
du, 6-62
edquota, 6-68
elm, 10-6
enable, 9-6, 9-55, 9-69, 9-76
exportfs, 8-19
fbackup, 8-18, 8-19, 8-57–64
find, 4-47, 4-49, 4-50, 4-63, 4-65, 4-68, 4-71, 4-76, 6-62
finger, 4-42, 4-57
frecover, 8-18, 8-19, 8-74–79
fsck, 6-78
ftio, 8-86
getprivgrp, 4-79
grep, 4-50
grpck, 4-50, 4-60, 4-72
init, 4-13, 4-87
ksh, 4-38
lifinit, 6-52
lifls, 6-51
lpadmin, 9-51, 9-56, 9-60, 9-63, 9-65
lpalt, 9-78, 9-81
lpana, 9-72, 9-83, 9-87
lpmove, 9-76
lpsched, 9-13, 9-37, 9-72, 9-76
lpshut, 9-51, 9-56, 9-65, 9-72
lpstat, 9-55, 9-60, 9-72, 9-73, 9-79
mediainit, 6-21
mkdir, 4-44
mkfs, 6-22
mknod, 6-18, 7-26
mkrs, 2-11–13
motd, 10-3
mount, 6-34
newfs, 6-22, 7-29
news, 2-24, 10-3
pwck, 4-50, 4-52, 4-54, 4-66
quot, 6-74
quota, 6-74
quotacheck, 6-71, 6-77
quotaoff, 6-72
quotaon, 6-71
reject, 9-6, 9-64, 9-67, 9-75

- `repquota`, 6-73
- `rlpdaemon`, 9-15
- `rsh`, 4-38
- `setprivgrp`, 4-8, 4-80
- `sh`, 4-38
- `shutdown`, 2-44, 3-9, 4-87, 4-88
- `swapinfo`, 7-5
- `swapon`, 7-30
- `tar`, 8-87
- `tcio`, 8-63, 8-77, 8-78, 8-79
- `tic`, 2-37
- `tset`, 2-28, 2-29
- `umount`, 6-48
- `untic`, 2-37
- `uucp`, 10-5
- `vipw`, 4-5
- `wall`, 10-4
- `write`, 10-4

computing swap space, B-1
concepts for the system administrator, 1-8, 1-9
`conf.c`, 2-43
`config`
- running, 2-43

`config.mk`, 2-43
configurable parameters, 2-49. *See also* system parameters
configuration description file, 2-41
configuring
- kernel, 2-38

conforming to FIPS, C-1
connect session accounting, 11-10, 11-24
console, 5-32
constructing a system, 2-1
`convertfs`, 6-58
core dump configuration, 7-15
`cpset`, 6-67
crash recovery
- boot from recovery tape, 8-84
- retoring files, 8-18

creating
- an automated backup schedule using HP-UX commands, 8-69–74
- an automated backup schedule using SAM, 8-28–38
- a printer class using `lpadmin`, 9-62
- backup kernel, 2-43
- device files, 6-17
- file systems, 2-18, 6-13
- file systems, using `newfs`, 6-17, 6-22
- file systems, using SAM, 6-14
- kernel, 2-38
- LIF volume, 6-51
- message of the day, 2-33
- recovery system, 2-7–13
- `terminfo` file, 2-37

`cron`
- problems caused by changing system clock, 2-18
- terminating in a cluster, 2-16
- terminating to set date and time, 2-16

crontab file, 8-70–74
C shell
- login files, 2-29, 2-34

`csh.login`, 2-29
`.cshrc`, 2-29
- editing, 2-34

customizing
- `/etc/inittab`, 2-31
- `/etc/issue`, 2-33
- `/etc/motd`, 2-33
- `/etc/rc`, 2-31
- message of the day, 2-33
- printer model scripts, 9-12
- SAM, 1-15, 4-21
- SAM interface colors, 1-25
- SAM interface fonts, 1-25
- system startup, 2-30
- the login prompt, 2-33
- users' editing environments, 2-34
- users' login environments, 2-34

customizing shutdown, 3-11
cwall, 10-5

D

date, 2-16, 2-17
  format, 2-16
  setting, 2-16, 2-17
DDS format (DAT) tape capacity, 8-16
deactivating users account, 4-24, 4-51
default group, 4-2. *See also* primary group
default printer, 9-5
detail log file (SAM), 1-45
DEV_BSIZE, 7-7
device drivers
  adding to kernel using SAM, 2-46
  printers, 9-29, 9-48, 9-49
  removing from kernel using SAM, 2-46
device files, 9-13
  block, 6-18, 7-27
  character, 6-20, 7-27
  creating, 6-17, 7-27
  definition, 6-2
  listing, 6-20, 7-28
devices. *See* peripherals
device swap, 7-3
  adding using **swapon**, 7-25
  removing, 7-22, 7-34
device swap, adding with SAM, 7-18
device swap space
  allocating, 7-7
df, 6-61
dfile, 2-41
  creating, 2-41
  in a cluster, 2-41
  running config on, 2-43
directory
  /etc/filesets, 2-62
  /system, 2-62
disabling device swap, 7-22
disabling printers, 9-40, 9-69
disk drive, 5-36
  moving using HP-UX commands, 5-34
  moving using SAM, 5-13
  removing using HP-UX commands, 5-42
  removing using SAM, 5-24
disk layout, 6-9, 7-28
disk quotas
  block limits, 6-65
  described, 6-64
  file limits, 6-65
  hard limits, 6-65
  individual users, 6-69
  planning, 6-65
  prototype user, 6-68
  reaching hard limits, 6-75
  setting up, 6-65
  soft limits, 6-65
  turning off, 6-72
disk sections
  block device files, 6-2
  character device files, 6-2
disk space
  manpages, 2-19
disk space usage accounting, 11-17
disktab file, 7-28
disk type, 6-26
disk usage
  accounting, 11-10
  bdf, 6-61
  df, 6-61
  du, 6-62
  limiting with disk quotas, 6-64
  quot, 6-74
  quota, 6-74
  repquota, 6-73
displaying user account information, 4-28, 4-55
documentation

on-line (manpages), 2-19
doss_mem_byte parameter, A-13
dskless_fsbufs parameter, A-14
dskless_node parameter, A-16
dst parameter, A-17
du, 6-62
dump area configuration, 7-15

E

editing **/etc/passwd**, 4-5
editing system files
  /etc/csh.login, 2-34
  /etc/inittab, 2-31
  /etc/issue, 2-33
  /etc/motd, 2-33
  /etc/profile, 2-34
  /etc/rc, 2-31
editing user files
  .exrc, 2-34
  .profile, **.cshrc**, etc., 2-34
EDITOR environment variable, 4-44, 4-50, 4-52, 4-54, 4-65, 4-71
edquota, 6-68
  -p, 6-68
  -t, 6-69
effective group, 4-2
electronic mail, 10-6
  elm, 2-22
  mail, **mailx**, 2-22
  setting up, 2-22
elm, 10-2, 10-6
  setting up, 2-22
email (*see* electronic mail), 2-22
enabling file system swap
  on boot, 7-41
  using **swapon**, 7-38
enabling printers, 9-42, 9-69
ENV
  setting for **.kshrc**, 2-29
.environ, 2-29
environment file
  .cshrc, 2-29
  .environ, 2-29
  /etc/csh.login, 2-29
  /etc/group, 2-28
  /etc/inittab, 2-28
  /etc/issue, 2-29
  /etc/motd, 2-29
  /etc/passwd, 2-28
  /etc/profile, 2-29
  /etc/rc, 2-28
  /etc/ttytype, 2-28, 2-29
  .exrc, 2-29
  .kshrc, 2-29
  local files, 2-29
  .login, 2-29
  .profile, 2-29
environment file **/etc/inittab**, 4-85
environment variable
  EDITOR, 4-5, 4-44, 4-50, 4-52, 4-54, 4-65, 4-71
  ENV, 2-29
  LPDEST, 9-10
  TERM, 2-35
  TZ, 2-14
/etc/checklist
  quota option, 6-66
/etc/exports, 6-42
/etc/filesets directory, 2-62
/etc/hosts, 6-42
.exrc, 2-29, 2-34

F

fbackup
  active files, 8-20, 8-24, 8-57
  backup levels, 8-8
  crossing NFS mount points, 8-19
  excluded files, 8-6
  graph file, 8-6
  included files, 8-6
  multiple devices, 8-58, 8-64
  syntax, 8-57

fbckup
  examples, 8-60
Federal Information Processing Standard
    (FIPS), C-1
file
  /usr/adm/fbackupfiles/dates, 8-59
  bcheckrc, 6-47, 6-77
  checklist, 6-44
  conf.c, 2-43
  config.mk, 2-43
  crontab, 11-4
  csh.login, 4-38
  .cshrc, 2-34, 4-38
  disktab, 6-9, 6-26
  d.profile, 4-39
  /etc/csh.login, 2-14, 2-34
  /etc/d.profile, 2-34
  /etc/group, 2-28, 4-6, 4-36, 4-50,
    4-58, 4-61, 4-68, 4-72, 4-73, 4-74,
    4-77
  /etc/hosts, 2-33
  /etc/inittab, 2-28, 2-31, 4-12, 4-13,
    4-84, 4-85
  /etc/issue, 2-29, 2-33
  /etc/logingroup, 4-6, 4-36, 4-41,
    4-50, 4-58, 4-61, 4-68, 4-72, 4-73,
    4-74, 4-77
  /etc/motd, 2-29, 2-33
  /etc/passwd, 2-28, 4-5, 4-18, 4-34,
    4-42, 4-48, 4-51, 4-53, 4-55, 4-61,
    4-65, 4-67
  /etc/profile, 2-14, 2-34
  /etc/ptmp, 4-5
  /etc/rc, 2-14, 2-28, 2-31, 11-3, 11-32
  /etc/ttytype, 2-28
  .exrc, 2-29, 2-34
  .kshrc, 2-34
  .login, 2-34, 4-38
  .profile, 2-34, 4-38
  profile, 4-38
  quotas, 6-66
  rc, 6-47
  /SYSBCKUP, 2-42
  ttytype, 2-29
  /usr/adm/fbackupfiles/dates, 8-8,
    8-9
  /usr/bin/x11start, 2-26
  /usr/spool/lp/cmodel/rcmodel,
    9-16, 9-56
  /usr/spool/lp/lpana.log, 9-72,
    9-83
  /usr/spool/lp/smodel/rsmodel,
    9-16, 9-56
file access permissions, 4-2
file group ownership, 4-2
file name length, 6-55
file ownership, 4-2
files
  access control lists, 4-11
  access permissions, 4-4, 4-9, 4-13
  creating access control list entries,
    4-43
  /etc/conf/dfile, 2-41
  locating by access control list entry,
    4-48, 4-65, 4-71
  locating by both user and group
    ownership, 4-65, 4-71
  locating by file ownership, 4-47, 4-49,
    4-63, 4-65, 4-68, 4-76
  locating by file type, 4-49, 4-65
  locating by group ownership, 4-63,
    4-65, 4-68, 4-76
  ownership, 4-4, 4-9, 4-39
  removing access control list entries,
    4-48, 4-50, 4-63, 4-66, 4-76, 4-78
  replacing access control list entries,
    4-71
  system, 2-58, 2-62
fileset
  NONHPTERM, 2-35
  SAM, 1-21
  X11-RUN, 1-21

fileset partitions, 2-62
filesets, 2-62
file system
  block size, 6-25
  bytes per inode, 6-25
  checking consistency, 6-78
  fragment size, 6-25
  parameters, 6-22, 6-24
  reserved area, 6-25
  root, 2-9
  swap, 7-11
file systems
  capacity, 6-61
  CD-ROM, 6-9
  creating, 2-18, 6-13
  HFS, 6-9
  listing with **bdf**, 6-61
  modifying file name length, 6-55
  mountable, 6-6
  mounting, 6-29
  mounting at bootup, 6-44
  moving, 6-53
  NFS, 6-9
  setting up, 2-18
  types, 6-9
  unmounting at shutdown, 6-50
  unmounting using **umount**, 6-48
  usage, 6-61
file system swap, 7-3
  adding using SAM, 7-23
  adding using **swapon**, 7-36
  allocating, 7-10
  enabling on boot, 7-41
  guidelines, 7-10
  removing, 7-42
  selecting file system, 7-10
  system performance, 7-10
find, 6-62
fragment size file system parameter, 6-25
frecover
  active files, 8-75
  crossing NFS mount points, 8-19
  examples, 8-77–79, 8-83
  syntax, 8-75, 8-83
  viewing index file on device, 8-83
fs_async parameter, A-19
fsck, 6-36, 6-58, 6-78
  -p, 6-46
fsck command, 6-78
full backups, 8-2, 8-8–11, 8-67

G

gecos information, 4-42
getty
  entry for each terminal in **/etc/inittab**, 2-31
GID, 4-2, 4-7, 4-36, 4-58, 4-67
graph file (backups), 8-6
group, 2-28
group-ID, 4-7, 4-36, 4-58, 4-67
group ID, 4-2
group membership, 4-6, 4-58, 4-67
group ownership, 4-2, 4-63, 4-68, 4-76
groups, 4-5
  adding, 2-21, 4-30, 4-58
  adding users to, 4-33, 4-41, 4-72
  defining membership, 4-36, 4-50
  maximum membership, 4-5
  passwords, 4-7
  removing, 4-31, 4-61
  removing users from, 4-33, 4-50, 4-74
  special privileges, 4-8, 4-79

H

HFS file systems, 6-9
host name
  obtained from **/etc/hosts**, 2-33
how to use **rmfn**, 2-63
HP format cartridge tape capacity, 8-15
HP-UX
  constructing a system, 2-1

installing, 2-4
installing for a cluster, 2-5
shut down, 3-9
updating, 2-4
updating in a cluster, 2-5
HP-UX cluster
changing run-levels, 4-87
HP-UX cluster administration, 1-8, 1-9
HP-UX configuration
printer drivers, 9-29, 9-48, 9-49
HP-UX Reference, 1-9
setting up on-line, 2-19
HP VUE, 2-25

I

increasing swap space, 7-4
incremental backups, 8-3, 8-8–11
index files (backup), 8-63
creating using **fbackup**, 8-59
creating using SAM, 8-23, 8-27, 8-34
viewing using **frecover**, 8-83
viewing using SAM, 8-51, 8-53, 8-55
inittab, 2-28
context-dependent file in a cluster, 2-31
editing, 2-31
installing
HP-UX, 2-4
HP-UX for a cluster, 2-5
optional software, 2-4
optional software in a cluster, 2-5
peripherals, 2-6
Installing and Updating HP-UX, 2-4
Installing Peripherals, 2-6
interface scripts (printer), 9-3, 9-6
interleaved swapping, 7-8
issue
editing, 2-33

K

kernel
backup copy (/SYSBCKUP), 2-42
backup kernel for cluster client, 2-42
configuring, 2-38
pseudo-drivers listed, 2-57
reconfiguring to add/remove device drivers using SAM, 2-46
reconfiguring to modify special devices using SAM, 2-51
reconfiguring to modify system parameters using SAM, 2-49
reconfiguring using HP-UX commands, 2-40
when to reconfigure, 2-39
kernel devices. *See* special devices
Korn shell
login files, 2-29, 2-34
.kshrc, 2-29
editing, 2-34

L

lifinit, 6-52
lifls, 6-51
LIF volumes, 6-51
initialization, 6-52
limiting disk usage, disk quotas, 6-64
line-printer spooler
setting up, 2-23
line printer spooling system, 9-1
local disk drive
file system swap, 7-11
locally mounted file system
file system swap, 7-11
local printer, 9-3, 9-14, 9-25, 9-51
locking files for read only, 4-8, 4-80
locking processes into memory, 4-8, 4-80
log files (SAM)
detail, 1-45
summary, 1-44

verbose, 1-45
.login, 2-29
editing, 2-34
log in, 4-2
login
customizing the prompt, 2-33
customizing users' login files, 2-34
message of the day, 2-33
login directory, 4-36, 4-37
long file names, 6-23, 6-55
disabling, 6-60
enabling using convertfs, 6-58
enabling using SAM, 6-57
LPDEST environment variable, 9-10
lp spooler
accepting print requests, 9-19, 9-67
adding a local printer, 9-25, 9-51
adding a network-based printer, 9-33, 9-61
adding a remote printer, 9-30, 9-56
adding printers, 9-25–34, 9-51–61
canceling print requests, 9-73
changing a printer fence priority, 9-44, 9-71
checking status, 9-39, 9-72
collecting printer activity statistics, 9-20, 9-72, 9-83
commands, 9-6
components of, 9-8
controlling with HP-UX Commands, 9-22, 9-45–87
controlling with SAM, 9-22, 9-23–44
creating a printer class, 9-62
device files, 9-13, 9-56
disabling printers, 9-19, 9-40, 9-69
displaying printer activity statistics, 9-83–87
enabling printers, 9-19, 9-42, 9-69
interface scripts, 9-6, 9-11
LPDEST environment variable, 9-10
moving all print requests, 9-75
moving selected print requests, 9-78
network-based printer, 9-14
plotters, 9-18
print destinations, 9-10
printer classes, 9-9
printer models, 9-11, 9-56
printer names, 9-8, 9-56
printer priorities, 9-17, 9-56
printer queues, 9-6
print request, 9-4
print request identification number, 9-14
print request priorities, 9-17, 9-81
print requests, 9-6
priorities, 9-17
rejecting print requests, 9-19, 9-64, 9-67
remote print requests, 9-15
remote spooling, 9-6, 9-15
removing a printer, 9-35, 9-64
removing a printer class, 9-64
removing printers, 9-64, 9-65
request directories, 9-6
scheduler, 9-13
setting up, 9-21, 9-45
starting scheduler, 9-37, 9-65, 9-72
stopping scheduler, 9-37, 9-38, 9-65, 9-72
system default printer, 9-10, 9-25, 9-30, 9-52, 9-56
viewing printer request status, 9-23, 9-79
viewing printer status, 9-23, 9-79

M

magnetic tape capacity, 8-15
mail, 10-2
setting up, 2-22
mailx, 10-2
setting up, 2-22
major number, 6-19

make
problems caused by changing system clock, 2-18
Managing Clusters of HP 9000 Computers, 2-5
managing peripherals, 5-1
manpages
disk space, 2-19
removing source files, 2-20
setting up, 2-19
manuals related to system administration, 1-6
maxdsiz parameter, A-20
maxfiles_lim parameter, A-22
maxfiles parameter, A-21
maxssiz parameter, A-23
maxswapchunks parameter, A-24
maxswapchunks parameter, 7-7
maxtsiz parameter, A-25
maxuprc parameter, A-26
maxusers parameter, A-27
media capacity
DDS format (DAT) tape, 8-16
HP format cartridge tape, 8-15
magnetic tape, 8-15
mediainit, 6-21
memory
virtual, B-1
mesg, 10-2
mesg parameter, A-28
message of the day
posting, 2-33
minfree file system parameter, 6-25
minor number, 6-18, 7-27
minswapchunks parameter, A-29
mkfs, 6-22
file system parameters, 6-22
mknod, 6-18, 7-26
mkrs, 2-9–13
mode
single-user, 2-44
model script (printer), 9-4
modem
moving using HP-UX commands, 5-31
moving using SAM, 5-11
removing using HP-UX commands, 5-41
removing using SAM, 5-22
modifying
special devices using SAM, 2-51
system parameters using SAM, 2-49
the login prompt, 2-33
motd, 10-2, 10-3
editing, 2-33
mount, 6-34, 6-45
-a, 6-44
mountable file systems, 6-6
mount directory, 6-6, 6-29
mounting auxiliary file systems, 6-7
mounting file systems, 6-6, 6-29
at bootup, 6-44
mounting NFS file systems
using HP-UX commands, 6-42
using SAM, 6-38
mount -p, 6-45
moving file systems, 6-53
moving peripherals
disk drive, 5-13, 5-34
local printer or plotter, 5-5, 5-27
root disk drive, 5-36
tape drive, 5-8, 5-29
terminal or modem, 5-11, 5-31
the system console, 5-32
msgmap parameter, A-30
msgmax parameter, A-32
msgmnb parameter, A-33
msgmni parameter, A-34
msgseg parameter, A-35
msgssz parameter, A-36
msgtql parameter, A-37
multiple devices (backup), 8-58

multi-user mode, 4-2

N

nbuf parameter, A-38
ncallout parameter, A-40
ndilbuffers parameter, A-41
netisr_priority parameter, A-42
network-based backups, 8-58, 8-62
network-based printer, 9-4, 9-14, 9-33, 9-61
networking
  documentation, 2-21
  setting up, 2-21
newfs, 6-22, 7-8, 7-29
news, 10-2, 10-3
  setting up, 2-24
nfile parameter, A-43
nflocks parameter, A-44
NFS file system, 6-9
  adding using **mount**, 6-42
  crossing mount points for backups using **fbackup**, 8-19
  crossing mount points for backups using SAM, 8-23, 8-27, 8-29, 8-34
  crossing mount points for recovery using **frecover**, 8-19
  crossing mount points for recovery using SAM, 8-38, 8-41, 8-44, 8-47
  mounting with SAM, 6-38
ngcsp parameter, A-45
ninode parameter, A-46
NONHPTERM fileset, 2-35
non-standard terminals
  setting up, 2-35
nproc parameter, A-47
npty parameter, A-48
nswapdev parameter, A-49
nswapfs parameter, A-50
num_cnodes parameter, A-51

O

on-line documentation
  setting up manpages, 2-19
operating system
  installing, 2-4
  installing for a cluster, 2-5
  parameters, A-1
  updating, 2-4
  updating in a cluster, 2-5
optional software
  installing and updating, 2-4
  installing and updating in a cluster, 2-5
overriding parameter defaults, 6-24

P

parameters, file system
  block size, 6-25
  bytes per inode, 6-25
  fragment size, 6-25
  reserved area, 6-25
parameters, system, A-1
partitions (fileset groups), 2-62
passwd, 2-28
password
  if you've forgotten your root password, 2-7
passwords, 4-34, 4-35
PATH, 11-5
peripherals
  adding, 2-6, 5-4
  adding a local printer, 9-25, 9-51
  adding a network-based printer, 9-33, 9-61
  adding a remote printer, 9-30, 9-56
  installing, 2-6
  Installing Peripherals, 2-6
  moving, 2-6
  moving using HP-UX commands, 5-27–38
  moving using SAM, 5-5–17

not supported by SAM, 5-2
removing, 2-6
removing a printer, 9-64
removing using HP-UX commands, 5-39–43
removing using SAM, 5-18–26
plotter, 9-18. *See also* printer
posting a message of the day, 2-33
post-installation tasks, 2-7
prerequisites (for the system administrator), 1-6
primary group, 4-2, 4-67
primary swap
changing, 7-13
prime time, 11-7
print destinations, 9-3, 9-10
printer
cancel model script, 9-4
classes, 9-9, 9-62
device drivers, 9-29, 9-48, 9-49
environment variable `LPDEST`, 9-10
interface scripts, 9-3, 9-11
local, 9-3
logical, 9-3
model scripts, 9-4, 9-11
moving using HP-UX commands, 5-27
moving using SAM, 5-5
names, 9-8
network-based, 9-4
queues, 9-6
remote, 9-5
removing using HP-UX commands, 9-64
removing using SAM, 5-18, 9-35
setting up the line-printer spooler, 2-23
statistics, 9-20, 9-72, 9-83
status model script, 9-4
system default, 9-5, 9-10
printer class, 9-4, 9-64
printer fence, 9-44, 9-71
printer interface scripts, 9-6
printer name, 9-4
printing
spooled (*see* line-printer spooler), 2-23
print priority, 9-5
print queues, 9-4
print request, 9-4
print request identification number, 9-4, 9-14, 9-73
print requests, 9-6, 9-14, 9-73
print routing (*see* line-printer spooler), 2-23
priorities (printers and print requests), 9-17
process accounting, 11-8, 11-11, 11-32, 11-37
`.profile`, 2-29
editing, 2-34
program
`/etc/config`, 2-43
`/etc/init`, 2-31
`/etc/mkrs`, 2-9
`/etc/mkrs.tool`, 2-9
`/etc/update`, 2-39
`/usr/bin/x11start`, 2-26
prompt
login, 2-33
pseudo-driver
defined, 2-56
list of subsystems and drivers, 2-57

Q

`quot`, 6-74
`quotacheck`, 6-71, 6-77
`quotaoff`, 6-72
`quotaon`, 6-71

R

raw device file
  See *character* device file, 6-2
`rc`, 2-28
  editing, 2-31
reactivating users account, 4-26, 4-53
real-time priorities, 4-8, 4-80
`reboot_option` parameter, A-55
reconfiguring the kernel, 2-38
recovering data. *See* restoring data
  creating a recovery system, 2-7–13
recovery system
  booting, 2-9
  creating, 2-7–13
  device files, 2-10, 2-12
  directories and files in, 2-9
  procedure for making, 2-10
  security, 2-11
reinstalling HP-UX
  to increase primary swap, 7-16
remote printer, 9-5, 9-14, 9-16, 9-30, 9-56
remote spooling, 9-5
remote spooling daemon, 9-5, 9-15
remote system administration, 1-42
removing
  access control list entries, 4-48, 4-50, 4-63, 4-66, 4-76, 4-78
  a user group, 4-31, 4-61
  device drivers from kernel using SAM, 2-46
  peripherals, 2-6
  printer class, 9-64
  printers, 9-35, 9-64, 9-65
  subsystems, 2-56, 2-58
  subsystems using SAM, 2-59
  system files, 2-58, 2-62
  users, 4-19, 4-47
  users from groups, 4-33, 4-50, 4-74
removing device swap, 7-22, 7-34
removing file system swap, 7-42
removing peripherals
  disk drive, 5-24, 5-42
  printer or plotter, 5-18, 5-39
  tape drive, 5-20, 5-40
  terminal or modem, 5-22, 5-41
reporting quotas status
  `quot`, 6-74
  `quota`, 6-74
  `repquota`, 6-73
`repquota`, 6-73
request directories, 9-6
responsibilities of a system administrator, 1-7
restoring data
  all files, 8-18, 8-38, 8-44, 8-75, 8-78
  cartridge tape data blocking, 8-77
  cartridge tapes, 8-77, 8-79, 8-87
  DDS format (DAT) tape, 8-78, 8-79, 8-86
  `frecover`, 8-18, 8-74, 8-75–79
  `frecover` examples, 8-77–79
  `frecover` syntax, 8-75
  from a hard disk using `dd`, 8-81
  index files, 8-52, 8-54, 8-83
  individual files, 8-18, 8-41, 8-47, 8-74, 8-79
  magnetic tape, 8-78, 8-86
  other utilities, 8-86, 8-87
  retrieving index from tape, 8-83
  to a new location, 8-78
  using HP-UX commands, 8-74–82
  using SAM, 8-38–43, 8-44–50
`retry_alive_period` parameter, A-56
`rmfn`
  how to use, 2-63
  removing dependent filesets, 2-62
  removing system files, 2-62–64
  removing unneeded filesets, 2-62
  symbolic links, 2-62
root disk, 5-36
root file system, 2-9, 6-5

run-level, 4-3, 4-12
  2, 4-12, 4-85
  changing, 4-86, 4-87
  changing in an HP-UX cluster, 4-87
  creating new, 4-12, 4-84
  s, 4-3, 4-12, 4-85, 4-88–89
running `config`, 2-43

S

SAM
  access to help, 1-13
  adding and removing subsystems, 2-59
  adding entry for terminal to `/etc/inittab`, 2-31
  customizing the adding and removing a user procedure, 4-21
  customizing the object list, 1-15
  customizing the X window interface, 1-25
  entering, 1-23, 1-26
  exiting, 1-24
  getting into the online help system, 1-12
  logging actions, 1-44
  main menu, 1-23
  overview, 1-11
  primary components, 1-11
  reconfiguring the kernel to add/remove device drivers, 2-46
  reconfiguring the kernel to modify special devices, 2-51
  reconfiguring the kernel to modify system parameters, 2-49
  remote system administration, 1-42
  returning to main menu, 1-24
  tasks, 1-10
  terminal interface, 1-26
  X window interface set up, 1-21
`SAM` fileset, 1-21
SAM logging
  detail level, 1-45
  summary level, 1-44
  turning on, 1-44
  verbose level, 1-45
SAM terminal interface, 1-26
  changing windows, 1-40
  checkboxes, 1-38
  choosing a menu item, 1-37
  control buttons, 1-29
  entering SAM, 1-26
  exiting SAM, 1-32
  functional area navigation, 1-32
  function keys, 1-30
  menubar, 1-36
  menu buttons, 1-37
  navigation with keys, 1-39
  opening a menu, 1-36
  radio buttons, 1-38
  selecting an object, 1-34
  softkeys, 1-30
  unavailable menu items, 1-37
`sbtab`, 2-9
`scroll_lines` parameter, A-58
security, 1-8, 1-9
`selftest_period` parameter, A-59
`semaem` parameter, A-61
`sema` parameter, A-60
`semmap` parameter, A-62
`semmni` parameter, A-64
`semmns` parameter, A-65
`semmnu` parameter, A-66
`semume` parameter, A-67
`semvmx` parameter, A-68
`sendmail`
  setting up, 2-22
`server_node` parameter, A-69
`serving_array_size` parameter, A-71
setting
  date, 2-17
  system clock, 2-14
  system date, 2-16

system time, 2-16
time zone (`TZ`), 2-14
setting date, 3-3
setting internet protocol address, 3-3
setting system name, 3-3
setting time, 3-3
setting time zone, 3-3
setting up
disk quotas, 6-65
electronic mail, 2-22
elm, 2-22
file systems, 2-18
line-printer spooler, 2-23
mail, **mailx**, 2-22
manpages, 2-19
networking, 2-21
news, 2-24
on-line *HP-UX Reference* (manpages), 2-19
recovery system, 2-7–13
sendmail, 2-22
system accounting, 2-27
users and groups, 2-21
X-Windows, 2-26
shell
Bourne, 2-34
C, 2-34
Korn, 2-34
shell initialization files, 4-38
shmem parameter, A-73
shmmax parameter, A-74
shmmni parameter, A-76
shmseg parameter, A-77
short file names, 6-23, 6-55
shut down, 3-9
shutdown authorization, 3-11
shutting down the system, 3-9
single-user mode, 4-3, 4-88–89
required to configure kernel, 2-44
software
installing and updating, 2-4
installing and updating in a cluster, 2-5
special devices
modifying using SAM, 2-51
special group privileges, 4-79
special privilege groups, 4-8
special privileges
accessing **setuid** and **setgid** system calls, 4-8, 4-80
changing file ownership, 4-8, 4-80
locking files for read only, 4-8, 4-80
locking processes into memory, 4-8, 4-80
real-time priorities, 4-8, 4-80
spooled printing (*see* line-printer spooler), 2-23
spooler (*see* line-printer spooler), 2-23
startup
automatic OS selection, 3-7
csh, 4-38
customizing, 2-30
default HP-UX system, 3-6
files, 4-38
file system check, 3-5
keysh, 4-38
ksh, 4-38
prerequisites, 3-2
program, 4-36, 4-38
required files, 3-2
rksh, 4-38
rsh, 4-38
selecting a system, 3-8
sh, 4-38
system configuration, 3-3
status model script, 9-4
subsystem
adding, 2-56
adding using HP-UX commands, 2-56
adding using SAM, 2-59
pseudo-drivers for subsystems, 2-57
removinging, 2-56

removing using HP-UX commands, 2-58
removing using SAM, 2-59
summarizing and reporting accounting information, 11-12, 11-56
summary log file (SAM), 1-44
superuser
if you've forgotten your root password, 2-7
survey
assessing users' needs, 2-2
swap
defined, 7-1
file system, 7-11
swapinfo, 7-5
swapon, 7-30
-a, 7-31
-e, 7-31
-f, 7-31
-p, 7-30
parameters, 7-37
swap priority, 7-12
swap space
allocating, 7-7
assigning priority, 7-12
calculating, 7-4
computing, B-1, B-3
determining current amount, 7-5
device, 7-3
estimating requirements, 7-6
file system, 7-3
implications of changing, 2-8
increasing, 7-4
swchunk parameter, A-78
swchunk parameter, 7-7
swchunks parameter, 7-24
/SYSBCKUP, 2-42
system
constructing, 2-1
files, 2-62
name and host name, 2-33
parameters, 2-49
setting clock, 2-14
setting date and time, 2-16
setting up accounting, 2-27
shut down, 3-9
system accounting
corrupted files, 11-74
crontab entries, 11-4
daily usage, 11-5, 11-63
directory structure, 11-15
errors, 11-66
files, 11-81
holidays, 11-73
installation, 11-3, 11-9
logging in, 11-15
monthly usage, 11-72
overview, 11-1, 11-2, 11-7
shell scripts, 11-76
system data flow, 11-13
system administration
concepts, 1-8, 1-9
HP-UX cluster, 1-8, 1-9
installing and updating HP-UX, 1-8, 1-9
installing peripherals, 1-8, 1-9
manual page references, 1-9
prerequisites, 1-6
related manuals, 1-6
responsibilities, 1-7
system security, 1-8, 1-9
system backups, 8-3
system clock
problems you can cause by changing, 2-18
setting, 2-14
system console
moving using HP-UX commands, 5-32
system date and time
setting, 2-16, 2-17

system default printer, 9-5, 9-10, 9-25, 9-30, 9-52, 9-56
/system directory, 2-62
system files
  described, 6-10
  removing, 2-58
system parameters, A-1
system recovery, 8-84
system security, 1-8, 1-9

T

tape drive
  moving using HP-UX commands, 5-29
  moving using SAM, 5-8
  removing using HP-UX commands, 5-40
  removing using SAM, 5-20
tasks
  after installing HP-UX, 2-7
TERM
  setting, 2-35
terminal interface (SAM), 1-26
terminals
  adding entry to /etc/inittab, 2-31
  creating a terminfo file, 2-37
  moving using HP-UX commands, 5-31
  moving using SAM, 5-11
  non-HP, 2-35
  non-standard, 2-35
  removing using HP-UX commands, 5-41
  removing using SAM, 5-22
  /usr/lib/terminfo/*, 2-35
terminfo
  creating a new file, 2-37
  files under /usr/lib/terminfo, 2-35
time
  Canadian Standard Time, 2-15
  format, 2-16
  setting, 2-16
timeslice parameter, A-79
timezone parameter, A-80
time zone (TZ)
  examples, 2-15
  form of declaration, 2-14
  setting, 2-14
  tzset library routine, 2-14
total accounting records, 11-8, 11-22, 11-27, 11-52, 11-56
tset
  and /etc/ttytype, 2-28, 2-29
ttytype, 2-29

U

UID, 4-3, 4-18, 4-35, 4-42
umount, 6-48
  -a, 6-50
unlockable_mem parameter, A-81
unmounting file systems
  using umount, 6-48
update
  using to add subsystems, 2-56
  using to load HP subsystems, 2-39
updating
  HP-UX, 2-4
  HP-UX in a cluster, 2-5
  optional software, 2-4
  optional software in a cluster, 2-5
updating HP-UX (from a previous release), 1-8, 1-9
user account information, 4-28, 4-55
user_ID, 4-3, 4-18, 4-35, 4-42
user IDs, 6-67
users
  account information, 4-28, 4-55
  adding, 2-21, 4-16, 4-34
  adding a group, 4-58
  adding users to groups, 4-72
  assessing needs, 2-1
  assigning IDs, 6-67

changing primary group membership, 4-67
deactivating account, 4-24, 4-51
defining passwords, 4-35
group membership, 4-6
login directory, 4-37
passwords, 4-34
reactivating account, 4-26, 4-53
removing, 4-19, 4-47
removing from groups, 4-74
startup program, 4-36, 4-38
survey, 2-2
using_array_size parameter, A-82
utility
cron, 2-16, 2-18
elm, 2-22
mail, 2-22
mailx, 2-22
make, 2-18
mkrs, 2-9–13
news, 2-24
rmfn, 2-62–64
sendmail, 2-22
update, 2-4, 2-39, 2-56
uucp, 10-2, 10-5

V

verbose log file (SAM), 1-45
vipw editor, 4-5
virtual memory, B-1

W

wall, 10-2, 10-4
windows, 2-26. *See also* X Windows
worksheet, computing swap space, B-3
write, 10-2, 10-4

X

X11-RUN fileset, 1-21
.x11start, 2-26
x11start, 2-26
X window interface (SAM), 1-21
X Windows
setting up, 2-26
/usr/bin/x11start, 2-26
.x11start, 2-26

WIN AN HP CALCULATOR!

Your comments help us determine how well we meet your needs. Returning this card with your name and address enters you in a quarterly drawing for an HP calculator*.

System Administration Tasks
B1864-90010 E0892

What operating system and hardware do you use? (Type: `uname -rvm` and write the displayed information on the following line.)

__________________ ______ __________________

How much have you used this manual?

______ Extensively ______ Often ______ Occasionally ______ Not at all

----fold here--fold here----

Complete this section only if you have used this manual. Use the column labeled "NC" if you have no comment or opinion regarding that topic.

	Agree					Disagree	NC
The manual is well organized.	○	○	○	○	○	○	○
It is easy to find information in the manual.	○	○	○	○	○	○	○
It tells me clearly what I need to know.	○	○	○	○	○	○	○
It is easy to perform step-by-step procedures.	○	○	○	○	○	○	○
Overall, the manual meets my expectations.	○	○	○	○	○	○	○

Please take the time to describe any problems you've had or any suggestions that would improve our product/manual. Use additional pages if needed. The more specific your comments, the more useful they are to us. Thank you.

Comments:

----fold here--fold here----

○ **Check here if you would like a reply.**

* *Offer expires 8/1/94.*

↑ *Please tape here* **Please print/type the following information** *Please tape here* ↑

Name: ______________________ Telephone: ______________________

Company: ____

Address: ____

City: ______________ State: ______ Zip Code/Country: __________

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST CLASS MAIL PERMIT NO. 37 LOVELAND, COLORADO

POSTAGE WILL BE PAID BY ADDRESSEE

Learning Products HP-UX
Hewlett-Packard Company
3404 East Harmony Road
Fort Collins CO 80525-9988

System Administration Tasks
B1864-90010 E0892

HEWLETT PACKARD

Printed in USA E0892

Reorder No. or
Manual Part No.
B1864-90010

Manufacturing
Part No.
B1864-90010

B1864-90010