

CTIX™ ADMINISTRATION TOOLS MANUAL

Copyright © 1989 by Convergent, Inc., San Jose, CA. Printed in USA.

Third Edition (November 1989) 09-02318-01

All rights reserved. No part of this document may be reproduced, transmitted, stored in a retrieval system, or translated into any language without the prior written consent of Convergent Technologies, Inc.

Convergent makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Further, Convergent reserves the right to revise this publication and to make changes from time to time in its content without being obligated to notify any person of such revision or changes.

Convergent, Convergent Technologies and NGEN are registered trademarks of Convergent, Inc.

Art Designer, AutoBoot, AWS, Chart Designer, ClusterCard, ClusterNet, ClusterShare, Context Manager, Context Manager/VM, CTAM, CT-DBMS, CT-MAIL, CT-Net, CTIX, CTOS, CTOS/VM, CWS, Document Designer, GT, IMAGE Designer, IWS, MiniFrame, Network PC, PC Emulator, PC Exchange, Phone Memo Manager, PT, S/50, S/120, S/320, S/640, S/1280, S/Series, Series/286i, Series/386i, Server PC, Shared Resource Processor, Solution Designer, SRP, TeleCluster, The Cluster, The Operator, Voice/Data Services, Voice Processor, WGS/Calendar, WGS/DESKTOP, WGS/Mail, WGS/Office, WGS/SpreadSheet, WGS/WordProcessor, WorkGroup Servers, and X-Bus are trademarks of Convergent, Inc.

UNIX and RFS are trademarks of AT&T.

This manual was prepared on a Convergent Technologies S/320 Computer System and printed on an Apple LaserWriter II Printer.

About This Documentation

What are the Administration Tools?

With the development of the UNIX operating system came a need for a *system administrator* to perform day to day maintenance on the system. Typically, the administrator had to learn *shell* commands in order to communicate with the system, even to perform basic tasks like adding a user.

More recently, UNIX systems have been set up in environments where the administrator does not have the time or inclination to learn shell commands. Hence, a need for a bridge between the administrator and the shell arose. The *CTIX administration tools* were created to meet that need.

Note: The shell is your CTIX working environment. If you see a #, \$, or % prompt when you log in, your working environment is one of the CTIX programmer's shells.

If you are new to CTIX, see Appendix A for more information on shells and other basic concepts.

When you type the **adman** command from the shell on systems running CTIX, you invoke a series of screens that display lists of commands and options, called *menus*. By selecting commands and options from these menus, you can perform many system administration tasks, such as configuring system hardware, monitoring system status, mounting remote file systems, or performing a backup.

Thus, systems running CTIX can be set up and maintained more easily in environments where the administrator is nontechnical, inexperienced, or both.

The administration tools allow a user to perform certain nonprivileged functions, such as changing his own password or checking the printer status, thus relieving the administrator of certain tasks.

Who Should Use this Manual?

Whether or not you have previous experience with CTIX, you can use the *CTIX Administration Tools Manual* to learn more about the system and how to perform tasks using the administration tools. This manual provides an introduction to CTIX system administration and describes the tools used to automate many of the system administrator's responsibilities.

If you are an experienced system administrator, you can learn how to perform certain administration tasks in a friendly environment. Use this manual in conjunction with the *S/Series CTIX Administrator's Guide* for a complete set of system administration instructions.

How this Manual Is Organized

The following is an overview of CTIX system administration.

Chapter 1, "Getting Started," explains what you need to know before you begin, how to begin, and how to manipulate and move between the administration tools menus.

Chapter 2, "User Administration," shows how to manage the user accounts on the system. It also shows nonprivileged users how to perform management functions on their own accounts.

Chapter 3, "System Status," shows how to gather and interpret information about the status of your system.

Chapter 4, "Backup and Restore," discusses principles and procedures for preserving data, and describes how to recover from system damage by restoring the information preserved using the system backup functions.

Chapter 5, "Disk and File System Administration," discusses disk descriptions and configurations, how to manage file systems, and how to add and delete swap space.

Chapter 6, “SCSI Tape Administration,” discusses SCSI tape drive management functions used by the system administrator and by the nonprivileged user.

Note: The SCSI Tape Service package is only available on SCSI-based systems.

Chapter 7, “Terminal Administration,” shows how to add or delete terminal logins, how to monitor a terminal’s status, how to tune RS-422 lines for maximum performance, and how to add a new remote I/O processor.

Chapter 8, “Printer Administration,” describes printer management functions used by the system administrator and by the nonprivileged user.

Chapter 9, “UUCP Administration,” shows how to set up and maintain electronic mail on your computer and other systems, in order to exchange information between systems.

Chapter 10, “Network Administration,” briefly discusses the principles of managing a network and refers the reader to the *CTIX Network Administrator’s Guide*.

Chapter 11, “Remote File Sharing Administration,” describes the procedures for using the CTIX administration tools to manage the services provided by the Remote File Sharing package.

Chapter 12, “Network File System Administration,” describes the procedures for using the CTIX administration tools to manage the Network File System.

Chapter 13, “Troubleshooting,” contains instructions on problem solving and preventive maintenance. It also describes common problems that can occur and possible solutions.

Appendix A, “Basic Concepts,” explains fundamental CTIX concepts for those unfamiliar with the CTIX system.

Appendix B, “Keyboard Tables,” provides tables that match the actual key names on several CTIX terminals with the virtual key names used in this manual. Refer to this appendix to determine which keys to press on your particular terminal.

About This Documentation

Appendix C, “Network File System vs. Remote File Sharing,” provides a comparison.

Appendix D, “PT and GT Terminals and Keyboards,” provides information for users of the PT/GT line of keyboards. This information is provided for compatibility with earlier versions of hardware.

Conventions Used in this Manual

The following conventions are used throughout this manual:

- Boldface indicates literal characters, such as the CTIX command **adman**, which appear or must be typed exactly as shown.
- Boldface characters followed by a number in parentheses, such as **sh(1)**, are CTIX commands or file formats that are described in the *CTIX Operating System Manual*, also known as the “man pages.” The number in parentheses denotes the section where the man page is located.
- Boldface with the first letter capitalized (**Return**) refers to a virtual keyname.

Since this release of CTIX administration tools runs on many terminal types (and therefore, many different keyboards), this manual refers to keys by virtual (symbolic) key names. For example, where this manual reads **Enter**, you might press **Go**, **Do**, **Linefeed**, or something else, depending on the type of terminal you are using.

See Appendix B, “Keyboard Tables,” to determine the actual key names on your keyboard that match the virtual key names given in this manual.

- Italics (*Share Resources*) indicate that the item is a menu option.
- Italics (*menu*) followed by a definition indicate that the item can be found in the glossary at the end of this manual.

- The ^ symbol indicates that you should hold down **Control** and press another key simultaneously. For example, **^Tab** means you should press **Control**, and while holding it down, press **Tab**.
- The dash (-) indicates that you should press two keys at the same time. For example, **Shift-Help** means you should press both the **Shift** and the **Help** key simultaneously.
- The dollar sign (\$) represents the default programmer's shell prompt; type the command that follows the prompt, not the dollar sign itself.
- The pound sign (#) represents the superuser prompt; type the command that follows the prompt, not the pound sign itself.

Related Documentation

For further information on system administration, consult the *S/Series CTIX Administrator's Guide* or the *CTIX Operating System Manual*.

For detailed information on network administration, see the *CTIX Network Administrator's Guide*.

—

—

—

CTIX™ ADMINISTRATION TOOLS MANUAL

Copyright © 1989 by Convergent, Inc., San Jose, CA. Printed in USA.

Third Edition (November 1989) 09-02318-01
Update Notice 1 (October 1990) 09-02615

All rights reserved. No part of this document may be reproduced, transmitted, stored in a retrieval system, or translated into any language without the prior written consent of Convergent Technologies, Inc.

Convergent makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Further, Convergent reserves the right to revise this publication and to make changes from time to time in its content without being obligated to notify any person of such revision or changes.

Convergent, Convergent Technologies and NGEN are registered trademarks of Convergent, Inc.

Art Designer, AutoBoot, AWS, Chart Designer, ClusterCard, ClusterNet, ClusterShare, Context Manager, Context Manager/VM, CTAM, CT-DBMS, CT-MAIL, CT-Net, CTIX, CTOS, CTOS/VM, CWS, Document Designer, GT, IMAGE Designer, IWS, MiniFrame, Network PC, PC Emulator, PC Exchange, Phone Memo Manager, PT, S/50, S/120, S/320, S/640, S/1280, S/Series, Series/286i, Series/386i, Server PC, Shared Resource Processor, Solution Designer, SRP, TeleCluster, The Cluster, The Operator, Voice/Data Services, Voice Processor, WGS/Calendar, WGS/DESKTOP, WGS/Mail, WGS/Office, WGS/SpreadSheet, WGS/WordProcessor, WorkGroup Servers, and X-Bus are trademarks of Convergent, Inc.

UNIX and RFS are trademarks of AT&T.

This manual was prepared on a Convergent Technologies S/320 Computer System and printed on an Apple LaserWriter II Printer.

Contents

Chapter 1. Getting Started

Introduction	1-1
What Tasks Can Adman Perform?.....	1-2
Setting Up a New System	1-2
Maintaining a Previously Configured System	1-3
Nonprivileged Functions	1-4
Entering the Administration Tools	1-4
Nonprivileged Access.....	1-4
Privileged Access.....	1-5
Exiting the Administration Tools	1-6
How to Get Help.....	1-7
Selecting and Using Forms and Menus	1-8
Moving Within Forms and Menus	1-8
Moving Between Forms and Menus	1-8
Screen Layout	1-9
Keyboard Layout	1-11
Keys that Move the Cursor Between Fields	1-13
Keys that Move the Cursor Within Fields.....	1-14
Keys that Perform an Action.....	1-15
Keys that Perform Other Movements.....	1-16

Chapter 2. User Administration

Introduction	2-1
List User Accounts.....	2-2
Change Your Password	2-4
Add a User.....	2-5
Add a Group.....	2-7

Change User Information	2-8
Change a User's Password	2-9
Delete a User	2-10
Bar a User	2-12
Re-admit a User	2-12
Where to Go from Here	2-13

Chapter 3. System Status

Introduction	3-1
View Hardware Inventory	3-2
Error Log Functions.....	3-4
View Summary Report	3-4
View Detailed Report	3-5
Reset the Error Log	3-6
Console Log Functions	3-6
View the Console Log	3-7
Reset the System Console.....	3-8
Enable/Disable System Activity Reporting.....	3-8
Enable/Disable Process Accounting.....	3-9
Where to Go from Here.....	3-10

Chapter 4. Backup and Restore

Introduction	4-1
Backup Functions	4-2
Complete Backup.....	4-4
Incremental Backup.....	4-6
Partial Backup	4-7
User Backup	4-8
Backup Status Messages	4-9
Backup Quality	4-10

Restore Functions.....	4-11
View Tape Contents.....	4-13
Complete Restore	4-14
Partial Restore	4-15
Restore Status Messages.....	4-19
Where to Go from Here.....	4-20

Chapter 5. Disk and File System Administration

Introduction	5-1
View the Disk Description.....	5-3
Configure a Disk.....	5-5
Planning the Partitioning of a Disk	5-6
How to Bring the System to Single-user Mode.....	5-7
Using the Disk Configuration Tool	5-8
Procedure for Configuring a Disk	5-13
How to Return the System to Multi-user Mode.....	5-16
View or Change Partition Uses	5-16
Determining the Correct Disk	5-17
Determining Partition Uses.....	5-17
Making Changes to Partitions	5-18
File System Operations.....	5-19
Swap Space Operations.....	5-20
Procedure for Viewing or Changing Partition Uses	5-21
Monitor Disk Usage.....	5-22
List Files of a Certain Age	5-24
List Largest Files	5-24
List Largest Users of Disk Space	5-25
Where to Go from Here.....	5-26

Chapter 6. SCSI Tape Administration

Introduction	6-1
View SCSI Tape Status	6-2
Add a SCSI Tape Drive	6-4
Determining that the SCSI Tape Drive Functions Correctly	6-5
Determining the Processor Board	6-5
Procedure for Adding a Tape Drive	6-5
Change Entry Information	6-7
Delete a SCSI Tape Drive	6-8
Where to Go from Here	6-10

Chapter 7. Terminal Administration

Introduction	7-1
Enable a Login on a Serial Port	7-2
Determining the Processor Board	7-3
Determining the Connector	7-6
Determining the Baud Rate	7-8
Determining the Terminal Type	7-8
Disable a Login on a Serial Port	7-9
Configure Cluster Lines and Devices	7-10
Change the Number of Drops/Lines	7-11
Change the Number of Cluster Terminal Logins	7-12
Add or Remove an RIOP	7-12
Extracting an RIOP's Unique ID Number	7-13
Determining the RIOP Software Release Level on your System	7-14
Procedure for Configuring Cluster Lines and Devices	7-17
View Port Status	7-18
Where to Go from Here	7-21

Chapter 8. Printer Administration

Introduction	8-1
View Print System Status	8-2
View Print Queue Status	8-4
Add a Printer	8-4
Determining If the Printer Functions Correctly	8-5
Determining the Connection Type	8-5
Parallel Connections	8-5
Serial Connections	8-5
Remote Connections	8-6
Determining the Printer Name	8-7
Determining the Model Name	8-7
Determining the Processor Board	8-9
Determining the Serial Port Number	8-10
Determining Whether the Remote System is Ready	8-10
Procedure for Adding a Printer	8-10
Change Printer Status	8-12
Remove a Printer	8-13
Set the Default Printer	8-14
Start or Stop the Print System	8-14
Make a Printer Model	8-15
Specifications for Both Parallel and Serial Printers	8-15
Additional Specifications for Serial Printers	8-16
Where to Go from Here	8-18

Chapter 9. UUCP Administration

Introduction	9-1
Show Systems Entries	9-2

Rename This System	9-4
Add a Remote System Entry	9-4
Before Adding a Remote System Entry	9-5
Direct Link	9-7
Sockets Link	9-7
TLI Link	9-7
Phone Link	9-8
Procedure for Adding a Remote System Entry	9-8
Change Entry Information	9-11
Delete an Entry	9-12
Add a Modem to a Port	9-12
Delete a Modem from a Port	9-14
Where to Go from Here	9-14

Chapter 10. Network Administration

Introduction	10-1
Networking Concepts	10-2
User Equivalence	10-3
Machine Equivalence	10-4
Network Administration Procedures	10-4
Machine Status	10-5
Network Users	10-7
Network Setup	10-9
Add an Equivalent User	10-9
Delete an Equivalent User	10-10
Add an Equivalent Machine	10-11
Delete an Equivalent Machine	10-12
Add a Network Service	10-12
Network Service Descriptions	10-13
Network Service Security Considerations	10-14
Delete a Network Service	10-15
Add a New Host Entry	10-16

Change a Host Entry	10-18
Delete a Host Entry	10-18
Network Interface Statistics	10-19
Active Connections.....	10-19
Network Interface.....	10-20
Routing Tables	10-21
Memory Usage	10-23
Protocol Statistics	10-23
Where to Go from Here.....	10-25

Chapter 11. Remote File Sharing Administration

Introduction	11-1
Remote File Sharing.....	11-1
RFS Administration Procedures	11-3
Creating a New Domain.....	11-6
Procedure for Creating a New Domain	11-6
Adding a System to an Existing Domain.....	11-11
Registering a System on the Primary: Primary Administrator Procedures	11-11
Completing the Addition: Non-Primary Administrator Procedures	11-13
Additional Domain Configuration Functions	11-16
Listing Systems Currently in Your Domain	11-17
Adding an Entry for a Primary from a Different Domain	11-17
Managing Secondary Name Servers	11-19
Listing Secondary Name Servers.....	11-19

Adding Secondary Name Servers	11-20
Removing Secondary Name Servers	11-21
Deleting a Specific System from Your Domain	11-22
Deleting All Systems from Your Domain	11-23
Starting and Stopping RFS.....	11-23
Procedure for Starting and Stopping RFS.....	11-24
Sharing Resources.....	11-26
Viewing Advertised Resources	11-28
Viewing Mounted Remote Resources	11-28
Viewing the Remote Resources You Can Use	11-28
Advertising Your Resources.....	11-29
Removing an Advertised Resource	11-31
Mounting Remote Resources	11-32
Unmounting Remote Resources	11-33
Mapping or Excluding Users and Groups	11-33
Procedure for Mapping or Excluding Users and Groups	11-34
Changing Your RFS Password.....	11-36
Displaying the Current Primary Name Server	11-38
Transferring Name Server Responsibilities.....	11-38
Where to Go from Here.....	11-39

Chapter 12. Network File System Administration

Introduction	12-1
Network File System Terms and Concepts	12-1
NFS Administration Procedures	12-3
Setting up NFS on Your Server	12-4
Starting the NFS	12-5
Procedure for Stopping NFS	12-7
Checking the Network File System Status	12-8
Sharing Resources	12-9
Viewing the Local Machine's Exported Resources	12-11
Viewing Mounted Remote Resources	12-11
Viewing Remote Machines Mounted on Your Local Resources	12-11
Viewing the Remote Resources You Can Use	12-12
Exporting Your Local Resources	12-13
Removing a Local Resource from the Export List	12-14
Mounting Remote Resources	12-16
Unmounting Remote Resources	12-17
Where to Go from Here	12-18

Chapter 13. Troubleshooting

Introduction	13-1
User Administration Problems	13-4
System Status Problems	13-6
Backup Problems	13-6
Restore Problems	13-8
Terminal Administration Problems	13-9

Contents

Printer Administration Problems	13-10
Disk and File System Administration Problems	13-12
UUCP Administration Problems	13-15
Terminal Usage Problems	13-16
RFS Administration Problems	13-17
NFS Administration Problems	13-19
SCSI Tape Drive Administration Problems	13-23
When All Else Fails	13-23
Preventive Maintenance	13-24
Where to Go from Here	13-25

Appendix A. Basic Concepts

What Is CTIX?	A-1
The CTIX Shell	A-1
The CTIX Environment	A-2
Who Is the System Administrator?	A-2
What Are File Systems?	A-3
Accessing File Systems	A-3
CTIX File Structure	A-3
File System Security	A-5
Passwords	A-6
Privileges	A-6
Superuser Privileges	A-6
User Modes	A-7
Access Modes	A-7
How to Change Modes	A-8
Where to Go from Here	A-9

Appendix B. Keyboard Tables

Introduction	B-1
Generic (Dumb) Terminal Keyboards	B-3
PT/GT Terminal Keyboards	B-5
TO-250 and TO-300 Terminal Keyboards	B-8
VT-100 Terminal Keyboard	B-10
VT-220 Terminal Keyboard	B-12
Wyse-85 Terminal Keyboard	B-14

Appendix C. Network File System Versus Remote File Sharing

Which is Best?	C-1
Advantages in Using NFS	C-1
Advantages in Using RFS	C-2

Appendix D. PT and GT Terminals and Keyboards

Using PT or GT Terminals	D-1
Terminal Modes	D-1
Exiting menus	D-2
Keyboard Layout	D-2

Glossary

Index

Contents



Figures

1-1	Administration Tools Main Menu	1-6
1-2	General Screen Layout	1-9
1-3	TO250 and TO300 Keyboard Layout	1-12
1-4	PT Keyboard Layout	1-13
2-1	User Administration Menu	2-2
2-2	Sample List of User Accounts	2-3
2-3	Sample Login Information for User 'denise'	2-6
3-1	System Status Menu	3-1
3-2	Sample Hardware Inventory Screen	3-2
3-3	Sample Summary Error Report	3-5
3-4	Sample Console Log Contents	3-7
4-1	Backup and Restore Menu	4-2
4-2	Write-Protect Arrow on a QIC Tape	4-5
4-3	QIC Tape Installation	4-6
4-4	Sample View Tape Contents Screen	4-14
4-5	Sample Partial Restore: Enter Pathnames Screen	4-18
4-6	Sample Partial Restore: Select Files from List Screen	4-19
5-1	Disk and File System Administration Menu	5-3
5-2	Sample Disk Description	5-5
5-3	Sample Proposed State of the Disk Screen	5-10
5-4	Sample View/Change Partition Uses Screen	5-19
5-5	Sample Disk Usage Screen	5-23
6-1	SCSI Tape Administration Menu	6-2
6-2	Sample SCSI Tape Status Screen	6-3
6-3	Sample SCSI Tape Connection Information Screen	6-6
6-4	Sample SCSI Tape Change Entry Information Screen	6-8
6-5	Sample Select a SCSI Tape to Delete Screen	6-9
7-1	Terminal Administration Menu	7-2
7-2	Rear Inside View of a LeftHanded S/640	7-4
7-3	Sample Terminal and Connector Information Screen	7-7
7-4	Example of an RIOP Configuration	7-15

Contents

7-5	Sample Configure Cluster Lines and Devices Screen	7-16
7-6	Sample View Port Status Screen	7-19
8-1	Printer Administration Menu	8-2
8-2	Sample Print System Status Screen	8-3
8-3	Sample Serial Printer and Connector Information	8-9
8-4	Sample Serial Printer Options Screen	8-18
9-1	UUCP Administration Menu	9-2
9-2	Sample Display of Other Systems	9-3
9-3	Sample Confirm Adding Remote System Screen	9-10
10-1	Network Administration Menu	10-5
10-2	Sample Remote Machine Statistics Screen	10-6
10-3	Sample Network Users Screen	10-8
10-4	Sample Network Interface Activity Screen	10-20
10-5	Sample Routing Tables Screen	10-22
10-6	Sample Protocol Statistics Screen	10-24
11-1	RFS Management Menu	11-5
11-2	Set Up Your Machine to Run RFS	11-7
11-3	Configure the Domain	11-12
11-4	Start or Stop RFS	11-25
11-5	Share Resources	11-27
11-6	Map or Exclude Remote Users or Groups	11-35
11-7	Change Your RFS Password	11-37
11-8	Display Current Primary Name Server	11-38
12-1	NFS Management Menu	12-4
12-2	Start NFS	12-6
12-3	Stop NFS	12-8
12-4	Share Resources	12-10
12-5	View ng Available Remote Resources	12-12
12-6	Export a Local Resource	12-13
12-7	Remove a Local Resource from Export List	12-15
12-8	Mount Remote Resources Server	12-16
A-1	CTIX Directory Structure	A-4
D-1	PT Keyboard Layout	D-2

Tables

4-1	Backup Summary Chart	4-3
4-2	Restore Summary Chart	4-12
7-1	S/22X, S/320, S/480, and S/640 Serial Port Numbering	7-20
7-2	S/80, S/280, and S/40XX Serial Port Numbering	7-21
8-1	Printer Models.....	8-8
13-1	Troubleshooting.....	13-2

—

—

—

Chapter 1

Getting Started

Introduction

This chapter shows you how to get started with **adman**, the CTIX program that invokes the administration tools. You will learn to:

- Enter and exit the administration tools
- Get help
- Move the cursor within and between forms and menus
- Make selections

The administration tools consist of a series of screens displaying *forms* and *menus* that allow you to perform certain system functions without having to learn shell commands.

A form is a display containing *fields* of various types. Fields vary in shape and size, depending on the number and format of the items inside. Some fields take up the whole screen, others take up enough space for only a few characters. Depending on the type of field, items in the field can be selected or edited, or if the field is for viewing only, neither selected nor edited. (See Figure 1-2, “General Screen Layout,” for more examples of field types.)

As opposed to a form, a menu is actually a field of selectable noneditable items. In other words, you can choose an item on a menu list, but you cannot change any of the items on the list. A menu may take up an entire screen, or only part of a screen.

This chapter will be especially helpful if you have never used **adman** before, since it provides you with the basics of **adman** tool use. The remaining chapters assume knowledge of these basics.

What Tasks Can Adman Perform?

The following sections describe many of the tasks you can accomplish using the administration tools, whether you are setting up a new system, maintaining a previously configured system, or performing nonprivileged functions.

Note: The CTIX administration tools can be used to perform many system functions; however, you should use the “S/Series CTIX Administrator’s Guide” to learn more about the full responsibilities of system administration.

Setting Up a New System

The following is a partial list of tasks with which the administration tools can help, if you are setting up a new system:

- Setting up user accounts. See “Add a User,” “Add a Group,” and “Change a User’s Password,” in Chapter 2.
- Starting system status checking. See “Error Log Functions” and “Console Log Functions,” in Chapter 3.
- Backing up your system. See “Backup Functions,” in Chapter 4.
- Configuring your disk. See “Configure a Disk,” in Chapter 5.
- Making a file system on a disk that is configured. See “View or Change Partition Uses,” in Chapter 5.
- Adding a SCSI Tape device. See “Add a SCSI Tape Drive” in Chapter 6.

- Adding terminals. See “Enable a Login on a Serial Port” and “Configure Cluster Lines and Devices,” in Chapter 7.
- Setting up your printer system. See “Add a Printer” and “Set the Default Printer,” in Chapter 8.
- Adding systems to the electronic mail system. See “Add a Remote System Entry,” in Chapter 9.
- Choosing between the Network File System and Remote File Sharing. See Appendix C, “Network File System or Remote File Sharing.”

Maintaining a Previously Configured System

If you are maintaining a previously configured system, the administration tools can help you with

- Managing user accounts. See Chapter 2.
- Safeguarding the system. See “Bar a User” and “Change a User’s Password,” in Chapter 2; “Console Log Functions,” in Chapter 3; “Complete Backup” and “Incremental Backup,” in Chapter 4; and “Disable a Login on a Serial Port,” in Chapter 7.
- Restoring lost files. See Chapter 4.
- Looking over your system. See “List User Accounts,” in Chapter 2; “View Hardware Inventory,” “Error Log Functions,” and “Console Log Functions,” in Chapter 3; “View the Disk Description,” in Chapter 5; “View Port Status,” in Chapter 7; “View Printer System Status,” in Chapter 8; and “Show Systems Entries,” in Chapter 9.
- Solving problems that may occur on your system. See Chapter 13.
- Using PT or GT terminals on your server. See Appendix D, “PT and GT Terminals and Keyboards.”

Nonprivileged Functions

If you are not a system administrator, the functions below may be of interest:

- Seeing who the other users are. See “List User Accounts,” in Chapter 2; and “View Port Status,” in Chapter 7.
- Managing your account. See “Change Your Password,” in Chapter 2.
- Getting to know your system. See “View Hardware Inventory,” “Error Log Functions,” and “Console Log Functions,” in Chapter 3.
- Checking the printer status. See “View Print System Status,” in Chapter 8.

Entering the Administration Tools

For examples of privileged and nonprivileged system administration functions, see “What Tasks Can Adman Perform?” at the beginning of this chapter.

Nonprivileged Access

To perform nonprivileged functions within the administration tools:

1. Log into the system.
2. From the shell, type the command:

```
$ adman
```

3. Press **Return**.

Privileged Access

To perform system administration functions that require superuser status:

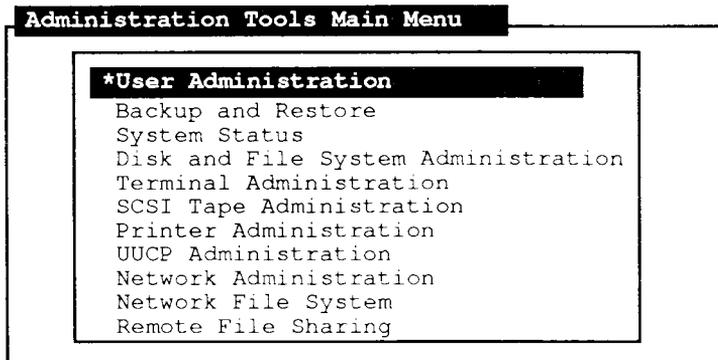
1. Log into the system.
2. From the shell, type the command:
`$ su`
3. Press **Return**.
4. Type the superuser password and press **Return**.
Superuser status is signified by the # prompt.
5. Type the command:
`# adman`
6. Press **Return**.

Caution

Having superuser status allows you access to very powerful system capabilities. Careless use can result in accidental destruction of all data on the system. **Never** disclose the superuser password to anyone, or leave your terminal in superuser mode when you are not present.

For more information on superuser mode and other basic CTIX concepts, see Appendix A.

After you enter the administration tools, the first screen that appears is called “Administration Tools Main Menu.” The menus displayed in the administration tools are affected by the hardware and software options installed on your system. For example, if you do not have TCP/IP installed on your system, you do not see the *Network Administration* option on the main menu.



Select a function and press 'Enter', or press 'Cancel' to exit.

471.5

Figure 1-1. Administration Tools Main Menu

Exiting the Administration Tools

To exit the administration tools, press **Cancel**. On some systems, if you have selected many forms or menus, you may have to press **Cancel** several times to exit the **adman** program. Press **Cancel** once at each menu or form, until you return to the shell prompt.

***Note:** You can always exit an administration tool without executing currently selected items by pressing **Cancel** (^X if on a PT or GT in emulate mode). If you are not sure which key on your keyboard to press to perform a function, see Appendix B, “Keyboard Tables.”*

How to Get Help

You can make selections (using the **Up**, **Down**, **Tab**, and **Return** keys), and you can explore the various forms and menus for each tool with relative safety (using the **Enter** and **Cancel** keys). For more information on how to make selections, see “Selecting and Using Forms and Menus,” later in this chapter.

If your selection will undo a current configuration or destroy data, a confirmation screen is usually displayed, allowing you one last chance to exit (**Cancel**) without executing currently selected items. In the few instances where a confirmation screen is not displayed, this manual warns you.

If you are still confused or lost after you read the associated chapter in this manual, try the following sources for help:

- The prompt line provides information on which keys to use for your terminal. Watch the screen for messages telling you what to do in the current context. See Figure 1-2 for a sample. You can always exit the current form (without executing currently selected items) by pressing **Cancel**. Occasionally, you may see the message: **Press any key to continue**. Do exactly that.
- Press the **Help** key (or the appropriate key for your terminal) to display more information about a function.
- The display can become garbled if the system sends a message to the screen while a menu is displayed. In this case, use ^L to redraw your screen.

- If you encounter a problem using the administration tools, or if you make a mistake, see Chapter 13, “Troubleshooting,” for possible help and instructions.
- If these solutions do not resolve the problem, contact the technical support representative from the vendor who supplied your system.

Selecting and Using Forms and Menus

The following sections describe the basic elements of forms and menus and explain which keys you press to move the cursor and make selections.

Moving Within Forms and Menus

Most forms and menus allow you to move the cursor freely within them. Moving within forms means moving the cursor within a field or menu (using **Up**, **Down**, **Forward**, or **Back**), or from one field to another (using **Tab** or **Return**).

In a menu, the cursor location indicates the current (highlighted) selection. Some menus allow you to make more than one selection; when this is true, the prompt line tells you so, and you use the **Mark** key to make your choices.

Moving Between Forms and Menus

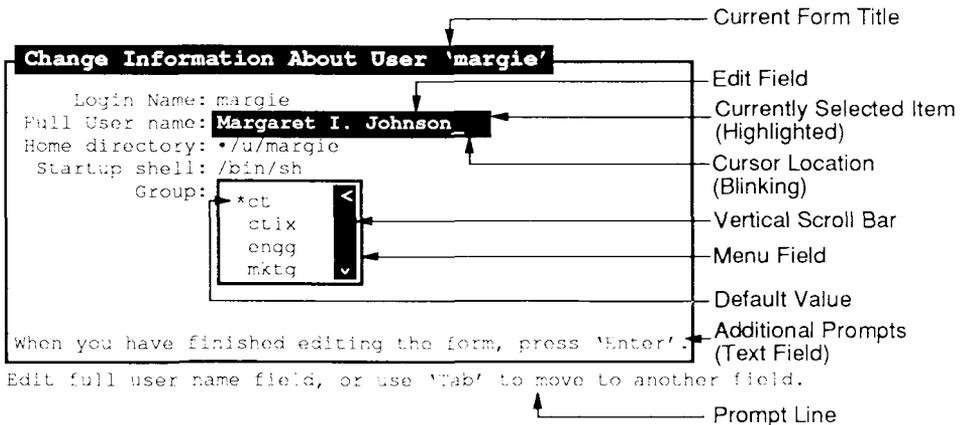
From the screen called “Administration Tools Main Menu,” you can go to another form or menu by moving the cursor to a selection (using the **Up** and **Down** keys) and then pressing the **Enter** key. (See Appendix B, “Keyboard Tables,” if you are not sure which key to press on your terminal.)

To continue moving down (forward) through a series of forms and menus, make another selection and press **Enter**. To move up (backward) through a series of forms and menus without executing currently selected items, press **Cancel**.

Screen Layout

Screens within the administration tools follow a general layout. Figure 1-2 illustrates many of the standard form and menu features, most of which are self-explanatory, such as Current Form Title. Features that are not self-explanatory, such as the asterisk (*), are described following the illustration. To display a screen similar to Figure 1-2, you must be root and

1. From the main menu, select *User Administration*. Press **Enter**.
2. Select *Change User Information*. Press **Enter**.
3. Select a user. Press **Enter**.



471 57

Figure 1-2. General Screen Layout

Chapter 1

- Cursor** The *cursor* indicates your position on the screen and highlights (brightens) the current selection. Select an item with the cursor (using the **Up**, **Down**, and **Tab** keys) and notice how it becomes highlighted.
- Edit Field** When selected, *edit fields* become highlighted (brightened) on the screen. You can add, delete, or modify the information inside by selecting the field and then typing from your keyboard. Examples in Figure 1-2 of edit fields are *Full User Name*, *Home Directory*, and *Startup Shell*.
- Menu Field** *Menu fields* provide a selection of either executable commands or assignable values. For example, in Figure 1-2 the menu field *Group* is a selection of assignable values; the Administration Tools Main Menu is a menu field of executable commands.
- You cannot edit menu fields, but by moving the cursor within them (using the **Up** and **Down** keys), you can select items.
- Some menu fields allow you to choose more than one item, using the **Mark** key to make selections. See “Partial Restore,” in Chapter 4, for an example of a multi-selection menu field.
- Asterisk** *Asterisks* (*) indicate predefined (*default*) selections. The administration tools always provide default values for edit and menu fields, even if the default is null (as in the case of an empty edit field). In Figure 1-2, the default value in the menu field *Group* is *ct*.
- You can change a default by moving the cursor (with the **Up** and **Down** keys); the asterisk moves with the cursor, indicating the change. To save your selection in a menu field, press **Tab** to move to another field.
- Text Field** You can neither select nor edit a *text field*; it is for viewing only. Examples of text fields are prompt lines, Help screens, error messages, and reports generated by the system, such as the Console Log Report.

In Figure 1-2, *Login Name* is a text field. The *Change User Information* tool does not allow you to change a user's login name; therefore, you can neither select nor edit this field.

Vertical
Scroll Bar

The shaded vertical bar with an arrow at the top or bottom (or both) indicates there is more information in the direction of the arrow than is shown. You can scroll through the additional information by moving the cursor in the direction of the arrow (using the **Up**, **Down**, **Page**, and **Shift-Page** keys).

View-only (text) fields and menu fields often contain vertical scroll bars when the list of information or choices exceeds the vertical length of the field.

Some screens, such as *List User Accounts*, described in Chapter 2, are meant for viewing only, and consist entirely of one or more text fields. The format of these screens varies with the information displayed.

Keyboard Layout

The following sections describe the keyboard layout for the TO-250, TO-300, and PT keyboards. A summary of virtual keys and uses is included. For detailed information relating these virtual keys to specific keys on your particular keyboard see Appendix B, "Keyboard Tables."

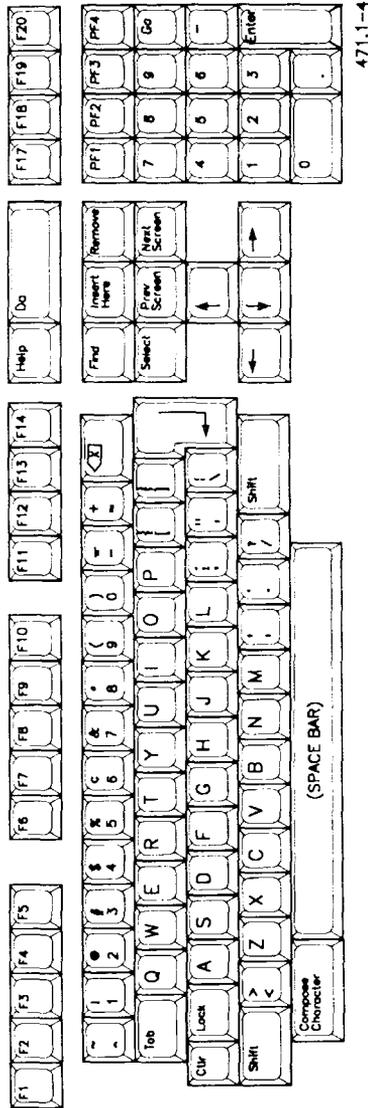
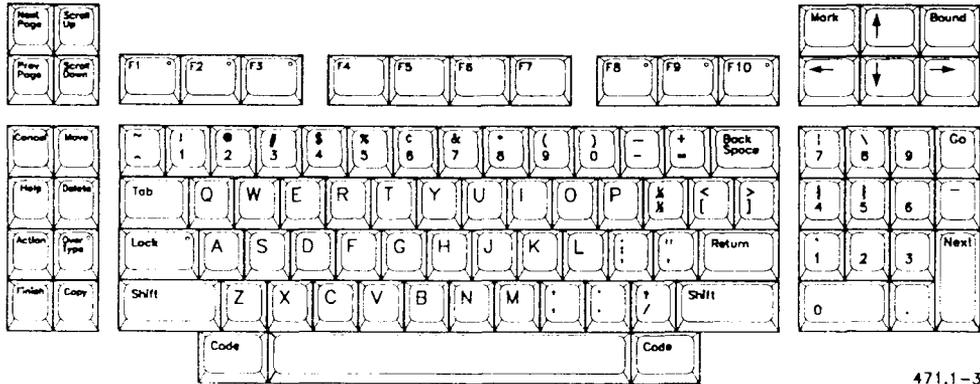


Figure 1-3. TO-250 and TO-300 Keyboard Layout



471.1-3

Figure 1-4. PT Keyboard Layout

Keys that Move the Cursor Between Fields

Virtual Key	Motion
Tab	Moves the cursor to the next field, cycling through all fields and returning to the first field.
Back Tab	Moves the cursor to the previous field, cycling in the opposite direction to Tab .

Keys that Move the Cursor Within Fields

Virtual Key	Motion
-------------	--------

Return	Moves the cursor to the next field, cycling through all fields and returning to the first field, but if the screen contains only one field, the Return key moves the cursor to the next item within the field. If there is a vertical bar indicating additional choices not displayed, pressing the Return key causes the display to scroll.
---------------	---

Up	Moves the cursor higher one item at a time. If the cursor is located on the highest choice in a field, Up moves the cursor to the next higher field, cycling through all fields and returning to the first field.
-----------	--

Down	Moves the cursor lower one item at a time. If the cursor is located on the lowest choice in a field, Down moves the cursor to the next lower field, cycling through all fields and returning to the first field.
-------------	---

Note: To save your selection in a menu field, use the **Tab** key, not the **Up** and **Down** keys, to move the cursor to another field.

Forward	Moves the cursor to the right one character at a time. It does not erase the characters as it moves over them.
----------------	--

Back	Moves the cursor to the left one character at a time. Like the Forward key, it does not erase the characters as it moves over them.
-------------	--

Backspace	In an edit field, the Backspace key erases the previous character.
------------------	---

Delete Character	In an edit field, the Delete Character key, like the Back Space key, erases the previous character.
-------------------------	---

Note: *If you are using a PT or GT, the key that interrupts functions is configurable; it is normally the **Delete** key, but it does not have to be. In functions that take you outside a form or menu, such as *Change Your Password*, use the **Backspace** key to edit keyboard input.*

a-z and **A-Z** In menu fields, the letters **a-z** and **A-Z** move the cursor to the first menu item beginning with the letter(s) typed. In edit fields, the letters **a-z** and **A-Z** appear as you type them.

Keys that Perform an Action

Virtual Key	Action
Enter	Signals that you have completed the selection process and are ready to proceed. When a confirmation screen is displayed, the Enter key activates (executes) the current selection.
Exit	Closes the current form or menu without executing currently selected items, and moves you one or more steps backward through the series of menus. In the main menu, Exit exits the administration tools.
Cancel	Closes the current form or menu without executing currently selected items, and moves you one or more steps backward through the series of menus. In the main menu, Cancel exits the administration tools.

Caution

On a PT or GT in emulate mode, use **^X** (instead of the key labelled **Cancel**) to exit without executing the current selection. Using the key labelled **Cancel**, rather than **^X** (which corresponds to the virtual "Cancel" key), may prevent your terminal from responding to further keystrokes.

Help	Displays further information regarding the function at hand.
Control	Pressed simultaneously with another key to perform an alternate function of the other key; this is also called a <i>control sequence</i> , and is designated in this manual by the \wedge symbol followed by the designated key. For example, on a PT or GT in emulate mode, the control sequence to be used in place of the virtual Cancel key is displayed as $\wedge X$.
Interrupt	Use Interrupt to interrupt a function called by adman , such as the <i>Backup and Restore</i> tool.

Note: *On all CTIX terminals, the **Interrupt** key is configurable. Unless CTIX has been configured to use a different key, the default **Interrupt** key on a PT or GT is the key labelled **Delete**; on a TO-250 the default **Interrupt** key is **Shift-Backspace**.*

To determine the default **Interrupt** key for your terminal, check to see if your terminal type is one of the ones listed in Appendix B. If not, you can check with the vendor who supplied your terminal.

Keys that Perform Other Movements

Virtual Key	Motion
Page	Displays the next page of information. It scrolls one page at a time and may beep if no more information is available. This key is especially useful for scrolling quickly through view-only displays, such as the <i>List User Accounts</i> screen, described in Chapter 2, "User Administration."
Shift-Page	Similar to the Page key above, scrolling in the opposite direction.

- **Roll Down** Moves the text up the screen, allowing you to see further down the page. It can be used in menus as well as in view-only screens.
- **Roll Up** Similar to the **Roll Down** key, but it moves the text down the screen, allowing you to see what precedes the data currently displayed.

—

—

—

Chapter 2

User Administration

Introduction

The *User Administration* tool enables a system administrator to manage user accounts and to help maintain a secure environment. It also enables nonprivileged users to change their own password and to list user accounts.

Note: Every user can contribute to overall system security by maintaining his or her own password and file protection.

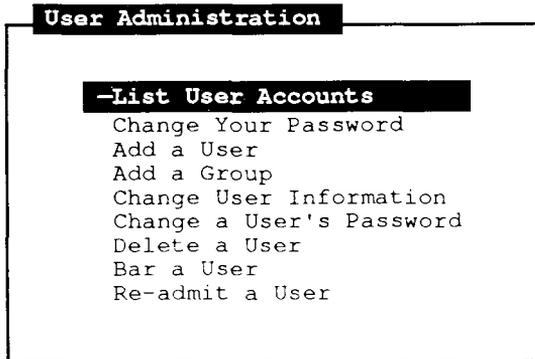
See Appendix A, “Basic Concepts,” for more information on security measures.

In this chapter you will learn how to

- list user accounts
- change your password
- add a user
- add a group
- change user information
- change a user’s password
- delete a user
- bar a user
- re-admit a user

To access these functions, from the main menu, select *User Administration*. Press **Enter**.

The User Administration menu, similar to Figure 2-1, is displayed.



Select a function and press 'Enter', or press 'Cancel' to exit

471.6

Figure 2-1. User Administration Menu

List User Accounts

This tool shows you who the users are on your system; it tells you their login names, full names, home directories, and default shells.

1. From the main menu, select *User Administration*. Press **Enter**.
2. Select *List User Accounts*. Press **Enter**.

List of User Accounts			
Login	Name	Home	Shell
denise	Denise J. Johnson	/u/denise	/bin/sh
margie	Margaret Johnson	/u/margie	/bin/sh
fab4	uucp call in for Fabfour	/usr/spool/uucppub	/usr/lib/uucp/uucico
gomer	Gomer Pyle	/u/gomer	/bin/sh
qtdl	Gt 1.0 232 auto-download	/	/usr/local/bin/qtdl
isam	ISAM Administrator	/usr/isam	
jim	James T. Kirk	/u/jim	/bin/sh
larry	uucp call in for larry	/usr/spool/uucppub	/usr/lib/uucp/uucico
dash	Dashiel Hammet	/u/dash	/usr/local/bin/csh
ptdl	Pt 1.0 232 auto-download	/	/usr/local/bin/ptdl
aggie	Agatha Christie	/u/aggie	/bin/sh
tdl	Pt/Gt 232 auto-download	/	/usr/local/bin/tdl
vinnie	Vince Tarranova	/u/vinnie	/bin/sh
perry	Perry Mason	/u/perry	/bin/sh

Press ^C to exit the form.

4717

Figure 2-2. Sample List of User Accounts

The view-only screen in Figure 2-2 contains the following text fields:

- Login** Lists all the user accounts on the system. User accounts may refer to names of actual users, like **john**, or to system users with a *uid* greater than 99, like **PTDL** (PT Download program). **PTDL** is used when a PT is initialized. (For more information on terminal downloading, see Chapter 5, "Disk and File System Administration.")
- Name** Provides more information about the user account. It lists the full name of the user or the name of the system application.
- Home** Shows you the user's home directory. Often your home directory is where you perform the majority of your work.
- Shell** Tells you which command interpreter is executed when the user logs in. Usually this column contains one of the two standard shells: the Bourne shell or the C shell. The Bourne shell is the *default shell* and is

designated as `/bin/sh`. Some users prefer the C shell, which is designated as `/usr/local/bin/csh`. (See Appendix A for more information on shells.) If this column is blank, the Bourne shell is executed.

Change Your Password

This tool allows you to change your own password, whether you are a nonprivileged user or the system administrator. Passwords are the principal form of security on the system. (See Appendix A for a detailed discussion of passwords.)

1. From the main menu, select *User Administration*. Press **Enter**.
2. Select *Change Your Password*. Press **Enter**.

The system displays a confirmation message.

3. Press **Enter** to continue, or **Cancel** to exit without changing your password.

The screen clears and prompts you for the new password.

4. Type the new password. Press **Return**.

When you type your password, the characters you type are not displayed. The system confirms your password by asking you to retype it.

Your password must be at least six characters long, (only the first eight characters are significant), and it must contain at least one numeric and one alpha character; otherwise, CTIX displays an error message. If you get an error message, type a password that qualifies.

5. Retype the new password. Press **Return**.

You must use your new password the next time you log in.

Add a User

As a system administrator, you will frequently be asked to “put someone on the system” or “give someone an account.” This means adding a user.

Each time a user is added, **adman** creates an entry in the CTIX password file(s). S/Series systems provide two password files: `/etc/passwd` and `/etc/shadow`. If the file `/etc/shadow` exists on your system, you will be given the opportunity to add a password for each new user at the time you add the user. For more information on the `/etc/shadow` file refer to the `shadow(4)` manpage.

1. From the main menu, select *User Administration*. Press **Enter**.
2. Select *Add a User*. Press **Enter**.
3. Type in the user’s login name. Press **Enter**.
4. If you wish, modify the default (system supplied) values given for home directory, startup shell, and group name.

Do not specify a home directory path that includes more than two nonexistent directories at the end of the path. For example, do not specify `/a/b/c/d/e`, where only `/a` exists. The system can only create one directory layer at a time.

You must specify a name in the user’s full name field.

5. Press **Enter** to execute the form.

The system displays a message confirming successful execution.

If the shadow file facility is available on your system, the system prompts you for a password when you add a user. Otherwise, the system prompts new users to create their own password when they log in the first time. If you prefer to assign a password immediately after you add a user, and the shadow file is not

Chapter 2

available on your system, use the procedure called *Change a User's Password* in this chapter.

You can determine whether the user addition was successful by logging in as the new user. If there is a problem, refer to Chapter 13, "Troubleshooting," for help.

The screenshot shows a terminal window titled "User Administration" with a sub-header "Add A User". Below this is a section titled "Login Information for User 'denise'". The fields are as follows:

- Login Name: denise
- Full User name: Denise J. Johnson
- Home directory: /u/denise
- Startup shell: /bin/sh
- Group: *ct (selected from a dropdown menu)

The dropdown menu for the Group field lists the following options: *ct, ctix, engg, and mktg. Below the form, a message reads: "When you have finished editing the form, press 'Enter'."

Edit denise's full user name field, or use 'Tab' to move to another field.

471.8

Figure 2-3. Sample Login Information for User 'denise'

The screen shown in Figure 2-3 contains the following fields:

- Login Name** The login name of the user, customarily the user's first name or three initials in lowercase letters. In the example, the user's login name is **denise**. Login names must be eight or fewer characters.
- Full User Name** More information about the user. For example, Denise's full name is displayed.

Home Directory	Specify the full pathname, using the same name as the login name. (For more information on pathnames, see Appendix A, “Basic Concepts.”) The system supplied pathname (default) for Denise’s home directory is /u/denise .
Startup Shell	If the user prefers to work in the C shell, backspace over the default shell, and substitute the entry /usr/local/bin/csh . See Appendix A for a brief explanation, or see sh(1) and csh(1) in the <i>CTIX Operating System Manual</i> for more information on shells.
Group	This boxed field lists available groups the user can join. Move the cursor through the choices and determine the appropriate group to assign the user to. In the example, denise is a member of the group ctix .

Add a Group

Most systems start with all users originally assigned to one group. Depending on the security level of your files, members of this group may be able to access your files. However, if a small number of users is working on one project, and they do not want everyone in the larger, originally assigned group able to access the project files, adding a group just for them allows them to limit access of their files to group members.

There are two ways to give a user membership in a new group. The first way is to change the user’s assigned group by using *Change User Information*, described later in this chapter. In this case, the user remains a member of only one group.

The second way to give a user membership in a new group is to assign the user to the new group in addition to the originally assigned group. See the chapter in the *S/Series CTIX Administrator’s Guide* that discusses adding users to groups for detailed instructions.

Caution

Groups can be useful, but they pose a security risk: if security is of the utmost importance on your system, do not set up groups other than the one to which all users belong. (See the *S/Series CTIX Administrator's Guide* for more information on maintaining security.)

1. From the main menu, select *User Administration*. Press **Enter**.
2. Select *Add a Group*. Press **Enter**.
3. Type the group name.
4. Press **Enter** to execute.

The system displays a message confirming successful execution.

Change User Information

The first screen displayed in this tool is the list of users from which to choose. The next screen displays the information just as you typed it when you added the user. (See Figure 1-2 for an example.) You cannot change the user's login name with this tool, but you can change the full user name, startup shell, group or home directory.

Note: If you change the user's home directory **adman** creates the new directory but does not move the user's files from his former home directory. Refer to UNIX documentation for information on moving files.

For a description of each field displayed on this screen, see “Add a User,” earlier in this chapter.

1. From the main menu, select *User Administration*. Press **Enter**.

2. Select *Change User Information*. Press **Enter**.
3. Select a user. Press **Enter**.
4. Modify the appropriate fields.
5. Press **Enter** to execute.

The system displays a message confirming successful execution.

Change a User's Password

Use *Change a User's Password* to assign users a new password if they forget their password. If you prefer, use this tool also to assign new users a password after you use *Add a User*; although, the first time a user logs in, he is prompted to create a password. If you use the `/etc/shadow` file on your system, you will be prompted for a password at the time you add a new user.

There are several levels of user restrictions, ranging from password protection to account removal. Preventing unauthorized persons from logging in (and possibly causing harm to your system) is a basic security requirement and is a critical part of your responsibilities as system administrator.

Some users may want to keep the same password indefinitely. In this case, you should inform the user of the security risk this poses and strongly encourage him to change it; do not change it for him.

1. From the main menu, select *User Administration*. Press **Enter**.
2. Select *Change a User's Password*. Press **Enter**.
3. Select the appropriate user. Press **Enter**.

The system displays a confirmation message.

4. Press **Enter** to continue, (or **Cancel** to exit without changing the user's password).

The screen clears and prompts you for the new password.

5. Type the new password. Press **Return**.

When you type the password, the characters you type are not displayed. The system confirms the password by asking you to retype it.

The password must be at least six characters long (only the first eight characters are significant), and it must contain at least one numeric and one alpha character; otherwise, CTIX displays an error message. If you get an error message, type a password that qualifies.

6. Retype the new password. Press **Return**.

Delete a User

When a user should not have access to the system, for example, when an employee has left the company, it is wise to delete his account. Advise the user's manager of your plans *prior* to taking any action, as the manager may need access to the account.

Also, consult the user's manager for the appropriate action to take with the user's files, and archive them before you take the action. An *archive* is a copy of a file that is put on a tape separate from any complete or incremental backup tape the file may already be on. Archive tapes should be recorded in the log, along with backup tapes. Refer to *User Backup*, described in Chapter 4, for instructions on archiving files.

The manager may tell you to do one of the following:

If the task is:

You should:

Leave them alone

Archive them, and then leave them alone. It is important to keep a copy of a user's files exactly as the user left them; archiving allows you to do this.

You can bar the user, or change the user's password

to prevent the former employee from accessing the system.

Move them Archive them, and then move them to the directory the manager specified. Refer to the chapter in the *S/Series CTIX Administrator's Guide* that discusses moving a user's files.

Archive them Archive them.

Remove them Archive them, and then delete them.

1. From the main menu, select *User Administration*. Press **Enter**.
2. Select *Delete a User*. Press **Enter**.
3. Select the appropriate user. Press **Enter**.

The system displays a confirmation message.

4. Press **Enter** to continue (or **Cancel** to exit without deleting the user).

If there are files in the user's home directory, you are prompted to choose

- Don't backup and don't remove
- Backup and then remove
- Don't backup but do remove

The system displays a message confirming successful execution.

Bar a User

Barring a user from the system is different from deleting a user. When you bar users from the system, you prevent them from logging in, but you leave their account intact. For example, a consultant may work on a particular project on your system for a few months, leave, and then return a few months later. It is more efficient to bar and re-admit him than to delete and recreate his account.

1. From the main menu, select *User Administration*. Press **Enter**.
2. Select *Bar a User*. Press **Enter**.
3. Select the appropriate user.
4. Press **Enter** to execute.

The system displays a message confirming successful execution.

Re-admit a User

When you re-admit a user, you return his login privilege. His password does not change; it is the same as it was when the user was barred from the system.

1. From the main menu, select *User Administration*. Press **Enter**.
2. Select *Re-admit a User*. Press **Enter**.
3. Select the appropriate user.
4. Press **Enter** to re-admit the user.

The system displays a message confirming successful execution.

Where to Go from Here

For more specific information about the files and commands the administration tools use to perform user administration, refer to the following items in the *S/Series CTIX Administrator's Guide* and the *CTIX Operating System Manual*:

/etc/passwd

This file contains user account information.

/etc/group

This file contains group account information.

/etc/shadow

This file contains user password information.

/usr/bin/passmgmt

This command updates information in the password files. It works with **/etc/passwd** and **/etc/shadow**.

/usr/bin/pwconv

This command installs and updates **/etc/shadow** with information from **etc/passwd**.

/usr/bin/unpwconv

This command installs and updates **/etc/passwd** with information from **etc/shadow**, removing **/etc/shadow** when complete.

passwd

This command is used to change passwords. It allows the nonprivileged user to change his own password and the superuser to change any user's password.

—

—

—

Chapter 3

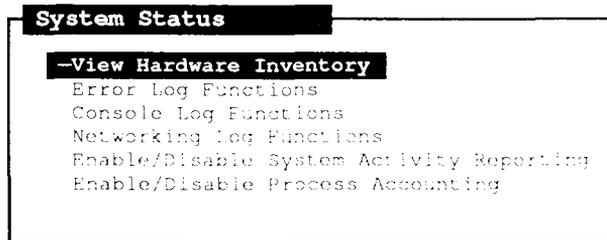
System Status

Introduction

The S/Series system provides many ways for you to monitor use of system resources, detect potential problems before they occur, and keep records of system activity.

This chapter discusses the differences between the various types of system monitoring functions, how to start and stop, how to reset, and clear old statistics.

To access these functions from the main menu, select *System Status*. Press **Enter**.



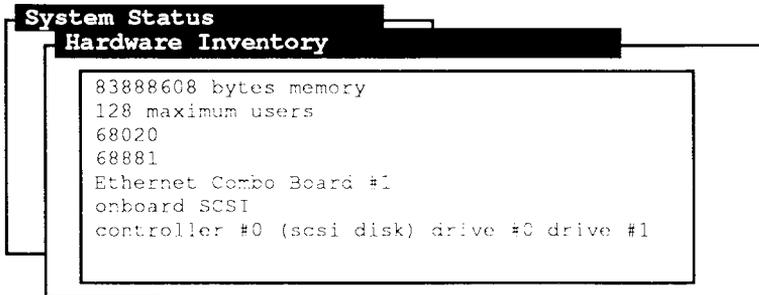
471.9

Figure 3-1. System Status Menu

View Hardware Inventory

As shown in Figure 3-2, the *View Hardware Inventory* tool lists the basic hardware elements of your system. You should be aware of these elements, because they affect your system's operation, and you may be asked about them at one time or another by a service representative or a product vendor.

1. From the main menu, select *System Status*. Press **Enter**.
2. Select *View Hardware Inventory*. Press **Enter**.



Press 'Cancel' to exit this form.

471.10

Figure 3-2. Sample Hardware Inventory Screen

The following basic hardware elements can be displayed on your screen:

- | | |
|---------------|--|
| Memory | All information and executable programs in the system are stored in <i>memory</i> . The amount of memory varies from system to system; in Figure 3-2, the system shown contains 7MB of memory. |
| Maximum Users | This field is not currently used. |

Processor	This number, either 68020 or 68040, refers to the Motorola microprocessor used in your system.
68881	The MC68881 (on an S/80, S/480, or S/640) or MC68882 (on an S/280) floating-point processor is present.
VME Interface	Indicates that your system contains SMD disks or other Virtual Memory Expansion devices. On the <i>Hardware Inventory</i> screen, VME bus configuration information is displayed below the <i>Controller</i> information. Each VME bus device is displayed with its slot number, device type, and board addresses. (See the <i>S/Series CTIX Administrator's Guide</i> for more information on the VME bus.)
232 Board #	Shows how many serial boards your system contains.
422-4	Indicates the presence of an RS-422 cluster board. The last digit shows the number of channels (four, in this example).
Ethernet Combo Board #	Shows how many Ethernet/RS-232 boards are present.
SCSI Combo Board #	Shows how many SCSI/RS-232 boards are present.
onboard SCSI	Shows that the internal (main) bus on this system is a SCSI bus.
onboard Ethernet	Main bus has Ethernet.
Controller	A board installed in your system that manages peripheral devices, such as disks and tape drives. This line displays the disk controller number and the drives controlled by this controller.

enet	An Ethernet/RS-232 board is present or a CMC Ethernet board is in EEPROM.
scsi	A SCSI (Small Computer Systems Interface) is present.
hwfloat	Hardware floating point is present. (Floating point is integral to 68040-based systems.)

For more information on these and other hardware inventory elements, see **hinv(1M)** in the *CTIX Operating System Manual*.

Error Log Functions

The system error-detecting process generates a log with general error information. The error log functions allow you to

- View a summarized error report
- View a summarized error report with a system profile
- Reset the error log

View Summary Report

The summary error report shows the error status of your system. It displays unrecovered and recovered errors, I/O operations, errors unable to be logged, and the date of the earliest and latest entry into the report. If your system has a VME bus, the summary error report also includes VME bus device error information.

1. From the main menu, select *System Status*. Press **Enter**.
2. Select *Error Log Functions*. Press **Enter**.
3. Select *View Summary Report*. Press **Enter**.

System Status
Error Log Functions
Error Log Display

```
Summary Error Report   Prepared on Nov 9 15:43   Page 1
Error Types: All
Limitations:
Date of Earliest Entry: Thu Nov 9 05:00:08 1989
Date of Latest Entry: Thu Nov 9 05:00:08 1989

Total Stray Interrupts           - 0
Total Serial Driver Errors       - 0
```

Press 'Cancel' to exit the form.

471.11

Figure 3-3. Sample Summary Error Report

View Detailed Report

The detailed error report includes a system profile in addition to the information shown in the summary error report. The system profile displays the operating system version, the system type, the amount of system memory, and the last time the error log was reset. If your system has a VME bus, the detailed error report also includes VME bus device error information.

1. From the main menu, select *System Status*. Press **Enter**.
2. Select *Error Log Functions*. Press **Enter**.
3. Select *View Detailed Report*. Press **Enter**.

Reset the Error Log

Resetting the system error log clears the old data out of the log and copies it into another log (deleting the previous old data), thereby keeping the error log current and brief.

1. From the main menu, select *System Status*. Press **Enter**.
2. Select *Error Log Functions*. Press **Enter**.
3. Select *Reset Error Log*. Press **Enter**.

The system displays a confirmation message.

4. Press **Enter** to confirm, (or **Cancel** to exit without resetting the error log).

The system displays a message confirming successful execution.

Console Log Functions

The *console* is a terminal to which the system sends important status information. The terminal can be a real terminal, or a file representing an imaginary terminal. If the console specified is a file, all information that would otherwise appear on the console screen is sent to the specified file. The system console log differs from the system error log in that it records system status and activity messages in addition to errors.

If this report shows error messages about “deferred bad blocks” or “panic mode,” and your system is experiencing operating problems, use the *S/MT Series Diagnostics Manual* to determine the source of the error(s), or contact your service representative.

The console log functions allow you to

- view the console log
- reset the system console

View the Console Log

It is very important that you monitor the console log frequently. This log informs you when your system needs immediate attention, for example, when you are out of resources such as disk space.

Refer to Chapter 13, “Troubleshooting,” for more information on what to do when you receive serious error messages.

1. From the main menu, select *System Status*. Press **Enter**.
2. Select *Console Log Functions*. Press **Enter**.
3. Select *View Console Log*. Press **Enter**.

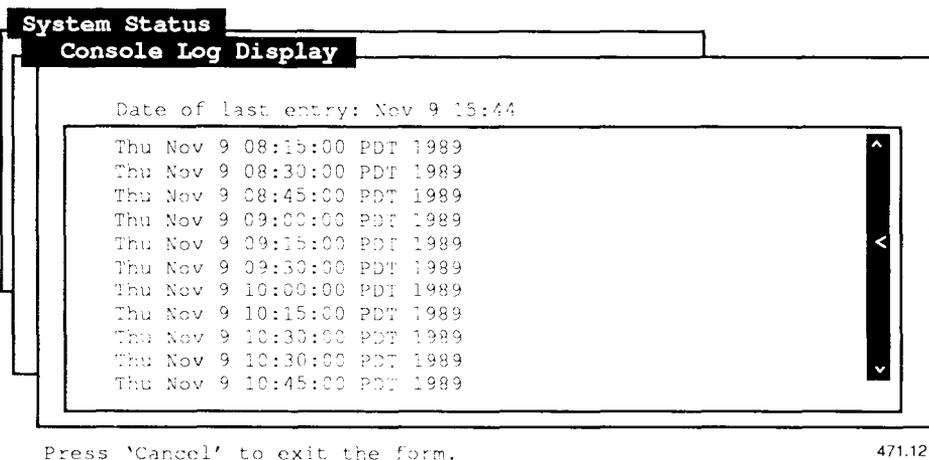


Figure 3-4. Sample Console Log Contents

The console log displays the most current information first. Note that the only messages displayed in Figure 3-4 are date messages. The date is automatically entered into the log at regular intervals to help you determine the approximate

time a problem occurred. By scrolling back through these messages, you may find older information indicating when the system was turned on or off.

Reset the System Console

Resetting the console log keeps a copy of the old messages (deleting the previous old messages) and starts a fresh log for the new ones.

Since a date message is printed in the console log every fifteen minutes, the console log grows rapidly. The system automatically resets the console log when it reboots; however, every now and then you may want to reset the log yourself (for example, if it gets difficult to view all the contents).

Note: Do not reset the console log until you have attended to all the messages, and none require further investigation.

1. From the main menu, select *System Status*. Press **Enter**.
2. Select *Console Log Functions*. Press **Enter**.
3. Select *Reset System Console*. Press **Enter**.

The system displays a confirmation message.

4. Press **Enter** to confirm, (or **Cancel** to exit without resetting the system console).

The system displays a message confirming successful execution.

Enable/Disable System Activity Reporting

The System Activity report includes detailed statistics regarding disk input and output activities, file access activities, and other system-wide measurements.

This tool allows you to turn the reporting process on or off, thereby opening the report to accept entries, or closing it to further entries.

1. From the main menu, select *System Status*. Press **Enter**.
2. Select *Enable/Disable System Activity Reporting*. Press **Enter**.

The system displays the current status of the System Activity Reporting function.

3. Press **Enter** to change the current setting (or **Cancel** to exit without changing the current setting).

The system displays a message confirming successful execution.

Note: It is a good idea to leave the System Activity Reporting and Process Accounting functions disabled unless you intend to measure system performance or resource usage, or you have some other specific purpose: these functions use valuable disk resources and generate reports that consume large amounts of disk space.

Enable/Disable Process Accounting

The Process Accounting function records resource utilization and monitors system activities such as login records and system shutdowns; it also allows you to charge fees to specific login accounts for disk usage. As with System Activity Reporting, you can turn Process Accounting either on or off.

1. From the main menu, select *System Status*. Press **Enter**.
2. Select *Enable/Disable Process Accounting*. Press **Enter**.

The system displays the current status of the Process Accounting function.

3. Press **Enter** to change the current setting (or **Cancel** to exit without changing the current setting).

The system displays a message confirming successful execution.

Where to go From Here

For more information on the console and the console log, read the chapter in the *S/Series CTIX Administrator's Guide* that discusses system maintenance and troubleshooting. Also refer to Chapter 13, “Troubleshooting,” for troubleshooting assistance.

For more information on viewing a System Activity report, read the chapter in the *S/Series CTIX Administrator's Guide* that discusses the System Activity package, particularly the `sar` command. You might want to print the activity reports on a weekly or biweekly basis and then remove them, since they can grow quite large.

For more information on viewing a Process Accounting report, read the chapter in the *S/Series CTIX Administrator's Guide* that discusses process accounting. As with the activity reports, you might want to print the accounting reports on a weekly or biweekly basis to control disk space.

For more specific information about the files and commands used to perform system status functions, refer to the following items in the *S/Series CTIX Administrator's Guide* and the *CTIX Operating System Manual*.

acct

This command represents the set of commands involved in process accounting.

hinv

This command inventories the system hardware.

sar

This command invokes system activity reporting.

/etc/log/confile

This is the console log file.

/usr/adm/acct

This directory contains process accounting reports.

/usr/adm/sa

This directory contains system activity reports.

—

—

—

Chapter 4

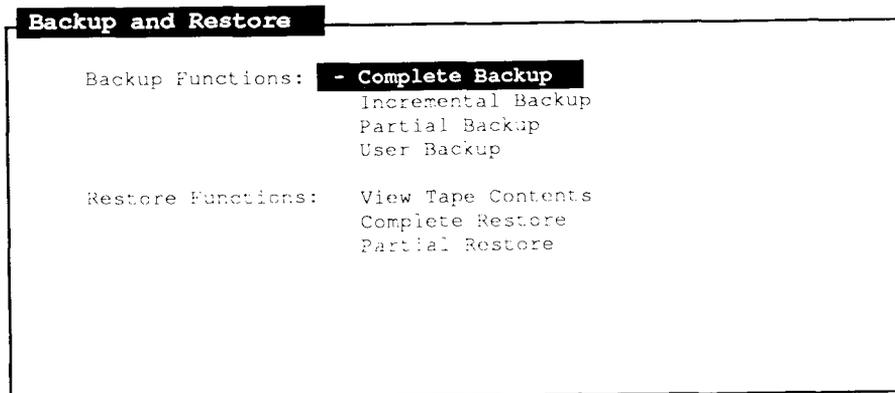
Backup and Restore

Introduction

A *backup* is a duplicate of the information stored on your fixed disk(s), and any currently mounted remote filesystems. To avoid backing up remotely mounted filesystems, unmount them before starting the backup operation. Because the duplicate data is preserved on a separate storage medium, you are protected from losing valuable work if something goes wrong with your system. Backups on an S/Series system are usually stored on a quarter-inch tape cartridge (QIC). The administration tools assume you are using a QIC in drive 0.

A *system restore* is the opposite of a system backup. A backup takes information from a disk and copies it onto a tape; a restore takes information from a tape and copies it onto a fixed disk.

To access the backup or restore functions from the main menu, select *Backup and Restore*. Press **Enter**.



Select a function and press 'Enter', or press 'Cancel' to exit.

471.13

Figure 4-1. Backup and Restore Menu

Backup Functions

Providing backups that are thorough, current, and easy to restore is one of your key responsibilities as a system administrator. This section discusses the types of backups, how to do them, when to do them, and how to assure their success. The goal is to have the latest version of every file easily available so that restores can be done as efficiently as possible.

While backups help protect against system damage, they are also used to retrieve an older version of a particular file; therefore, keep the backup tapes for a reasonable length of time before you recycle them. Table 4-1 summarizes a good backup schedule and suggested retention periods.

Table 4-1. Backup Summary Chart

Backup	Frequency	Retention
Permanent, complete	Monthly	Indefinitely
Regular, complete	Weekly	Four weeks
Incremental	Daily	Two weeks
Partial	As needed	Indefinitely
User	As needed	Indefinitely

Backups are for your users, so let them know your schedule. Most users try to stay off the system when they know you are backing up their files. Pick a time when the least activity on the system occurs, and try to perform backups during the same time each day.

Caution

If files in the system are busy, then the backup or restore will fail to include those files. That is why it is best to perform backup/restore operations with no users on the system.

Complete Backup

A complete backup copies your entire system, along with any mounted remote filesystems onto one or more tapes. Complete backups can be regular or permanent. The only difference between the two is the length of retention; the procedure for each is identical.

Regular Complete Backup	You should completely back up your system every week. These backup tapes should be kept for four weeks and are called <i>regular, complete backups</i> .
Permanent Complete Backup	Every fourth week, a regular, complete backup should be performed as usual, and should be set aside for permanent safekeeping. These backups are called <i>permanent, complete backups</i> . As a further precaution, you might consider storing these at a different site.

If you have remotely mounted resources on your system, those resources will be backed up also. If you do not intend to backup remotely mounted resources, unmount them before beginning the backup process. See Chapter 11, “Remote File Sharing Administration” and Chapter 12, “Network File System Administration” for instructions on unmounting remote resources.

1. From the main menu, select *Backup and Restore*. Press **Enter**.
2. Select *Complete Backup*. Press **Enter**.
3. The system displays a “Ready Tape” message. Make sure the write-protect arrow (see Figure 4-2) on the tape cartridge is *away* from SAFE; then insert the tape cartridge into the drive (see Figure 4-3), and close the latch.
4. Press **Enter**.

The system displays each filename being backed up.

5. If there is more data than can fit on one tape, the system prompts you to remove the first tape, insert the next tape, and press **Return**. Do so only if you see a message requesting such actions.

The backup then continues, and the system displays each filename being backed up.

6. Wait until you see the message **Press any key to continue**. Press any key. Remove the tape from the drive.
7. Label the tape. Turn the write-protect arrow on the tape cartridge to **SAFE** to prevent the tape being overwritten.

See “Backup Status Messages” later in this chapter for more information.

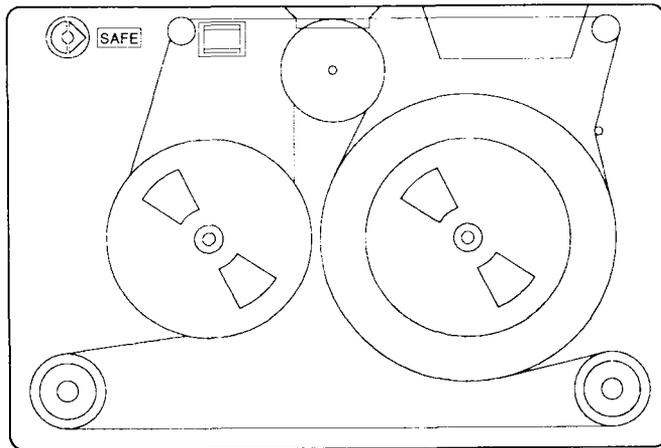


Figure 4-2. Write-Protect Arrow on a QIC Tape

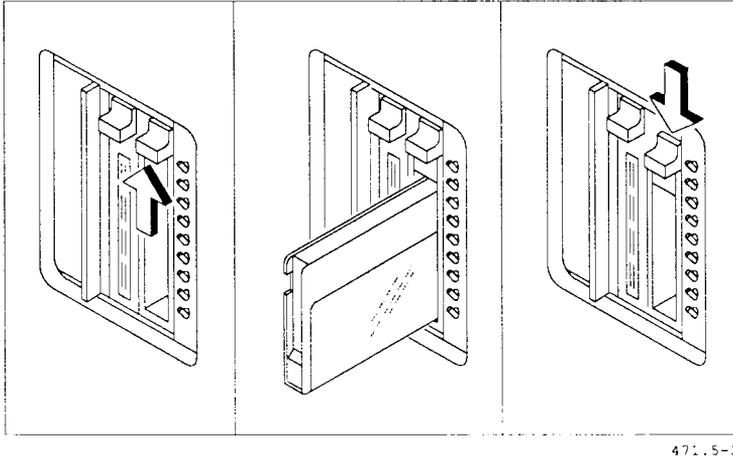


Figure 4-3. QIC Tape Installation

Incremental Backup

Incremental backups contain only the files that have changed since the last complete backup was performed. Incremental backups are smaller, take less time, and should be performed more often than complete backups: perform incremental backups daily to ensure adequate coverage.

1. From the main menu, select *Backup and Restore*. Press **Enter**.
2. Select *Incremental Backup*. Press **Enter**.

3. The system displays a “Ready Tape” message. Make sure the write-protect arrow (see Figure 4-2) on the tape cartridge is *away* from SAFE; then insert the tape cartridge into the drive (see Figure 4-3), and close the latch. Press **Enter**.
4. The system displays each filename being backed up.
5. If there is more data than can fit on one tape, the system prompts you to remove the first tape, insert the next tape, and press **Return**. Do so only if you see a message requesting such actions.

The backup then continues, and the system displays each filename being backed up.

6. Wait until you see the message **Press any key to continue**. Press any key. Remove the tape from the drive.
7. Label the tape. Turn the write protect arrow on the tape cartridge to SAFE to prevent the tape being overwritten.

See “Backup Status Messages” later in this chapter for more information.

Partial Backup

Partial backups allow you to select a particular file or directory tree to archive, specified by the full pathname. Partial backups are also one way to move files from one system to another.

1. From the main menu, select *Backup and Restore*. Press **Enter**.
2. Select *Partial Backup*. Press **Enter**.
3. Type in the full pathname of the file or directory to be backed up.
4. Press **Enter**.

The system displays the files to be backed up.

5. Press **Enter** to confirm the list of files to be backed up.

6. The system displays a “Ready Tape” message. Make sure the write-protect arrow (see Figure 4-2) on the tape cartridge is *away* from SAFE; then insert the tape cartridge into the drive (see Figure 4-3), and close the latch.

7. Press **Enter**.

The system displays each filename being backed up.

8. If there is more data than can fit on one tape, the system prompts you to remove the first tape, insert the next tape, and press **Return**. Do so only if you see a message requesting such actions.

The backup then continues, and the system displays each filename being backed up.

9. Wait until you see the message **Press any key to continue**. Press any key. Remove the tape from the drive.
10. Label the tape. Turn the write protect arrow on the tape cartridge to SAFE to prevent the tape being overwritten.

See “Backup Status Messages” later in this chapter for more information.

User Backup

User backups allow you to archive the files in a user’s home directory. Always do a user backup before removing a user’s files.

1. From the main menu, select *Backup and Restore*. Press **Enter**.
2. Select *User Backup*. Press **Enter**.
3. Select the user whose files you want to backup. Press **Enter**.

The system displays the files to be backed up.

4. Press **Enter** to confirm the list.

5. The system displays a “Ready Tape” message. Make sure the write-protect arrow (see Figure 4-2) on the tape cartridge is *away* from SAFE; then insert the tape cartridge into the drive (see Figure 4-3), and close the latch.

6. Press **Enter**.

The system displays each filename being backed up.

7. If there is more data than can fit on one tape, the system prompts you to remove the first tape, insert the next tape, and press **Return**. Do so only if you see a message requesting such actions.

The backup continues, and the system displays each filename being backed up.

Label each tape. Turn the write protect arrow on the tape cartridge to SAFE to prevent the tape being overwritten.

8. Wait until you see the message **Press any key to continue**. Press any key. Remove the tape from the drive.

See “Backup Status Messages” for more information.

Backup Status Messages

A backup may take several minutes or over an hour, depending on the amount of information to be backed up. You do not need to stay at your terminal during the backup; however, pay attention to the following status messages, which may be displayed:

File list build begins...

Informs you that the backup is building the list of files to be backed up.

Removing *filex* from filelist.

If you get this message, the file called *filex* is not included in the backup.

See “Where to Go from Here” later in this chapter for more information.

Chapter 4

Backup begins...

Informs you that the file list has been created and the files are starting to be copied to tape. The files are displayed on the screen as they are copied.

Backup interrupted (or canceled) by user.

Displayed if you stop the backup before it is complete. It asks you to confirm whether the interruption is intentional, or whether it is accidental and you want to continue the backup.

Insert reel number X, then type Return.

Indicates the backup has filled one tape, and it is safe to remove the tape and insert another one.

Backup complete.

Indicates the backup finished successfully. It is followed by the number of blocks of information that were transferred to the tape.

Backup failed.

Indicates the backup did not finish successfully. Refer to Chapter 13, “Troubleshooting,” for help.

Backup Quality

Besides doing backups regularly, you should keep an accurate log of the following items:

- tape number
- date of backup
- type of backup
- contents
- volume number (if the backup uses more than one tape)

Good records help you find the right backup tape quickly and also make restoring files easier.

The other major factor in backup quality is the tape itself. Occasionally, a tape suffers from wear and tear or arrives in defective condition from the factory. Receiving defective tapes from the factory is rare, but it does occasionally occur.

If you are uncertain about the quality of a backup tape, try to read the contents of the tape. (See “View Tape Contents” later in this chapter for instructions.) It is not necessary for you to verify every backup, or every tape, but you should perform this test occasionally, even if you do not suspect any tape faults. Testing a tape you plan to use for permanent backups is a good preventive maintenance technique.

Another simple task you should perform to maintain the quality of a backup tape is to retension each cartridge before you first use it, and after every eight hours of use. Keeping tape cartridges properly tensioned helps ensure their reliability and full life service. To retension a tape cartridge, insert it into the drive, close the door, and from the shell prompt, type:

```
tsioctl -c retension /dev/rmt0
```

Press **Return**.

Restore Functions

The goal of performing backups is to have the latest version of every file easily available so that restores can be done as efficiently as possible. This section explains the different types of restores, when to use each type, and how to assure their success.

In a rushed situation, you can save time by using your backup log to quickly determine and find the correct backup tape. See “Backup Quality,” in this chapter, for a discussion of what information should be kept in a backup log.

Chapter 4

The restore functions shown in Figure 4-1 are designed to take advantage of the different types of backups. Use Table 4-2 as a reference, when reading the sections that follow.

Table 4-2. Restore Summary Chart

Type of Restore	From Type of Backup	To Restore
Partial	Complete	The latest version of a file or a directory
Partial	Incremental	The latest version of a file or a directory
Partial	Partial	A file or a directory from an archive
Partial	User	A file or directory from a user's home directory
Complete	Complete	All files on the system
Complete	Incremental	All files on the system that have changed since the last complete backup
Complete	Partial	An entire archive
Complete	User	A user's home directory

When a restore is needed, attend to it as quickly as possible, whether it is a single file you need to restore, or an entire file system you need to reconstruct. See Chapter 5, "Disk and File System Administration," and Appendix A, "Basic Concepts," for more information on file systems.

Caution

If files in the system are busy, then the backup will fail to include those files. That's why it is best to perform backup/restore operations with no users on the system.

View Tape Contents

This tool helps you determine whether or not a tape contains the file(s) you want to restore. Use this tool to list files with their security levels (mode), owners, sizes, dates of last modification, and full pathnames. (For more information on security levels, see Appendix A, "Basic Concepts.")

Note: It may take the system several minutes to build the list of files on the tape before they are displayed.

1. From the main menu, select *Backup and Restore*. Press **Enter**.
2. Select *View Tape Contents*. Press **Enter**.
3. The system displays a "Ready Tape" message. Make sure the write-protect arrow (see Figure 4-2) on the tape cartridge is turned *toward* SAFE; then insert the tape cartridge into the drive (see Figure 4-3), and close the latch.
4. Press **Enter**.

The system displays the names of files on the tape.

5. Remove the tape from the drive.

If the file you need to restore is not listed, check your backup log to determine which backup the file may be on. You can also view the contents of a tape without actually loading the tape. See "Where to Go from Here" later in this chapter for more information.

View Tape Contents

Mode	Owner	Size	Date		Name
100644	denise	7195	Nov 19 16:27:22 1989		doc/admintools2/tool
100644	denise	10092	Nov 30 17:28:23 1989		doc/admintools2/tools.a
100644	denise	8333	Nov 29 16:27:22 1989		doc/admintools2/tools.b
100644	denise	1536	Nov 9 16:32:42 1989		doc/admintools2/tools.front
100644	denise	12168	Nov 18 16:27:22 1989		doc/admintools2/tools.gloss
100644	denise	10751	Nov 9 16:27:23 1989		doc/admintools2/tools.l
100644	denise	17439	Nov 9 16:27:23 1989		doc/admintools2/tools.l0
100644	denise	19399	Nov 9 16:27:24 1989		doc/admintools2/tools.l1
100644	denise	13039	Nov 9 16:27:24 1989		doc/admintools2/tools.l2
100644	denise	15117	Nov 9 16:27:24 1989		doc/admintools2/tools.l3
100644	denise	10914	Nov 29 16:27:25 1989		doc/admintools2/tools.l4
100644	denise	10064	Nov 9 16:27:25 1989		doc/admintools2/tools.l5
100644	denise	12292	Nov 19 16:27:25 1989		doc/admintools2/tools.l6

Press 'Cancel' to exit the form. 47114

Figure 4-4. Sample View Tape Contents Screen

Complete Restore

Restoring completely means unconditionally copying all the files on a tape onto the disk. You will probably need to do a complete restore if your system has suffered major disk damage.

Caution

Doing a complete restore unconditionally overwrites all existing files with older versions of the files. For example, if a file was changed after you did a backup, the older version (the version on tape) is restored and overwrites the newer version.

If the backup tape contains mounted remote filesystem files on it, the current files will be overwritten.

1. Determine the correct tape from your backup records.
2. Unmount any currently mounted remote filesystems.
3. From the main menu, select *Backup and Restore*. Press **Enter**.
4. Select *Complete Restore*. Press **Enter**.
5. The system displays a “Ready Tape” message. Make sure the write-protect arrow (see Figure 4-2) on the tape cartridge is turned *toward* SAFE; then insert the tape cartridge into the drive (see Figure 4-3), and close the latch.
6. Press **Enter**.

The system displays each filename being restored.

7. If the data resides on more than one tape, the system prompts you to remove the first tape, insert the next tape, and press **Return**. Do so only if you see a message requesting such actions.

The restore then continues, and the system displays each filename being restored.

8. Wait until you see the message **Press any key to continue**. Press any key. Remove the tape from the drive.

See “Restore Status Messages” later in this chapter for more information.

Partial Restore

Partially restoring files from a backup tape means you selectively choose which files on the tape you want to restore, as distinct from restoring everything on the tape. If a user has requested the restore, find out the following facts:

- the full pathname of the file or directory to be restored

- the date the file was last modified or the date of the version the user wants

Check your backup log to determine the correct *tape* to use. For example, if the user requested that you restore the file `/u/john/memo.sk`, and the last time the user modified the file was 3 days ago, the file would probably be on the next incremental backup taken after that date.

The *Partial Restore* tool allows you to choose the method by which you prefer to specify filenames: either by typing the full pathnames or by selecting from the tape file list.

As shown in Figure 4-5, you can type in up to four pathnames to be restored at a time. *Wild cards* allow you to refer to more than one file using a particular character. For example, you could restore all of `/u/john` and `/u/joe` by typing `/u/jo*` as a pathname. The asterisk is called a wild card, since it refers to anything that may come after the `"/u/jo"` character string.

Another wild card is the question mark. The question mark matches a single character, as distinct from the asterisk, which matches any number of characters. For example, typing `/u/john/report?` would refer to the files in john's directory named `report1`, `report2`, `reports`, and so on.

An example of selecting filenames from the tape file list is shown in Figure 4-6. To perform a partial restore:

1. First determine the correct *tape* from your backup log.
2. From the main menu, select *Backup and Restore*. Press **Enter**.
3. Select *Partial Restore*. Press **Enter**.
4. Choose the method of specifying files to restore. Press **Enter**.
5. If you chose to type the filenames from your keyboard, type in up to four full pathnames of the files or directories to be restored. (Wildcards are allowed.) Press **Enter** and proceed to Step 7.

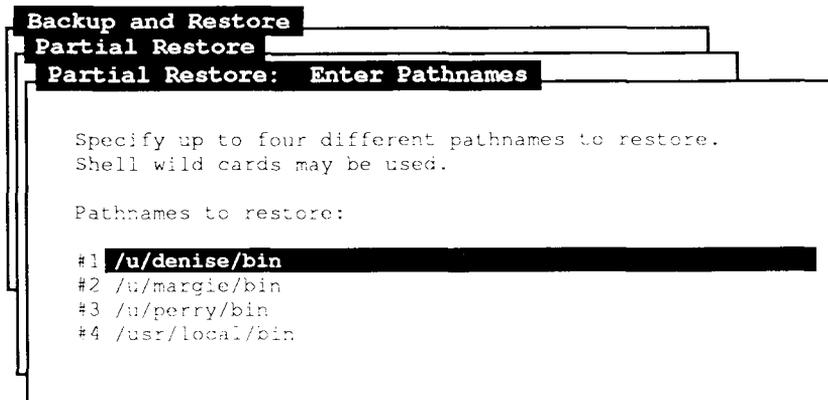
If you chose to select filenames from the tape file list, the system displays a “Ready Tape” message. Make sure the write-protect arrow (see Figure 4-2) on the tape cartridge is turned *toward* SAFE; then insert the tape cartridge into the drive (see Figure 4-3), and close the latch. Press **Enter**.

It may take the system several minutes to build the list of files on the tape before they are displayed.

6. Select up to 50 filenames to restore (using the **Mark** key). Proceed to Step 8.
7. The system displays a “Ready Tape” message. Make sure the write-protect arrow (see Figure 4-2) on the tape cartridge is turned *toward* SAFE; then insert the tape cartridge into the drive (see Figure 4-3), and close the latch.
8. Press **Enter**.

The system displays each filename file being restored. If a filename is not displayed, it is not on the tape.

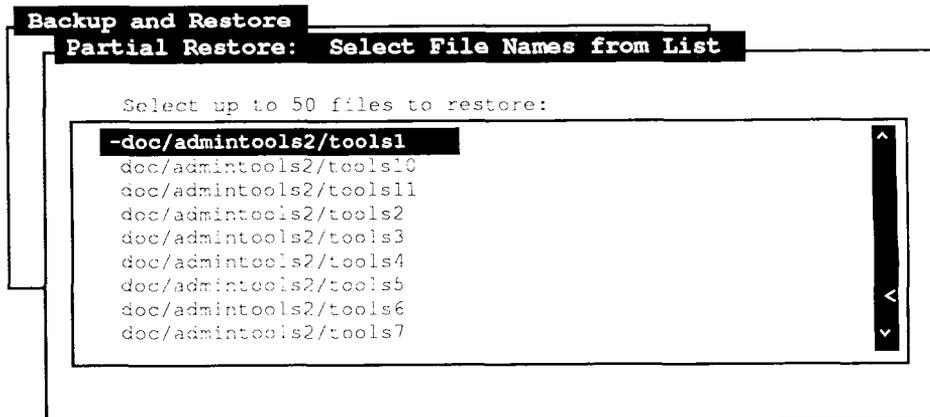
9. If the data resides on more than one tape, the system prompts you to remove the first tape, insert the next tape, and press **Return**. Do so only if you see a message requesting such actions.
The restore then continues, and the system displays each filename being restored.
10. Wait until you see the message **Press any key to continue**. Press any key. Remove the tape from the drive.



Enter one pathname per line; press 'Enter' to start restore program.

471.15

Figure 4-5. Sample Partial Restore: Enter Pathnames Screen



Press 'Mark' for each file to restore, 'Enter' to begin restore program.

471.16

Figure 4-6. Sample Partial Restore: Select Files from List Screen

The restore is successful when you have confirmed that the file has been restored to the correct place, and when the user who requested the restore has permission both to read the file and to write to it. Be sure to inform the requester of the completed restore.

You can check the success of the restore by typing the `ls -l` command from the shell. This command displays information about a file, such as its size, the date it was last modified, its owner, and its security level. (Refer to the *CTIX Operating System Manual* for details on the `ls` command.) See “Restore Status Messages” for more information.

Restore Status Messages

A restore may take several minutes or more than an hour, depending on the amount of information to be restored. You do not need to stay at your terminal during the restore; however, you should pay attention to the following status messages that may be displayed:

Attempting to restore unconditionally (or lost files only).

Displayed only during a partial restore, this message indicates your selection has been confirmed and is being searched for on the tape.

Restore begins...

Informs you that the files are starting to be copied from the tape to the disk. The files are displayed on the screen as they are restored.

Restore interrupted by user.

Displayed if you stop the restore before it is complete. It asks you to confirm whether the interruption is intentional or accidental, and if you want to continue the restore.

Insert reel number X, then type Return.

Indicates that the backup used more than one tape and that it is safe to remove the tape and insert the next one in the series.

Restore complete.

Indicates the restore finished successfully. It is followed by the number of blocks of information that were restored.

Restore failed.

Indicates the restore did not finish successfully. Refer to Chapter 13, “Troubleshooting,” for help.

Where to Go from Here

For more specific information about the commands used to perform system backups, refer to the following items in the *S/Series CTIX Administrator's Guide* and the *CTIX Operating System Manual*:

cpio

This command is used to back up and restore information using a tape. It can also be used to move large directories within the system.

find

This command is used to search through the system for certain files, and to perform a backup of those files.

/usr/lib/adman/logxx

This file is a log created in the backup process that contains the list of files that were backed up. If you want to check the contents of a backup tape, you can look at this log instead of loading the tape and using the *View Tape Contents* tool. This log is found in the above file, where xx is the day of the backup. Note that if space is scarce, these logs can be removed without harming the system.

/usr/lib/adman/compexcl.l

/usr/lib/adman/incexcl.l

These files are used to exclude certain files from the backup. If there are files displayed in the **Removing filex from filelist** message that you do want backed up, or if you want to add files to the excluded list, use an editor to modify this file. (Many introductory UNIX books that describe how to use a UNIX editor are available commercially.)

/usr/lib/adman/lastcomp

/usr/lib/adman/lastinc

These files record the date of the last complete and incremental backups, respectively.

/tmp

The administration tools use this directory to hold files created during the backup process, that is, the list of files to be backed up. Note that **/tmp** contains files that are temporary; they are removed automatically when the system is turned on and are also removed periodically by the system.

For more specific information about the files and commands used to perform system restores, refer to the *S/Series CTIX Administrator's Guide* and the *CTIX Operating System Manual*.

—

—

—

Chapter 5

Disk and File System Administration

Introduction

Disk and file system administration involves managing the disk storage space on your system. In this chapter you will learn to

- determine a disk's characteristics
- organize a disk and separate it into partitions
- change the use of a partition on a disk
- monitor disk usage
- generate various disk usage statistics

A *disk* is a device on your system for storing large amounts of information. Two kinds of "on-board" disks for an S/Series system are 5 1/4-inch disks, ST506s and SCSI (Small Computer System Interface) disks. Another disk that can be used in some S/Series systems is the Storage Module Drive (SMD). An SMD usually holds more data than an ST506 disk. To use an SMD, your system must have VME (Virtual Memory Expansion) capability.

A *disk controller* is a processor board on your system that performs low-level operations relating to disk input and output. One ST506 controller supports up to three ST506s, one SMD controller supports up to two SMDs, and a SCSI bus supports up to seven peripheral devices, such as disks.

To make them easier to manage, disks are divided into smaller sections, called *partitions*. Note that partitions are sometimes referred to as *slices*: the terms are synonymous and are used interchangeably. A partition begins and ends on a *track* boundary. On a non-SCSI drive, a track boundary is normally a multiple of

Chapter 5

8 or 16 blocks; for SCSI disks, a track is one 1024-byte block. A *block* is a unit of measurement for data, and can be either *logical* (1024 bytes) or *physical* (512 bytes).

Each disk has at least one and, at most, 16 partitions. In order for users to be able to create files in a disk partition, you must create a *file system* to hold those files. When you make a file system, you create the data structures that support file and directory operations in a disk partition.

A file system often contains files and directories that are logically grouped together. For example, all of the users' home directories can be located in a file system called `/u`. Library files and many of the programs invoked by shell commands are typically placed in a file system called `/usr`. (See Appendix A, "Basic Concepts," for more information on CTIX shells and file systems.)

The *system disk*, typically (but not necessarily) "on-board drive 0," is the *boot device*, containing `/unix` (the system image). Use *View/Change Partition Uses*, described later in this chapter, to identify the system disk; it has a partition called "Root File System," which contains `/unix` and most of the essential system files and programs.

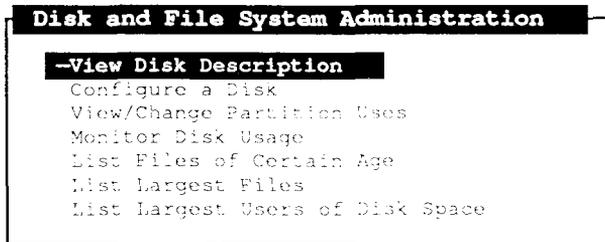
File systems must be *mounted* (attached directly or indirectly to the root file system) to be accessible to users. You must specify an empty directory to serve as the *mount point*. If the directory you specify does not exist, the tool creates the directory for you; however, the directory immediately above it must exist.

The mount point is the place a new file system takes in the CTIX file system hierarchy; thus, the full pathname of the mount point is prefixed to all the files mounted onto that point. For example, if you mount a file system on the empty directory `/u/ed`, all files in the file system being mounted will begin with the pathname prefix `/u/ed`.

Note that the system creates a **lost+found** directory in the new file system; this directory is used by the **fsck** (file system checking) program.

The number of file systems that can be mounted at any one time, regardless of the total number of partitions that contain file systems, is a system configurable parameter, set to 16 by default. Each partition can have one file system; often, all the partitions on a disk contain file systems.

Partitions without file systems are used for *swap space* (auxiliary storage for internal memory in a virtual memory operating system, such as CTIX) and for other special applications, such as a database. To use these functions from the main menu, select *Disk and File System Administration*. Press **Enter**.



Select a function and press 'Enter', or 'Cancel' to exit.

471.17

Figure 5-1. Disk and File System Administration Menu

View the Disk Description

This tool allows you to select a disk and view the contents of the *Volume Home Block* (the block of data at the beginning of a disk that describes physical characteristics of the disk, partition information, and terminal download images).

Chapter 5

A *terminal download image* is the software required to run a PT (programmable terminal) or GT (graphics terminal) when the PT or GT is being run as an “intelligent” terminal. The functions of an intelligent terminal (as opposed to those of a *dumb* terminal) are directed by a program.

If the terminal download image is specified in the system disk description (the system disk is typically, though not necessarily, the first drive on controller 0), the image can be transferred to the memory in a PT or GT when you boot the terminal. “Terminal Modes,” in Appendix D, explains the steps involved.

1. From the main menu, select *Disk and File System Administration*. Press **Enter**.
2. Select *View Disk Description*. Press **Enter**.
3. Select a disk. Press **Enter**.

Note that the size of each partition shown in Figure 5-2 is in logical (1024 byte) blocks. For more information on the Volume Home Block and how this information is used, see the *S/Series CTIX Administrator's Guide*.

Description of Controller 0: On-board drive 0

```

Partition list:
#      Size in 1K blocks      type      HD
                                name      117041
                                cylinders  918
                                heads      15
                                sectors     17
                                informattedbytes 612
                                sloprate    14
                                hilech
                                ecc
                                badlocktable 2
                                loader      /user/lib/iv/loader
                                dump       1024
                                downloadarea 290

Terminal download images:
100  /user/lib/iv/ws100.422
200  /user/lib/iv/ws100.422
    
```

Press 'Cancel' to exit the form.

471.52

Figure 5-2. Sample Disk Description

Configure a Disk

The *Configure a Disk* tool allows you to change the boundaries of some partitions on a selected disk.

You bring the system to single-user mode, specify changes to individual partitions, backup (optionally) individual file systems that will be destroyed, confirm all changes, and then start the configuration program.

Planning the Partitioning of a Disk

In determining whether or not to change partition boundaries on a disk, consider the following reasons for creating separate partitions:

- You may have more than one use for a particular disk, such as file systems, swap space, or database and/or other applications.
- You may want to limit the growth of a particular user or application that can otherwise consume massive amounts of space undetected.
- You may want to limit the potential for loss of data. For example, data corruption in a directory file can cause all of the data below that block in the file system hierarchy to be lost. (Regular backups also can prevent major losses.)
- You are fairly certain that, because of the predictable nature of the users involved, it is highly unlikely that partitioning the disk (establishing limitations on disk space usage) will create an inconvenience later.

Generally, it is a good idea to isolate users' files from the root and `/usr` file systems. You may want all users to share a file system (`/u`, for example), or you may want separate file systems for groups of users.

Consider the following reasons why partitioning a disk may also become an inconvenience:

- On a disk with limited space, the needs of users may vary over time, thus creating the need for repartitioning.
- Depending on the amount of data and the number of users involved, reconfiguring and restoring from backup can become a complex, time consuming process.
- Some partitions may go relatively unused while others are totally full.

How to Bring the System to Single-user Mode

To configure a disk, you must first bring the system to *single-user* mode. Bringing the system to this mode ensures that no other users are accessing data on a disk that you are in the process of configuring.

To bring the system to single-user mode, wait until all other users have logged off, then follow these steps:

1. Exit **adman**.
2. Log in as **root**, if you have not already done so.
3. Type the shell command that prints the current working directory:

```
# pwd
```

and press **Return**. If you are not in the / directory, change the working directory to / by typing:

```
# cd
```

and pressing **Return**.

4. Type:

```
# /etc/shutdown
```

and press **Return**. (*/etc/shutdown* allows you to send a warning message to any users currently logged in before taking the system to single-user mode.)

5. When you see the # prompt, you have reached single-user mode, and you can continue with the *Configure a Disk* procedure, below.

Using the Disk Configuration Tool

So that you can enter your *terminal type* if the system asks you to, determine what type of terminal you are using before proceeding.

Caution

It is possible to accidentally destroy entire file systems while configuring disks. Be sure to perform a Complete Backup before selecting *Configure a Disk*.

The first menu displayed in the tool lists all of the disk drives on your system. A disk is identified by its drive number, controller type, and controller number. The drive number is determined by the cable connector attached to the drive. The controller type is either on-board (ST506), SMD, or SCSI.

The controller number is determined by the configuration of your CTIX *kernel*, the part of CTIX that manages system resources. For example, if you have both on-board disks and SMD disks, controller 0 can be either the ST506 controller or the SMD controller, depending on the way CTIX was installed and on whether your kernel was reconfigured.

Similarly, the Disk number depends on the *jumpering* on the device, if the disks are SCSI. For example, you may have drive 0 and drive 2. There is no drive 1; drive 2 was defined as such by the jumpering.

When you select a disk from the first menu, the tool first verifies that the volume structures are valid and readable, and then it gathers information about the partitions on that disk.

If the tool detects an error when it performs the initial checks, write down the error message. If you receive the message “Volume Home Block is unreadable,” the data on the disk is inaccessible and probably lost. You can often reformat a disk whose volume structures are unreadable by using a diagnostics tape, or call the technical support representative from the vendor who supplied your system.

The tool is unable to make changes to a disk that contains overlapping partitions and reports an error if any are found. To remove overlapping partitions, you should read the appropriate sections in the *S/Series CTIX Administrator's Guide*. The following is a general overview of the process required to remove overlapping partitions. The process of removing overlapping partitions is beyond the scope of this manual and involves a basic knowledge of using an editor and working from the shell to modify partition information.

1. Create a disk description file using the **iv -d** command from the shell.
2. Use a text editor, such as **vi**, to modify the disk description file. A dollar sign (\$) following a starting block specification in the partition information section of the file means that the partition extends to the end of the disk. Remove all dollar signs following starting block specifications, except for the last \$, since the last partition extends to the end of the disk)
3. Run the **iv -u** command to change partition information.

For more information on the **iv(1)** command and the elements of a disk description file, see the *CTIX Operating System Manual* and the *S/Series CTIX Administrator's Guide*.

The second menu lists all of the current partitions on a selected disk. Note that the tool is NOT able to determine whether or not a partition contains a database. If there is a file system in a partition, the tool identifies it by its file system name; if there is a database in a *raw* partition, the tool is only able to determine that there is no file system present. A partition is ineligible for changes to its boundaries under the following circumstances:

- The partition is Partition 0 (Reserved Area).
- The partition is a critical system resource, such as main swap or root file system.
- The partition contains a file system needed by **adman**.
- The partition is currently mounted.

Caution

Any time you change the boundaries of a partition that contains data, all of the data in that partition is destroyed.

Before the tool runs the configuration program, you are given the opportunity to backup any file systems that will be destroyed.

Controller 0: On-board drive 0

Part- ition	File system	Use	1K Blks	Free 1K Blks	Label	Cur Mnt
0		Reserved Area	1360			
1		Root fs	16000	4369	/	
2		main Swap	8000			
3		/usr fs	20000	5687	usr	/usr
-4		/u fs	20000	-2281	u	

Total: 110161

Only partitions marked with an asterisk in the 'Filesystem' column are eligible for modification.

After you have finished modifying partitions, press 'F6' to confirm the proposed disk layout.

Select an eligible partition for modification and press 'Enter'.



47118

Figure 5-3. Sample Proposed State of the Disk Screen

The screen shown in Figure 5-3 contains the following columns:

Partition	A section (slice) of the disk. Note that the last partition extends to the end of the disk.
Elig	Only partitions marked with an asterisk (*) in this column are eligible for modification. (Partition 0 is always reserved and cannot be modified.) A “++” symbol in this column indicates that boundary (starting and/or ending block) changes are to occur as a result of the changes you specified.
Use	The contents of the partition, to the extent that the tool can determine the contents. The root file system, main swap, add-on swap, and other file systems (identified by “fs”) are identified. The file system name in this column corresponds to the normal mount point for the file system.
1K Blks	The total number of logical (1K) blocks in the partition. Note that the tool adjusts the value you specify in a partition change so that the partition begins and ends on a track boundary, normally a multiple of 8 or 16 blocks (on non-SCSI disks). (On SCSI disks, a track is one logical block.) The total beneath the box represents the total size of the disk in 1K blocks.
Free 1K Blks	The number of free logical blocks in the partition if it contains a file system. After you propose changes, this number is recalculated to reflect the “fit” of the current file system in the new partition. For example, if you propose to shrink the partition to a point below where the current file system could fit, a negative value is displayed.
Label	The partition label, if there is one. (The label is what is specified to the CTIX labelit command, and is used to help you identify the partition contents. For example, the adman program labels a partition when it creates a file system in it.)
Cur mnt	The mount point for the partition if its file system is currently mounted.

Chapter 5

Depending on the eligibility of adjacent partitions, you are given the options *SHRINK*, *EXPAND*, *SPLIT*, and *COMBINE*, or only *SPLIT*. If your drive is already divided into the maximum number of partitions, *SPLIT* is disallowed and only *SHRINK*, *EXPAND* and *COMBINE* display. In each of these operations where you specify size, blocks are 1K (1024 bytes), and your input is adjusted so that partitions begin on track boundaries.

You can specify the size as either an absolute size or as a relative (difference + or -) size. For example, to change a 40,000 block partition to 30,000 blocks, either type 30000 or type -10000.

When you shrink a partition, you make it smaller by giving the extra blocks to an adjacent partition. Correspondingly, when you expand a partition, you take blocks from an adjacent partition. When you combine partitions, you make one partition out of two adjacent partitions.

In each of these four operations (*SHRINK*, *EXPAND*, *SPLIT*, and *COMBINE*), two partitions are actually involved: the partition you selected for modification, and an adjacent partition that changes as a consequence of the operation. Thus, if no adjacent partition is eligible (perhaps because there are only two partitions on the disk, one of which is the Reserved Area), only the *SPLIT* option is displayed.

When you split a partition, only that partition is changed. To create a new partition, split an existing partition.

After the reconfiguration is complete, the system displays a list of *orphaned* file systems (that is, file systems that were previously mounted onto directories in file systems that have been destroyed). You must redefine the orphaned file systems' mount points.

For example, if the directory **/u/margie** was the mount point for a file system called **/u/margie/letters**, and the file system called **/u** was destroyed, then you must recreate a new file system called **/u** with an empty directory called **margie**, before you can mount **/u/margie/letters**.

(To create a file system, see "View or Change Partition Uses," later in this chapter.)

Procedure for Configuring a Disk

1. Once you have brought the system to single-user mode, type:

/etc/dcnfstart

and press **Return**. If you are asked to enter your terminal type, do so and press **Return**.

2. When the *Configure a Disk* screen is displayed, select a disk. Press **Enter**.
3. Select a partition. Press **Enter**.

Only partitions marked with an asterisk (*) in the *Elig* column are eligible for modification.

4. Select a modification. Press **Enter**.

Only modifications that are possible for the partition you selected are displayed in the menu.

No modifications to the disk are actually made until after you select *CONFIRM* and the system displays a final confirmation message, and you then press **Enter**.

5. If you chose *SHRINK* or *EXPAND*, type the relative number of blocks (preceded by a + or -) or the absolute number of blocks for the modification specified, press **Tab**, mark the partition to add or delete blocks from. Next press **Enter**.

If you chose *SPLIT*, type the absolute number of blocks for either the first or the second part of the selected partition, press **Tab**, mark the partition to be this size (the first or second).

If you chose *COMBINE*, select the partition to be merged with the partition you initially chose (sometimes there is only one partition that can be combined), and press **Enter**.

6. The ten highlighted boxes displayed across the bottom of the screen correspond to the ten function keys on your keyboard.

Press the designated function key to do the following:

(F3) - undo all currently selected modifications

(F6) - confirm all currently selected modifications and proceed to final confirmation / back up procedure

Otherwise, select another partition to modify, press **Enter**, and go to Step 4.

7. If you pressed F6 (*CONFIRM*), and if no file systems are to be destroyed by the modification(s) currently selected, the system displays a “last chance” confirmation message. Press **Enter** to confirm the changes you selected. Go to Step 10.

If you pressed F6 (*CONFIRM*), and there are file systems to be destroyed by the modification(s) currently selected, the system displays a *Backup* screen.

8. The *Backup* screen displays a list of file systems that will be destroyed as a result of the proposed modifications to the disk; it prompts you to select file systems for backup.

If you do not want to back up any of the file systems to be destroyed during reconfiguration, but want to continue the confirmation process, press **Exit** (not **Cancel**) and go to Step 10.

The first column in the *Backup* screen identifies file systems by their normal mount points, if any. The second column identifies the current partition number, the third column identifies the partition number after the disk is reconfigured, and the fourth column notes any file system “fit” problems in the event that you plan to reload the same data back into the partition.

If you want to backup any of the file systems to be destroyed during reconfiguration, select the file systems (using the **Mark** key), and press **Enter**.

9. The system displays the following message:

Put quarter-inch tape in drive and press Return:

To perform the backup:

- Make sure the write-protect arrow (see Figure 4-2) on the tape cartridge is *away* from SAFE; then insert the tape cartridge into the drive (see Figure 4-3), and close the latch.
- Press **Enter**.

The system displays each filename being backed up.

If the backup program fails, (for example, because the tape is not writable), you are given the opportunity to either ignore the failure (continue with the configuration process), abort the configuration process, or try to backup the same file system again. If you choose to ignore the failure, the program backs up the next file system (if any more were selected) or proceeds to the final confirmation message.

- Wait until the following message is displayed:

{Press any key to continue.}

Press any key. Remove the tape.

- If there were additional file systems, you will be asked to go thru this process again, starting at the beginning of this step (Step 9).
- The system displays a message asking you how to proceed.

Press **Enter** to continue the confirmation process.

10. The system displays a “last chance” confirmation message.

Press **Enter** to confirm the changes you selected.

11. The system displays a *Reconfiguration Complete* message upon successful completion. Press **Cancel** to exit this form.

Press **Enter** to select another disk for reconfiguration, or press **Cancel** to exit.

How to Return the System to Multi-user Mode

To return the system to multi-user mode after you exit *Configure a Disk*, do the following:

1. From the single-user shell, press **Exit** (**^D** on most terminals).
2. When prompted for run-level, if you are not using RFS type **2** and press **Return**. If you are using RFS type **3**, because remote file sharing uses this run level.

View or Change Partition Uses

This tool allows you to (1) view partitions and their current uses on a selected disk, or (2) change partition uses on a selected disk. Partition uses are file systems, swap space, special applications, and so forth. The tool is designed principally to assist you in creating and mounting file systems.

Caution

Any time you create a new file system in a partition that contains data, the data in that partition is destroyed. If you plan to create a new file system, backup your system before using this tool.

The first-level menu displays a list of all the disks on your system. The second-level menu displays a list of all current partitions on a selected disk. From the second menu, you can make new file systems, mount or unmount file

systems, and add or delete swap space. For a discussion on creating new partitions on a disk, see “Configure a Disk,” earlier in this chapter.

Determining the Correct Disk

A disk is identified by its drive number, controller type, and controller number. The drive number is determined by the cable connector attached to the drive. The controller type is either on-board ST506, SMD, or SCSI.

The controller number is determined by the configuration of your CTIX kernel. For example, if you have both on-board ST506 disks and SMD disks, controller 0 can be either the ST506 controller or the SMD controller, depending on the way CTIX was installed and on whether your kernel was reconfigured.

Similarly, the disk number depends on the *jumpering* on the device, if the disks are SCSI. For example, you may have drive 0 and drive 2. There is no drive 1; drive 2 was defined as such by the jumpering.

Note: It is important that you know which disk you have selected and what data is on the disk. The second-level menu can help you identify a disk if you cannot identify the disk by controller number, type, and drive.

Determining Partition Uses

When you select a disk from the first menu, the tool first verifies that the volume structures are valid and readable, and then it gathers information about the partitions on that disk. The tool is unable to make changes to a disk that contains overlapping partitions and reports an error if any are found. For a discussion on how to remove overlapping partitions, see “Using the Disk Configuration Tool,” earlier in this chapter.

If the tool detects an error when it performs these initial checks, write down the error message. If you receive the message “Volume Home Block is unreadable,” the data on the disk is inaccessible and probably lost. You can often reformat a

disk whose volume structures are unreadable by using a diagnostics tape, or you can call the technical support representative from the vendor who supplied your system for help.

The second menu identifies partitions containing file systems; note that the tool is NOT able to determine whether or not a partition contains a database. If there is a file system in a partition, the tool identifies it by its file system name; if there is a database in a *raw* partition, the tool is only able to determine that there is no file system present.

The tool provides warnings regarding file systems that will be destroyed by a proposed change to the current configuration.

Making Changes to Partitions

Not all operations can be performed on all partitions.

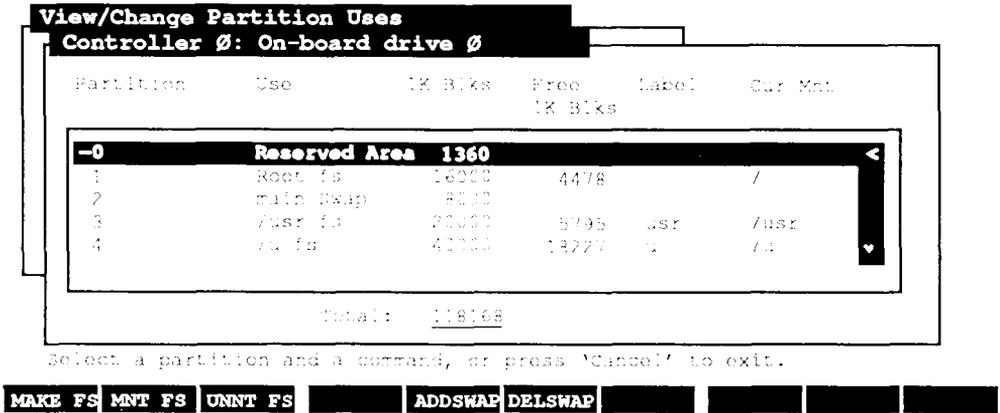
In addition, specific operations have their own qualifications. For example, you cannot unmount a file system that is not currently mounted.

A partition is ineligible for changes under the following circumstances:

- The partition is Partition 0 (Reserved Area).
- The partition is a critical system resource, such as main swap or root file system.
- The partition contains a file system needed by **adman**.
- You cannot mount a file system in a partition that does not currently contain a file system.

The system provides explicit error messages in each of the above cases.

See the descriptions following Figure 5-3 for an explanation of the fields displayed in Figure 5-4.



471 19

Figure 5-4. Sample View/Change Partition Uses Screen

File System Operations

The tool allows you to make a new file system, mount an existing file system, or unmount a file system currently mounted.

When mounting a file system, you must specify the mount path (the place a new file system takes in the directory hierarchy). The mount path must be a full pathname and must reference an empty directory; that is, a directory that contains no files or subdirectories.

You can mount an existing file system with read-only or with write permissions on a specified mount point, and you can either arrange for the file system to be mounted automatically each time the system reboots, or leave the reboot

Chapter 5

procedure as it is. For example, to mount a file system temporarily in a place different from its normal mount point, you will probably want to leave the reboot procedure as is.

You can mount only clean file systems (not in need of repair): if the file system is corrupt, the system displays an error and discontinues the operation. To fix a corrupt file system, run **fsck** (the file system check program) from the shell. (For more information on **fsck**, see the *S/Series CTIX Administrator's Guide* and the *CTIX Operating System Manual*.)

Unmounting a file system makes its files inaccessible to users and to many user programs. For example, the files in unmounted file systems are not included when you run *Backup and Restore*, described in Chapter 4.

To change a file system's mount point, you must first unmount the file system before mounting it somewhere else. You cannot unmount a file system that is "busy" (currently accessed by users, or with a file system mounted underneath). The **fuser(1M)** program can be used from the shell to determine who is using the file system and to remove processes associated with the file system so that the file system can be unmounted.

Swap Space Operations

The tool allows you to add or delete swap partitions. For information on how to determine if you need more swap space, see the *S/Series CTIX Administrator's Guide*. Experience can tell you how much swap space you need, 4MB of total swap space is the minimum under any circumstance.

By default, the second partition on the system disk is the *main swap* partition: there must be one such device available to CTIX. Do not decrease the main swap partition. CTIX also uses *add-on swap* partitions to increase the amount of available swap space.

$$\text{Total Swap} = \text{Main Swap} + \text{All Add-on Swap}$$

A sign that swap space is too small is the failure of shell commands with messages like “not enough space,” or the message “running low on swap,” in the Console Log (described in Chapter 3, “System Status”).

Procedure for Viewing or Changing Partition Uses

1. From the main menu, select *Disk and File System Administration*. Press **Enter**.
2. Select *View/Change Partition Uses*. Press **Enter**.
3. Select a disk. Press **Enter**.
4. The ten highlighted boxes displayed at the bottom of the screen correspond to the ten function keys on your keyboard.

Select a partition and then press the appropriate function key to do the following:

- (F1) - Make a File System
 - (F2) - Mount a File System
 - (F3) - Unmount a File System
 - (F5) - Add Swap Space
 - (F6) - Delete Swap Space
5. If you selected MAKE FS, type the mount point, and select the file system size. The tool supports file systems of either 1KB or 4KB blocks.
 - If you plan to store many small files on your file system 1K blocks are more efficient, since this minimizes wasted space during reads and writes.
 - If you plan to store large files 4K blocks are more efficient, since large files would not be as fragmented on the disk.

If you selected **MNT FS**, type the mount point, select whether to make the change to the reboot procedure, and select the file system's permissions.

If you selected **UMNT FS**, select whether to make the change to the reboot procedure.

If you selected **ADDSWAP**, select whether to make the change to the reboot procedure.

If you selected **DELSWAP**, select whether to make the change to the reboot procedure.

6. Press **Enter** to execute your selection.

The system displays a confirmation message and warns you if any data will be destroyed by the proposed changes.

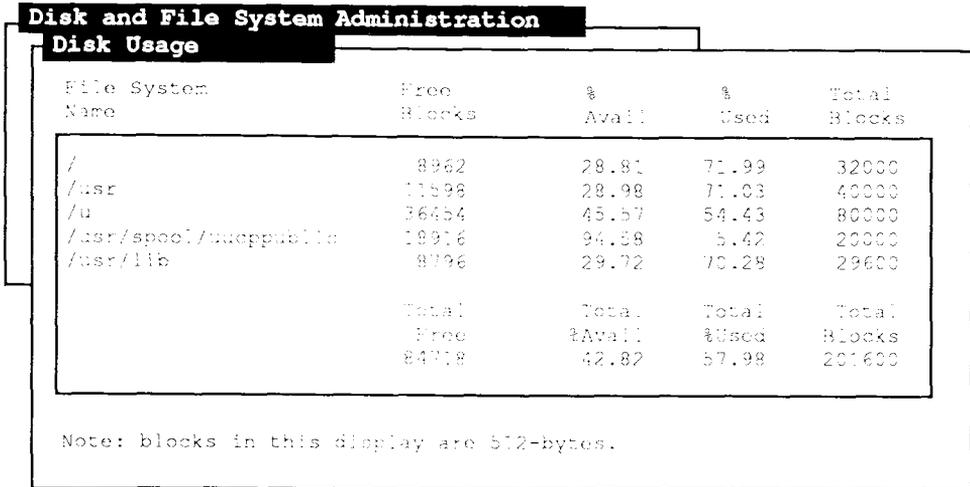
7. Press **Enter** to confirm your selection.

The system displays a message confirming successful execution of the changes to the partition you selected.

Monitor Disk Usage

This tool displays disk space usage for currently mounted file systems. Total figures for all file systems combined are also displayed at the bottom of each column.

1. From the main menu, select *Disk and File System Administration*. Press **Enter**.
2. Select *Monitor Disk Usage*. Press **Enter**.



Press 'Cancel' to exit.

471.20

Figure 5-5. Sample Disk Usage Screen

The *Disk Usage* screen contains the following statistics:

- Name** The file system name is the current mount point for the file system.
- Free blocks** The absolute number of physical (512 byte) blocks available.
- % Avail** The percentage of the total number of blocks available.
- % Used** The percentage of the total number of blocks used.
- Total blocks** The absolute number of physical blocks allocated to the file system.

List Files of a Certain Age

This tool allows you to list all files of a certain age on your system. Use it to find old files that can be removed. To search the entire system, type / for the pathname.

Note that the larger the *directory tree* specified, the longer the system takes to assemble a file list.

1. From the main menu, select *Disk and File System Administration*. Press **Enter**.
2. Select *List Files of a Certain Age*. Press **Enter**.
3. Type the full pathname of the directory to search. Press **Return**.
Do not use any wildcard characters in the pathname.
4. Type the minimum age in days, if other than the default.
5. Press **Enter** to execute.

List Largest Files

This tool allows you to identify the largest files on your system. Use it to find files that grow and are now taking up too much disk space (for example, log and spool files), or other large files that are wasting space. Enter the full pathname of the directory you want to search. To search the entire system, type / for the pathname.

Note that the larger the directory tree specified, the longer the system takes to assemble a file list.

1. From the main menu, select *Disk and File System Administration*. Press **Enter**.
2. Select *List Largest Files*. Press **Enter**.

3. Type the full pathname of the directory to search. Press **Return**.
Do not use any wildcard characters in the pathname.
4. Type the number of files you want in the list.
5. Press **Enter** to execute.

List Largest Users of Disk Space

This tool displays the ten largest users of disk space on the system. You can use this tool to monitor relative disk space usage among users and to help manage space allocation on the system.

1. From the main menu, select *Disk and File System Administration*. Press **Enter**.
2. Select *List Largest Users of Disk Space*. Press **Enter**.
The system displays a confirmation message.
3. Press **Enter** to confirm execution.

Where to Go from Here

Read the section in the *S/Series CTIX Administrator's Guide* on checking file system integrity. When a file system is checked, it is examined by the system for errors and inconsistencies within its structure. If you run the program `fsstat`, and it fails, run `fsck` (the file system checking program).

Caution

Unmount the file system, unless it is the root file system, before running `fsck`. This is to make sure there is no user activity on the file system while `fsck` is running: leaving the file system mounted and available to users during the check can severely damage it.

You will also want to run `fsck` on the following occasions:

- when you use the maintenance tape
- when the system comes up in Admin Mode (state 6)
- when you detect file system problems

For more specific information about the files and commands used to perform disk administration, refer to the following items in the *S/Series CTIX Administrator's Guide* and the *CTIX Operating System Manual*:

`fsck`

This command checks and repairs damaged file systems.

`fsstat`

This command displays a file system's status.

`mkfs`

This command creates a file system.

mount

This command mounts a file system in the directory structure.

swap

This command allows you to add or delete a swap area that is additional to main swap.

/dev/dsk/c#d#s#

/dev/rdisk/c#d#s#

These are special files provided by CTIX so that programs have a standard way to access peripheral devices.

/etc/checklist

This file lists the file systems to be checked when the system is rebooted.

/etc/fstab

This file instructs the system where to mount a particular file system when the system is rebooted.

—

—

—

Chapter 6

SCSI Tape Administration

Introduction

This chapter explains your computer's SCSI drive system: it provides basic information about how to manage SCSI tape drives, and tells you what you should learn from your tape drive's installation manual.

Note: This service is only available on SCSI based systems. To see if your system has a SCSI device present, see Chapter 3, "System Status", section "View Hardware Inventory."

The *SCSI Tape Administration* tool allows you to easily manage the SCSI tape drives on your system. With it, you can

- view the tape drive status
- add and remove tape drives
- change tape drive status

The **tape drive** system contains several components, which are described in detail in the *S/Series CTIX Administrator's Guide* in the chapter on device drivers. If you have a SCSI based system, your first tape drive is already configured for you. Use *View SCSI Tape Status* to verify the configuration of your first tape drive. To access the SCSI tape functions from the main menu, select *SCSI Tape Administration*. Press **Enter**.

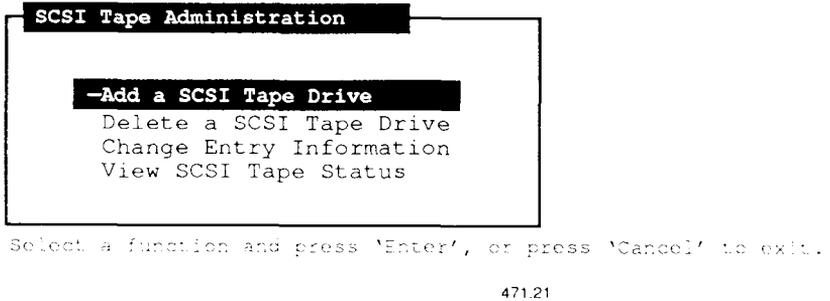


Figure 6-1. SCSI Tape Administration Menu

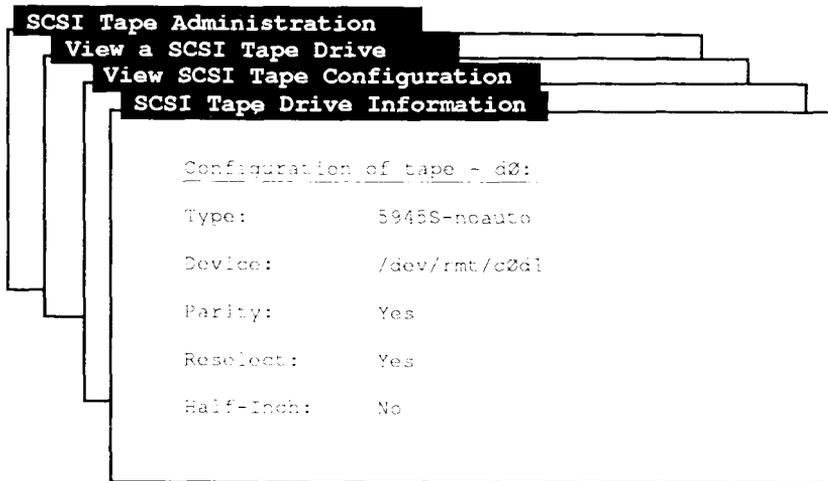
View SCSI Tape Status

Viewing the SCSI tape status allows you to monitor the state of the SCSI tape drive(s) on your SCSI based system. Even if you have not added any tape drives, you will be able to view the status of the drive supplied with your system.

Note: To detect and remedy potential problems before they occur, the system administrator should monitor the SCSI tape drive system status regularly.

1. From the main menu, select *SCSI Tape Administration*. Press **Enter**.
2. Select *View SCSI Tape Status*. Press **Enter**.
3. Select the processor whose devices you want to view.
4. Select the tape drive you would like to view status of and press **Enter**.

5. Configuration information is displayed. See Figure 6-2 for sample configuration information. The tape drive configuration shown in this sample is for the supplied SCSI tape drive.



Press 'Cancel' to exit the form.

471.2

Figure 6-2. Sample SCSI Tape Status Screen

The fields on the *View SCSI Tape Configuration* screen are described below

- Device The name of the drive, when you added it.
- Target Value 0-6 depending on how the device is jumpered.
- Address

Select one of these drives to see additional configuration information. To select a drive see Figure 6-3.

The fields on the *Status Information* screen are described below

Device type	The type of the drive, when you added it.
Device Path	Using the processor and target values you selected when you added it, a device path was created to enable access to the device.
Parity set	This field should always show “Yes”. It indicates that parity checking is set.
Reselect set	This field should always show “Yes”. It indicates that the system supports reselect/disconnect . These commands allow the drive to continue an operation that was temporarily suspended.
Half-inch	Displays “Yes” for half-inch tape, “No” otherwise.

Add a SCSI Tape Drive

This tool configures a new tape drive for the system. Before you can add a SCSI tape drive, you must first determine

- that the tape drive functions correctly on its own (self-test)
- the tape drive type and that it is supported by CTIX
- whether your tape drive is a half-inch tape drive
- the target address (dependent on the jumpering on the SCSI tape drive when you installed it)
- the processor board to which you will add the tape drive

Determining that the SCSI Tape Drive Functions Correctly

Make sure the tape drive is functioning correctly on its own by following the instructions in the tape drive manual. Set the tape drive up and perform the self-test.

Determining the Processor Board

The drives are usually *daisy chained* off the single SCSI bus; so to determine the processor board, select the appropriate processor.

For more information on the processor board, see Chapter 7, "Terminal Administration."

Procedure for Adding a Tape Drive

The first SCSI tape drive is already added for you. To add additional SCSI tape drives:

1. From the main menu, select *SCSI Tape Administration*. Press **Enter**. The SCSI Tape information screen is displayed. See Figure 6-3 for a sample menu.

```
SCSI Tape Administration
SCSI Tape Connection Information

Procedure to add a SCSI tape drive to slot 0:

Tape Drive Type: -dumb
Tape Drive Name:  tape-dl
Target Address for Drive:
Drive is Half-Inch:  Yes

Use 'Tab' to move between fields. When you have finished
making selections, press 'Enter'.
```

Press '^C', select the drive type, or use 'Tab'.

471.1

Figure 6-3. Sample SCSI Tape Connection Information Screen

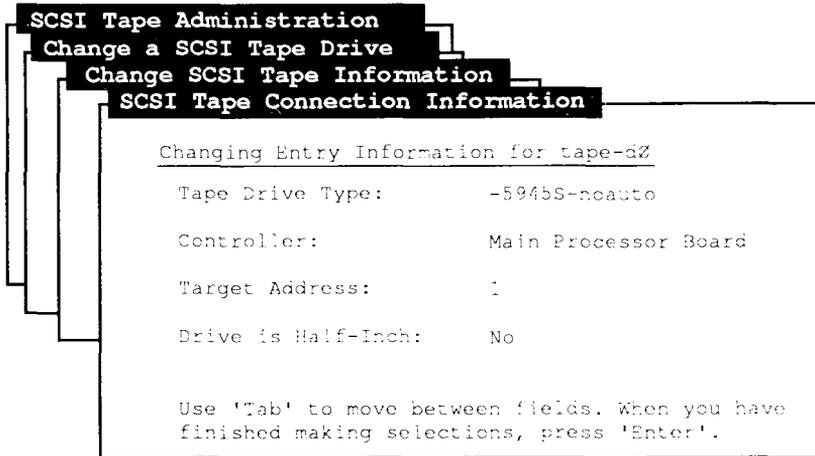
2. Select *Add a SCSI Tape Drive*. Press **Enter**.
3. Select the Processor Board. Press **Enter**. The SCSI Tape Connection Information screen is displayed; see Figure 6-3 for a sample menu.
4. Select the Tape Drive Type. (Use ^C to display a pop-up menu with a list of available types. Make your selection and press **Exit** to return from the pop-up menu.) Press **Tab**.
5. Select a Drive Name. (Use ^C to display a pop-up menu with a list of available names. Make your selection and press **Exit** to return from the pop-up menu.) Press **Tab**.
6. Select the Target Address for the drive. Press **Tab**.
7. Select whether or not your supported tape size is half-inch. Press **Tab**.

8. When you have made all your selections, press **Enter**.
9. The system displays a confirmation message showing the requested tape drive setup.
10. Press **Enter** to add the tape drive.
The system displays a message confirming the successful addition.

To test the newly added SCSI tape drive, go to the View SCSI Tape Status menu and see that the drive is listed along with the attributes you selected. Next, using the device path listed, put a tape in the drive and try to use the drive. Another method of testing the drive is to exit the administration tools and from the shell type: **scsimap -d**. Check the listing to see that the new drive is listed with the correct attributes.

Change Entry Information

1. From the main menu, select *SCSI Tape Administration*. Press **Enter**.
2. Select *Change Entry Information*. Press **Enter**.
3. Select the Processor whose devices you want to change.
4. Select the tape drive whose entry you intend to change and press **Enter**.
5. The Changing Entry Information screen appears. See Figure 6-4 for a sample menu. Press **Tab** to move to the field you intend to change. Press **^C** to see available choices. Select one and press **Tab** to go to another field. When you have made all the changes, press **Enter** to implement them.



Press '^C', select the drive type, or use 'Tab'.

471.4

Figure 6-4. Sample SCSI Tape Change Entry Information Screen

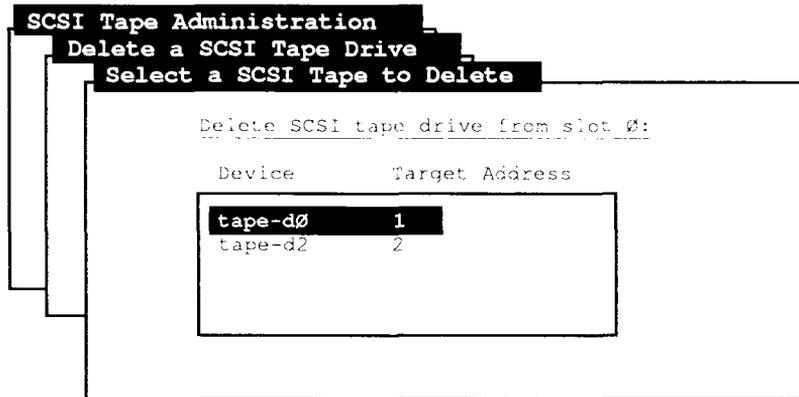
6. A confirmation screen appears.
7. Press **Enter** to confirm your changes.

Delete a SCSI Tape Drive

Delete a SCSI Tape Drive allows you to remove a SCSI tape drive from the system on a permanent basis. (Once you remove a SCSI tape drive, you must use *Add a SCSI Tape Drive* before you can use the tape drive again.)

1. From the main menu, select *SCSI Tape Administration*. Press **Enter**.

2. Select *Delete a SCSI Tape Drive*. Press **Enter**.
3. Select a processor. Press **Enter**. The Select a SCSI Tape to Delete menu will appear. See Figure 6-5 for a sample menu.



Select the SCSI tape drive to delete; press 'Enter', or press 'Cancel' to exit.

471.3

Figure 6-5. Sample Select a SCSI Tape to Delete Screen

4. Select a tape drive. Press **Enter**.
The system displays a confirmation message.
5. Press **Enter** to confirm removal of the tape drive.
The system displays a message confirming the successful removal.

Where to Go from Here

For more information and instructions, read the chapter in the *S/Series CTIX Administrator's Guide* that discusses the SCSI tape system.

For more specific information about the files and commands used to perform SCSI tape administration, refer to the following items in the *S/Series CTIX Administrator's Guide* and the *CTIX Operating System Manual*:

/etc/rcopts/KSCSI

This file contains SCSI tape driver entries to load.

/etc/system

This file contains SCSI tape initialization information.

scsimap(1M)

This command displays current configuration and allows updates based on **/etc/system** contents.

tapeset(1M)

This command initializes quarter-inch and half-inch tape drives.

Chapter 7

Terminal Administration

Introduction

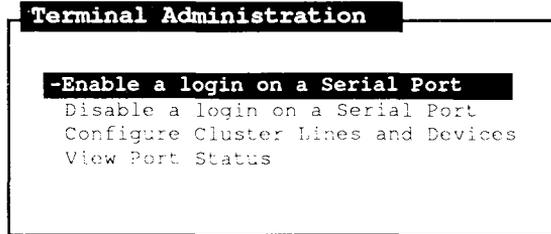
This tool allows you, as system administrator, to enable and disable serial (RS-232) terminal logins, to configure cluster (RS-422) lines and devices, and to see which ports currently have logged-in users. If you are not the system administrator, you may view the displays only.

A *port* is a connector on your S-Series System into which a cable (for a terminal, printer, or other device) is plugged. You cannot use a terminal that is physically connected to the system until you *enable* the associated port; this allows a login to occur on the port. *Disabling* a login disallows logins on the port.

There are two types of terminal ports: serial and cluster. A *serial port* supports one RS-232 terminal. A *cluster port*, also called a *channel*, supports up to 15 RS-422 terminals, remote I/O processors (RIOPs), or PCs running PC Exchange software.

The tool that configures cluster lines and devices is available only if your system has a *cluster board*, which is an optional device (with two or four channels) that you can install in your system so that cluster devices can be enabled. If you have a cluster board, the tool allows you to change drop/line CTIX *kernel* variables, change the number of cluster terminal logins, and add or remove RIOPs.

The kernel is the heart of the CTIX operating system; it contains the software that directs the various devices on the system. To use these functions from the main menu, select *Terminal Administration*. Press **Enter**.



Select a function and press 'Enter'.

471.53

Figure 7-1. Terminal Administration Menu

Enable a Login on a Serial Port

Before you can enable a serial port, you must first determine the following:

- the processor board into which the terminal is plugged
- the connector into which the terminal is plugged
- the baud rate (communication speed) of the terminal
- the terminal type

Determining the Processor Board

The first-level menu of this tool displays a list of all I/O processor boards on your system and asks you to select the processor to which the peripheral is connected. You can determine which processor board a peripheral is connected to, by opening the back of your S/Series System and noting which connector the peripheral cable is plugged into, or, in the case of RIOPs, knowing the unique ID. See the section “Add or Remove an RIOP” for details on how to find out the unique ID.

All systems have a *main processor* (sometimes called *main CPU*) board. In some S/Series machines the main CPU is the left-most board as you look at the system from the rear; in other S/Series machines the main CPU is the right-most board. See Figure 7-2 for a rear inside view of a typical ‘left-handed’ S/Series system.

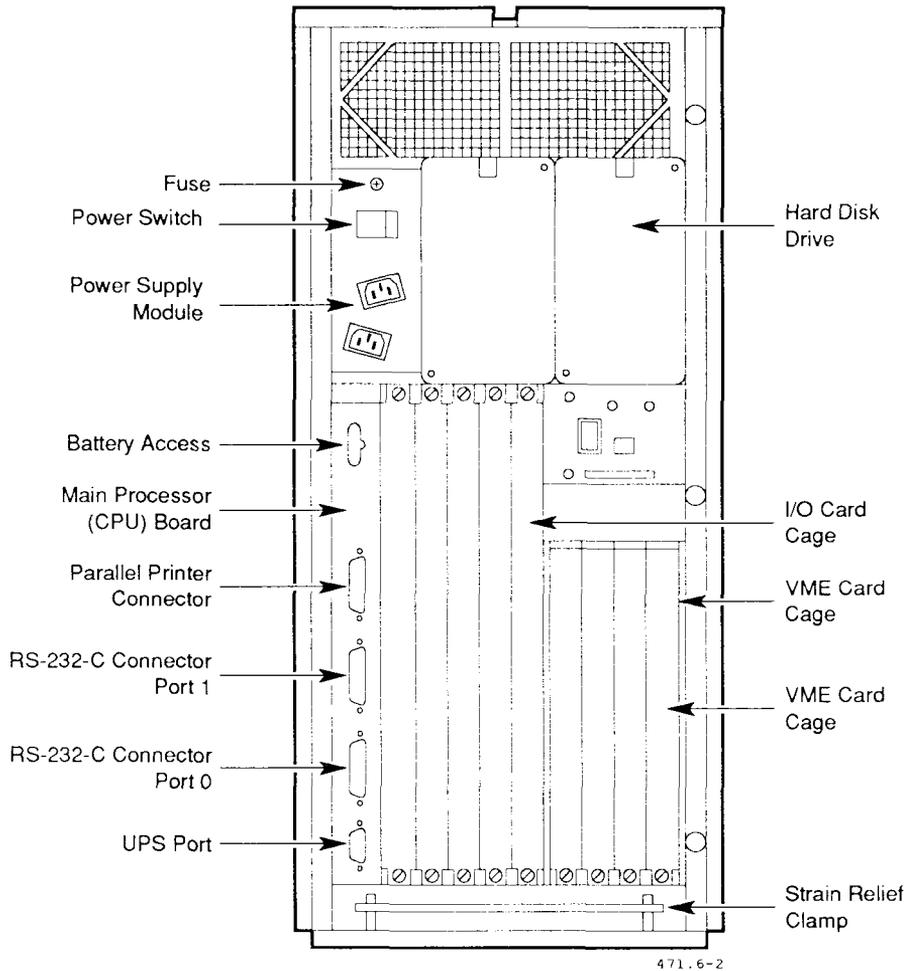


Figure 7-2. Rear Inside View of a Left-Handed S/640

The main CPU board on each S/Series machine contains the following number of RS-232 ports:

Machine	Number of Ports on the CPU Board
S/80	Eight RS-232 connectors, labeled Ports 0–7: Port 0 is the topmost connector.
S/280	Six RS-232 connectors, labeled Ports 0–5: Port 0 is the topmost connector.
S/480	Two RS-232 connectors, labeled Channel 0 and Channel 1.
S/640	Two RS-232 connectors, labeled Channel 0 and Channel 1.
S/4040	Ten RS-232 connectors, labeled Port 0, Port 1, and A00–A07.

Your system might also have I/O expansion boards that have RS-232 ports: these processor boards are either located in *slots* in the rear of the machine, or they are cluster (RS-422) devices (RIOPs) that support RS-232 communication.

RIOPs are daisy-chained to an RS-422 line. (See “Configuring Cluster Lines and Devices,” later in this chapter, for more information on RS-422 lines.) Each RIOP’s unique ID number is displayed with the RS-422 channel number in the first-level menu of this tool. It is important that you know the unique ID number of the RIOP in question. If you have not labeled the RIOP and do not know what the number is, refer to “Add or Remove an RIOP,” later in this chapter, for information about how to identify an RIOP’s unique ID.

For expansion boards other than RIOPs, such as the Ethernet/RS-232, SCSI/RS-232, and IOP-16 boards, the first-level menu of this tool also displays the number (or letter) of the slot in which each processor board is located. Slots are numbered sequentially from the main CPU forward (slot A on 68040-based machines and slot 0 on 68020-based machines), with the first expansion board in slot 1 or B (adjacent to the main CPU), the second in slot 2 or C, and so forth.

Only S/640 and S/480 machines have 10-connector and 20-connector I/O expansion boards. A 10-connector board occupies one slot only and has one row of connectors labeled Channel 0–9 (from bottom to top). A 20-connector board occupies two slots. The first side is labeled Channel 0–9 and is always installed in the slot to the left. The second side is labeled Channel 10–19.

The menu displays a 20-connector board as two I/O expansion boards. Since the 20-connector board is always installed with the board labeled Channel 0–9 in the leftmost slot, then if your system has the CPU board installed on the right, the slot number for channels 0–9 is higher than the slot number for channels 10–19. Conversely, if your system has the main CPU installed on the left, the slot number for channels 0–9 is lower.

For more information on determining hardware components, see the installation manual for your system.

Determining the Connector

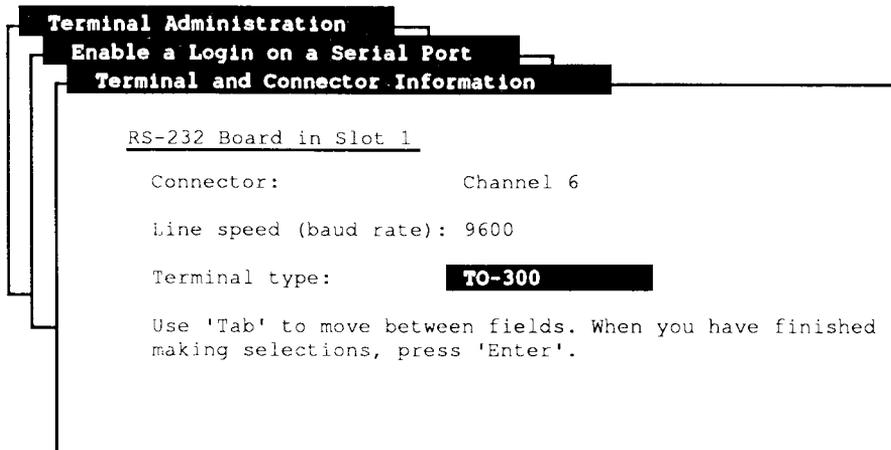
The second-level menu of this tool allows you to select a connection on the processor board you selected. Each item in the menu corresponds to a *Port* label on the processor board. As with determining the processor, you can determine which port to select by opening the back of your system and noting which connector the peripheral cable is plugged into, or, in the case of RIOPs, looking at the RIOP itself.

The connector number in the menu corresponds to the port label on the machine, with the following exceptions:

- On S/640 and S/480 expansion boards, menu selections begin with Channel 0 and continue to the maximum number of channels on the board. If you are trying to determine a connector on a 20-channel RS-232 board, the channels labeled 0–9 correspond exactly to the menu items displayed, and the channels labeled 10–19 are offset by 10; that is, Channel 10 (on the second board) corresponds to Channel 0 in the menu, and so forth.
- In the case of Ethernet/RS-232 and SCSI/RS-232 boards, on which channels are labeled 2–7, Channel 2 on the board corresponds to Channel 0 in the menu, and so forth.
- In the case of RIOPs, the channel number in the menu corresponds exactly to the connector label on the RIOP itself.

Note that the *Terminal Administration* and *Printer Administration* tools first check to see what processor boards (including RIOPs) are installed on the system, and that the menus in these tools list only the ports currently available in the particular context. For example, if you are trying to enable a serial terminal, only the lines that are currently disabled are selectable. If you are adding a printer, only the lines that are not configured for terminal logins are displayed: if you want to use a different line, you must first disable the terminal login.

If you need more help in determining the correct connector, see “Determining the Processor Board,” earlier in this chapter, or see the installation manual for your system.



471.23

Figure 7-3. Sample Terminal and Connector Information Screen

Determining the Baud Rate

Choose the baud rate that is appropriate to the device connected to the serial port. Most terminals operate at 9600 baud when connected directly to the system.

Determining the Terminal Type

The terminal type depends on the particular brand and model of your terminal. If you are connecting a terminal that is not on the list in Appendix B, refer to the chapter in the *S/Serial CTIX Administrator's Guide* that discusses adding a terminal for instructions.

Note: The administration tools do not run on terminals specified as **dumb**: dumb terminals do not support the screen-oriented capabilities needed by the tools.

1. From the main menu, select *Terminal Administration*. Press **Enter**.
2. Select *Enable a Login on a Serial Port*. Press **Enter**.
3. RIOPs (if any) that are up or booting are displayed along with other available processor boards currently installed.

Select the processor board the terminal is plugged into. Press **Enter**.

4. The system displays only those ports that currently don't have logins enabled. To change the default port, press **^C**. (A *pop-up menu* is displayed.) Make your selection and press **Exit** to return from the pop-up menu. Press **Tab**.
5. To change the default baud rate, press **^C** and make a selection. (Press **Exit** to return from the pop-up menu.) Press **Tab**.
6. Type the correct terminal type, if different from the default. (The default is *your current* terminal type.) Press **Enter**.

If there is a printer or a UUCP device currently configured for the port, the system displays a confirmation message to delete that configuration.

If there is a printer or a UUCP device currently configured for the port, the system displays a confirmation message to delete that configuration.

Unless you confirm the deletion of the current configuration, the tool does not enable a login on the port.

7. Press **Enter** to enable the port. The system displays a message confirming the successful enabling of the login on the specified board and connector.

Disable a Login on a Serial Port

You can restrict terminal usage, without physically disconnecting terminal cables, by disabling login privileges on the port a terminal is connected to. Be careful not to disable a port that is being used by an authorized user. (You can check the port status by using the View Port Status function.)

Read the previous section, “Enable a Login on a Serial Port,” to learn how to identify the processor and the connector in the procedure below.

1. From the main menu, select *Terminal Administration*. Press **Enter**.
2. Select *Disable a Login on a Serial Port*. Press **Enter**.
3. Select the processor board the terminal is plugged into.
4. The system displays only those channels that currently have logins enabled.

Select the channel you want to disable.

The system displays a confirmation message if a UUCP configuration is affected.

5. Press **Enter** to disable the port.

The system displays a message confirming the successful disabling of the login on the specified board and connector.

Configure Cluster Lines and Devices

This tool allows you to *tune* cluster lines by selecting the following options:

- change the number of cluster terminal logins
- change the number of drops/lines
- add or remove an RIOP

Note: *To support cluster channels, you must have a Cluster Expansion board installed. If you do not have a Cluster Expansion board in your system, this option is not displayed on the Terminal Administration menu.*

When configuring your system, you are allowed up to a maximum of four cluster lines (channels), and up to a maximum of 15 drops (devices) per cluster line. As distributed, the CTIX kernel is configured for four cluster lines and eight drops per line. This means that four lines are usable and that each line can support eight devices, such as PCs running PC Exchange software, RIOPs, or RS-422 terminals. This tool does not configure or identify PCs on a cluster line.

It is important to note that since RS-422 terminals communicate with the host machine at a different line speed from the line speed used by PCs running PC Exchange software and RIOPs, RS-422 terminals cannot be combined with other devices on the same line. You do not have to set the line speed yourself: CTIX does it for you according to the type of device first powered up on the line.

If you have RIOPs and cluster terminal logins on the same cluster channel, use this tool to disable all cluster terminal logins (that is, change the number of cluster terminal logins to 0).

Enabling an RIOP RS-232 terminal is accomplished with the *Enable a Login on a Serial Port* tool, described earlier in this chapter. The RIOP device must be online and correctly configured to enable or disable logins associated with its RS-232 ports.

Note: After you change the drop/line configuration, you must shutdown the system and reboot before the change is effective. (It is not necessary to reboot after changing the number of cluster terminal logins.)

Change the Number of Drops/Lines

Unlike serial channel logins, which are enabled or disabled one per channel, each cluster line has from 0 to 15 possible terminal logins. If you have four RS-422 terminals on the line and you want to enable two more, use this tool to change the number of logins to six.

If you try to reduce the number of drops or lines, and that change will leave enabled logins without drops, the tool warns you with a confirmation message. If you then confirm the change, the tool disables logins on the affected devices. The tool does not allow you to disable your own login.

When you change the number of lines, you change the kernel value for the number of cluster lines to be polled. You cannot directly specify which lines will be polled: if only one line is configured, it is Channel 0; if two lines are configured, they are Channel 0 and 1, and so forth.

When you change the number of drops, you change the kernel value for the number of devices that will be polled on a cluster line. If the line itself is not being polled, then the value for drops is meaningless.

The number of drops per line applies to all lines: you cannot specify a value of four drops for one line and eight for another line.

The number of drops per line does not need to be exactly the same as the number of devices you actually connect to the line, but the number of drops must be at least as large as the actual number of devices. For optimal performance, you should minimize polling of nonexistent devices; however, sometimes this cannot be helped. For example, if you have 12 PCs on one line and two cluster terminals on another line, there must be at least 12 drops per line.

If you have fewer devices on the line than current tuning allows, it is a good idea to tune the line for the number of devices actually using it: this is because CTIX polls the lines for the configured number of drops, and unused drops result in wasted polling and therefore less than optimal performance.

If your cluster board has only two channels, there is no overhead (performance degradation) for drops configured for non-existent channels.

If the drop/line configuration has been changed since the last system reboot, the tool does not allow you to change cluster terminal logins. If, for example, you want to enable 12 RS-422 terminals and the line is currently tuned for eight, first tune the line for 12 drops, reboot the system, and then change the number of cluster terminal logins to 12.

Change the Number of Cluster Terminal Logins

As with serial ports, you cannot use a terminal physically connected to a cluster port until the channel is enabled, which allows a login to occur on the channel.

To enable terminals on cluster channels, you must specify the channel number and the number of logins to be allowed on that channel.

Add or Remove an RIOP

If there is RIOP software on your system, you can use this tool to add or remove RIOPs. You must add a new RIOP before you enable RS-232 terminal logins, printers, modems, or other devices associated with it.

Removing an RIOP frees up the RS-232 terminal numbers associated with it. If you need to take the RIOP offline and replace it with another RIOP, you should remove the first one before you add the second.

Each RIOP device has a unique ID number (encoded in its ID PROM). You must know this number to add or remove the device, and to enable or disable a serial login on an RIOP port. This unique ID number is the only means by which the administration tools can identify and configure the device.

Note that you can physically disconnect an RIOP from one channel and connect it to another channel on the same cluster board *without* using this tool: that is, the only time you *configure* (add or remove) an RIOP is when you first add it to the system or when you permanently remove it from the system.

Extracting an RIOP's Unique ID Number

If you do not know an RIOP's unique ID number, you can extract the number by doing the following:

1. Connect a 9600-baud terminal to port 0 or a 1200-baud terminal to port 1 on the RIOP in question.
2. Power-cycle the RIOP (that is, turn the power on, or if it is already on, turn it off and then on again).

Two lines of text are displayed:

- The first gives the RIOP EEPROM version number and is of the form

RIOP *x.y*

where *x.y* is the version.

- The second line gives the unique ID and is of the form

ID: 0x20*nnnnnn*

where *nnnnnn* is the six-digit hexadecimal unique ID.

The **0x20** portion of the number is not significant and is never specified to **adman**. For example, if the number is 0x2000042E, then the unique ID is 00042E, or simply 42E. When you add a new RIOP, you can enter either the full six-digit number or you can omit the leading zeros.

It is a good idea to label each RIOP with its unique ID, since the system always refers to the device by this number.

Determining the RIOP Software Release Level on your System

To add an RIOP, you must also know the release level of the RIOP software on your system (for example 1.00); this information is contained in the *Software Release Notice* for the RIOP. Another source for this information is the file `/install/RiopRel`.

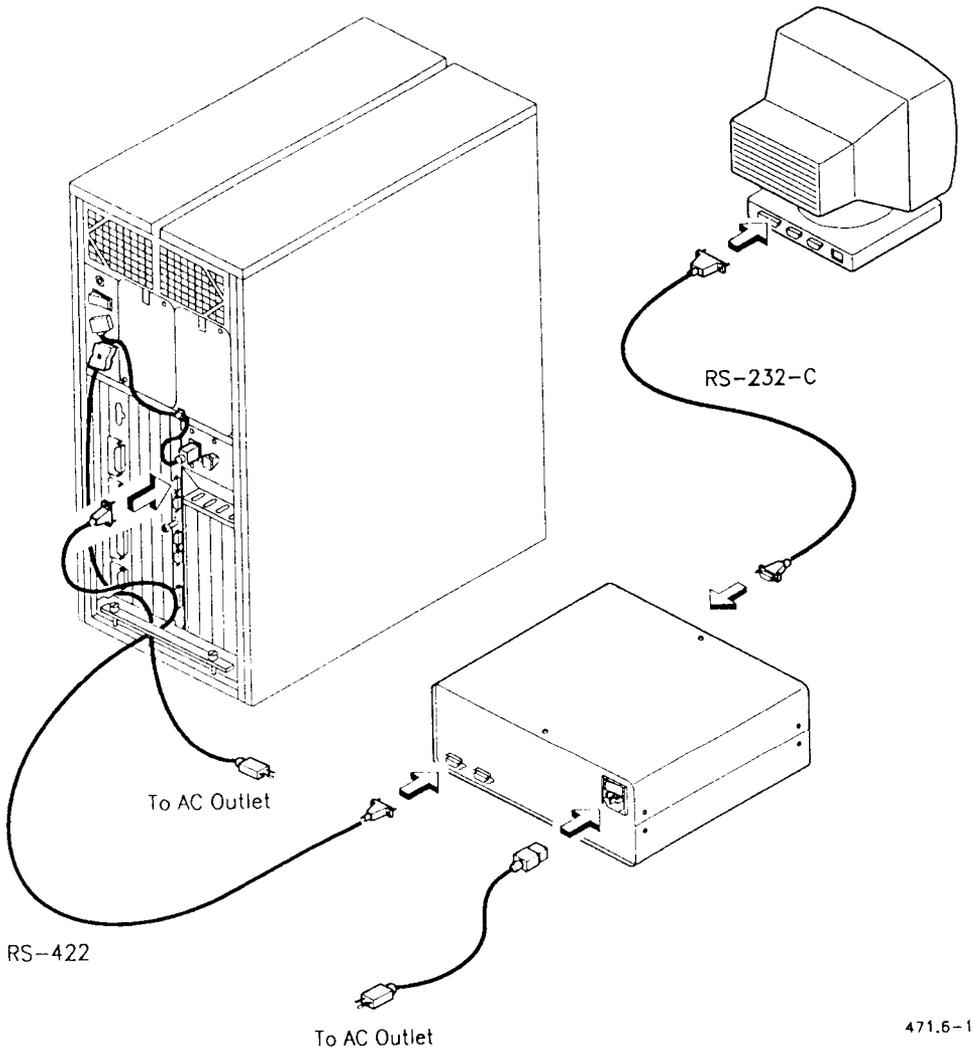


Figure 7-4. Example of an RIOP Configuration

Chapter 7

Configure Cluster Lines and Devices			
Channel	Max Drops	Cluster Terminals	RIOPs
0	0	0	0
1	0	0	0
2	0	0	0
3	0	0	0

Cluster board has 4 channels.

Press 'F1' or 'F2' to change drops or terminals.

DROPS	CL TERM								
-------	---------	--	--	--	--	--	--	--	--

471 54

Figure 7-5. Sample Configure Cluster Lines and Devices Screen

The screen displayed in Figure 7-5 contains the following columns:

- Channel** Each channel is a port on the cluster board.
- Max Drops** Each channel can have up to 15 drops per line.
- Cluster Terminals** Displayed are the number of cluster terminals currently enabled on each channel. The maximum number is 15, if the number of drops is set to 15.

RIOPs Displayed are the number of remote I/O processors currently enabled on each channel. An RIOP must be *up* or *booting* (not turned off or disconnected) to appear in the display.

The maximum number of RIOPs per line is 15, if the number of drops is set to 15. The system maximum number of RIOPs (not per channel) is 32.

Procedure for Configuring Cluster Lines and Devices

1. From the main menu, select *Terminal Administration*. Press **Enter**.
2. Select *Configure Cluster Lines and Devices*. Press **Enter**.
3. The ten highlighted boxes displayed across the bottom of the screen correspond to the ten function keys on your keyboard. Press the designated function key to
 - (F1) - change the drops per line configuration
 - (F2) - change the number of cluster terminal logins
 - (F3) - add or remove an RIOP (if RIOP software is installed)
4. For changing drops per line, whatever you specify will be the same on all cluster lines.

For changing cluster logins, select the channel number and the number of logins to be allowed.

For adding RIOPs, type the unique ID number and the RIOP Release number. For removing RIOPs, select the RIOP from the menu.
5. When you have finished making changes, press **Enter**.

The system displays a confirmation message with a list of the changes requested and a warning regarding the effect of the proposed changes on cluster devices currently enabled.

6. Press **Enter** to execute the proposed changes.

The system displays a message confirming the successful reconfiguration.

7. If you made changes to the drops/line configuration, you must reboot the system for the changes to be effective.

To shutdown and reboot the system:

1. Exit the administration tools and log out.
2. Log in as **root**.
3. At the shell prompt, type **shutdown**. (The **shutdown** program allows you to send a warning message to logged in users and allows a grace period for them to log out.)
4. When the system displays a prompt telling you it is okay to reboot the system, type **reboot**.

Wait until you see the login prompt before typing again.

View Port Status

Viewing the port status allows you to see which users are logged into the system.

For each user currently logged in, the display shows the login name, the port, the date and time of the last login, length of time since the last keystroke, and the process identification number (PID) the system assigned the user when he logged in.

1. From the main menu, select *Terminal Administration*. Press **Enter**.
2. Select *View Port Status*. Press **Enter**.

The port numbers in Figure 7-6 are referred to as TTY numbers. The TTY number for each port on 68020-based machines, and for Port 0 and Port 1 on 68040-based machines, is displayed as `ttyxxx`, where `xxx` is a three digit decimal number. On all other ports on 68040-based machines, the TTY number is displayed as `ttyaxx`, where `a` designates the I/O slot and `xx` is a two digit decimal number. This number is mapped to the connector number of the port (see Tables 7-1 and 7-2) used in both the *Enable* and the *Disable Logins on a Serial Port* tools, described earlier in this chapter. A period (.) in the display represents the port you are currently logged into or indicates that the port is currently active.

Ports in use:				
Login ID	Port	Since	Last Activity	PID
denise	tty004	Apr 12 12:40	0:01	226
edl	tty005	Apr 12 12:41	.	227
root	tty006	Apr 12 12:37	.	228
margie	tty007	Apr 12 12:39	.	229

"." indicates activity within the last minute

Press 'Cancel' to exit the form.

471.55

Figure 7-6. Sample View Port Status Screen

Use Table 7-1 to place the TTY number for terminals connected to boards other than RIOPs, SCSI/RS-232, or Ethernet/RS-232 boards on S/22X, S/320, S/480, or S/640 systems.

Table 7-1. S/22X, S/320, S/480, and S/640 Serial Port Numbering

TTY	Connection Type	I/O Slot	Connector
000-001	serial	CPU	0-1
002-011	serial	I01	0-9
012-021	serial	I02	0-9
022-031	serial	I03	0-9
032-041	serial	I04	0-9

Use Table 7-2 to place the TTY number for terminals connected to expansion boards on S/80, S/280, and S/4040 systems.

Table 7–2. S/80, S/280, and S/4040 Serial Port Numbering

Machine	TTY #	Type	I/O Slot	Connector
S/80	000–007	serial	CPU	0–7
S/80	008–015	serial	I01	0–7
S/280	000–005	serial	CPU	0–5
S/280	006–013	serial	I01	0–7
S/280	014–021	serial	I02	0–7
S/4040	000–001	serial	CPU (A)	0–1
S/4040	a00–a07	serial	CPU (A)	2–9
S/4040	b00–b11	serial	B	0–11
S/4040	c00–c11	serial	C	0–11
S/4040	d00–d11	serial	D	0–11

Where to Go from Here

For more information on configuring terminals, read the chapter in the *S/Series CTIX Administrator's Guide* that discusses configuring new terminals and the terminal numbering scheme, and the section on system initialization procedures.

For more specific information about the files and commands used to perform terminal administration, refer to the following items in the *S/Series CTIX Administrator's Guide* and the *CTIX Operating System Manual*.

/etc/inittab

This file (modified by **adman**) instructs the system how to configure the ports on the system. It designates the ports on which logins are allowed, port communication speeds, and the program used to monitor the port.

/etc/riop/rtab

This configuration file for RIOPs is modified by **adman**.

/etc/ttytype

This file designates the terminal type assigned to each port on the system.

telinit

This command instructs the system to reread **/etc/inittab** when you change the login privilege on a port, in order to make the change take effect immediately. Otherwise, the system waits for five minutes or until a user logs in or out (whichever comes first), at which time it automatically reads **/etc/inittab**. **Telinit** is also used to change the run-level of the system.

Chapter 8

Printer Administration

Introduction

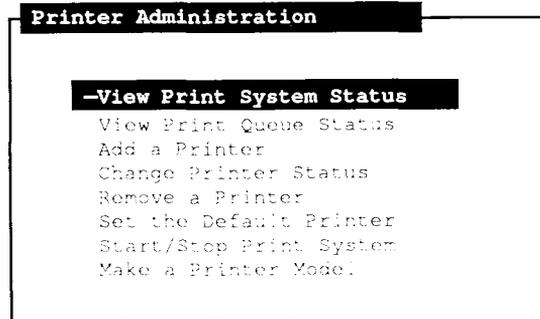
This chapter explains your computer's print system: it provides basic information about printers and how to manage them, and tells you what you should learn from your printer's installation manual.

The *Printer Administration* tool allows you to easily manage the printers on your system. With it, you can do the following:

- monitor the print system and the status of requests
- add and remove printers
- modify printer status
- set a system default printer
- start and stop the flow of files to be printed
- create description files (models) for each printer

The CTIX administration tools consider a *line printer* to be a parallel or serial printer connected to your computer. The term *printer* refers to a *destination*.

The **lp** (line printer) system contains several components, which are described in detail in the *S/Series CTIX Administrator's Guide*. To access the printer functions from the main menu, select *Printer Administration*. Press **Enter**.



Select a function and press 'Enter'.

471.22

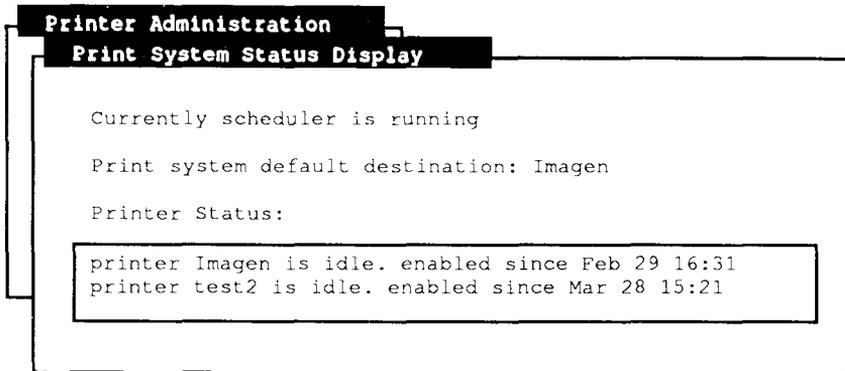
Figure 8-1. Printer Administration Menu

View Print System Status

Viewing the print system status allows you to monitor the state of the printers on your system.

Note: To detect and remedy potential problems before they occur, the system administrator should monitor the **lp** system status regularly.

1. From the main menu, select *Printer Administration*. Press **Enter**.
2. Select *View Print System Status*. Press **Enter**.



Press 'Cancel' to exit the form.

471.24

Figure 8–2. Sample

The fields on the *Print System Status* screen are described below

Scheduler Status	If the scheduler is running, print requests are being sent to printers that are enabled. If the scheduler is not running, printers do not receive print requests.
Default Destination	This field shows which printer receives all print requests when no particular printer is specified. If you want to change the default printer, you can use <i>Set the Default Printer</i> . (See “Where to Go from Here,” later in this chapter, for more information on lp .)
Printer Status	Printer Status displays the status of all printers currently enabled (able to execute print requests). In Figure 8-2, the status of <i>Imagen</i> and <i>test2</i> is idle.

View Print Queue Status

Viewing the print queue status allows you to monitor jobs (print requests) that are queued up (waiting) to be printed. Each job in the queue has an entry that shows the request ID (consisting of the printer name and the job number), the user who initiated the request, the size of the request in bytes, and the date and time **lp** queued the job. The job currently printing is also identified.

Note that a job sent to a remote printer (a printer connected to a remote system) often does not show up in the queue status. This is because your system removes the request from its queues when it sends the job to the remote system. When the remote system receives the request, it places the print job in its queue for that printer.

1. From the main menu, select *Printer Administration*. Press **Enter**.
2. Select *View Print Queue Status*. Press **Enter**.

Add a Printer

This tool configures a new printer for the **lp** spooling system. Before you can add a printer, you must first determine the following:

- That the printer functions correctly on its own (self-test)
- Connection type (parallel, serial, or remote)
- Printer name
- Model name (or whether you need to make a new model beforehand)
- Processor board
- Connector number (if serial)
- Whether the remote system is ready (if remote)

If you need to create a printer model, see “Make a Printer Model” for information on what else must be determined before you can add the printer.

Determining If the Printer Functions Correctly

Make sure the printer functions correctly on its own by following the instructions in the printer manual. Set the printer up and perform the self-test.

Determining the Connection Type

The steps involved in adding a printer depend on the type of connection existing between the printer and your system. Parallel, serial, and remote connections are discussed below.

Parallel Connections

A *parallel connection* transmits data from a computer to a printer in groups of bits, rather than one character at a time. The system can have, at most, two parallel printers: one on the main processor board and one on an IOP (I/O processor) board or on a cluster board. If you do not have an IOP board or cluster board in your S/Series machine, the second parallel printer option is not displayed.

Serial Connections

A *serial connection* transmits data from a computer to a printer one bit at a time. A serial (RS-232) connector can be on the main processor board or on an I/O expansion board, such as an Ethernet/RS-232 board, SCSI/RS-232 board, IOP-16 board, or remote IOP (RIOP) board.

For detailed information on connectors and processor boards, see “Determining the Connector,” and “Determining the Processor Board,” in Chapter 7, “Terminal Administration.”

Remote Connections

A *remote printer* is a printer physically connected to a remote system and accessed from your system. You can add a remote printer to the **lp** system (on your system), but the printer must also be configured on the remote system in order for you to be able to access it.

When you select the remote option, you are asked to select the command your system will use to communicate print requests to the remote system. Two commands can be used.

One is **uux** (UNIX-to-UNIX execute), which is a UUCP (UNIX-to-UNIX copy) command. In this case, the list of systems you may select to do remote printing is taken from the `/usr/lib/uucp/Systems` file. You may add systems to this file by selecting *UUCP Administration* from the main menu.

The alternative to **uux** is **rcmd**, which is a networking command. Using **uux** is a more secure way to execute remote print requests than **rcmd**.

Note: *TCP/IP must be installed on your system before you can run rcmd. See the CTIX Operating System Manual for more details.*

When you choose **rcmd**, the list of systems you may select from to do remote printing is taken from the `/etc/hosts` file. You may add systems to this file by selecting *Network Administration* from the main menu.

To use **rcmd**, user **lp** must have equivalent status on the remote system. (This means that user **lp** does not need to provide a password when logging in to the remote machine.) The practice of making users equivalent on different machines is risky, since password protection is not enforced once the user has logged in on one machine.

To make **lp** equivalent on the remote machine, the administrator of that (remote) machine can do the following:

1. Log in as **root**.
2. Run **adman** and select *Network Administration*, *System Setup*, and *Add an Equivalent User*.
3. Enter your machine name as the machine entry, **lp** as the remote user, and **lp** as the local user.

After you select the method of sending print requests, you are asked to supply the name of the specific printer to be used on the remote system. If you do not supply a printer name, the default printer on the remote system is used.

Determining the Printer Name

Select a name (not over 14 characters long) that you associate with the printer. For example, the name of a Diablo 630 printer could be the brand name, Diablo, or perhaps Diablo2, if you have more than one printer from the same manufacturer.

Determining the Model Name

Selecting a *model* gives the **lp** system detailed information about your printer, including how to format your printout. A model is a program specifying a sequence of steps to be performed when a print job is sent to a particular printer. All of the associated options are described under “Make a Printer Model.”

Note: It is important for all of the options in the printer model you select to exactly match the settings on the printer you are adding.

The directory `/usr/spool/lp/model` contains several sample models, some of which are listed in Table 8-1. You can use a text editor from the shell to look at the `stty(1)` options in these files. If you need a model not provided with CTIX, use *Make a Printer Model* to add an appropriate model.

Table 8–1. Printer Models

Model Option	Printer Type
1640	DASI 1640 serial printer
dumb	Standard (generic) parallel printer
f450	DASI 450 parallel printer
hp	Hewlett-Packard hp2361a parallel line printer
prx	Printronix serial printer
pprx	Printronix parallel line printer

These models refer to the needs of specific printer hardware, and should generally not be used. Use *Make a Printer Model* for any printer being added.

```
Printer Administration
Connection Type for New Printer
Serial Processor Board
Serial Printer and Connector Information

ETHERNET Combo Board in Slot 1:

Printer name:      Laser01

Connector:        Channel 3

Model:            dual

Use 'Tab' to move between fields. When you have finished
making selections, press 'Enter'.
```

Enter a name for this printer.

471.25

Figure 8–3. Sample Serial Printer and Connector Information

Determining the Processor Board

See “Determining the Processor Board,” in Chapter 7, “Terminal Administration,” for a detailed discussion on processor boards.

Determining the Serial Port Number

When adding a serial printer, you must determine which *connector* (also called a channel or port) to attach the printer to. There may be more than one *processor board* installed on your S/Series, each board containing one or more connectors. More information is available on determining the processor board and connector number in Chapter 7, “Terminal Administration.”

Determining the Serial Port Number

When adding a serial printer, you must determine which *connector* (also called a channel or port) to attach the printer to. There may be more than one *processor board* installed on your S/Series, each board containing one or more connectors. More information is available on determining the processor board and connector number in Chapter 7, “Terminal Administration.”

The printer administration tool displays the connectors currently available on the processor you specify. Choose the connector number listed in the menu that is mapped to the connector’s silk-screened label on the processor board.

If you want to add a printer to a port that currently has a login enabled, you must first use *Terminal Administration* to disable the login on that port.

For a description of the settings (such as, baud rate, stop bits, parity, hardware tabs, and carriage motion) that may also need adjusting on the printer itself, see “Additional Specifications for Serial Printers,” later in this chapter.

Determining Whether the Remote System is Ready

When adding a remote printer, check with the administrator of the remote system to see that the remote device is configured appropriately on the remote system, and that the remote system is ready to serve as a host so that your system can access the remote printer.

Procedure for Adding a Printer

1. From the main menu, select *Printer Administration*. Press **Enter**.
2. Select *Add a Printer*. Press **Enter**.
3. Select the type of connection. Press **Enter**.

4. If Serial:

- Select the Processor Board. Press **Enter**.
- Type the Printer Name. Press **Tab**.
- Select a Connector. (Use **^C** to display a pop-up menu with a list of available connectors. Make your selection and press **Exit** to return from the pop-up menu.) Press **Tab**.
- Select a model. (Use **^C** to display choices.) Press **Enter**.

If Parallel:

- Type the Printer Name. Press **Tab**.
- Select a Processor Board, if appropriate. Press **Tab**.
- Select a Model. (Use **^C** to display choices.) Press **Enter**.

If Remote:

- If both UUCP and TCP/IP are installed, choose either **uux** or **rcmd** as the method of sending print requests. Press **Enter**.
- Type the (local) printer name. Press **Tab**.
- Select the remote machine (using **^C** and then **Exit**). Press **Tab**.
- Type the printer name on the remote system. Press **Enter**.

5. The system displays a confirmation message showing the requested printer setup.

If there is currently no default printer specified, you are asked whether or not you want the new printer to be the system default. You are not required to have a default printer; therefore, you can choose not to make the new printer the system default.

6. Press **Enter** to add the printer.

The system displays a message confirming the successful addition.

To test the newly added printer, exit the administration tools and from the shell type:

\$ lp file (if the new printer is the system default)

\$ lp -dprintername file (otherwise)

where *file* is the name of a file to be printed. A good test file is */etc/rcopts/README*.

To see how the file looks when printed out on the screen, type the following from the shell:

\$ cat file

If the file prints out the same as it looks on the terminal, your printer addition was successful. If the file does not print out the same as it looks on the terminal, refer to Chapter 13, “Troubleshooting,” for help.

Change Printer Status

This tool allows you to enable or disable a printer. When you change a printer's status, you can enter a reason for the change; *View Print System Status* displays the reason when selected.

1. From the main menu, select *Printer Administration*. Press **Enter**.
2. Select *Change Printer Status*. Press **Enter**.
3. Select a printer. Press **Enter**.
4. Press **Enter** to change the current status.
5. Type the reason you are changing the status (optional).
6. Press **Enter** to confirm the change.

Remove a Printer

If you want to temporarily disable a printer, use *Change Printer Status*. *Remove a Printer* allows you to remove a printer from the system on a more permanent basis. (Once you remove a printer, you must use *Add a Printer* before you can use the printer again.)

If you try to remove the *default printer* (see “Set the Default Printer”), the system warns you and then gives you the opportunity to specify a different default printer. A default printer is not required.

If there are print jobs queued up for the printer you want to remove (see “View Print Queue Status”), this tool displays an error message telling you there are queued requests. You can use *View Print Queue Status* to identify jobs that are queued; then you can exit **adman** and (from the shell) **cancel** or move (using **lpmove**) the print requests in the queue that are waiting for the printer you want to remove.

For example, you can type:

```
$ cancel jobname
```

where **jobname** consists of *printername-number*, meaning the name of the printer and the job number. See the *S/Series CTIX Administrator's Guide* for more information on cancelling print requests.

1. From the main menu, select *Printer Administration*. Press **Enter**.
2. Select *Remove a Printer*. Press **Enter**.
3. Select a printer. Press **Enter**.

The system displays a confirmation message.

4. Press **Enter** to confirm removal of the printer.

The system displays a message confirming the successful removal.

Set the Default Printer

If no printer is specified with a print request, the *default printer* executes the request. Use this tool to select the system default printer.

If you want to set up a personal default destination different from the system default printer, refer to the chapter in the *S/Series CTIX Administrator's Guide* that discusses setting up user environments.

1. From the main menu, select *Printer Administration*. Press **Enter**.
2. Select *Set the Default Printer*. Press **Enter**.
3. Select a printer. Press **Enter**.

Start or Stop the Print System

Starting the print system allows it to send print requests to a printer, and stopping the print system prevents it from doing so. Choosing the option *Stop now and DO NOT START at reboot* disables the print system scheduler permanently; that is, the scheduler will not be enabled when the system is rebooted.

1. From the main menu, select *Printer Administration*. Press **Enter**.
2. Select *Start/Stop the Print System*. Press **Enter**.
3. If the print system scheduler is currently running, select one of the following:
 - *Stop scheduler now but DO NOT CHANGE reboot*.
 - *Stop scheduler now and DO NOT START at reboot*.

If the scheduler is not currently running, select one of the following:

- *Start scheduler now but DO NOT CHANGE reboot*.
 - *Start scheduler now and start with EACH reboot*.
4. Press **Enter** to confirm.

Make a Printer Model

To correctly format printer output, the **lp** system requires printer-specific *description files*. This tool allows you to add a printer description file (model) to the system.

Note that by using *Add a Printer* and scrolling through the Model field, you can determine which models already exist. See “Determining the Model Name” and Table 8-1, earlier in this chapter, for a description of many of the printer models provided with CTIX. If there is not an appropriate model on your system for the printer you want to add, create a new model using *Make a Printer Model*.

Before you can create a printer model, you must determine whether you want the model for a parallel printer or a serial printer.

Specifications for Both Parallel and Serial Printers

The following characteristics are specified for both parallel and serial printer models:

Model Name Select a model name that clearly identifies your printer. Printers can be very similar, with only one or two distinguishing characteristics.

For example, say you have two Diablo printers: Diablo-A, which can print at 9600 baud, and Diablo-B, which can only print at 1200 baud. Give them model names that make it easy to tell them apart, like Diablo96 and Diablo12, rather than Diablo-A and Diablo-B.

Connection Type The connection type is either parallel or serial. Additional information on the different types of connections can be found in “Add a Printer,” earlier in this chapter.

Banner Page	A banner page is a page printed before the print request that typically shows the login name of the user who sent the request, the name of the file printed, and the date and time the file was printed.
Trailing Pages	This option specifies the number of pages to be ejected at the end of a print request.

Additional Specifications for Serial Printers

For a serial printer model, you must determine the characteristics described in “Specifications for Both Parallel and Serial Printers,” (above) in addition to the following serial line characteristics:

Baud Rate	The <i>baud rate</i> or communication speed is optimally 9600 baud.
Stop bits	<i>Stop bits</i> are the bits that inform the system when one character ends and another begins.
Parity	<i>Parity</i> is a method of checking for communication errors.
Hardware tabs	<i>Hardware tabs</i> are tab stops that are set by the printer, rather than by the software.
Carriage Motion	The <i>carriage motion</i> is what the system generates at the end of a line, usually a carriage return (CR) and a newline (NL). For some printers the system generates only a newline, or no carriage motion at all.

It is important that the characteristics you specify (when making a model) match your printer’s actual setup. For example, if your printer does not print at 9600 baud, select the baud rate option displayed on the screen that matches the speed of your printer.

Note: In addition to setting the serial line characteristics through the administration tools, you may need to reset certain switches on the serial printer itself.

Refer to the printer installation manual for instructions, if physically setting the printer's specifications is necessary.

1. From the main menu, select *Printer Administration*. Press **Enter**.
2. Select *Make a Printer Model*. Press **Enter**.
3. Type the Model Name. Press **Tab**.
4. Select the Connection Type. Press **Enter**.
5. Select the appropriate options for the following:
 - Banner (Yes or No) Press **^C** to view a list of choices. Press **Tab**.
 - Trailing Pages (None, One, Two, or Three). Press **^C** to view a list of choices. Press **Tab**.
6. For serial models only, select the following:
 - Baud Rate (110, 300, 1200, 2400, 4800, 9600, or 19200)
 - Parity (Odd, Even, or Disabled)
 - Stop Bits (One or Two)
 - Tabs (Yes or No)
 - New Line / Carriage Return (NL -> CR-NL, CR -> NL, or None)
7. Press **Enter**.
8. The system displays a confirmation message.
Press **Enter** to add the new printer model.

```
Printer Administration
Make A Printer Model
Serial Printer Options for New Model 'hp01'

Banner:      No          Stop bits:  Two
Trailing pages: None     Tabs       Yes
Baud rate:   9600        New line/CR: NL -> CR-NL
Parity:      Odd

Use 'Tab' to move between fields. When you have finished
making selections, press 'Enter'.
```

Press '^C', select banner, and press 'Exit'.

471.26

Figure 8—4. Sample Serial Printer Options Screen

Where to Go from Here

There are a few additional printer administration functions the system administrator might find useful, such as assigning a class name to a group of printers, or moving print requests from one destination to another. For more information and instructions, read the chapter in the *S/Series CTIX Administrator's Guide* that discusses the `lp` system.

For more specific information about the files and commands used to perform printer administration, refer to the following items in the *S/Series CTIX Administrator's Guide* and the *CTIX Operating System Manual*:

accept

This command allows a destination to accept print requests.

cancel

This command cancels a print request. You must specify the request ID (obtained from **lpstat**).

disable

This command prevents a destination from printing a request.

enable

This command allows a destination to print a request.

lpmove

This command moves print requests from one destination to another.

lpsched

This command starts the **lp** scheduler.

lpshut

This command stops the **lp** scheduler.

lpstat

This command displays **lp** status information.

reject

This command prevents a destination from accepting print requests.

/etc/rcopts/LP

This is a file modified by the administration tools that instructs the system to enable the scheduler when the system is turned on.

/usr/spool/lp/model

This directory contains the printer description files.

—

—

—

Chapter 9

UUCP Administration

Introduction

The *UUCP Administration* tool configures the UUCP (UNIX-to-UNIX copy) subsystem so that you can exchange mail and other files electronically with other *nodes* (computers). This tool appears in the administration tools main menu only if you are logged in as root.

A *remote system* is a system to which you are connected via phone, direct (RS-232 cable), or network link. A network is a group of systems using a special protocol to communicate with one another. In this chapter you will learn how to

- list the remote systems with which you can exchange mail and other files
- add and remove remote systems
- change the node name of your system
- make changes to the current setup
- add and remove modems

To access these functions from the main menu, select *UUCP Administration*. Press **Enter**.

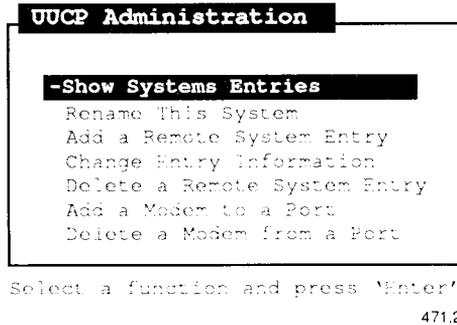


Figure 9-1. UUCP Administration Menu

Show Systems Entries

This tool allows you to list the names of remote systems with which you can exchange mail.

1. From the main menu, select *UUCP Administration*. Press **Enter**.
2. Select *Show Systems Entries*. Press **Enter**.
3. Select a System. Press **Enter**.
4. To display your system's Login Name and Password on the remote system you selected, press **Enter**.

Note: System administrators can see more information about remote systems than is shown on the Display of Other Systems screen by using Change Entry Information, described later in this chapter.

UUCP Administration
 Display of Other Systems

SYSTEM	TIME	BAUD RATE	METHOD	PHONE METHOD
test1	Any	9600	Direct	unused
test2	Any	unused	TCP	unused
test3	Any	1200	Phone	4084342848
test4	Any	unused	TCP	unused
test5	SaSu1700-0900	300	Phone	4081234567
test6	Call-In-Only			
test7	Wk0900-1700	1200	Phone	4084342848
test8	SaSu2300-0500	9600	Direct	unused
*test9	Wk1700-0900	unused	TCP	unused

For more information, select a system and press 'Enter'.

471.28

Figure 9-2. Sample Display of Other Systems

Rename This System

This tool allows you to enter a new UUCP node name for your system. You can also use this tool to determine the current name of your system.

If you are linked to an Ethernet network, this tool changes the *host name database* so that your host name matches your node name. [For more information on the host name database, see the **hostname(1)** man pages.]

Be sure to inform the users on both your system and all remote systems when you rename your system. Every host on the network should use the same host name database.

1. From the main menu, select *UUCP Administration*. Press **Enter**.
2. Select *Rename This System*. Press **Enter**.
3. Type the new UUCP/Network Name. Press **Enter**.

The system displays a confirmation message.

4. Press **Enter** to rename your system.

The system displays a message confirming the successful renaming of your system.

Add a Remote System Entry

Adding a remote system allows your users to exchange mail with the users on another system.

Since a remote system must have a user account on your system to successfully log in, you need to specify the login name that the remote system is to use when calling your system. There is no *default* remote system login name; you must supply a remote login name. It is more secure to assign a remote system its own unique login name and password. This allows you to remove the password entry if you decide not to allow the remote system to log in at some future time.

Additional restrictions can be imposed via the **Permissions** file. For more information, see the chapter in the *S/Series CTIX Administrator's Guide* that discusses UUCP.

Note that *Add a Remote System Entry* allows you to create more than one entry for a remote system, but the tool does not permit you to create an entry that is entirely inconsistent with another entry for the same system (for example, Call In Only and Call Out). However, it is your responsibility to ensure that a more restrictive entry is not being overridden by a less restrictive entry for the same system (for example, calls allowed at any time versus calls allowed only at night).

Use *Show Systems Entries* to identify multiple entries for the same system. If you want only one entry for a system that has an existing entry, use *Change Entry Information*, not *Add a Remote System Entry*.

Before Adding a Remote System Entry

Before you begin the process of adding a remote system entry, there are a few things you should determine. The items described below are requested by *Add a Remote System Entry*:

Remote Name	The UUCP <i>node name</i> of the system you are adding.
Direction of Calls	You can allow calls to go out only, in only, or in either direction. Note that you are prompted for the Remote Login Name, Remote Password, Days Calls Allowed, and Hours Calls Allowed, only if you do not choose Call In Only.
Login Name	The login account the remote system uses to log into your system. You are prompted for this and Password only if you do not choose Call Out Only.

Chapter 9

Password	The password the remote system must use to log into your system.
Remote Login Name	The login account your system uses to log into the remote system. If you choose not to use nuucp , the default mail login name, make sure the name you choose has a valid account on the remote system.
Remote Password	The password your system uses to gain access to the remote system.
Days Calls Allowed	Refers to the days of the week your system can call the remote system.
Hours When Calls Allowed	<p>Refers to the hours during the day your system can call the remote system, which is useful for limiting outgoing calls to hours when phone rates are cheaper.</p> <p>You can specify different days of the week and different hours when calls are allowed from those displayed by modifying the Systems file. For more information, see “Where to Go from Here,” later in this chapter.</p>
Type of Connection	The steps involved in adding a remote system depend on the type of communication link used to send mail. Types available are direct link, TLI link, Sockets link and phone link. The communication links are described in the following sections.

Direct Link

A *direct link* means your system is connected to the remote system using an RS-232 cable.

The two systems communicate through this cable. When you use a direct link to exchange mail, the **adman** program requests the port location and the baud rate.

- **Port Location.** You must let the system know the location of the serial port you want to use of the direct connection. The **adman** program first asks which board the port is on, then asks you to specify which port on the chosen board.
- **Baud Rate.** As with a phone link, your system needs to know the speed at which the remote system can exchange mail over the direct link.

Sockets Link

A *Sockets link* means your system and the remote system are connected through an Ethernet network using the sockets interface. For more information, see the *CTIX Operating System Manual*.

Note: This option requires that you have the TCP/IP networking package installed on your system.

TLI Link

A *TLI link* means your system and the remote system are connected via an Ethernet network using the transport layer interface. For more information, see the *CTIX Operating System Manual*.

Note: This option requires that you have the RFS networking package and TCP/IP installed on your system.

Phone Link

A *phone link* means your system and the remote system use a *modem* to communicate over the telephone lines. A modem is a device on each system that translates the analog signals coming over the telephone line into digital data signals the computer understands.

When you use a phone link to exchange mail, the administration tools request the remote system's phone number and communication speed (baud rate). Note that the correct phone number, called a *dialing sequence*, may need to include a digit to get an outside line, or a character to cause a delay. (For more information on dialing sequences, see the chapter in the *S/Series CTIX Administrator's Guide* that discusses UUCP.)

Note: Using a phone link also requires a modem connected to a port on your system. For more information and instructions, see "Add a Modem to a Port," later in this chapter.

Procedure for Adding a Remote System Entry

1. From the main menu, select *UUCP Administration*. Press **Enter**.
2. Select *Add a Remote System Entry*. Press **Enter**.
3. Type the Remote System Name. Press **Tab**.
Select the Direction of Calls. Press **Enter**.
4. If call-ins are allowed, type the Login Name to be used by the remote system. Press **Enter**.

5. If there is not currently a login account on your system for the remote system, the option to create a login is displayed. To create a login for the remote system:
 - Press **Enter**.
 - Type the remote system's password. The password must be at least six characters long, (only the first eight characters are significant), and it must contain at least one numeric and one alpha character. Press **Return**.
 - Retype the remote system's password. Press **Return**.
 - Press any key to continue.
 6. If call-outs are allowed
 - **Backspace** over **nuucp**, and type the Login Name your system uses on the remote system, if different from **nuucp**. (You need to coordinate the Login Name and password (if any) with the administrator of the other system.) Press **Tab**.
 - Type the password your system will use to log into the remote system. Press **Tab**.
 - Make selections for Days and Hours outgoing calls are allowed, and for Type of Connection. (Press **^C** to view choices.) Press **Enter**.
 7. If Phone link:
 - Type the phone number.
 - Select the Baud Rate.
 - Press **Enter**.
- If Direct link:
- Select the Serial Processor Board. Press **Enter**.
 - Select the Connector. (Press **^C** to view choices.)

Chapter 9

- Select the Baud Rate. (Press ^C to view choices.)
- Press **Enter**.

If Sockets or TLI link, press **Enter**.

The system displays a confirmation screen showing the options selected.

8. Press **Enter** to execute the addition.

The system displays a message confirming the successful addition of the remote system.

```
UUCP Administration
Change a Remote System
Options for Local to Call Remote System
Phone Number of Remote System/Connection Line Speed
Confirm Adding Remote System

This system can call in both directions; remote system is
'vars'.

Login name on remote:      'nuucp'
Password on remote:       'scil88'
Connection type:          'phone' at 1200 baud
Phone number:              '4342848'
Days remote can be called: 'Any'
Times remote can be called: 'Any Time'

Press 'Enter' to confirm new entry for 'vars', 'Cancel' to deny.
471.29
```

Figure 9-3. Sample Confirm Adding Remote System Screen

Change Entry Information

This tool allows you to make changes to any or all of the specifications involved in adding a remote system.

The default menu selections displayed in this tool are those of the remote system's current setup, and can thus be used to provide detailed information about remote systems within your electronic mail network.

1. From the main menu, select *UUCP Administration*. Press **Enter**.

2. Select *Change Entry Information*. Press **Enter**.

3. Select the entry to be changed. Press **Enter**.

4. To change the entry name for the remote system **Backspace** over the Remote System Name displayed and enter a new name. Press **Tab**.

Select the Direction of Calls. Press **Enter**.

5. If call-ins are allowed, type the Login name the remote system will use when calling your system.

6. Type any changes to the Remote Login Name and the Remote Password. Press **Tab** to continue.

If call-outs are allowed, select any changes to Days and Hours for outgoing calls, and to the Type of Connection. Press **Enter**.

7. (Phone links only) Type any changes to the dialing sequence and baud rate. Press **Enter**.

(Direct links only) Type any changes to the connector number and baud rate. Press **Enter**.

The system displays a confirmation screen showing the options selected.

8. Press **Enter** to execute the changes.

The system displays a message confirming successful execution.

Delete an Entry

This tool allows you to delete a remote system entry, thus removing the entry from the list of systems you can call and/or systems that can call you. Note that, in the case of multiple entries for the same system, the tool removes only the entry you specify.

1. From the main menu, select *UUCP Administration*. Press **Enter**.
2. Select *Delete a Remote System Entry*. Press **Enter**.
3. Select the Remote System Entry you want to delete. Press **Enter**.

The system displays a confirmation message.

4. Press **Enter** to delete the entry.
5. The system displays a message confirming the deletion.

Add a Modem to a Port

Using a telephone link to exchange electronic mail requires a modem connected to a port that is specifically configured to send and receive electronic mail. Adding a modem to a port requires your knowing

- the processor
- connector number
- baud rate

(For more information on *ports* and *processors*, see “Enable a Login on a Serial Port,” in Chapter 7.)

Note that each phone link does not require its own modem. You can use one link for more than one machine; one port with a modem should suffice for your system.

If you want to add a modem that is not displayed on the menu of modem types, see the section in the *S/Serial CTIX Administrator's Guide* on adding an entry to the **Dialers** file.

1. From the main menu, select *UUCP Administration*. Press **Enter**.
2. Select *Add a Modem to a Port*. Press **Enter**.
3. Select the Processor. Press **Enter**.
4. Press **^C** to view choices for each of the following steps:
 - Select the Connector.
 - Select the Direction of Calls.
 - Select the Baud Rate.
5. If the modem will make outgoing calls, a menu of modem types is displayed. Select a modem type. (This information is used to specify the login expect-send sequence when the modem dials another system. If the wrong modem type is specified, when your system tries to dial another system, your system will send the modem instructions in a form it cannot understand or implement.)
6. Press **Enter**.

The system displays a confirmation message.
7. Press **Enter** to add the modem.

The system displays a message confirming the successful addition.

Delete a Modem from a Port

This tool allows you to delete a modem from a port. Note that if the modem was used for a *Call In Only* connection, there is a login on the terminal line: you may want to use *Terminal Administration* to disable the login.

1. From the main menu, select *UUCP Administration*. Press **Enter**.
2. Select *Delete a Modem from a Port*. Press **Enter**.
3. Select the modem you want to delete.

The system displays a confirmation message.

4. Press **Enter** to delete the modem.

The system displays a message confirming the successful deletion.

Where to Go from Here

For more specific information about the files and commands used to perform UUCP administration, refer to the following items in the *S/Series CTIX Administrator's Guide* and the *CTIX Operating System Manual*:

/etc/rcopts/NODE

This is a file modified by the administration tools that contains the name of your UUCP system name. This file is read when the system is first booted.

/usr/lib/uucp/Devices

This file designates the characteristics of the port each remote system uses to send and receive mail. Each port used to send electronic mail must have an entry in the Devices file.

/usr/lib/uucp/Dialers

This file describes the call-placing protocols for automatic call units (ACUs). ACUs are also called dial-out (smart) modems. If your modem is not listed on the menu of modem types, you must construct an entry for it in this file.

See the *S/Series CTIX Administrator's Guide* for information on adding an entry to **/usr/lib/uucp/Dialers**.

/usr/lib/uucp/Permissions

This file specifies the login names remote systems are allowed to use to log into your system. This file also specifies the restrictions, if any, to be placed upon each remote system (whether it is bidirectional or call out only).

/usr/lib/uucp/Systems

This file (modified by the administration tools) describes the remote mail systems linked to your system, including a login script necessary to establish communication with the remote system.

mailx(1), mail(1)

These commands are used for sending and reading mail messages within your system, or from one system to another.

uucp(1)

You can use this command to send files from one system to another using a direct, phone, or network link.

—

—

—

Chapter 10

Network Administration

Introduction

As system administrator, you can use the *Network Administration* tool to perform the network administration functions listed below. Full documentation of CTIX network administration can be found in the *CTIX Network Administrator's Guide*.

Note: The Network Administration features described in this chapter are only available on your system if you have TCP/IP installed.

In this chapter you will learn how to

- check the status of machines on the network
- monitor network users
- add and delete equivalent users and equivalent machines
- add and delete network services
- add, change, and delete host entries
- generate various network interface statistics

Networking Concepts

The following subsections explain certain concepts a network administrator should know. If you are already familiar with network administration, and you only need to know how to use the **adman** program to perform network administration functions, skip to the section “Network Administration Procedures.”

For more detailed information on terms and concepts discussed in this section, refer to the following items in the *CTIX Network Administrator's Guide*:

A computer *network* is an interconnected group of two or more machines, set up to communicate with one another. CTIX networks use three types of connections:

- RS-232 cables (UUCP, SLIP)
- Phone lines (UUCP, SLIP)
- TLI, Sockets, or Token Ring (using TCP/IP transport protocol)

A *host* is a single computer on a network. A *host entry* is the record describing a particular machine in the *host database*; this database contains information about each machine on the network. Each host on the network should have identical copies of this database, called */etc/hosts*.

Each host has a name which is either a simple name (*node name*), determined by the **uname** command at boot time, or a full *Internet name*, consisting of the node name and an Internet domain name separated by a period (.). For example, an S/480 with a node name **grumpy** in an Internet domain **xyzcorp.COM** uses the host name **grumpy.xyzcorp.COM**.

A service exists on each computer which translates the host name into an internetwork address. This allows a program to identify a host by either its name or its address.

Each computer on a TCP/IP network has a unique *Internet address*. This address identifies the network to which the host is connected and the logical location of the host on the network.

A *network gateway* is a computer (host) that passes data from one network to another type of network. A *network bridge* is a computer (host) that passes data from one network to another similar network. Both bridge and gateway computers are connected to more than one network and generally have more than one network address.

A *network service* is a program running on a networked computer that provides a service to users of that computer or other users on the network. Network services are sometimes called *daemons*; their names often end with the letter *d*.

Network commands are programs that users can run to access network services. These programs can be anything from simple utilities to complex applications. A program running a network command is called a *client*. A client uses services on a server.

User Equivalence

User equivalence is the mapping between a user on a remote host and a user on a local host. A user on a remote host can log into the local host using a local user name, and be granted the local user's privileges, without knowing the corresponding user password.

When you declare a remote user equivalent to yourself, that user can use the following services on your machine *without supplying a password*: **rshd** (remote shell server, used for commands such as **rcmd** and **rcp**); **rlogind** (remote login server); and **rexecd** (remote execution server).

User equivalences compromise the security of your system, since they allow remote users to gain access to resources on your system without password authentication. Equivalences are useful in certain circumstances; for example, when one user has accounts on several different systems. Equivalences are required when a remote system gains access to your printer using the **rcmd** program. This is an option when you add a remote printer using the printer administration functions described in Chapter 8.

Machine Equivalence

Machine equivalence allows users on a remote host to log into the local host (provided their login names are the same on the remote and local machines).

When you declare a remote machine equivalence, *any* user (except root) on the remote machine who has an account on your machine (with the same login name) can use the following services on your machine *without supplying a password*: **rshd** (remote shell server, used for commands such as **rcmd** and **rcp**); **rlogind** (remote login server); and **rexecd** (remote execution server).

Machine equivalences are a potential threat to the security of your system, since they can allow large numbers of remote users access to resources on your system without password authentication.

When a remote system is declared equivalent to yours, its security must be as good as local security. One insecure system declared as equivalent can compromise the security of an entire network.

Network Administration Procedures

To access these functions from the main menu, select *Network Administration*. Press **Enter**.

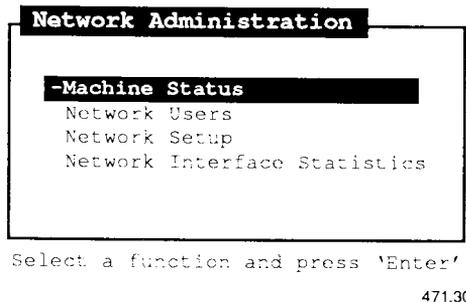


Figure 10-1. Network Administration Menu

Machine Status

This tool displays the status of the machines (hosts) on the local network. Information displayed for each machine includes the machine's name, whether its network connection is up or down, how long the machine has been in its current state, the number of logged in users, and the recent *load* on the machine. The load represents the average number of processes ready to run on a machine at any given time, measured over the last one, five, and fifteen minutes.

Only machines running the `rwhod` service are listed in this display. (To add this service on your local machine, use *Add a Network Service* under "Network Setup," described later in this chapter.)

1. From the main menu, select *Network Administration*. Press **Enter**.
2. Select *Machine Status*. Press **Enter**.

Machine	Status	Time	Users	Load
B10L-GW	up	42+19:54,	0 users,	load 0.00, 0.00, 0.00
Ernie	up	7+10:22,	1 user,	load 0.00, 0.00, 0.00
Mitil	up	27+13:40,	0 users,	load 0.00, 0.00, 0.00
intlmtg	up	33+10:00,	0 users,	load 0.00, 0.00, 0.00
pilot	up	28+12:09,	5 users,	load 3.00, 3.00, 3.00
scribe	up	13+11:28,	0 users,	load 0.00, 0.00, 0.00
slave	up	0:47,	1 user,	load 0.00, 0.00, 0.00

Press 'Cancel' to exit the form.

471.31

Figure 10-2. Sample Remote Machine Statistics Screen

The screen displayed in Figure 10-2 contains the following fields:

- Machine** The machine that is sending status information.
- Status** A machine is either up or down, and is considered down if it has not sent your machine its status for five minutes or more.
- Time** The amount of time the machine has had its current status. The format is *days + hours:minutes*.

Users	The number of users who are currently logged in and have used the system within the last hour.
Load	The average system load (number of processes ready to run) over the last one, five, and fifteen minutes.

Network Users

This tool displays the users currently logged in on all the *nodes* (hosts) on the local network. The displayed (see Figure 10-3) information for each user includes the user name, the machine name, the terminal, the date and time the user logged in, and the idle time (if the user has not typed in the last minute).

You can select a user to whom you are *equivalenced* (see “Add an Equivalent User” below) on a remote machine and get detailed process status information. Note that if a user is logged in on more than one terminal, there is more than one line of information displayed for him.

Only machines running the **rwhod** service are listed in this display. (To add this service on your local machine, use *Add a Network Service* under “Network Setup,” described later in this chapter.)

1. From the main menu, select *Network Administration*. Press **Enter**.
2. Select *Network Users*. Press **Enter**.
3. To display more information on an equivalent user, select the user and press **Enter**.

Press **Cancel** to exit the tool.

Network Users			
USER	WHERE	LOGIN TIME	IDLE TIME
-dai	pilot:tty264	Apr 11 13:40	7:59
david	scribe:tty256	Apr 11 16:59	1:52
greg	intlmktg:tty256	Mar 30 16:28	1:47
greg	pilot:tty259	Apr 8 07:09	13:00
joanne	pilot:tty265	Apr 8 15:56	
log	pilot:tty256	Apr 11 14:35	6:34
lpw	Mitil:ttyp01	Apr 11 12:04	4:56
mitydoc	pilot:tty004	Apr 25 07:57	
nancy	scribe:tty012	Apr 11 17:09	4:47
nspltmgr	pilot:tty266	Apr 11 15:27	
pcx	Ernie:ttyconsole	Apr 11 11:36	:10

For more information, select a user and press 'Enter'.

471.32

Figure 10-3. Sample Network Users Screen

The screen displayed in Figure 10-3 contains the following fields:

- User** The login name of the user whom the status line concerns.
- Where** The machine and terminal on which the user is logged in.
- Login Time** The date and time (in 24-hour time) that the user logged into the system.
- Idle Time** The hours and minutes since the user entered data into his terminal.

Network Setup

This tool allows you to administer your machine's network setup, including the following capabilities:

- add or remove equivalent remote users (nonprivileged users can also use this tool).
- add or remove equivalent remote machines.
- add or remove network services.
- add, change, or remove host database entries. Note that, to be effective, any changes must be propagated throughout the network.

Caution

Network equivalences, especially machine equivalences, seriously threaten the security of your system. When a remote system is declared equivalent to yours, its security must be as good as local security. One insecure system declared as equivalent can compromise the security of an entire network.

Add an Equivalent User

Whether you are a privileged or nonprivileged user, this tool allows you to give a remote user equivalence privileges on the local machine.

The user you specify can use the following services on your machine without using a password: **rlogind** (remote login service), **rshd** (remote shell service), **rexecd** (remote execution service), and **ouucpd** (old network uucp service). For more information about services available, see “Add a Network Service,” later in this chapter.

Equivalences are useful in certain situations, such as when one user has accounts on several different systems. Equivalences are required when a remote system accesses your printer via the **rcmd** program: this is an option in the *Printer Administration* tool.

To allow a remote system to use your printer via **rcmd**, select the remote host machine, type **lp** as the remote user, and select **lp** as the local user. (In addition to these steps, the remote system must configure a printer as remote to your system via **rcmd**, and the printer must be configured correctly as a serial or parallel printer on your system.)

1. From the main menu, select *Network Administration*. Press **Enter**.
2. Select *Network Setup*. Press **Enter**.
3. Select *Add an Equivalent User*. Press **Enter**.
4. Press **^C** to display the list of Remote Hostnames. Select a hostname and press **Enter**. Then press **Tab**.
5. Type the Remote Host User you want to make equivalent and press **Tab**.
6. Press **^C** to display the list of Local Users. Select the appropriate user and press **Enter**.
7. The system displays a confirmation message.
Press **Enter** to add the equivalent user.

Delete an Equivalent User

This tool allows you to remove an equivalent user from your system.

1. From the main menu, select *Network Administration*. Press **Enter**.
2. Select *Network Setup*. Press **Enter**.
3. Select *Delete an Equivalent User*. Press **Enter**.

4. Press **^C** to display the list of Remote Hostnames. Select a hostname and press **Enter**.
5. Type the equivalent Remote Host User you want to delete.
6. Press **^C** to display the list of Local Users. Select the appropriate user and press **Enter**.
7. The system displays a confirmation message.
Press **Enter** to delete the equivalent user.

Add an Equivalent Machine

This tool allows you to add a machine equivalent to your own machine. When you add a remote *machine equivalence*, any user (except root) with an identical login name on the remote machine can log into your machine as the (identical) local user, with identical privileges.

Users on the equivalent machine can use the following services on your machine without using a password: **rlogind** (remote login service), **rshd** (remote shell service), **rexecd** (remote execution service), and **ouucpd** (old network uucp service). For more information about services available, see “Add a Network Service,” later in this chapter.

Caution

Machine equivalences are an especially dangerous threat to the security of your system, since they allow potentially large numbers of remote users to access resources on your system without password authentication.

When a remote system is declared equivalent to yours, its security must be as good as local security. One insecure system declared as equivalent can compromise the security of an entire network.

1. From the main menu, select *Network Administration*. Press **Enter**.
2. Select *Network Setup*. Press **Enter**.
3. Select *Add an Equivalent Machine*. Press **Enter**.
4. Select the machine to be made equivalent. Press **Enter**.
5. The system displays a confirmation message.
Press **Enter** to add the equivalent machine.

Delete an Equivalent Machine

This tool allows you to delete any machines that are currently equivalent.

1. From the main menu, select *Network Administration*. Press **Enter**.
2. Select *Network Setup*. Press **Enter**.
3. Select *Delete an Equivalent Machine*. Press **Enter**.
4. Select the equivalent machine to be deleted. Press **Enter**.
5. The system displays a confirmation message. Press **Enter** to delete the equivalent machine.

Add a Network Service

Adding a network service allows users on remote machines to use that service on your machine. For example, making **rlogind** (remote login service) available allows users on remote machines to remotely log into your machine.

A *network service* is a program running on a networked computer that provides a service to users on the network. A computer running a service is called a *server*. Services are sometimes called **daemons**; their names often end with the letter **d**.

For example, **inetd** (the internet daemon), is a program that runs at all times, listening for remote users trying to connect for a login session. When it “hears” one of these users, it starts up a process that allows the login to occur (with proper security checking).

The full list of services that can be made available consists of **ouucpd**, **rwhod**, and services with valid entries in **/etc/inetd.conf**. Except for **ouucpd** and **rwhod**, all services are spawned only when needed by the “super-service” **inetd** [see **inetd(1M)** in the *CTIX Operating System Manual*] and are terminated at the completion of a remote request. Thus they appear in the process table only while satisfying a particular remote request.

Network Service Descriptions

Note that there are security considerations when selecting services to be made available. These are discussed after service descriptions below:

rwhod	Host status service; collects and distributes information about hosts on the local network, including the local host; must be running for the administration tools to display network status information.
ouucpd	Network UUCP file transfer service in which the client (remote) machine must run a Convergent-specific version of UUCP over TCP/IP.
ftpd	DARPA Internet File Transfer Protocol service; services ftp requests.
telnetd	DARPA TELNET virtual terminal protocol service; services telnet requests.
rshd	Remote shell service; required for programs such as rcmd and rcp which execute a noninteractive shell.
rlogind	Remote login service; services rlogin requests.

Chapter 10

rexecd	Remote execution service; services rexec(3) requests.
uucpd	network UUCP file transfer service in which the client (remote) machine must run a version of UUCP over TCP/IP based on the Honey-Danber implementation.
fingerd	Remote user information service; services finger and, on some other systems, name requests.
tftpd	DARPA Trivial File Transfer Protocol service; services tftp requests.
talkd	Remote user communication service; notifies a user that someone (for example, on a remote machine) wants to initiate a conversation; required for the talk program.

Network Service Security Considerations

Some of the services pose security risks. Services are listed below in descending order of risk, with explanations as to why the service is risky. If security is of utmost concern to you, you probably will not want to make any of the most risky services available to remote users.

The least secure services are the following:

tftpd	Does not enforce any password authentication; although only publicly readable files may be transferred, the search permissions of the directories leading to the files accessed are not checked.
fingerd	Allows any user on a remote machine to obtain a list of users on your machine (that is, remote users can find out who has password entries on your system).
rwhod	Same as above, although more secure because users must be logged in to be displayed.

The following services are less risky, but of some concern:

rexecd, rlogind	Password authentication avoided if user or machine is declared equivalent on your machine.
rshd, ouucpd	
talkd	Possible for remote users to obtain a list of users on your system, although it would be tedious to do so, and not likely to be complete.

Other services require password authentication and are in other ways more secure than those listed above.

1. From the main menu, select *Network Administration*. Press **Enter**.
2. Select *Network Setup*. Press **Enter**.
3. Select *Add a Network Service*. Press **Enter**.
4. To view the full list of network services on your machine, use **Tab** to move to the text field, and use the arrow keys to cursor through the text items. Select a service and press **Enter**. (No confirmation is required.)

Delete a Network Service

This tool allows you to delete services currently available.

1. From the main menu, select *Network Administration*. Press **Enter**.
2. Select *Network Setup*. Press **Enter**.
3. Select *Delete a Network Service*. Press **Enter**.
4. Select the service you want to make unavailable. Press **Enter**.
5. The system displays a confirmation message. Press **Enter** to delete the service.

Add a New Host Entry

This tool allows you to add a new host entry to your system's hostname database. The hostname database contains an entry for each host that shares the network, including the local host. Each entry specifies, at minimum, a unique hostname and address. Networking programs (for example, services such as **ftp**) use the database to match hostnames to addresses. (This matching of names to addresses is sometimes called *hostname resolution*.)

Currently, the hostname database is contained in a single file, `/etc/hosts`, which is modified by this tool; it should be the same on all machines that share the network. That is, any change to the hostname database must be propagated throughout the network for it to be effective.

For this reason, it is usually best to maintain the file from a central location: any additions, changes, or deletions are entered on a single machine, and that machine copies its version of `/etc/hosts` to all the other machines on the network.

The information required to construct a new host entry is described below. Refer also to the *CTIX Network Administrator's Guide* and `hosts(4)` in the *CTIX Operating System Manual*.

Host Name	The official name of the host. Use the host's UUCP node name; this name should be no longer than eight characters. ¹ The tool checks your entry to make sure it is unique in the database.
Host Address	Must be in Internet format. The simplest form is the net.node (Class A) address, where net is the network number and node is the unique number you are assigning to a machine interface. (For example, 8.24 would be a valid

1. If your system has a registered Internet domain name, see the *CTIX Network Administrator's Guide* for additional configuration information.

address for a node on network number 8.) The tool checks your entry to make sure the network number is valid, that the address is unique in the hostname database, and that the address is in valid Internet format.

Host Aliases	Alternate names for the host. You can enter a space-separated list of these. Each alias must be a unique name in the file. (The tool checks to make sure this is true.)
Comments	A section supplied for your own use that is not used by networking programs.

To add a new host entry:

1. From the main menu, select *Network Administration*. Press **Enter**.
2. Select *Network Setup*. Press **Enter**.
3. Select *Add a New Host Entry*. Press **Enter**.
4. Type the Hostname. Press **Return**.
5. Type the Network Address. Press **Return**.
6. Type any Aliases. Press **Return**.
7. Type any Comments. Press **Enter**.
8. The system displays a confirmation message. Press **Enter** to add the host entry.

Change a Host Entry

This tool allows you to change the information in a host entry. Note that changing a host name disturbs the net-UUCP configuration on your machine: if you haven't already done so, you should change the appropriate UUCP remote system entry.

1. From the main menu, select *Network Administration*. Press **Enter**.
2. Select *Network Setup*. Press **Enter**.
3. Select *Change a Host Entry*. Press **Enter**.
4. The entries displayed are those in the current host database.
Select a host to change and press **Enter**.
5. Type the new hostname if the name is different. Press **Enter**.
6. Type the Network Address. Press **Return**.
7. Type any Aliases. Press **Return**.
8. Type any Comments. Press **Enter**.
9. The system displays a confirmation message. Press **Enter** to change the host entry.

Delete a Host Entry

This tool allows you to delete a host entry from your system's database. If you have configured a net-UUCP entry for this system, you will need to delete the appropriate UUCP remote system entry.

1. From the main menu, select *Network Administration*. Press **Enter**.
2. Select *Network Setup*. Press **Enter**.
3. Select *Delete a Host Entry*. Press **Enter**.

4. Select an entry to delete and press **Enter**.
5. The system displays a confirmation message with the current host database information for the selected entry. Press **Enter** to delete the entry.

Network Interface Statistics

This tool allows you to display various network related statistics, such as the following:

- Active Connections
- Network Interface
- Routing Tables
- Memory Usage
- Protocol Statistics

Active Connections

This tool allows you to display the connections that are currently active on the local machine. Each entry describes a connection and specifies the protocol, receive and send queue sizes (in bytes), the local and remote addresses (name and port number of each), and the status of the connection. (Status is meaningful only for *connection-oriented protocols* and depends on the specific protocol in use.)

1. From the main menu, select *Network Administration*. Press **Enter**.
2. Select *Network Interface Statistics*. Press **Enter**.
3. Select *Active Connections*. Press **Enter**.

Network Interface

This tool allows you to display cumulative interface statistics since the last system boot. Each line is an entry for an interface on the local machine and displays the name of the interface, the largest packet that can be transmitted through the interface (Mtu, maximum transmission unit), the name of the network, the host machine name on the network, the number of input and output packets transmitted, the number of input and output errors, and the number of collisions.

1. From the main menu, select *Network Administration*. Press **Enter**.
2. Select *Network Interface Statistics*. Press **Enter**.
3. Select *Network Interface*. Press **Enter**.

Network Interface Activity							
Name	Mtu	Address	Ipkts	Ierrs	Opkts	Oerrs	Collis
en0	1500	slave	75001	0	6443	0	0
lo0	2048	loopback	122	0	122	0	0

Press 'Cancel' to exit the form.

471.33

Figure 10-4. Sample Network Interface Activity Screen

Routing Tables

This tool allows you to display the currently defined routes to the various networks and their current state and use.

A *route* is a CTIX data structure that contains information about how to direct data from one host to another. All routes on a given host (taken collectively) make up its *routing tables*. For a full explanation of routes, see the *CTIX Network Administrator's Guide*.

To see the currently defined routes:

1. From the main menu, select *Network Administration*. Press **Enter**.
2. Select *Network Interface Statistics*. Press **Enter**.
3. Select *Routing Tables*. Press **Enter**.

Network Administration
Network Statistics
Routing Tables

```
Routing tables
Destination      Gateway      Flags      Refcnt     Use     Interface
loopback         loopback    UH         0           0       0
B10-Net          slave       U          24          28      28
```

Press 'Cancel' to exit the form.

471.34

Figure 10-5. Sample Routing Tables Screen

Memory Usage

This tool allows you to display the status of the network managed memory area. The display shows the current status of the area of memory that the operating system uses for the network interface data.

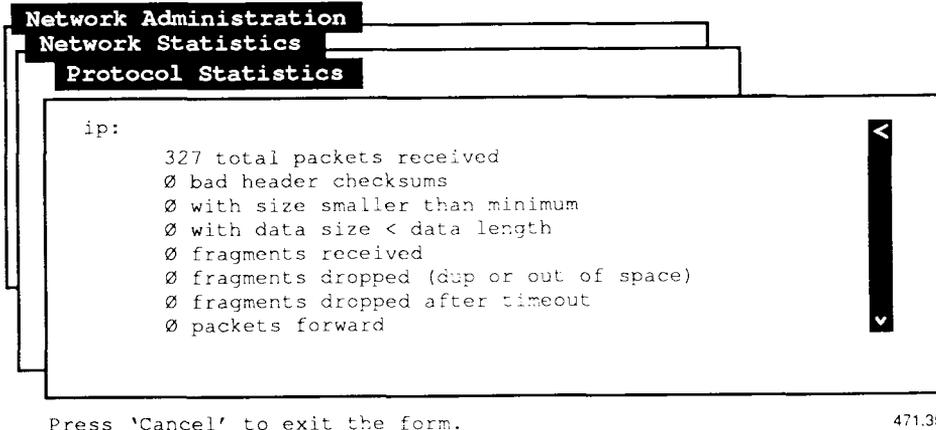
The basic unit of memory is the *mbuf*, which is currently defined as 128 bytes. The display shows the number of *mbufs* currently in use and what they are being used for, and the number that have been allocated. The display also shows the total amount of memory usage in thousands of bytes and the number of requests that have been refused because there was no space available. (When memory requests are refused, the interface is probably overloaded.)

1. From the main menu, select *Network Administration*. Press **Enter**.
2. Select *Network Interface Statistics*. Press **Enter**.
3. Select *Memory Usage*. Press **Enter**.

Protocol Statistics

This tool allows you to display the protocol-level errors that have occurred since the system was booted.

1. From the main menu, select *Network Administration*. Press **Enter**.
2. Select *Network Interface Statistics*. Press **Enter**.
3. Select *Protocol Statistics*. Press **Enter**.



```
Network Administration
Network Statistics
Protocol Statistics

ip:
  327 total packets received
  0 bad header checksums
  0 with size smaller than minimum
  0 with data size < data length
  0 fragments received
  0 fragments dropped (dup or out of space)
  0 fragments dropped after timeout
  0 packets forward
```

Press 'Cancel' to exit the form. 471.35

Figure 10-6. Sample Protocol Statistics Screen

Statistics are displayed as follows:

- ip Represents the Internet Protocol. Its function is to check for packet delivery.
- icmp Represents the Internet Control Message Protocol. Its function is to check for errors.
- tcp Represents the Transmission Control Protocol. It checks the reliability of connections.
- udp Represents the User Datagram Protocol. Its function is to check for datagram delivery.

Note: For more information on the options shown in the Network Interface Statistics menu, see the "CTIX Operating System Manual."

Where to Go from Here

For more specific information about network administration, refer to the *CTIX Network Administrator's Guide*.

/etc/inetd.conf

This file instructs the system which services can be made available to remote users.

/etc/hosts

This file contains the list of host systems on the network.

/etc/networks

This file contains a list of the networks on the Internet.

/etc/protocols

This file contains a list of the available protocols.

/etc/hosts.equiv

This file contains a list of the remote hosts with machine equivalence.

/usr/hosts/loopback

This interface program allows you to use the network protocols to communicate with your own host. **loopback** is used to check the networking software without making any assumptions about the state of the network media and other systems.

ruptime

The **adman** program uses this command to display the status of hosts on the local network. Information includes the length of time the host has been up, the number of active users logged in, and the system load.

Chapter 10

rwho

The **adman** program uses this command to display the status of users on the local network.

netstat

The **adman** program uses this command to display various network statistics.

Chapter 11

Remote File Sharing Administration

Introduction

This chapter describes the procedures for using the **adman** program to manage the services provided by the Remote File Sharing (RFS) package for the CTIX operating system.

Note: Remote File Sharing (RFS) is an optional software package. You need to install it on your system to have access to the features described in this chapter.

The first section discusses the basic capabilities of RFS. For detailed information on RFS, refer to the *S/Series CTIX Administrator's Guide*.

For a discussion of the advantages and disadvantages of using RFS vs. the Network File System (NFS) see Appendix C.

The balance of the chapter gives the information you need and provides the steps required when you use the **adman** program to perform administration tasks on a system running RFS.

Remote File Sharing

Remote File Sharing allows computers running UNIX System V Release 3 (or higher) to share *resources* (files, directories, or devices) selectively across a network. A system on a network can *advertise* the directory containing files to be shared. Other systems on the same network can then *mount* these directories. Once mounted, these remote files can be used in the same way that local files are used.

For administrative purposes, subsets of the machines on a network running RFS are grouped into *domains*. Each domain has one designated computer, known as the *Primary Name Server*, that is responsible for maintaining the list of resources in the domain, including information about how to reach them (their *network addresses*), and about resources they have advertised and remotely mounted. If machines in the domain want to share resources with other domains, the Primary Name Server must also know about those domains and their primary name servers.

One or more *secondary name servers* for the domain can also be designated, in case the Primary Name Server goes down or explicitly transfers control. It is important to designate at least one secondary name server. When the Primary goes down or transfers control, the secondary is given responsibility to function as a primary. When the Primary comes back up again, the secondary must explicitly transfer control back to it.

Unlike other distributed file systems used with the UNIX operating system, RFS is built into the operating system itself. This approach has two major advantages:

- | | |
|--------------|---|
| Transparency | Once you mount a remote resource on your system it looks to your users as though it is part of the local system. You can then use most standard UNIX system features on the resource. Standard commands and system calls, as well as other operations on files, behave the same for remote resources as for local resources. Applications should also work normally on remote resources without modification. |
| Security | Standard UNIX system file security measures are available to protect your resources. In addition, RFS includes the following security features: <ul style="list-style-type: none">• Only resources that you have elected to advertise can be shared, so access can be prevented by not advertising. |

- Resources can be advertised as read only, so that no remote system can write to the file or directory.
- When a resource is advertised, a list of systems that are allowed to have access to that resource can be explicitly specified. The advertised resource is not available to any system not on the list.
- Users and groups can be mapped to different values or excluded, to prevent (for example) a person with root privileges on one system from having root privileges on another.

Using the **adman** program, you can manage the functions that the Remote File Sharing service provides. By following the steps in the “RFS Administration Procedures” section of this chapter, you can use the **adman** menus to create a new domain, add your system to an existing domain, mount or advertise resources, protect sensitive resources from unauthorized use, or view lists of resources advertised by other systems.

RFS Administration Procedures

This section provides the procedures necessary for you to use the **adman** program to perform administrative functions on a system running RFS. The **adman** program allows you to use the capabilities of the RFS services discussed in the previous section.

Before you can start RFS on your system, you must either create a new domain on which your system is the Primary Name Server, or add your system to a currently existing domain. You can complete either of these tasks using the **adman** program. After this is completed and RFS is started, you can use **adman** to administer the functions of the Remote File Sharing service. You can view resources advertised by other systems, mount and use advertised resources, or advertise resources on your system that you want to make available to other systems.

The following list of steps provides an overview of the procedures for setting up a new RFS domain. The specific steps you should perform when you begin the actual setup procedures are provided in subsections that follow.

1. The machine that will be the Primary Name Server for the domain needs to be set up first. To do this, you use *Set Up Your Machine to Run RFS*. Specify your machine as the Primary Name Server and assign a name to the domain. You will be adding yourself to the domain, so assign yourself an RFS password when prompted to do so.
2. The Primary Name Server uses the Configure the Domain function to add machines to the domain. Each machine can be a member of one (and only one) domain, so make sure the machines you add aren't members of other domains.

Note: In fact, there is no easy way to make sure a machine is a member of only one domain. Ask the administrator of each machine if that machine is already a member of a different domain.

When you add a machine, you will be prompted to specify an RFS password: make a note of the password you assign and tell the password to the administrator of that machine.

Do *not* add a secondary name server until that machine has been set up to run RFS and has actually started RFS.

Note: If there are secondary name servers for the domain, at least one of them must be up and running RFS; otherwise, you will not be able to start RFS on the Primary Name Server if you have stopped it for some reason.

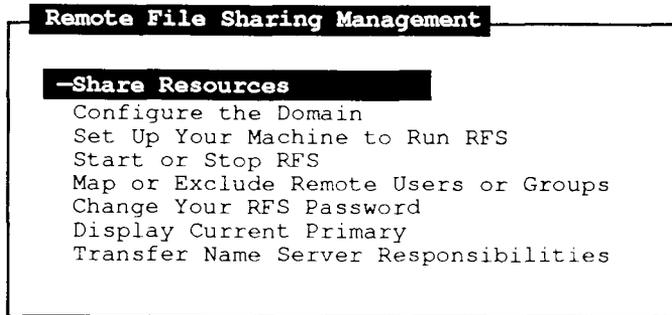
3. The machines that have been added to the domain by the Primary Name Server may now set themselves up to run RFS. In each case, enter the domain name and the name of the Primary Name Server. When prompted for an RFS password, specify the password that the Primary Name Server used when adding your machine.
4. Machines in the domain may now share resources with one another: that is, they can advertise resources on their own machine and they can mount other machines' resources.

5. The Primary Name Server continues to be configured for the domain by, for example, adding secondary name servers (see note above) and notifying the local Primary Name Server of the existence of primary name servers from different domains. The latter function is required if any machines in the current domain are to share resources with machines in different domains. The administrator of the Primary Name Server should tell the administrators of the machines in the current domain what other domains exist and can be contacted.

To view the RFS Management menu from the **adman** main menu:

1. Move the cursor to *Remote File Sharing (RFS) Administration*.
2. Press **Enter**.

The RFS Management menu, shown in Figure 11-1, is displayed:



Select a function and press 'Enter'.

471.36

Figure 11-1. RFS Management Menu

The subsections that follow describe how to use each of the functions displayed on the RFS Management menu. These subsections do not follow the order in which you see the functions on the RFS Management menu. Instead, the procedures explained here follow the path that an administrator would need to take to set up a newly installed system on an RFS network.

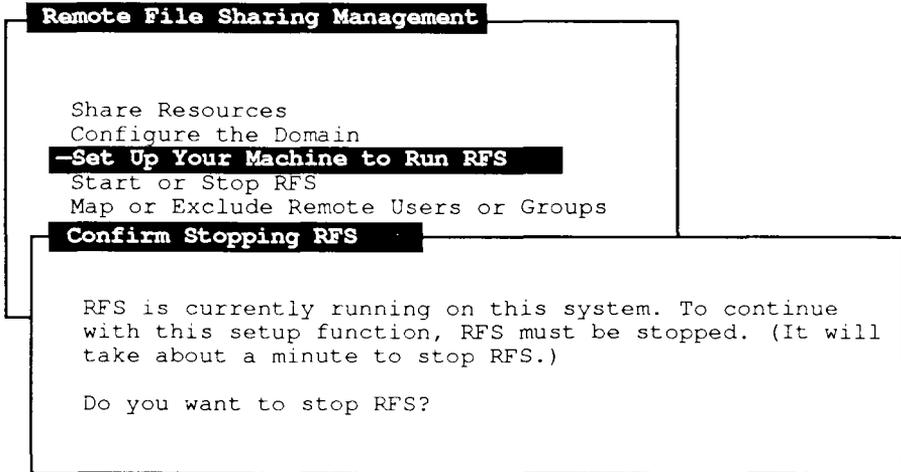
Creating a New Domain

This section explains the procedures for creating a new domain. If your machine is not the Primary Name Server and you plan to add your machine to a domain that already exists, skip to the next section, “Adding a System to an Existing Domain,” and follow the procedures provided.

To create a new domain, you must first decide two things: what to name the new domain and which machine will act as the domain’s Primary Name Server.

Procedure for Creating a New Domain

1. Log into the machine that you want to use for the Primary Name Server and run the **adman** program.
2. Move the cursor to *Remote File Sharing (RFS) Administration*.
3. Press **Enter**.
4. From the RFS Management menu, select *Set Up Your Machine to Run RFS*, and press **Enter**.
5. If RFS is currently running, a message is displayed informing you that RFS must be stopped to perform this procedure, similar to Figure 11-2.



Press 'Enter' to confirm, 'Cancel' to deny.

471.37

Figure 11-2. Set Up Your Machine to Run RFS

If you do not see this message, skip to Step 6 and continue with the procedure. Otherwise, press **Enter** to stop RFS. When the system displays a message stating that RFS has been stopped, press **Exit**.

6. If this is the *first* time you've set up your machine after installing the software, you may be asked if it's okay to use TCP/IP as the transport provider (network). Press **Enter** to confirm. Otherwise, you are prompted to enter the name of a different transport provider.

7. You are now prompted for the name of your new RFS domain and the name of the Primary Name Server for the new domain. The Domain and Primary Name Server Information window is displayed. (This occurs after the initial setup; once you've completed the initial setup, even if you change the setup or reboot your system, this will not appear.)

Note: If this system has never been part of an RFS domain, no defaults are displayed in the window.

8. **Backspace** over the current domain name (if any), type the name you have chosen for your domain, and press **Tab**.
9. In the Primary Name Server field, **Backspace** over the current name (if any) and type the name of your own machine. Press **Enter**. The Confirm Domain and Primary Server Information window is displayed to verify your selections.
10. If the selections displayed are correct, press **Enter**.
11. Next, the system displays a notice informing you that you will be asked to supply a password to add this system to the domain. Press **Enter** to continue.

12. You are prompted to enter a password for the primary name server of this RFS domain. (in this case, your own machine is the primary name server). This password is used for validation when RFS is started.

Note: Each system in a domain must have a password. Here, the Primary Name Server (this system) is being added to the new domain. The Primary Name Server is, itself, a member of the domain and must have its own password.

13. Type a password that you can easily remember: you will be asked to supply it the first time you start RFS. (You will not see the characters that you type on the screen.) Press **Return**.
14. You are prompted to retype your password for confirmation. Retype your password and press **Return**. Press any key to continue.

15. After entering a password for your system, you are asked whether you want to start RFS now and leave the reboot procedure as it is, or start RFS every time the system is rebooted. If your selection causes RFS to start only for the current session, the next time that your system reboots, RFS will not be automatically started. See “Starting and Stopping RFS,” later in this chapter, for more information about changing the rebooting procedure.

Make your selection and press **Enter**. (The system takes a minute to start NFS.)

16. If you see a message stating that the host password does not match the system’s, ignore it as you will be changing the password in the next step. Simply press **Cancel** for now.
17. A password notice is displayed again. Press **Enter**.
18. The next screen prompts you, again, for password information.

*Note: RFS requires that the password be stored in two places: in a file that only the Primary has, and also in a file on the local machine. Since your system is the Primary, **adman** must arrange for both files to be updated.*

19. Since this system is the Primary Name Server, you will be entering the same password that you entered in the previous steps.
Type the same password that you specified previously for the ‘old password,’ and press **Return**.
20. Type a new password and press **Return**.
21. Retype the new password for confirmation, and press **Return**. Press any key to continue.

22. When RFS is started, the system displays a message informing you that RFS has been set up on your machine. (You will see that RFS was started with warnings. You may ignore the warning about the passwords as you have just corrected the situation.) Press **Exit** to return to the RFS Management menu.

At this point, you have completed the setup procedure for creating a new domain.

Adding a System to an Existing Domain

The initial portion of the procedure for adding your system to an existing domain registers your machine name on the Primary Name Server of the domain. This part of the operation must be performed by the system administrator for the Primary Name Server of the domain to which you want to add the system.

The following two subsections describe all of the steps necessary to add your system to an existing domain. The first subsection provides the procedures that the system administrator of the Primary Name Server for the domain must perform to register your system name on the Primary Name Server. The second subsection describes the procedures that you, as system administrator for your machine, must perform to complete the operation.

Registering a System on the Primary: Primary Administrator Procedures

This portion of the procedure for adding a system to an existing domain is performed on the Primary Name Server of that domain. This subsection is addressed to the administrator of the Primary Name Server.

To add a system to an existing domain, you, as the administrator of the Primary Name Server for that domain, must register the machine name for the system being added on your machine (the Primary). To do this you must:

1. Log in as root on the Primary Name Server for the domain to which you want to add the new system.
2. Run the **adman** command, select *Remote File Sharing (RFS) Administration* from the **adman** main menu, and press **Enter**.
3. From the RFS Management menu, select *Configure the Domain* and press **Enter**. (This option is *only* available on the Primary Name Server.) The Configure the Domain Menu, similar to Figure 11-3, is displayed.

```
Remote File Sharing Management
Domain Configuration for Domain 'rfs1'

-List All Systems in Current Domain
Add an Entry for a Primary from a Different Domain
Administer Secondary Name Servers in Current Domain
Add a System to the Domain
Delete A System from the Domain
Delete All Systems in the Domain
```

Select a function and press 'Enter'.

471.38

Figure 11-3. Configure the Domain

From this menu, you can perform additional domain configuration tasks that are not addressed in this section. Refer to the section “Additional Domain Configuration Functions,” later in this chapter for the procedures for using each of these functions.

4. Select *Add a System to the Domain* and press **Enter**. A list of systems that can be added to the domain is displayed.

Note: You will be prompted to assign an RFS password to the machine you are adding. You must communicate the password to the administrator of the new system: it will be necessary for him or her to supply it when setting up that system.

5. Select your system from this list, and press **Enter**.
6. Next, you are prompted to enter a password for the machine you're adding to the RFS network. This password is used for validation of that system when RFS is started.

Type a password for the new machine. Then press **Return**. The characters will not be displayed on the screen.

Again, it is important that the system administrator for the system being added to the domain be informed of this password. He or she will need to provide it when setting up that system.

7. Retype the password for confirmation, and press **Return** again. Then press any key to continue.

The selected system has now been added to the list of systems in the current domain.

The procedures for registering your system's name on the Primary Name Server are now complete. However, that system will not be added to the domain until its system administrator performs the procedures in the following subsection.

Completing the Addition: Non-Primary Administrator Procedures

This portion of the procedure for adding a system to an existing domain is performed on the system being added to the domain. This subsection is addressed to the administrator of the machine that is being added to the domain. After the system administrator for the Primary Name Server completes the steps provided in the previous subsection, you can add your system to that domain.

1. From the system that is being added, run the **adman** program and select *Remote File Sharing (RFS) Administration* from the **adman** main menu.
2. From the RFS Management menu, select *Set Up Your Machine to Run RFS* and press **Enter**.

If RFS is currently running, a message is displayed informing you that RFS must be stopped to perform this procedure. If you do not see this message, skip to Step 4 and continue with the procedure. Otherwise, press **Enter** to stop RFS. When the system displays a message stating that RFS has been stopped, press **Exit**.

3. If this is the *first* time you've set up your machine after installing the software, you may be asked if it's okay to use TCP/IP as the transport provider (network). Press **Enter** to confirm. Otherwise, you will be prompted to enter the name of a different transport provider. (This will only occur after the initial setup; once you've set up once, even if you change it or reboot your system, this will not appear).
4. You are now prompted for the name of your new RFS domain and the name of the Primary Name Server for the new domain. The Domain and Primary Name Server Information window is displayed.
5. **Backspace** over the current domain name (if any), type the name of the domain to which you are adding your system, and press **Tab**.
6. If necessary, **Backspace** over the current Primary Name Server name and type the name of the Primary Name Server of the domain to which you are adding your system. Press **Enter**.

The Confirm Domain and Primary Server Information window is displayed to verify your selections.

7. If the selections displayed are correct, press **Enter**.

8. You are asked whether you want to start RFS now and leave the reboot procedure unchanged, or start RFS every time the system is rebooted. If your selection causes RFS to start only for the current session, the next time that your system reboots, RFS will not be automatically started. See “Starting and Stopping RFS,” later in this chapter, for more information on changing the reboot procedure.

Make your selection and press **Enter**.

9. Next, the system displays a notice informing you that you will be asked to supply a password to add this system to the domain. Press **Enter** to continue.
10. You are prompted to enter the old password for the your system.

Type the password that the system administrator of the Primary Name Server assigned to your system. You will not see the characters that you type on the screen. Then press **Return**.

Note: Each system in a domain must have a password. You must enter the password that was assigned to your system by the administrator of the Primary Name Server.

11. You are prompted for a new password. Type a new one and press **Return**.
12. You are prompted to retype your password for confirmation.
Retype your password and press **Return**. Then press any key to continue.
13. When RFS is started, the system displays a message informing you that RFS has been set up on your system. Press **Exit** to return to the RFS Management menu.

You have completed adding your system to an existing domain.

Additional Domain Configuration Functions

Note: The functions presented in this section are available on the Primary Name Server only. For this reason, this section is addressed to Primary Name Server administrators.

In the previous section, the Add a System to the Domain function from the Domain Configuration menu (Figure 11-4) was used to add a system to your domain. There are five additional functions available on the Domain Configuration menu. These functions allow you, as administrator of the Primary, to perform the following administrative tasks:

- view a list of the systems that are currently in the domain
- add entries for Primary Name Servers from different domains
- list, add, or delete systems designated as secondary name servers in your domain
- delete a specific system from your domain
- delete all of the systems from your domain

When you use any of the functions from the Domain Configuration menu, you must be logged into the Primary Name Server for the domain.

The subsections that follow describe the procedures for using each of these functions. Refer to the “Adding Your System to an Existing Domain” section of this chapter for the procedures for adding a specific system to an existing domain.

Listing Systems Currently in Your Domain

To view a list of systems that are currently in your domain:

1. From the RFS Management menu, select *Configure the Domain*.
2. Press **Enter**. The Domain Configuration menu is displayed.
3. Select *List All Systems in Current Domain*.
4. Press **Enter**.

Adding an Entry for a Primary from a Different Domain

This function allows you to add entries to your domain configuration for Primary Name Servers in other domains. This does not give these servers authority for your domain. It simply advises your Primary Name Server of the existence and the address of the other domains for the purpose of sharing resources with the members of those domains.

You don't necessarily need to have entries for every domain any member of your domain wishes to reach. RFS has a concept of *neighboring domains*: if, for example, a member of your domain wants a list of advertised resources in a domain that you haven't added, your Primary Name Server queries the other primaries it can reach directly (through entries you've added) to see if it can get a referral to the target domain. This type of search requires that you have at least one entry for a primary from a different domain.

To add an entry for a Primary Name Server from a different domain:

1. From the Domain Configuration menu, move the cursor to *Add an Entry for a Primary from a different Domain* and press **Enter**.
2. If RFS is currently running, the system displays a message asking if you are sure you want to stop RFS.

If you see this message, press **Enter** to stop RFS. Then press **Exit** to continue.

Chapter 11

3. A screen is displayed prompting you to enter the domain name and the Primary Name Server for that domain.
4. Enter the domain name where the Primary Name Server you want to add resides and press **Tab**.
5. Enter the name of the Primary Name Server you are adding and press **Enter**.
6. You are asked whether you want to start RFS now and leave the reboot procedure as it is, or start RFS every time the system is rebooted. If your selection causes RFS to start only for the current session, the next time that your system reboots, RFS will not be automatically started. See “Starting and Stopping RFS,” later in this chapter, for more information on changing the reboot procedure.

Make your selection and press **Enter**.

7. Next, the system displays a notice informing you that you will be asked to supply a password to add this system to the domain. Press **Enter** to continue.
8. You are prompted to enter the old password for the your system.

Type the password that the system administrator of the Primary Name Server assigned to your system. You will not see the characters that you type on the screen. Then press **Return**.

Note: Each system in a domain must have a password. You must enter the password that was assigned to your system by the administrator of the Primary Name Server.

9. You are prompted for a new password. Type a new one and press **Return**.
10. You are prompted to retype your password for confirmation.
Retype your password and press **Return**. Then press any key to continue.
11. When RFS is started, the system displays a message informing you that RFS has been set up on your system. Press **Exit** to return to the RFS Management menu.

The system displays a confirmation message stating that the specified entry has been added.

Managing Secondary Name Servers

This function allows you to list, add, or delete secondary name servers in your domain. If the Primary Name Server for your domain goes down, one of the secondary name servers, if any are designated, will automatically take over.

*Note: The **adman** program does not allow you to specify the ordering of eligibility of secondary name servers. They are, however, eligible in the order that you add them.*

To manage secondary name servers:

1. From the Domain Configuration menu, move the cursor to *Administer Secondary Name Servers in Current Domain* and press **Enter**.

The system displays a message asking if you are sure you want to stop RFS.

2. Press **Enter** to stop RFS. Then press **Exit** to continue.

The Administer Secondary Name Servers Menu is displayed. The subsections that follow describe the use of each of the functions on this menu.

Listing Secondary Name Servers

Selecting the first option on the Administer Secondary Name Servers menu displays a sorted list of secondary servers you've added to the domain.

*Note: It is important that this list does not contain machines that cannot take over for the Primary Name Server: for example, a machine that is no longer in your domain. The **adman** program checks to see if the machine is in your domain when you first add it as a secondary name server, but does not check after that. You should check this list occasionally to make sure that each of the listed entries is valid.*

To display a list of secondary name servers:

1. From the **Administer Secondary Name Servers** menu, move the cursor to *List Secondary Servers*.
2. Press **Enter**. A list of the secondary name servers for your domain is displayed.

Adding Secondary Name Servers

The second option on the **Administer Secondary Name Servers** menu allows you to designate machines in your domain as secondary name servers.

Before you add a secondary name server to your domain, check with the administrator of the machine to make sure that the machine is up and running RFS.

To add a secondary name server to your domain:

1. From the **Administer Secondary Name Servers** menu, move the cursor to *Add a New Secondary Entry*.
2. Press **Enter**. A list of possible machines is displayed. This list consists of machines you've added to the domain but have not yet designated as secondary name servers.
3. Select the machine you want to add as a secondary and press **Enter**.

The system displays a message stating that the machine has been added as a secondary name server.

The system displays a message stating that the machine has been added as a secondary name server.

Removing Secondary Name Servers

The final option on the Administer Secondary Name Servers menu allows you to remove secondary name server responsibilities from machines in your domain that you have previously designated as secondary name servers. You should use this function to remove any machines that become ineligible to take over Primary Name Server responsibilities.

To remove secondary name server responsibilities from a machine in your domain:

1. From the Administer Secondary Name Servers menu, move the cursor to *Delete an Existing Secondary Entry*.
2. Press **Enter**. A list of machines that are currently designated as secondary name servers for your domain is displayed.
3. Select the machine from which you want to remove secondary name server responsibility and press **Enter**.
4. After you specify all your changes and exit the Administer Secondary Name Servers in the Current Domain menu, the system displays a message stating that the selected machine has been removed from the list of secondary name servers.
5. You are asked whether you want to start RFS now and leave the reboot procedure as it is, or start RFS every time the system is rebooted. If your selection causes RFS to start only for the current session, the next time that your system reboots, RFS will not be automatically started. See “Starting and Stopping RFS,” later in this chapter, for more information on changing the reboot procedure.

Make your selection and press **Enter**.

6. Next, the system displays a notice informing you that you will be asked to supply a password to add this system to the domain. Press **Enter** to continue.

7. You are prompted to enter the old password for the your system.
Type the password that the system administrator of the Primary Name Server assigned to your system. You will not see the characters that you type on the screen. Then press **Return**.
Note: Each system in a domain must have a password. You must enter the password that was assigned to your system by the administrator of the Primary Name Server.
8. You are prompted for a new password. Type a new one and press **Return**.
9. You are prompted to retype your password for confirmation.
Retype your password and press **Return**. Then press any key to continue.
10. When RFS is started, the system displays a message informing you that RFS has been set up on your system. Press **Exit** to return to the RFS Management menu.

Deleting a Specific System from Your Domain

Delete a System from the Domain on the Domain Configuration menu allows you to select a current member of your domain and delete it from the list of current members. When you delete a system from your domain, that system will not be able to share resources with other systems until it is again added to your domain, or it is added to a different domain.

*Note: This function can be useful if a system password is forgotten: delete the system from the domain, add it again, and inform the administrator of the system of the new password. The administrator can then run the **rpasswd** program on his or her system to synchronize the passwords on the Primary Name Server and the local system.*

To delete a system from your domain:

1. From the Domain Configuration menu, move the cursor to *Delete a System from the Domain*.

2. Press **Enter**. A list of all of the systems currently in your domain is displayed.
3. Select the system you want to delete and press **Enter**.

The system displays a message stating that the selected system has been deleted from the domain.

Deleting All Systems from Your Domain

The final option on the Domain Configuration menu allows you to completely remove the domain by deleting all systems in it (including your own system). This function is useful when you want to reconfigure the domain from scratch, or abandon it entirely.

To delete all of the systems currently in your domain:

1. From the Domain Configuration menu, select *Delete All Systems in the Domain* and press **Enter**.

The system displays a message asking if you're sure you want to delete all systems from your domain.

2. Press **Enter** to confirm the operation.

The system displays a message stating that all systems have been deleted.

Starting and Stopping RFS

As an administrator, you may have occasion to start or stop RFS on your system. You might stop RFS for security reasons, for example, and then need to restart it. The Start or Stop RFS function allows you to stop RFS if it is running, and start RFS if it is stopped. You are asked if you want the change to affect the reboot procedure: if you are starting RFS now and want to start it every time the system reboots, then specify the change; if you are stopping RFS only temporarily, then do not change the reboot procedure; and so forth.

If your machine is the Primary Name Server, stopping RFS transfers name service responsibility to a secondary name server (if one is designated for this domain). If no secondary name server is designated, other machines in the domain will be unable to share resources.

Stopping RFS on any machine forcibly unmounts all remotely mounted resources and removes all previously advertised local resources from the advertised list.

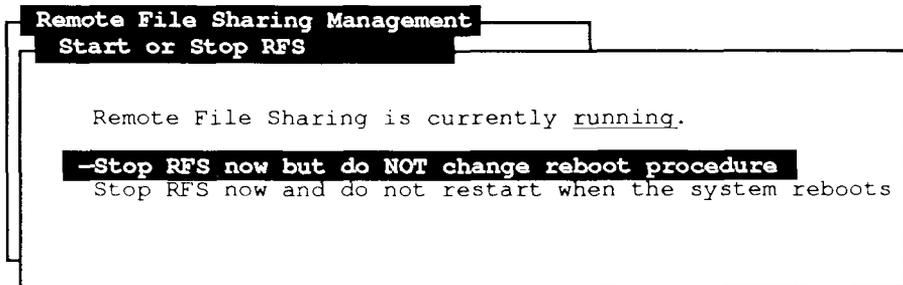
Starting RFS on any machine advertises all resources you have put on the advertised list and mounts remote resources you have specified for automatic mount.

There are many reasons RFS could fail to start. Most common, however, are difficulties relating to the Primary Name Server. Check to see whether the Primary Name Server is down and that no designated secondaries are up. If there is no acting Primary Name Server, your machine (if it is not a primary or a secondary) won't be able to start RFS. If all of the designated secondary name servers are down, the Primary Name Server won't be able to start RFS.

*Note: When you start RFS, the system changes to state 3. Previous versions of **adman** enabled terminals in state 2 only; therefore, you may need to remove terminals and add them again.*

Procedure for Starting and Stopping RFS

1. From the RFS Management menu, select *Start or Stop RFS*. The Start or Stop RFS Menu, similar to Figure 11-4, is displayed.



Select a function and press 'Enter', or press 'Cancel' to exit.

471.39

Figure 11-4. Start or Stop RFS

2. Press Enter.
3. If RFS *is not* currently running, a window allowing you to start RFS is displayed.
4. Select the first option to start RFS now and leave the reboot procedure unchanged. Select the second option if you want RFS to be started every time your system is booted.

When you start RFS, the system displays a message stating that RFS has started. Press any key to continue.

5. If RFS *is* currently running, a window allowing you to stop RFS is displayed.

To stop RFS, select the first option to stop RFS and have it start automatically the next time you boot the system. Select the second option to stop RFS and *not* have it start automatically the next time you boot the system.

6. When you stop RFS, the system displays a message asking if you're sure you want to stop it. Press **Enter** to confirm. Then, when you see a message stating that RFS has been stopped, press **Exit** to continue.
7. In either case, you are returned to the RFS Management menu.

Sharing Resources

Once RFS is running on the Primary Name Server, and one or more systems have been added to the domain, you can use RFS to share resources between the systems in the domain.

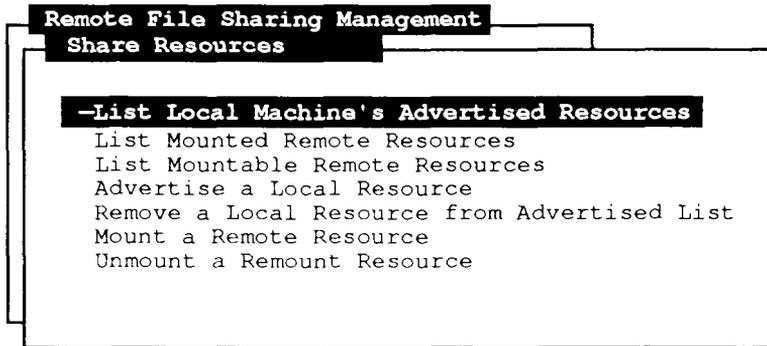
Note: To share resources with other machines, RFS must be running on your system.

In order to share a resource, you need to be able to view the list of what is currently advertised in your domain, as well as advertise the resources on your system that you want to share.

To perform resource sharing functions:

1. From the RFS Management menu, select *Share Resources*.
2. Press **Enter**.

The Share Resources Menu, similar to Figure 11-5, is displayed.



Select a function and press 'Enter'.

471.40

Figure 11-5. Share Resources

From this menu, you can perform any of the following functions:

- display a list of advertised resources
- display a list of currently mounted resources
- display a list of mountable remote resources
- advertise (or *unadvertise*) the resources on your system that you want to share
- mount (or *unmount*) remote resources

The following subsections describe each of the functions available at the Share Resources menu.

Viewing Advertised Resources

To view a list of the currently advertised resources in your domain, perform the following steps:

1. From the Share Resources menu, select *List Local Machine's Advertised Resources*. Press **Enter**.

The List of Advertised Resources window is displayed. This list shows the name of the resource, the directory in which the resource resides, and whether the resource has read only or read/write access permission assigned. To view a description and a list of systems that can use a particular resource select the resource and press **Enter**.

Viewing Mounted Remote Resources

To view a list of the currently mounted remote resources, perform the following steps:

1. From the Share Resources menu, select *List Mounted Remote Resources*. Press **Enter**.

The List of Mounted Remote Resources window is displayed. This window shows a list of the currently mounted resources, as well as the machines using each resource.

Viewing the Remote Resources You Can Use

To view a list of a particular domain's remote resources that are available to your system, perform the following steps:

1. From the Share Resources menu, select *List Mountable Remote Resources* and press **Enter**.
2. A screen is displayed prompting you to select the domain from which to compile the list of resources.

If you do not want to display the mountable resources in the current domain, **Backspace** over the current domain name and type the name of the domain whose mountable resources you want to view.

3. Press **Enter**.

The List of Mountable Remote Resources window is displayed. This window displays a list of resources in the selected domain that are currently available to be mounted. It includes the access permissions, the server name for each resource and a description of the resource.

Advertising Your Resources

To let other systems on an RFS network know what resources are available on your machine, perform the following steps:

1. From the Share Resources menu, select *Advertise a Local Resource*.
2. Press **Enter**.

The Advertise a Local Resource window is displayed. Use **Tab** to move between fields. When you have finished making selections, press **Enter**.

3. Type the full pathname of the file or directory that you want to share with other systems on the network and press **Tab**.
4. Enter a name for the resource you want to advertise and press **Tab**.

This is a symbolic name for the resource. By convention, the resource name is in capital letters, but this is not required.

5. Enter a brief description for the resource you want to advertise and press **Tab**.

Filling in this field is optional. The description you enter here is displayed when a list of advertised resources is shown.

6. Enter a space-separated list of client machines that have permission to mount the resource and press **Tab**.

This is another optional field. If this field is left blank, access to your advertised resource will be unrestricted. If you enter anything in this field, access to your advertised resource is limited to the machines/domains that you specify.

In this field, clients are specified as follows:

- If the client is a member of your domain, simply specify the client's machine name.
 - If the client is not a member of your domain, specify: *domainname.nodename*, where *domainname* is the name of the client's domain and *nodename* is the client's machine name.
 - To allow all members of a particular domain to use the advertised resource, simply enter the name of that domain.
7. In the next field, select either read/write access or read-only access for your advertised resource and press **Tab**.
 8. In the final field of this screen, select whether the resource will be automatically advertised when you bring up RFS or reboot your machine.
 9. When you have finished editing this screen, press **Enter**.
The system displays a message asking you to confirm the selections that you made.
 10. Press **Enter** to confirm your selections and advertise the resource, or press **Cancel** to return to the Advertise a Local Resource screen and modify your choices. If you confirm, the system displays a message stating that the resource has been advertised.
 11. Press **Exit** to return to the Share Resources menu. You have completed the procedure for advertising a local resource.

Removing an Advertised Resource

To stop advertising a resource that you are currently advertising, perform the following steps:

1. From the Share Resources menu, select *Remove a Local Resource from Advertised List* and press **Enter**.

A list of resources that you currently have advertised is displayed.

2. Select the resource you want to stop advertising and press **Tab**.
3. In the next field, select whether you want the resource to be removed from the list of resources that are automatically advertised each time you bring up RFS or reboot your system. Then press **Enter**.

The system displays a message asking if you are sure you want to remove the resource.

4. Press **Enter** to confirm the removal.

The system displays a message stating that the resource has been removed from the advertised list.

5. Press **Exit** to return to the Share Resources menu.

When you remove a local resource that is currently being used by remote users, the **adman** program asks you whether you want to forcibly unmount the resource on those machines.

The selected resource is no longer advertised on the network.

Mounting Remote Resources

To use a resource that another machine is currently advertising, perform the following steps:

1. From the Share Resources menu, select *Mount a Remote Resource* and press **Enter**. A screen is displayed prompting you for the domain name where the resource that you want to mount resides.
2. If the domain where the resource resides is different from the default (your current domain), **Backspace** over the default and enter the appropriate domain name. Then press **Enter**. The Mount Remote Resource window is displayed.
3. Select the resource that you want to use and press **Tab**.
4. Enter the full path name of a local directory where you want to mount the resource. If the specified directory does not currently exist, **adman** will create it for you, as long as the parent directory exists. Press **Tab**.
5. Next, you are asked if you want your system's users to write to the specified directory. Select Read/Write or Read-only, as applicable. Press **Tab**.
6. Select *Mount Now and EVERY TIME system reboots* or *Mount Now but do not change reboot procedure*. Press **Enter**.
7. A confirmation window showing your selections is displayed. If the displayed information is correct, press **Enter**.
8. A final window, stating that the resource has been mounted, is displayed. Press **Exit** to continue.

You have completed mounting a remote resource.

Unmounting Remote Resources

To stop using a remote resource, perform the following steps:

1. From the Share Resources menu, select *Unmount a Remote Resource* and press **Enter**.

The Unmount a Remote Resource window is displayed.

2. Select the resource that you want to stop using and press **Enter**.
3. Select *Unmount Now and Do Not Remount* or *Unmount Now and Remount*.

A message stating that the resource has been unmounted is displayed.

4. Press **Exit** to continue.

You have completed the procedure for unmounting a resource.

Mapping or Excluding Users and Groups

RFS has two levels of access checking. When you advertise a resource, you can specify a list of systems that are allowed to mount that resource. You can also specify whether the resource is available for read-only or read/write mounts.

The second level of access checking involves user IDs (uid) and group IDs (gid). The **adman** program arranges permissions on remotely mounted resources in such a way that users on the remote machine who have the same numerical user ID numbers as users on the local machine (the machine that advertises the resource) have the same user privileges. Correspondingly, the same group ID numbers confer group privileges. For example, if user A has a user ID 202 on Machine A, he or she has read/write permissions on files owned by the user whose ID is 202 on Machine B if those files are remotely mounted on Machine A.

Sometimes it isn't feasible to make all of the user and group IDs consistent between machines. To handle this, RFS has the ability to map user or group IDs according to the system they are coming from.

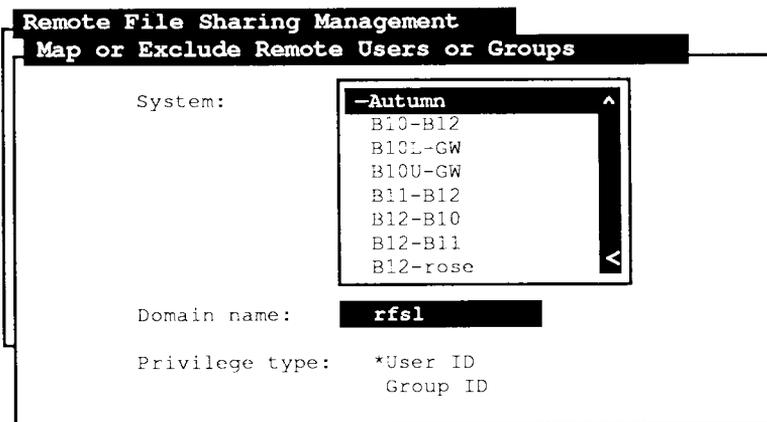
It is possible, using the **adman** program, to map user IDs between a user on a remote system and a user on your local system, as long as their user names are the same.

Note: The remote system must have RFS **adman** installed, and must be able to run the **rshd** daemon.

For information on more complex forms of user and group ID mapping, refer to the *S/Series CTIX Administrator's Guide*.

Procedure for Mapping or Excluding Users and Groups

1. From the RFS Management menu, select *Map or Exclude Users or Groups IDs* and press **Enter**. The Map or Exclude Remote Users or Groups Menu, similar to Figure 11-6, is displayed.



Select a host to which mapping or exclusion will apply.

471.41

Figure 11-6. Map or Exclude Remote Users or Groups

2. Move the cursor to the system you want to map or exclude and press **Tab**.
3. In the next field, **Backspace** over the default (your current domain) and enter the domain name for the system you want to map or exclude (if different from the default). Then press **Tab**.
4. In the last field, select whether you want to change user or group privileges.

Then press **Enter**.

The Map or Exclude Users or Groups window is displayed.

Note: In this window, use the **Tab** key to move between fields and use **^C** to display the full exclude or full map menus.

*The Exclude menu has all system users or groups preselected. To de-select an item, move the cursor to the item and use the **Mark** key (which toggles the selection on and off). Use the **Mark** key to select additional users or groups to exclude. Use **Exit** to return from the Exclude menu to the main form.*

*The Map menu has no preselected items. Use **^C**, **Mark**, and **Exit** as above.*

This window displays the current user or group ID rules for the selected system. You are also prompted for the following information:

- User or group names that you want to exclude. These users or groups will have “guest id” permissions for resources on your system. Refer to the *S/Series CTIX Administrator’s Guide* for information on “guest id” permissions.
- User or group names that you want to map. The reason for this mapping is that login names might be the same on two different systems (the same person has a login on both machines), but the associated IDs may not be the same. Use this mapping to make sure that users or groups have the same permissions for resources across different systems.

5. Enter the information in this window as appropriate.

Note: Be careful not to duplicate users or groups in the exclude and map lists. The **adman** program will report an error if this occurs.

For more detailed information on excluding or mapping users or groups, refer to the *S/Series CTIX Administrator's Guide*.

6. When you are satisfied with the information you have entered, press **Enter**.
7. The system tells you that the mapping was successful, or reports an error.
8. You are returned to the window in Step 2. You can (a) select Group ID, if you selected User ID previously, and continue with the same procedures on the host you originally selected, or (b) select a different host, or (c) press **Cancel** to exit this function.

Note: If you select the same type (User ID or Group ID) on the same host, you will overwrite the mapping that you just assigned.

Changing Your RFS Password

When you select *Change Your RFS Password* on the RFS Management menu, the Change Your RFS Password menu, similar to Figure 11-7, is displayed.

Remote File Sharing Management

Change/Synchronize RFS Password on Primary Server

This tool runs the 'rfspasswd' program for you. The program prompts you for your 'old password' and then your 'new password'. It synchronizes the new password on the primary server: passwords on your local machine and the primary server must match for remote mounts to succeed.

Enter your existing RFS password when prompted for the 'old password' and press RETURN. (If you are using the initial RFS setup tool, enter the RFS password supplied by the administrator on the primary when he or she added your machine to the domain.)

Press RETURN after responding to each prompt.

Press 'Enter' to invoke RFS password synchronization program.

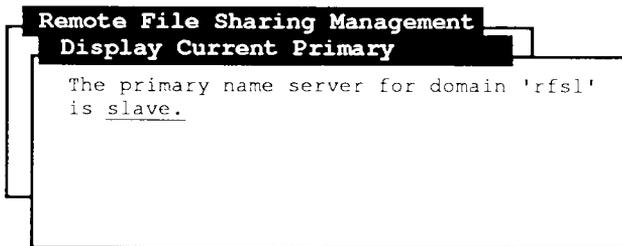
471.42

Figure 11-7. Change Your RFS Password

You are prompted for your 'old password' and then your 'new password.' This function synchronizes the new password on the Primary Name Server: passwords on your local machine and the Primary Name Server must match for remote mounts to be successful. When you are prompted for the 'old password,' enter your existing RFS password and press **Return**. Then enter and reenter your new password, pressing **Return** after responding to each prompt. If you have forgotten your old password, or if RFS keeps reporting that the old password doesn't match the password on the Primary Name Server, have the administrator of the Primary Name Server delete your system from the domain and add it again. The password that he or she assigns is the password you should enter for 'old' password.

Displaying the Current Primary Name Server

Selecting *Display Current Primary* from the RFS Management menu tells you which machine in your domain is the acting Primary Name Server. The Display the Current Primary Name Server Menu, similar to Figure 11-8, is displayed.



Press 'Cancel' to exit the form.

471.43

Figure 11-8. Display Current Primary Name Server

If the acting Primary Name Server is a secondary that has temporarily taken over Primary Name Server responsibility, the **adman** program tells you and also lists the originally configured Primary Name Server.

Transferring Name Server Responsibilities

Transfer Name Server Responsibilities on the RFS Management menu allows you to specify an acting Primary Name Server to pass Primary Name Server responsibilities to a different machine. You can execute this function only if your machine is currently the acting Primary Name Server.

If your machine is a secondary server that is currently acting as primary (for example, because the Primary Name Server is down or has taken RFS down), when you execute this function, responsibility is passed back to the original Primary Name Server (if it is up) or another secondary name server (if there is one).

RFS does not allow you to specify the machine to which name server responsibility will be transferred.

Note: If the original Primary Name Server goes down or takes RFS down, and if there is a configured secondary name server, name server responsibility is automatically passed to a secondary. When the Primary Name Server comes back up, the secondary that is acting as the Primary Name Server must use this function to explicitly transfer Primary Name Server responsibility for the original primary to take over.

Where to Go from Here

For more information on RFS files and commands, refer to the following items in the *S/Series CTIX Administrator's Guide* and the *CTIX Operating System Manual*:

`/etc/fuser`

This command identifies processes that are using the specified files or remote resources. This command is used to check what local users are currently accessing a remote resource.

`/etc/fumount`

This command unadvertises a resource and disconnects remote access to the resource. This command is used to force an unmount of one of your resources by all the systems that currently have the resource mounted.

Chapter 11

/etc/master

This file defines tunable parameter values, including Remote File Sharing tunable parameters.

/etc/init.d/rfs

This shell script starts up RFS, advertises resources, and mounts remote resources when you enter Remote File Sharing mode. (*S/Series CTIX Administrator's Guide* only.)

/etc/rmount

This shell script tries to mount a remote resource. If unsuccessful, it retries after waiting 60 seconds. It repeats forever.

/usr/bin/rfuadmin

This shell script defines the actions to be taken on your system when links to remote resources are dropped.

/usr/nserve/domain

This file contains your domain name. (*S/Series CTIX Administrator's Guide* only.)

/usr/nserve/rfmaster

This file contains the names and network addresses of the primary and secondary name servers for your domain.

/usr/nserve/loc.passwd

This file contains your system's RFS password.

/usr/nserve/auth.info/domain/passwd

This file resides on the Primary Name Server. It contains an RFS password for each system in the domain.

/usr/nserve/auth.info/uid.rules

This file contains the rules you set up for mapping remote users.

/usr/nserve/auth.info/gid.rules

This file contains the rules you set up for mapping remote groups.

adv

This command is used to make your advertised resources available to other users.

mount

This command is used to attach remote resources to your host.

nsquery

This command is used to list other systems' advertised resources.

rmntstat

This command is used to list your resources which other systems have mounted.

rumount

This command is used to cancel a queued remote resource mount request.

unadv

This command is used to “unadvertise”, to remove one of your currently advertised resources from the advertised list.

umount

This command is used to unmount a currently mounted resource.

Chapter 11

rmountall

This command is used to mount several remote file resources, using a file system table.

rmnttry

This command is used to attempt to mount remote resources.

rumountall

This command is used to unmount several remote file resources, using a file system table.

Chapter 12

Network File System Administration

Introduction

This chapter describes the procedures for using the **adman** program to manage the services provided by the Network File System (NFS) package for the CTIX operating system. For a discussion of the advantages and disadvantages of using RFS vs. the Network File System (NFS) see Appendix C.

Note: The Network File System (NFS) is an optional software package. You need to install it on your system to have access to the features described in this chapter.

You must have the TCP/IP package installed to use NFS.

The first section discusses the basic capabilities of the NFS. For detailed information on NFS, refer to the *S/Series CTIX Administrator's Guide*.

The balance of the chapter gives the information you need and provides the steps required to perform administration tasks on a system running NFS using the **adman** program.

Network File System Terms and Concepts

The Network File System allows computers to share files or directories selectively across a network. NFS not only allows file sharing between different types of machines, but, unlike Remote File Sharing (RFS), it allows the sharing of files between computers running different operating systems and file architectures. A system on a network can *export* the directory containing files it wants to share. Other systems on the same network can then *mount* these files or directories.

Once mounted, these remote files can be used in the same way that local files are used. Machines in an NFS environment communicate through a client/server model. A machine that provides resources to the network is a *server*, while a machine that employs these resources is a *client*. The server machine allows client machines on the network to access resources that reside on the server's local disk. A machine in an NFS network may act as both a server and a client.

Resources in an NFS environment must be *mounted* (attached directly or indirectly to the root file system) by the remote machine(s) that want to gain access to the resource. When you mount a resource using the **adman** program, you must specify an empty directory on your local server to serve as the *mount point*. If the directory you specify does not exist, the **adman** program creates the directory for you; however, the directory immediately above it must exist.

The server must *export* a local resource to make the resource available to selected remote clients. A client may then look at a list of exported resources, select one to mount, and mount that resource on an empty directory underneath its own root file system.

NFS offers several ways for the system administrator to control access to exported resources on the local machine:

- Only resources which you have exported can be shared, so access can be prevented by not exporting.
- Resources can be mounted as read-only, so that no remote or local system can write to the file or directory.
- When a resource is exported, a list of systems that are allowed to have access to that resource can be explicitly specified. The exported resource is not available to any system not on the list.

NFS does not distinguish between exported resources that are mounted for read-only or read/write on the local machine. You must export a resource without specifying permissions, since NFS does not currently provide a way to specify that a resource is available for read-only access.

Note: To prevent a remote machine's application from unsuccessfully writing to a read-only resource, it is the system administrator's responsibility to inform possible clients when a particular resource can be mounted for read-only.

Using the **adman** program, you can manage the functions that the Network File System provides. By following the steps in the "NFS Administration Procedures" section of this chapter, you can use the **adman** menus to set up NFS, start or stop NFS, mount or export resources, protect sensitive resources from unauthorized use, or view lists of resources exported by other systems.

NFS Administration Procedures

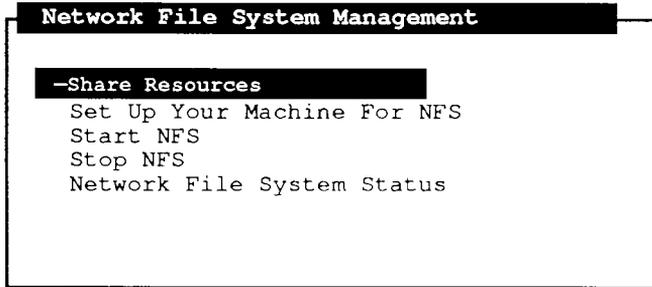
This section provides the procedures necessary for you to use the **adman** program to perform administrative functions on a system running the NFS. The **adman** program allows you to use the capabilities of NFS discussed in the previous section.

Before you can start NFS on your system, the NFS drivers must be loaded on your system. You can complete this task using the **adman** program. After this is completed and NFS is started, you can use **adman** to administer the functions of the Network File System. You can view resources exported by other systems, mount and use exported resources, or export resources on your system that you want to make available to other systems. As a system administrator, you can also stop NFS to perform tasks such as backup or restore. You can monitor the status of exported filesystems on your server and on accessible remote servers.

To view the NFS Management menu from the **adman** main menu:

1. Move the cursor to *Network File System (NFS) Administration*.
2. Press **Enter**.

The NFS Management menu, shown in Figure 12-1, is displayed:



Select a function and press 'Enter' or press 'Cancel' to exit.

471.44

Figure 12-1. NFS Management Menu

The subsections that follow describe how to use each of the functions displayed on the NFS Management menu. These subsections are presented in the order that an administrator would take to set up a newly installed system on an NFS network.

Setting up NFS on Your Server

Before you can export local resources or mount resources exported by remote machines, you need to use the Set Up Your Machine For NFS function to configure your local system. If your machine has been previously configured for NFS, or if you aren't sure, use the Network File System Status function to check the current state of NFS on your machine. Refer to the "Checking the Network File System Status" section for details.

The procedure for setting up NFS on your machine takes only a few simple steps.

1. From the NFS Management menu, select *Set Up Your Machine For NFS*, and press **Enter**.
2. The system displays a message stating that the NFS will be stopped to perform this operation. The nature of the message depends on the current state of the NFS.

If you currently have remote resources mounted on your machine, or if any of your server's exported resources are mounted by other machines, these mounts will be forcibly terminated when the NFS is stopped.

Press **Enter** to continue with the setup procedure.

3. After about a minute, the system displays a message stating that the NFS has been set up on your server.

After you have set up NFS on your machine, you will need to start the NFS running. Refer to the section on starting the NFS for instructions.

Starting the NFS

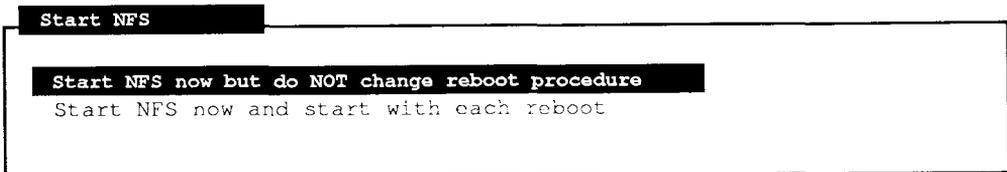
Whether you are starting NFS for the first time, or restarting NFS after performing system backups the process is the same. If you select this option and the NFS is already running, the function first stops NFS and unmounts all remotely mounted resources, then restarts the NFS.

1. From the NFS Management menu, select *Start NFS*.
2. The Start NFS Menu, similar to Figure 12-2, is displayed.
3. Select the first option to start NFS now and leave the reboot procedure as it is. Select the second option if you want NFS to be started every time your system is booted. Press **Enter**.
4. If NFS is already running, the system displays a message stating that the NFS will be stopped to perform this operation. The nature of the message depends on the current state of the NFS.

Note: If you currently have remote resources mounted on your machine, or if any of your server's exported resources are mounted by other machines, these mounts will be forcibly terminated when the NFS is stopped.

5. Press **Enter** to stop and restart NFS or **Cancel** to abort procedure.

When you start NFS, the system displays a message stating that NFS has started, and that it may take a few moments to complete all NFS mounts. Press any key to continue.



Select a function and press 'Enter', or press 'Cancel' to exit.

471 56

Figure 12-2. Start NFS

If you chose to start the NFS every time your system is booted, you can use the Stop NFS function to change the reboot procedure back to its original state. Refer to "Procedure for Stopping the NFS" below for further information.

Starting the NFS on your system exports all the resources you have previously placed on the exported list and mounts remote resources you have specified for automatic mount. This process takes a few minutes to complete.

Procedure for Stopping NFS

This function allows you as system administrator to stop the NFS if it is currently running. A nonprivileged user cannot use this function. Stopping the NFS on your system forcibly unmounts all remotely mounted resources. This can disrupt both local users, and users on remote machines mounted on local resources. As a system administrator, it is your responsibility to inform your local users and system administrators of remote machines using local resources before you stop NFS.

This menu is very similar in operation to the Starting the NFS menu.

1. From the NFS Management menu, select *Stop NFS*. The Stop NFS Menu, similar to Figure 12-3, is displayed.
2. A menu allowing you to stop NFS is displayed.
3. Select the first option to stop NFS now and leave the reboot procedure as it is. Select the second option if you want NFS to be stopped every time your system is booted.
4. When you stop NFS, the system displays a message asking if you're sure you want to stop it. Press **Enter** to confirm. Then, when you see a message stating that NFS has been stopped, press **Exit** to continue.
5. In either case, you are returned to the NFS Management menu.

```
Network File System Management
Stop NFS
-Stop NFS now but do NOT change reboot procedure
  Stop NFS now and do not restart when the system reboots

Select a function and press 'Enter', or press '^X' to exit.
```

471.46

Figure 12-3. Stop NFS

Checking the Network File System Status

As system administrator you will occasionally need to check the current status of the NFS on your server.

1. From the NFS Management menu, select *Network File System Status*. A status screen is displayed.
2. Press **Enter** to return to the NFS Management menu.

When you select the Network File System Status function, the system displays the current NFS status. Some possible messages are

- NFS is currently not set up. Its drivers are not loaded.
- NFS is currently set up. Its drivers are loaded, however, NFS is not currently running.

- This machine is currently running as an NFS client.
- This machine is currently running as an NFS server.

Sharing Resources

Once NFS is set up and running on your server, you can begin to share resources with other NFS servers and use exported remote resources on these machines.

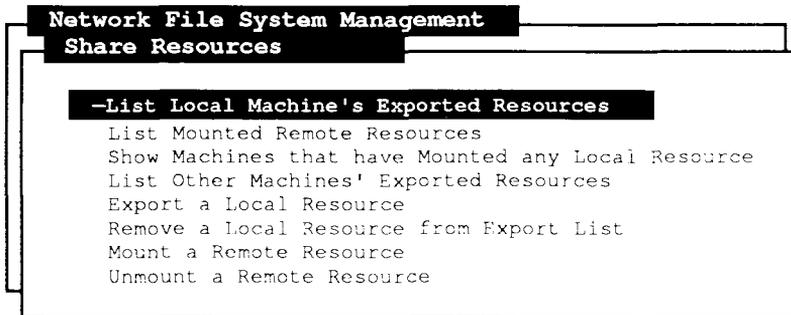
Note: To share resources with other machines, NFS must be running on your system.

In order to share a resource, you need to view the list of what is currently exported in your network, as well as export the resources on your system that you want to share.

To perform resource sharing functions:

1. From the NFS Management menu, select *Share Resources*.
2. Press **Enter**.

The Share Resources Menu, similar to Figure 12-4, is displayed.



Select a function and press 'Enter', or press 'Cancel' to exit.

471.45

Figure 12-4. Share Resources

From this menu, you can perform any of the following functions:

- display a list of exported resources
- display a list of currently mounted resources
- display a list of mountable remote resources
- export (or *unexport*) the resources on your system that you want to share
- mount (or *unmount*) remote resources

The following subsections describe each of the functions available at the Share Resources menu.

Viewing the Local Machine's Exported Resources

To view a list of the currently exported resources in your network from the Share Resources menu, select *List Local Machine's Exported Resources*. Press **Enter**.

The List of Exported Resources window is displayed. This list shows resources currently exported by your machine, and which machines have access to mount the resource. This is either a list of machines or "everyone."

Viewing Mounted Remote Resources

To view a list of the currently mounted remote resources from the Share Resources menu, select *List Mounted Remote Resources*. Press **Enter**.

The List of Mounted Remote Resources window is displayed. This window shows a list of the currently mounted resources, as well as the machines using each resource.

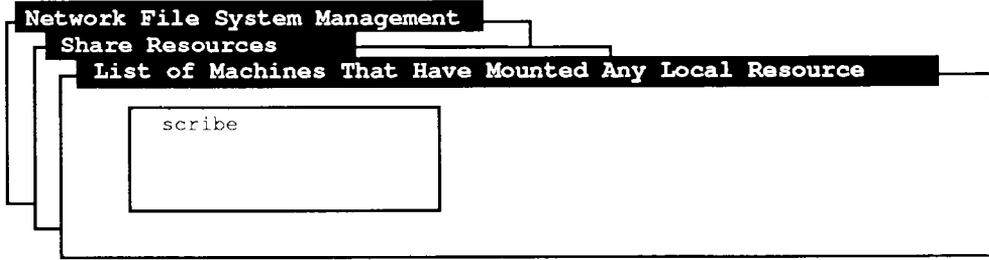
The first column contains the mount point of each resource. The second column contains the resource name preceded with the server that has exported the resource. The third column contains the access permissions. The permissions can be either read/write or read-only.

Viewing Remote Machines Mounted on Your Local Resources

To see a list of remote machines which are currently mounted on exported local resources:

From the Share Resources menu, select *Show Machines that have Mounted any Local Resource*. Press **Enter**.

The List of Mounted Machines that have Mounted any Local Resources screen is displayed. This window shows a list of the machines which are currently mounted on your local resources. See Figure 12-5 for a sample.



Press '^X' to exit the form.

471.49

Figure 12-5. Viewing Available Remote Resources

Viewing the Remote Resources You Can Use

To view a list of a particular server's remote resources that are available to your system, perform the following steps:

1. From the Share Resources menu, select *List Other Machines' Exported Resources* and press **Enter**.
2. A screen is displayed prompting you to enter the server name from which to compile the list of resources. Enter the name of the remote machine.
3. Press **Enter**.

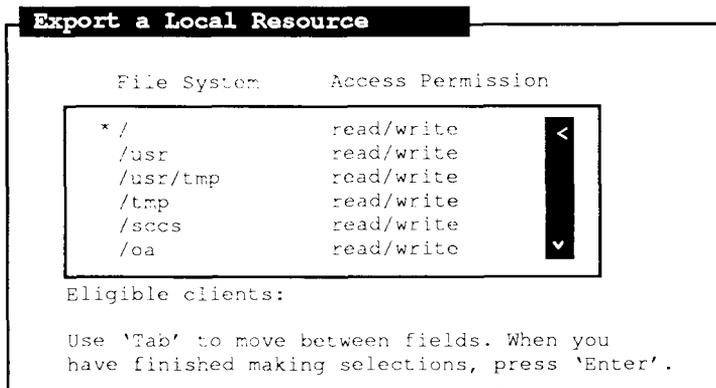
The List of Mountable Remote Resources of Server window is displayed. This window displays a list of resources on the selected server that are currently available to be mounted. It includes the file name for each resource and a list of the machines allowed access.

Exporting Your Local Resources

To let other systems on an NFS network know what resources are available on your machine, perform the following steps:

1. From the Share Resources menu, select *Export a Local Resource*.
2. Press **Enter**.

The Export a Local Resource window is displayed, similar to Figure 12-6 below.



Select a resource to be exported.

471.51

Figure 12-6. Export a Local Resource

3. Select a resource from the list of available resources. Press **Tab**.
4. Enter a space-separated list of client machines that have permission to mount the resource and press **Tab**.

This is an optional field. If you leave it blank, access to your exported resource will be unrestricted. If you enter anything in this field, access to your exported resource is limited to the machines/servers that you specify.

5. When you have finished editing this screen, press **Enter**.

The system displays a message asking you to confirm the selections that you made.

6. Press **Enter** to confirm your selections and export the resource, or press **Cancel** to return to the Export a Local Resource screen and modify your choices. If you confirm, the system displays a message stating that the resource has been exported.

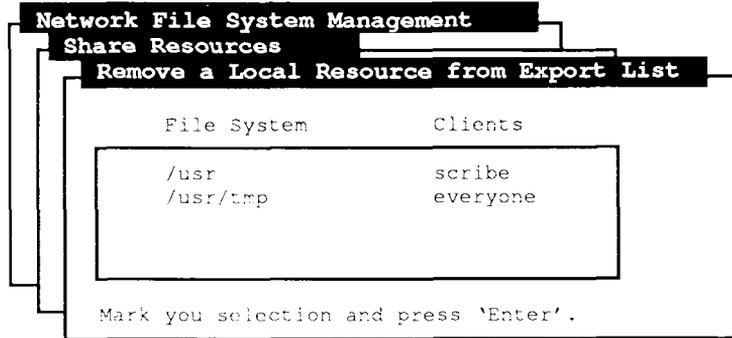
7. Press **Exit** to return to the Share Resources menu. You have completed the procedure for exporting a local resource.

Removing a Local Resource from the Export List

To stop exporting a currently exported resource, perform the following steps:

1. From the Share Resources menu, select *Remove a Local Resource from Exported List* and press **Enter**.

A list of resources that you currently have exported is displayed. The screen is similar to the one shown in Figure 12-7.



Press '^X' to exit the form.

471.47

Figure 12-7. Remove a Local Resource from Export List

2. Select the resource you want to stop exporting and press **Tab**. The system displays a message asking you if you are sure you want to remove the resource.
3. Press **Enter** to confirm the removal.

The system displays a message stating that the resource has been removed from the exported list.

4. Press **Exit** to return to the Share Resources menu.

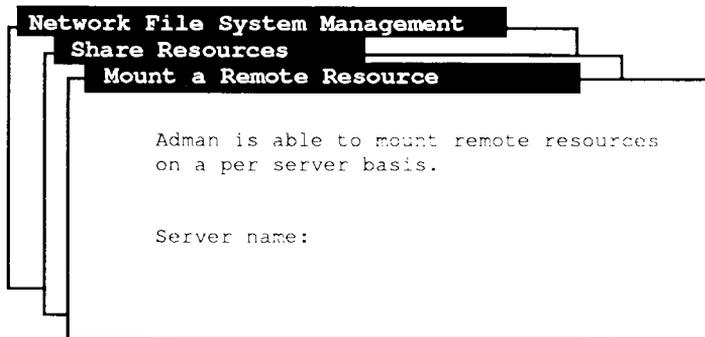
When you remove a local resource that is currently being used by remote users, the **adman** program asks you whether you want to forcibly unmount the resource on those machines.

The selected resource is no longer available to remote systems on the network.

Mounting Remote Resources

To use a resource that another machine is currently exporting, perform the following steps:

1. From the Share Resources menu, select *Mount a Remote Resource* and press **Enter**. A screen is displayed prompting you for the server name where the resource that you want to mount resides. See Figure 12-8.



Enter Server name and press 'Enter', or press 'Cancel' to exit the form.

471.48

Figure 12-8. Mount Remote Resources Server

Enter the server name, and press **Enter**.

2. The Mount a Remote Resource window is displayed.
 - Use **^C** to view available resources. Select the resource that you want to use and press **Tab**.
 - Enter the full pathname if you wish to mount only a subdirectory of the resource. **Tab** to the next field.

- Enter the full pathname of a local directory where you want to mount the resource. If the specified directory does not currently exist, **adman** will create it for you as long as the parent directory exists. Tab to the next field.
- Select *Read/write* to allow your local users to read and write to the resource, or select *Read-only* to prevent your local users from writing to the resource files. Tab to the next field.
- Select *Mount Now and EVERY TIME system reboots* or *Mount Now but do NOT change reboot procedure*. Tab to the next field.
- Select *Continually retry until mount succeeds*, or *Try to mount only once*.

Read the screen to check your selections. If all selections are correct, press **Enter**.

3. A confirmation window is displayed. Press **Enter** to continue, or **Cancel** to return to the previous screen.
4. A final window, stating that the resource has been mounted, is displayed. Press **Exit** to continue.

You have completed mounting a remote resource.

Unmounting Remote Resources

To stop using a remote resource, perform the following steps:

1. From the Share Resources menu, select *Unmount a Remote Resource* and press **Enter**.

The Unmount a Remote Resource window is displayed.

2. Select the resource that you want to stop using and press **Tab**.
3. Select *Unmount Now and Do Not Remount when system reboots* or *Unmount Now but do not change reboot procedure*.

4. Press **Enter**.
5. A confirmation screen is displayed. To confirm, press **Enter**.
A message stating that the resource has been unmounted is displayed.
6. Press **Exit** to continue.

You have completed the procedure for unmounting a resource.

Where to Go from Here

For more information on NFS files and commands, refer to the following items in the *S/Series CTIX Administrator's Guide* and the *CTIX Operating System Manual*:

/etc/exports

This file contains a list of file systems available for remote mounts.

/etc/group

This file contains a list of local groups.

/etc/hosts

This file contains a list of hosts on the network.

/etc/hosts.equiv

This file contains a list of remote hosts with matching-name equivalence.

/etc/fstab

This file contains associations between remote machine filesystems and the local mount points.

/etc/mountd

This daemon is an `rpc` server which answers the file system mount and exported file system information requests.

/etc/networks

This file contains a list of networks on your internetwork.

/etc.rhosts

This file contains a list of remote users.

mount

This command is used to allow you to mount a remote filesystem that has been exported by an NFS server.

showmount(1M)

This command is used to list all NFS clients that have remotely mounted a filesystem exported by the server.

umount

This command is used to unmount an exported filesystem.

—

—

—

Chapter 13

Troubleshooting

Introduction

This chapter deals with common problems and their solutions; it suggests ways to prevent problems before they occur, and describes what to do when all else fails.

Troubleshooting is nothing more than problem solving. *Troubleshooting* is the act of searching for the cause of a problem and correcting it. The following are the most important keys to effective troubleshooting:

- Try to relax. It is always easier to solve a problem when you are calm.
- Don't be afraid to ask for help. It is much better to enlist help when you need it than to leave problems unattended. You can receive help from other users as well as your service representative.
- Perform preventive maintenance.

Some common problems that may occur and solutions for solving them are described in this chapter. Table 13-1 describes common problems and refers you to the appropriate troubleshooting sections for possible solutions.

Chapter 13

Table 13-1. Troubleshooting

Symptom	For possible solutions see
User is unable to log in from any terminal	User administration Disk and File System Problems
User is unable to log in from an enabled terminal	Terminal Usage Problems Terminal Administration Problems
User is unable to run administration tools package on an enabled terminal	Terminal Administration Problems
User receives “no shell” message	User administration
User receives “no home directory” message	User administration
User is unable to access files	User administration RFS Administration Problems NFS Administration Problems
User can’t create a file in a directory	Disk and File System Problems
User can’t access some directories	Disk and File System Problems NFS Administration Problems RFS Administration Problems
Serious errors are present in the console log or the error report	System Status problems
The backup file list doesn’t include files you want to backup	Backup Problems
You accidentally interrupted backup	Backup Problems
You started the next sequence of backup without inserting a new tape	Backup Problems
You received the message “Backup failed”	Backup Problems

Table 13-1. Troubleshooting (cont.)

Symptom	For possible solutions see
You are unable to read the contents of a tape	Restore Problems SCSI Tape Problems
You started a restore by mistake	Restore Problems
You restored the wrong file	Restore Problems
You received the message "Restore failed"	Restore Problems
The scheduler status or default printer on the View Print System status is not what it should be.	Printer Administration Problems
The printer or queue status is not what it should be	Printer Administration Problems
The printer did not produce your request.	Printer Administration Problems
The printer prints, but the printout is garbled	Printer Administration Problems
The printer beeps, and a parity light goes on	Printer Administration Problems
You changed the status of a printer, but the change does not occur	Printer Administration Problems
You have run out of space on a disk	Disk and File System Problems
You are running out of swap space	Disk and File System Problems
You specified the wrong mount point	Disk and File System Problems NFS Administration Problems RFS Administration Problems
You specified the wrong partition in which to create a file system	Disk and File System Problems
You are unable to exchange mail with a system	UUCP

Table 13-1. Troubleshooting (cont.)

Symptom	For possible solutions see
You made a typing mistake	Terminal Usage Problems
You received your shell prompt unexpectedly, and nothing happens when you try to type something	Terminal Usage Problems
The function is taking an unusually long time to complete, or did not complete	NFS Administration Problems Terminal Usage Problems
The primary can not be brought up	RFS Administration Problems
You tried to mount a file system and got an error message	NFS Administration Problems RFS Administration Problems
You received an error message while using files	RFS Administration Problems NFS Administration Problems Disk and File System Problems
The tape drive did not implement your request	SCSI Tape Administration Problems Backup Problems Restore Problems

User Administration Problems

Problem: You have added a user, but he receives a “login incorrect” message and is unable to log in.

Solution: Verify his account using *List User Accounts*. If his account is present, give him a new password, using *Change a User’s Password*.

Problem: You have added a user, and he is able to log in, but he receives a “no shell” or “no home directory” message before he receives his prompt.

Solution: Use *Change User Information* or *List User Accounts* to make sure his account uses the correct shell and references the correct home directory.

Problem: You have added a group, but users are unable to access files even though they have the appropriate group privileges.

Solution: Read the section on the **chgrp** (1) command in the *CTIX Operating System Manual*.

Problem: You deleted a user accidentally.

Solution: If you did not remove his files, use *Add a User* to add him again, specifying a new home directory. Then copy the old files from his original home directory to the new home directory. To copy the files, specify the full pathname of the directory you are copying from and the full pathname of the new home directory. The format of the copy command is:

```
cp olddirectoryname/* newdirectoryname
```

If the old directory name was **/u/margie** and the new home directory name is **/u/johnson** then you would type **cp /u/margie/* /u/johnson** to copy the files.

If you removed his files, use *Add a User* to add him again, specifying his old home directory, then perform a restore to retrieve his files. (For instructions on performing a restore, see Chapter 4, “Backup and Restore.”)

Problem: You deleted a user’s account and removed his files without archiving them.

Solution: The user’s files should be on a permanent, complete backup. Restore them and then archive them.

Problem: You barred a user mistakenly.

Solution: Readmit the user by using *Readmit a User*.

- Problem: You readmitted a user, but he is unable to log in.
- Solution: Use *Change a User's Password* to give the user a new password.

System Status Problems

- Problem: Serious error messages are present in the console log; for example, a file system has run out of space.
- Solution: Determine when the message occurred and if it has already been attended to.
- Try to remedy the situation. For example, if it is a recent message informing you that a file system is out of space, determine what files are causing the file system to run out of space (using *List Largest Files*, described in Chapter 5). Tell their owner that (if possible) you need to remove them. If the files are log or spool files you can do without, remove them.
- Problem: There are more than just a few errors present in the error report.
- Solution: Call your service representative.

Backup Problems

- Problem: The backup file list does not include files that you want backed up.
- Solution: Press the **Interrupt** key (usually **Delete** on a PT or GT, **Shift-Backspace** on a TO-300) to halt the backup. Make sure the file system in question is mounted. (Use *Monitor Disk Usage*, described in Chapter 5, to see which file systems are mounted.)
- If you were doing a *Partial Backup* or a *User Backup*, make sure you are specifying the pathname or user correctly, then start the backup over.

If you were doing a *Complete Backup* or an *Incremental Backup*, and these files have been deliberately excluded in the past, use a text editor to remove the files from `/usr/lib/adman/compexcl.l`, then start the backup over.

Problem: You accidentally interrupted the backup.

Solution: Run **adman** again and start the backup over.

Problem: You started the next sequence of the backup without inserting the next tape (overwriting the tape with new information).

Solution: Press the **Interrupt** key (usually **Delete** on a PT or GT, **Shift-Backspace** on a TO-300) to halt the backup, run **adman** again, and start the backup over. The first backup is damaged, and you cannot restore any files from it.

Problem: You received the message: Backup Failed.

Solution: Remove the tape from the drive and make sure the write-protect arrow on the tape cartridge is pointing *away* from SAFE. If you still cannot write to the tape, retension it. From the shell, type

```
tsioctl -c retension /dev/rmt0
```

If you are still unable to write to the tape, exchange the tape for another. Try a few tapes from different boxes if necessary.

Next, try to read from the tape (using *View Tape Contents*).

Insert an old, successful backup tape and try to read from it. [Make sure the write-protect arrow on the tape cartridge is turned *toward* SAFE (see Figure 4-2), to ensure that you do not write over data currently on the tape.]

If you still cannot write to or read from any tape, call your service representative.

Restore Problems

Problem: You are unable to read the contents of a backup tape.

Solution: Refer to the solution for the “Backup Failed” message; however, make sure the write-protect arrow on the tape cartridge is turned *toward* SAFE (see Figure 4-2), so that you cannot write over data currently on the tape.

Problem: You started a restore by mistake.

Solution: Press the **Interrupt** key (usually **Delete** on a PT or GT, **Shift-Backspace** on a TO-300) to halt the restore.

Try to determine which files may have been accidentally restored before you interrupted the process. What was the last message displayed? If you had not received the message “Restore Begins” before you interrupted it, no files were restored.

If it was a complete restore, then use *View Tape Contents* to see the order in which the files were restored. If it was a partial restore, you should know which files were restored.

If you know who the owners of the files are, ask them to check the status of the files. You may have to restore the latest version of any file that the restore overwrote with an older version.

If the file is a system file, and the older version overwrote the newer version, try to restore the latest version of the file.

Problem: The wrong file was restored.

Solution: Confirm the full pathname with the owner.

If you had the right file but the wrong version, ask the owner if a later or earlier version is needed. Tell the owner when you last did backups, asking which tape is appropriate.

If you had the wrong file, you will need to restore the file you accidentally overwrote using the most recent backup. You will also need to notify the owner of the file you accidentally overwrote, since he may have made updates to the file since the last backup. You will also need to restore the file that originally required a restore.

Problem: You received the message: Restore Failed.

Solution: Refer to the solution for the “Backup Failed” message; however, make sure the write-protect arrow on the tape cartridge is turned *toward* SAFE (see Figure 4-2), so that you cannot write over data currently on the tape.

Terminal Administration Problems

Problem: You are unable to log in on a terminal you have enabled.

Solution: Turn up the brightness on the screen to make sure you can see the login message, if it is displayed.

Use *View Port Status* to doublecheck that the port is enabled.

Confirm the port or channel, processor board, and slot numbers. If the numbers match, make sure the terminal works by testing the terminal while it is unconnected to the system, or while it is connected to a port that is known to work correctly.

If you have a cable that is known to work correctly with a different terminal, swap cables.

If it is a serial terminal, make sure the baud rate you specified is set on the terminal.

Problem: You are unable to use the administration tools on an enabled terminal.

Solution: You must have your environment set up so that **adman** knows what type of terminal you are using. [For more information on the environment and the shell, see the **sh(1)** manpage.] The administration tools do not run on “dumb” terminals. (Appendix/0B, “Keyboard Tables,” lists some of the valid terminal types.) See the chapter in the *S/Series CTIX Administrator’s Guide* that discusses terminal configuration for information on determining terminal types.

To set your terminal type for the duration of the current login session, type the following from the shell (substituting your terminal type for *type*):

```
$ TERM=type; export TERM
```

If setting the **TERM** variable from the shell (as shown above) fixes the problem, disable the terminal and enable it again, this time specifying the correct terminal type.

Printer Administration Problems

Problem: The scheduler status or default printer on the *View Print System Status* screen is not what it should be.

Solution: Use *Start/Stop the Print System* to correct the scheduler status.

Problem: The printer or queue status on the *View Print System Status* screen is not what it should be.

Solution: Use *Change Printer Status*.

Problem: The printer did not produce your print request.

Solution: Use *View Print System Status* to see if the printer is disabled or if there is another valid reason for your file not being printed. If everything appears correct on the *View Print System Status* screen, print your file again.

If you still do not receive your request, check your mail; the Ip system sends you mail if it encounters an error in trying to print your request. For more information on reading your mail, see **mail(1)** in the *CTIX Operating System Manual*.

Problem: You have added a printer, but it does not print.

Solution: Make sure it passes the self-test. If it does not, refer to the printer manual for the service number, or call the vendor from whom you purchased the printer.

If it passes the self-test, and if you have a cable that is known to work correctly with a different printer, swap cables. Make sure the cable is attached correctly. (For more information, see the chapter in the installation manual for your system that discusses cabling and connectors.)

Also, make sure that the switches on the printer are set correctly. If you just made a new printer model for this printer, and it is a serial printer, check to see if you specified the correct baud rate.

If everything is correct, but the printer does not print, contact your service representative for assistance.

Problem: The printer prints, but your printout is unrecognizable or looks cluttered with unusual characters.

Solution: Make sure the communications switches are set correctly, especially the parity and baud rate switches. Make sure the printer is able to print at the set speed.

Problem: The printer beeps, and a parity light goes on.

Solution: The problem is probably in the parity bit switch. If your switches are set correctly, call your service representative for help.

Problem: You have changed the status of a printer, but the change does not actually occur. For example, you enabled a printer, but your print request is not produced.

- Solution:** Verify that the printer is enabled by using *View Print System Status*. If this screen indicates the printer should be printing, try submitting your print request again. If the printer is not functioning properly, see the solution for what to do when you have added a printer but it does not print.
- Problem:** A printer model exists for your printer, but your print request is not produced correctly.
- Solution:** Add another model, using a name that distinguishes it from the other printer model. Verify that the model options you select correspond to the switch settings on the printer.

Disk and File System Administration Problems

- Problem:** You have run out of space on a disk.
- Solution:** Use *List Largest Users of Disk Space* from the Disk and File System Administration menu to view a list of the ten largest users of disk space on your system.
- Advise the largest users of disk space to delete any unnecessary files and directories that are currently in their working areas.
- When they're enabled, both system activity reporting and system process accounting use up valuable disk space. Make sure that these functions are disabled when you find that disk space is getting scarce. Refer to the appropriate sections in Chapter 3, "System Status," for instructions on disabling these functions.
- After disabling system activity reporting and system process accounting you need to delete some of the files these two system monitoring functions create in order to free up disk space. If you were monitoring the system for a particular purpose, you may wish to backup these files before deleting them. See *S/Series CTIX Administrator's Guide* for a information on reading these reports, and how to find and remove these files.

If you are still low on disk space, try resetting the console log, the error log, and the networking log, as described in Chapter 3.

If none of the previous solutions works try the following:

1. Use *View/Change Partition Uses* from the Disk and File System Administration menu to select the disk, and determine the current mount points for each partition.
2. Use the Partial Backup function described in Chapter 4, “Backup and Restore,” to back up the specific directories determined to be mount points for the disk.
3. Use *Configure a Disk* from the Disk and File System Administration menu to reallocate space for the partitions on the disk.

Problem: You receive messages, either after the failure of shell commands or in the console log, indicating that you are running out of swap space.

Solution: Use *View/Change Partition Uses* from the Disk and File System Administration menu to find out whether you have an unused partition on any disk.

If such a partition exists, press **F5** to add swap space. Refer to the section “View or Change Partition Uses” in Chapter 5 for detailed instructions on adding swap space.

Problem: The system will not allow users to log in.

Solution: Use *View/Change Partition Uses* from the Disk and File System Administration menu to find out whether you have an unused partition on any disk.

If such a partition exists, press **F5** to add swap space. Refer to the “View or Change Partition Uses” section in Chapter 5 for detailed instructions on adding swap space.

Chapter 13

Problem: You can't create a file in a directory.

Solution: Change the reboot procedure to mount partitions for read/write permissions rather than read only as follows:

1. Use *View/Change Partition Uses* from the Disk and File System Administration menu to unmount and then mount the file system that contains the problem directory.
2. When you mount the file system, a screen is displayed prompting you to select the reboot procedure and the permissions to use when the file system is mounted. At this screen, make sure you select to mount the file system with normal read/write permissions.

Problem: You specified the wrong mount point.

Solution: Use *View/Change Partition Uses* to unmount the file system, then mount the file system on the appropriate mount point.

Problem: Some of your directories are not accessible.

Solution: The partition containing these directories is not mounted.

Use the *View/Change Partition Uses* from the Disk and File System Administration menu to mount the file system that contains the problem directory.

If this operation fails, the file system is "dirty." Use `fsck(1M)` to perform file system maintenance. Refer to the *CTIX Operating System Manual* for information on using `fsck(1M)`.

Problem: You specified the wrong partition in which to create a file system.

Solution: Read the chapter in the *S/Series CTIX Administrator's Guide* that discusses making file systems: the file system should be unmounted and remounted, and the `/etc/checklist` and `/etc/fstab` files need to be modified.

UUCP Administration Problems

Problem: You are unable to exchange mail with a system using a telephone link.

Solution: Examine `/usr/spool/uucp/.Log`, `/usr/spool/uucp/.Old`, or `/usr/spool/uucp/Log-WEEK` for error messages the system encountered while trying to communicate.

Make sure the telephone number is the dialing sequence that your system must use, not just the telephone number of the remote system. For example, the correct telephone number may be 123-4567, but your system may need to dial 9 first to get an outside line: the correct dialing sequence in this case might be 91234567. See the modem manual and the chapter in the *S/Series CTIX Administrator's Guide* that discusses UUCP for information on dialing sequences (sometimes called "chat" or "expect/send" sequences).

If you are using the correct dialing sequence, check the entries in the **Systems**, **Devices**, and **Dialers** files (in `/usr/lib/uucp`).

Problem: You are unable to exchange mail with a system using a direct link.

Solution: Examine `/usr/spool/uucp/.Log`, or `/usr/spool/uucp/.Old/*` for error messages the system encountered while trying to communicate.

If your system was dialing out, make sure the port is enabled on the remote system, that is, the system that is accepting the call.

If the remote system is calling you, check that the remote system is properly configured for a direct call-out connection.

If the remote system calls you, make sure there is a getty on the port on your system, and that your system knows about that system.

See the chapter in the *S/Series CTIX Administrator's Guide* that discusses UUCP for information about more complicated debugging procedures.

Terminal Usage Problems

Problem: Typing mistake.

Solution: **Backspace** over the incorrect character, and type in the correction.

Problem: You received your shell prompt unexpectedly, and nothing happens when you try to type something.

Solution: Follow these steps to reset the terminal:

1. Press **Return**.
2. Type

stty sane

3. Press **Return**.

If this fails, try pressing **Interrupt**. Then press **Return**.

If this fails, try pressing **Interrupt**, **Cancel**, or **Exit**. Then press **Return**.

Problem: The terminal does not respond or it seems like the function has taken an unusually long time to complete.

Solution: This could be caused by one of several problems. In this order, check

1. Your terminal; the keyboard may have come unplugged. If the keyboard is fully plugged in, make sure the connector in the back of your terminal is also completely plugged in.

2. The **adman** process; it may have hung. Press **Exit**. If you still do not receive your prompt, reboot your terminal by turning it off and back on.
3. Your system; it may have shut down unexpectedly. Follow the instructions in the chapter in the *S/Series CTIX Administrator's Guide* that discusses procedures to bring the system back up.
4. Your cable; it may need to be cleared. Sometimes disconnecting your cable from the system's I/O port and reconnecting it clears the system and gives you a fresh login.

RFS Administration Problems

The information in this section assumes that you are familiar with RFS concepts such as the relationship between RFS clients and RFS servers. The problems presented here are those you can encounter when using the **adman** program to administer Remote File Sharing. For more detailed troubleshooting information see the *S/Series CTIX Administrator's Guide*.

Problem: The Primary can not be brought up, and the following error message appears:

rfstart: timed out waiting for name server signal

Solution: If there are secondaries within your domain and all secondaries are currently down, the Primary will not successfully come up until after the secondaries are up.

Problem: You tried to mount an advertised resource and received the following error message:

mount: negotiations failed
mount: possible cause: machine password incorrect
mount: could not connect to remote machine

Solution RFS keeps an unencrypted password on each node in the file `/usr/nserve/auth.info/domain/passwd`. When RFS is started on this node, the unencrypted passwd in `/usr/nserve/loc.passwd` is compared with the encrypted password in the file `/usr/nserve/auth.info/domain/passwd` on the domain's primary name server machine. If these two passwords do not match a warning message appears to the console. The warning message will not stop RFS from starting, but when you attempt to mount a resource the error message listed above appears. To fix this run `rfpasswd` in order to make the password in `/usr/nserve/loc.passwd` on the slave node machine match the password in the file `/usr/nserve/auth.infor/domain/passwd` on the domain's primary name server machine. (See the *S/Series CTIX Administrator's Guide* for more details on this process.)

Problem You were happily working and suddenly received the following error message:

```
spipec: open ) failed, errno===63  
nsquery: cannot setup communication with the name server  
nsquery: possible cause: heavily loaded activity
```

Solution The configured number of allowable STREAMS was exceeded. This happens when there is a lot of activity and the number of STREAMS configured is too low. Resolve this by increasing `nstream`. `nstream` is contained in the `/etc/master` file. Another CTIX kernel must be built. In `/usr/sys/cf/dfilerfs` increase the value in the entry: `nstream 96` before rebuilding a new CTIX kernel. (See the *S/Series CTIX Administrator's Guide* for more details on this process.)

Problem You tried to mount an advertised resource and received the following message:

```
mount: Object is remote  
mount: cannot mount directory
```

Solution This can happen when a remotely advertised resource is mounted on top of a local directory and the local directory is used in the mount command of a local file system slice.

NFS Administration Problems

The information in this section assumes that you are familiar with NFS concepts such as the relationship between NFS clients and NFS servers.

When there are network or server problems, programs that access hard-mounted remote files fail differently than those that access soft-mounted remote files. Hard-mounted remote file systems cause programs to retry until the server responds again. Once a hard mount succeeds, programs that access hard-mounted files hang as long as the server fails to respond. In this case a message appears on the console, indicating that the server is not responding. Soft-mounted remote file systems return an error after trying for limited period of time. On a soft-mounted file system, programs receive an error when they try to access a file whose server is not responding.

Note: See Chapter 12, “Network File System Administration,” for more information on mounting remote resources.

In general when a client is having NFS problems, first check to see that the server is up and running.

Problem: You attempted to mount a file system and got the following error message:

mount: /dev/nfsd is already mounted, .. is busy, or allowable number of mount points exceeded.

Solution: Check the list of mounted remote filesystems to be sure the resource is not already mounted.

Problem: You attempted to mount a file system and got the following error message:

mount:cannot open < /etc/fstab>

Chapter 13

Solution: Check to see that the file `/etc/fstab` exists. You as a system administrator can modify this file.

Problem: You attempted to mount a file system and got the following error message:

... not in hosts database

Solution: The system name suffixed by the colon (:) in the mount request is not listed in the `/etc/hosts` file. Check the spelling of the hostname and the placement of the colon in the mount call.

Problem: You tried to mount a file system and got the following error message:

mount: directory argument <...> must be a full pathname

Solution: Specify the full pathname of the empty directory to be used as a mount point. This must be an absolute path starting at root (/).

Problem: You tried to mount a file system and got the following error message:

mount: ... server not responding(1):RPC_PMAP_FAILURE - RPC_TIMED_OUT

Solution: Check the server to which the mount is being attempted. It is either dead or its portmapper is dead or hung. Try to log into that machine. If that attempt succeeds, the problem may be in the portmapper. Run the following command from your system to test the portmapper on the server system:

rpcinfo -phostname

The result should be a list of registered programs; if not, kill and then restart the remote portmapper by stopping and starting NFS on the server.

Problem: You tried to mount a file system and got the following error message:

```
mount: ...server not  
responding:RPC_PROG_NOT_REGISTERED
```

Solution: **Mount** got through to the portmapper, but the NFS mount daemon **mountd** was not registered. Check the server to ensure that **/etc/mountd** exists and is running. If it is missing or not running, stop and start NFS on the server.

Problem: You tried to mount a file system and received the following error message:

```
mount: /dev/nfsd or ..., no such file or directory
```

Solution: The remote directory you specified does not exist on the server, or the local directory doesn't exist. Note that **/dev/nfsd** always appears in the message to represent the remote directory.

Problem: You tried to mount a file system and received the following error message:

```
mount: access denied for ...:...
```

Solution: The machine on which you attempted the mount is not in the server's export list for the file system to be mounted. Use **showmount(1)** as shown below, to display a list of the server's exported file systems. Type

```
# showmount -e hostname
```

If the desired file system is not listed, or the machine name or netgroup name is not in the user list for the file system, check the **/etc/exports** file on the server for the correct file system entry. A file system name that appears in the **/etc/exports** file but not in the **showmount** output indicates a failure in **mountd**: either it could not parse that line in the file, or it could not find the file system, or the filesystem name was not a local mounted file system. See the **exports(4)** manpage for more information.

This message can also be an indication that authentication failed on the server: it might be displayed because the machine attempting the mount is not in the server's export list, or because the server is not aware of the machine. Check the server's `/etc/exports` file.

Problem: You tried to mount a file system and received the following error message:

mount: ...:no such file or directory

Solution: The remote path on the server is not a directory. You must specify a directory.

Problem: Programs hang while performing file-related operations.

Solution: Check the NFS server to see if it is up. There is probably a problem in either one of the NFS servers, or with the local area network.

If a machine hangs completely, check the server(s) from which file systems have been mounted. If one (or more) is down, client machines can hang too. When the server comes back up, programs continue automatically.

If a soft-mounted server dies, other work should not be affected. Programs that timeout while trying to access soft-mounted remote files fail, but other file systems should work.

If other clients of the server seem to be functioning correctly, check the local area network connection.

It is possible that certain commands like `rpcinfo` will hang or timeout when gathering information on the local host. This may be the result of an improperly configured loopback interface. Make sure the entry `127.1 loopback` is present in `/etc/hosts` or the `hosts` Yellow Pages map and run `netstat -i` to check that it is currently configured.

SCSI Tape Drive Administration Problems

Problem: You are unable to read the contents of a tape.

Solution: Enter *View a SCSI Tape Drive* and check that the drive is listed. If not, then use *SCSI Tape Administration* to add the drive.

Problem: The tape drive did not implement your request.

Solution: Verify that you configured the tape drive correctly.

1. The target number should match the toggles on the device.
2. The tape size is correctly specified. (Half-inch or not).
3. The correct device type was selected.
4. Make sure the drive comes on line when powered up.

Problem: The tape drive to be added is not listed as an available type.

Solution: Using the *S/Series CTIX Administrator's Guide* add an entry to */etc/tapedrives* for your tapedrive.

When All Else Fails

Ask for help. Or, if the problem is not serious, leave it alone for a while and come back to it. Intuition plays a major part in most troubleshooting, so if you have run out of good ideas, maybe someone else has one, or you will think of one later. Do not forget you can always call your service representative; that is what they are there for.

Preventive Maintenance

Preventive maintenance is troubleshooting a potential problem before it occurs. You can use preventive maintenance to troubleshoot a potential problem before it occurs by checking the console log and the system error log on a routine basis. Read Chapter 3, “System Status.”

These are the things to watch for.

- Unexpected system shutdown. You can watch out for this by monitoring the console log. Usually (although not always), the system sends an error message to the console when it experiences a problem. Read “Monitoring the System Console” in Chapter 3, “System Status.”
- Disk space. Each file on the system uses a certain amount of disk space. Some files use more space than others, and some files keep growing in size until you reset or clear them. Keep a close watch on disk space, especially looking out for major reductions of available space in a short amount of time. For a list of specific files to monitor, read the chapter in the *S/Series CTIX Administrator's Guide* that discusses files that grow. Keep an eye on disk space using *List Largest Files*, described in Chapter 5, “Disk and File System Administration.” Watch especially for major reductions of available space in a short amount of time.

Some files to watch (that can usually be removed) include the following:

- `/usr/adm/sulog`
- `/usr/lib/cron/log`
- `/usr/tmp/*`
- `/tmp/*`

In addition, you can use *Monitor Disk Usage*, *List Files of a Certain Age*, and *List Largest Users of Disk Space*, described in Chapter 5, to find oversized and old files that can be removed, and to identify users or applications consuming too much space.

You might also want to turn your system on and off, or run the **shutdown** program followed by a system reboot (**reboot** command) approximately once a month. Doing this resets several files that can grow quite large, and also checks the file systems. However, be sure to bring the system to single-user mode before powering down the system.

Another potential source of disk cluttering files is the Network File System. When a file system is soft mounted from a heavily loaded server, NFS creates temporary files when it gives up after a timeout. Under such conditions, the server can become cluttered with these files. You, as the system administrator, should clean out these files periodically. These files are named **.nfsjunk###** (### stands for an arbitrary suffix). See the *S/Series CTIX Administrator's Guide* for instructions on removing files.

Where to Go from Here

The *S/Series CTIX Administrator's Guide* is your best source of information regarding the details of the functions the **adman** program performs.

In addition, the *S/Series CTIX Administrator's Guide* and the *CTIX Network Administrator's Guide* provide detailed information on some commands used to prevent problems before they occur. The following are commands that help prevent space inadequacy and abuse:

df

This command checks the amount of available disk space per file system.

du

This command checks the amount of disk space used in any directory or by any user.

—

—

—

Appendix A

Basic Concepts

What Is CTIX?

CTIX is an operating system based on the UNIX System V, Release Version 3.2, operating system; it is basically the same as UNIX with some enhancements.

An *operating system* is the software that manages the various processes running on your computer and provides you with an interface for controlling system resources. Resources include such things as memory space, application programs, printers, and terminals.

The CTIX Shell

In order to start a program in CTIX, you type in a command from the *shell*. The shell is a program invoked automatically by CTIX when you log into the system; it interprets the commands you type on the keyboard and then invokes the programs that perform your requests. Which shell you have is reflected by what you see when you log in to the system. If you have not changed the prompt string that was provided in your release of CTIX, then if you see a #, \$, or % prompt, your shell is one of the *programmer's shells*.

The CTIX Environment

CTIX allows you to set up and alter your working environment to suit your needs. For example, different versions of the shell are available, including the two standard programmer's shells, the System V shell and the C shell.

The System V shell is the default shell, designated as `/bin/sh`. Some users prefer the C shell, which is designated as `/usr/local/bin/csh`. The primary difference between the two is that the C shell provides a history mechanism, which allows you to abbreviate and repeat commands easily. More information on setting up a user's environment is available in the *S/Series CTIX Administrator's Guide*.

Who Is the System Administrator?

You are the system administrator if you are the person responsible for the overall well-being of the system. The system administrator is the focal point for all system-related problems and user questions. Your responsibilities as system administrator include the following:

- adding and removing users from the system
- performing backups to safeguard the system from accidental loss of data
- assuring the best level of security possible to protect against tampering
- turning the system on and off and scheduling maintenance

System administration also includes installing software onto the system. Instructions for installing software can be found in the release notice that accompanies the software.

What Are File Systems?

A CTIX *file system* is a convenient grouping of files and directories occupying a particular section (partition) of a disk.

Accessing File Systems

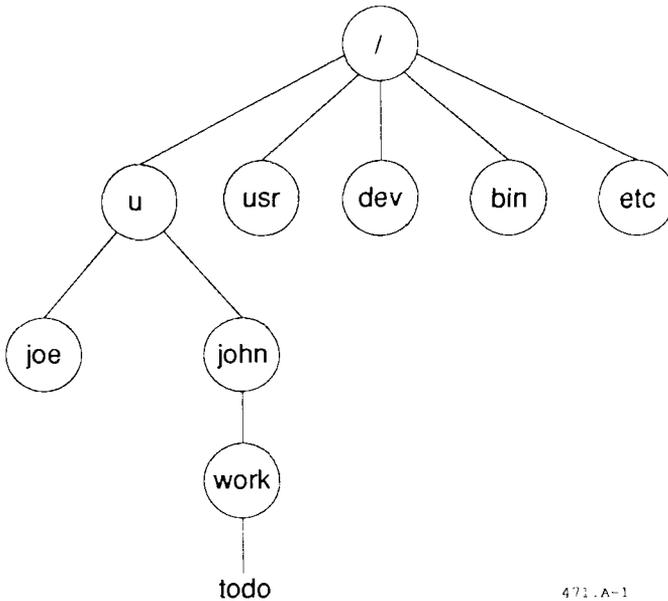
Unless a file system is *mounted* on a directory, it cannot be accessed. Mounting a file system on a directory is like opening the door to the file system: you can enter when it is open (mounted read/write), you can see what's inside when the door is open but the screen is locked (mounted read only), but you cannot do either when the door is closed (unmounted). The directory on which it is mounted forms the first part of the pathname of all files in the file system. For example, a file called `/doc/epicnovel/chap3` mounted on `/u/dave` becomes `/u/dave/doc/epicnovel/chap3`.

File systems are usually mounted automatically when you turn the system on; otherwise, they can be mounted when you use the **mount** command or when you mount them using the administration tools. More information on file systems can be found in Chapter 5, "Disk and File System Administration."

CTIX File Structure

A *directory* is a node that contains the files and directories underneath it: more precisely, it is a file whose data concerns the directory above it, the files and directories immediately below it, and itself.

The system may contain hundreds of directories, organized into an upside-down tree structure. At the top of the directory tree is the *root* directory. Underneath it are more directories, called subdirectories (underneath them are more subdirectories, and so on). Figure A-1 shows the basic CTIX directory structure.



471 .A-1

Figure A-1. CTIX Directory Structure

Where a file resides in the directory structure is specified by its *pathname*. For example, in Figure A-1, the file **todo** resides in **/u/john** (the slashes indicate directory levels). The *full pathname* of this file is **/u/john/work/todo**. Full pathnames always begin with a **/**. Relative pathnames never begin with **/**.

Note: Use the full pathname to reference a file when using the administration tools.

Each user has a unique directory for his files, called a *home directory*. Your home directory is where you are when you first log in, and its subdirectories are often where you perform the majority of your work. In Figure A-1, John's home directory is **/u/john**.

Root's home directory is /. Notice the name "root" matches the top of the directory tree; this is because everything on the system stems from the root directory.

Some other important directories shown in Figure A-1 are

- /u** The **/u** directory in this system contains the home directories of the users on the system; for example, **/u/john** and **/u/joe**. Usually, the directory containing users' home directories is a file system.
- /dev** The **/dev** directory contains all the devices in the system. For example, it contains the filenames associated with terminals, printers, and disks.
- /bin** The **/bin** directory contains many of the commands and utility programs that you type in from the shell, for example, **ls** and **cpio**. For more information on these and other commands, refer to the *CTIX Operating System Manual*.
- /etc** The **/etc** directory contains system administration commands and files. For example, the password file and the file system mount command (**mount**) reside in **/etc**.
- /usr** The **/usr** directory is often a file system. **/usr** contains various system directories, commands, and utility programs, for example, the accounting and **lp** system directories.

For more information on the CTIX directory structure, refer to the chapter in the *S/Series CTIX Administrator's Guide* that discusses CTIX system directories.

File System Security

There are two security measures available on the system: *passwords* and *privileges*. Using passwords prevents unauthorized people from logging into your system. Withholding privileges prevents unauthorized people from viewing and modifying your files. These security measures should be applied by nonprivileged users as well as system administrators.

Passwords

There are three keys to maintaining good password protection:

- Always have a password.
- Change your password regularly.
- Do not disclose your password to other people.

For instructions on implementing and ensuring password protection, read “Change Your Password” in Chapter 2, and “Add a Remote System Entry” in Chapter 9.

Privileges

Privileges are determined by the *mode* of a file: who can read, modify, and/or execute your files. The mode can be assigned on the basis of who the user is or it can depend on how much access to a file or directory is required by the user.

For example, to protect important files from being modified by other departments, you might assign those files a *read-only* mode for all departments other than yours. Thus you have denied other departments the privilege of modifying the files, but allowed them the privilege of reading them. Files that contain very sensitive data can be read-only for the owner and no access of any type for anyone else.

Superuser Privileges

As system administrator, you are distinguished from other users by your *superuser* privileges; the superuser has an account on the system called **root** that has the ability to read or modify any file in the system, regardless of the security level.

Users who are not system administrators are *nonprivileged users*. Nonprivileged users must have express permission to read or modify files other than their own.

In order to use your superuser privileges, you must enter superuser mode. Enter superuser mode by logging into the system as **root** and giving root's password, or by using the **su** command, described in the *CTIX Operating System Manual*. For instructions on privileged and nonprivileged access, see "Entering the Administration Tools," in Chapter 1.

Caution

Never leave your terminal in superuser mode when you are not present, and do not disclose the superuser password to anyone. Having superuser status allows you to accidentally destroy the entire system or to invade other users' privacy.

User Modes

Privileges are assigned on the basis of three user categories:

- user* User (owner) privileges allow only the owner of the file to access the file.
- group* Group privileges permit access to the file by certain other people designated as members of the group to which the file owner belongs.
- other* Other privileges allow access by users with no special permission: others are anyone and everyone on the system.

Access Modes

In turn, each of the user categories above (user, group, and other) may have the following types of access assigned:

- read* Read permission provides viewing access to a file. The file cannot be modified, but it can be copied and then the copy can be modified.

Appendix A

- write* Write permission provides modification access: ability to change or delete files. Be careful how you allow write permissions on your files and directories.
- execute* Execute permission provides the privilege to execute a file or to search a directory. You cannot look at the contents of a directory unless you have permission to read *and* permission to search the directory.

How to Change Modes

You can tell what the security mode of a file is by using the `ls -l` command from the shell or by using the *View Tape Contents* tool, described in Chapter 4.

There are two ways of presenting modes: alphabetic and numeric. You see the alphabetic form when you use the `ls -l` command from the shell. You see the numeric form when you use *View Tape Contents*. Shown below are examples of both forms:

Alphabetic: drwxrwxrwx

Numeric: 40777

Alphabetic Form. Notice that there are ten positions in the alphabetic mode. The positions are described as follows:

- 1 The first position shows the type of file. A file can be a directory (designated by a **d**), or a special file corresponding to a device, such as a terminal or disk partition (designated by a **b** or a **c**). For more information on special files, see **mknod** in the *CTIX Operating System Manual*, and the chapter in the *S/Series CTIX Administrator's Guide* that discusses disk organization.
- 2-4 The next three positions show the user's privileges (read, write, and/or execute).

5-7 The next three positions show the group's privileges (read, write, and/or execute).

8-10 The last three positions show the other privileges (read, write, and/or execute).

Numeric Form. To understand the numeric form, translate it into alphabetic form by adding the numeric values of the characters, where read (r) equals 4; write (w) equals 2; and execute (x) equals 1.

For example, a directory with an alphabetic form of `drwxr-xr-x` and a numeric form of 755 (4+2+1, 4+0+1, 4+0+1) is

- readable, writable, and executable by the owner
- readable and executable by the group
- readable and executable by all others on the system

Designating the Mode. When you create a file or directory, the system automatically assigns certain privileges. As distributed, CTIX creates all new files with a mode of 644, and all new directories with a mode of 755. (If you have not altered the default file creation mode in `/etc/profile`, then `umask` is set at 022, which produces the default modes above.)

To change the level of protection for a file, use the `chmod` command. For more information on `chmod(1)` and `umask(1M)`, see the *CTIX Operating System Manual*.

Where to Go from Here

If you want to learn more about the basic concepts of a CTIX system, refer to the computer section in your local bookstore for books that discuss the UNIX operating system: there are several books on the market, ranging from introductory to advanced.

—

—

—

Appendix B

Keyboard Tables

Introduction

Since this release of **adman** runs on many terminal types (and therefore, many different keyboards), this manual refers to keys by *virtual* (symbolic) key names. For example, where this manual reads **Enter**, you might press **Go**, **Do**, or **Linefeed**, or something else, depending on the type of terminal you are using.

This appendix provides keyboard tables for many of the standard terminal types. Each table matches the virtual key names used in this manual with the actual key names on a particular terminal type. To use this appendix:

- Find the appropriate keyboard table for your terminal type.
- Find the matching keys on your keyboard that correspond to the virtual keys listed in the table.

If you are using a terminal that is not listed in this appendix, you can type key sequences to perform many of the virtual key functions. Refer to the “Generic Keyboard” table for a list of key sequences that match virtual key functions.

Appendix B

The following terminal types are listed in this appendix:

- Generic (dumb)
- PT and GT (RS-422 or RS-232 connections)
- TO-250
- TO-300
- DEC VT-100 compatibles
- DEC VT-102
- DEC VT-220
- Wyse 85

Generic (Dumb) Terminal Keyboards

The following table translates virtual key names used in this manual to actual key names (or keystroke sequences) on a generic (dumb) terminal keyboard.

GENERIC KEYBOARD

When You See This Key Name	Type This Key Sequence
Back	Escape bw
Backspace	Back Space
Back Tab	Escape Tab
Cancel	Control-X
Control	Control
Delete Character	Delete
Down	Escape dn
Enter	LineFeed
Exit	Control-D
Forward	Escape fw
F1	Escape 1
F2	Escape 2
F3	Escape 3
F4	Escape 4

GENERIC KEYBOARD

When You See This Key Name	Type This Key Sequence
F5	Escape 5
F6	Escape 6
F7	Escape 7
F8	Escape 8
F9	Escape 9
F10	Escape 0
Help	Escape ?
Interrupt	Delete
Mark	Escape mk
Page	Escape pg
Return	Return
Roll Up	Escape ru
Roll Down	Escape dn
Shift-Page	Escape PG
Tab	Tab
Up	Escape up

PT/GT Terminal Keyboards

The following table translates virtual key names used in this manual to actual key names (or keystroke sequences) on a PT/GT terminal keyboard.

PT/GT KEYBOARD

When You See This Key Name	Type This Key Sequence
Back	Left Arrow
Backspace	Back Space
Back Tab	Code-Tab
Cancel	Cancel
	(Code-X if your terminal is in emulate mode)
Control	Code
Delete Character	Delete
Down	Down Arrow
Enter	Go
Exit	Finish
Forward	Right Arrow
F1	F1
F2	F2
F3	F3

Appendix B

PT/GT KEYBOARD

When You See This Key Name	Type This Key Sequence
F4	F4
F5	F5
F6	F6
F7	F7
F8	F8
F9	F9
F10	F10
Help	Help
Interrupt	Delete
Mark	Mark
Page	Next Page
Return	Return

PT/GT KEYBOARD

When You See This Key Name	Type This Key Sequence
Roll Up	Scroll Down
Roll Down	Scroll Up
Shift-Page	Prev Page
Tab	Tab
Up	Up Arrow

TO-250 and TO-300 Terminal Keyboards

The following table translates virtual key names used in this manual to actual key names (or keystroke sequences) on TO-250 and TO-300 terminal keyboards.

TO-250 and TO-300 KEYBOARDS

When You See This Key Name	Type This Key Sequence
Back	Left Arrow
Backspace	Back Space
Back Tab	Control Tab
Cancel	Control-X or F20
Control	Control
Delete Character	Back Space
Down	Down Arrow
Enter	Do
Exit	Control-D or F14
Forward	Right Arrow
F1	F1
F2	F2
F3	F3
F4	F4
F5	F5
F6	F6
F7	F7

TO-250 and TO-300 KEYBOARDS

When You See This Key Name	Type This Key Sequence
F8	F8
F9	F9
F10	F10
Help	Help
Interrupt	Shift-Back Space
Mark	Select
Page	Next Screen
Return	Return
Roll Up	Prev Screen
Roll Down	Next Screen
Shift-Page	Prev Page
Tab	Tab
Up	Up Arrow

VT-100 Terminal Keyboard

The following table translates virtual key names used in this manual to actual key names (or keystroke sequences) on a VT-100 terminal keyboard.

VT-100 KEYBOARD

When You See This Key Name	Type This Key Sequence
Back	Left Arrow
Backspace	Back Space
Back Tab	Escape Tab
Cancel	Control-X
Control	Control
Command	Control-K
Delete Character	Delete
Down	Down Arrow
Enter	Control-J
Exit	Control-D
Forward	Right Arrow
F1	Escape 1
F2	Escape 2
F3	Escape 3
F4	Escape 4
F5	Escape 5
F6	Escape 6

VT-100 KEYBOARD

When You See This Key Name	Type This Key Sequence
F7	Escape 7
F8	Escape 8
F9	Escape 9
F10	Escape 0
Help	Control-B
Interrupt	Delete
Mark	Control-A
Page	Escape pg
Return	Return
Roll Up	Escape ru
Roll Down	Escape dn
Shift-Page	Escape PG
Tab	Tab
Up	Up Arrow

VT-220 Terminal Keyboard

The following table translates virtual key names used in this manual to actual key names (or keystroke sequences) on a VT-220 terminal keyboard.

VT-220 KEYBOARD

When You See This Key Name	Type This Key Sequence
Back	Left Arrow
Backspace	Back Space
Back Tab	Escape Tab
Cancel	Control-X
Control	Control
Delete Character	Shift-Back Space
Down	Down Arrow
Enter	Do
Exit	Control-D
Forward	Right Arrow
F1	F6
F2	F7
F3	F8
F4	F9
F5	F10
F6	F17
F7	F18

VT-220 KEYBOARD

When You See This Key Name	Type This Key Sequence
F8	F19
F9	F20
F10	Escape 0
Help	Help
Interrupt	Shift-Back Space
Mark	Select
Page	Escape pg
Return	Return
Roll Up	Escape ru
Roll Down	Escape dn
Shift-Page	Escape PG
Tab	Tab
Up	Up Arrow

Wyse-85 Terminal Keyboard

The following table translates virtual key names used in this manual to actual key names (or keystroke sequences) on a Wyse-85 terminal keyboard.

WYSE-85 KEYBOARD

When You See This Key Name	Type This Key Sequence
Back	Left Arrow
Backspace	Back Space
Back Tab	Escape Tab
Cancel	Control-X
Control	Control
Delete Character	Shift-Back Space
Down	Down Arrow
Enter	Do
Exit	Control-D
Forward	Right Arrow
F1	F6
F2	F7
F3	F8
F4	F9
F5	F10
F6	F17
F7	F18

WYSE-85 KEYBOARD

When You See This Key Name	Type This Key Sequence
F8	F19
F9	F20
F10	Escape 0
Help	Help
Interrupt	Shift-Back Space
Mark	Select
Page	Escape pg
Return	Return
Roll Up	Escape ru
Roll Down	Escape dn
Shift-Page	Escape PG
Tab	Tab
Up	Up Arrow

—

—

—

Appendix C

Network File System Versus Remote File Sharing

Which is Best?

It is possible to run both NFS and RFS (Remote File Sharing) on your machine. This allows you to choose the communication method which best suits your particular situation.

Advantages in Using NFS

For example, you might choose the NFS to:

- Share resources with other NFS machines.
- Use the remote Procedure Call (RPC) mechanism. Refer to the *S/Series CTIX Administrator's Guide* for information on using the RPC.
- Share a subdirectory without making the entire upper level directory available.
- Share resources with a non-UNIX system.

Advantages in Using RFS

You might choose RFS to:

- Share resources with other RFS machines.
- Ensure security. If security is of the utmost importance on your system, using RFS to share resources is the wisest path. RFS contains security features NFS does not provide. Security for resources shared using the NFS is limited to the security features of the operating system.
- Remotely mount devices (special files).
- Preserve the file locking capability of applications you plan to use on the remote file system. Refer to the *S/Series CTIX Administrator's Guide* for further information.

Refer to Chapter 11, “Remote File Sharing Administration,” for details about using the **adman** program to set up and use RFS.

Appendix D

PT and GT Terminals and Keyboards

Using PT or GT Terminals

This information is supplied for use with the PT and GT terminals.

Terminal Modes

A PT or GT can be in one of three modes: *RS-422* download mode, *RS-232* download mode, or *RS-232* emulate mode. To put the terminal into *RS-422* mode, be sure the *RS-422* cable is attached to the appropriate connector on the back of your terminal, and simply turn your terminal on.

To put the terminal into emulate mode, be sure the *RS-232* cable is attached to the appropriate connector on the back of your terminal, and turn the terminal on while holding the space bar down. Hold the space bar down until you see a prompt ending with a colon (:), then type *e*.

Emulate mode is not recommended for use with the administration tools program, because it does not support the full range of keystroke sequences required by **adman**.

If you are using a PT or a GT in *RS-232* mode, it is recommended that you *download* your terminal: this provides the full range of keystroke sequences supported. To download your PT or GT, do the following:

1. Exit the administration tools, and log out.
2. At the login prompt, type **ptdl** (or **gtdl**, if using a GT).
3. When the system displays the login prompt again (after about one minute), log in as you normally would.

Exiting menus

Use ^X to exit without executing the current selection.

Keyboard Layout

Note: You can always exit an administration tool without executing currently selected items by pressing Cancel (^X if on a PT or GT in emulate mode). If you are not sure which key to press on your keyboard to perform a function, see Appendix B, "Keyboard Tables."

Figure D-1 shows the keyboard layout for the PT/GT keyboards. A summary of virtual keys and uses is included. For detailed information relating virtual keys to specific keys on the PT/GT keyboard see Appendix B, "Keyboard Tables."

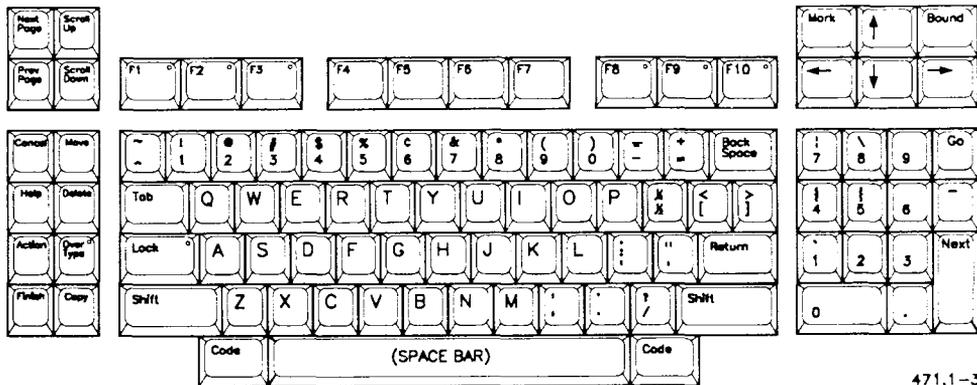


Figure D-1. PT Keyboard Layout

The key that interrupts functions is configurable; it is normally the **Delete** key, but it does not have to be. In functions that take you outside a form or menu, such as *Change Your Password*, use the **Backspace** key to edit keyboard input.

—

—

—

Glossary

A

add-on swap path

Pathname used to specify the location of swap space which is in addition to the main swap space.

adman

adman(1) is the CTIX command that allows you to use the administration tools.

administrator

An administrator is a person in charge of configuring host computers on a **network**.

adv

adv(1M) is the command by which a resource is advertised to other **host** computers on a **network**. It can be used with no options to display a listing of the **resources** currently available on the local machine.

advertise

To advertise a **resource** is to make it available for other **host** computers on the **network** (sharing a resource).

archive

An archive is a copy of a file that is put on a medium separate from any complete or incremental **backup** the file may already be on. Archives should be recorded in the backup log along with backups.

Glossary

B

backup

A backup is a copy of the information on the system preserved on a separate medium, usually a quarter-inch tape (QIC) on an S/Series system. Backups can be taken in different forms: a complete backup of the system, a backup of only the changes since the last complete backup was taken (called an incremental backup), or a backup of part of the system (called a partial or user backup).

baud rate

The baud rate refers to the speed at which data is communicated, measured in bits per second (bps).

bidirectional system

A system configured to send and receive information from other systems on a network.

block

A block is a unit of measurement for data, and can be either physical (512 bytes) or logical (1024 bytes). One byte is most commonly made up of eight bits. A bit (binary digit) holds a single 1 or 0, and is the smallest unit of information.

C

carriage motion

The carriage motion is what the system generates when you signal the end of a line, usually a carriage return and a line feed.

channel

A channel is a data transmission path between an S/Series System and a peripheral device, such as a terminal.

class

A class is a group of devices such as printers.

client

In a communications **network** such as an NFS network, the client is the requesting machine. The server is the supplying machine.

cluster channel

A cluster **channel** is a channel supporting RS-422 communication and up to 15 devices (such as PTs, GTs, RIOPs, or PCs running PC Exchange). Cluster channels require a Cluster Expansion board.

console

The console is an imaginary terminal to which the system sends important status information. The information is written to the console log file, which should be monitored frequently. On some computer systems, other than S/Series systems, the console is a dedicated terminal you use when you turn the system on or off, and the status messages may be printed in addition to being stored in a log.

controller

A controller is a processor board installed in your system that manages peripheral devices, for example, disk and tape drives.

CTIX

CTIX is an operating system derived from UNIX System V. It is basically the same as UNIX with some enhancements added.

CTIX programmers shell

The CTIX programmer's **shell** is one of the command interpreters for the CTIX operating system. There are two standard programmer's shells: the Bourne shell, `/bin/sh`, which is often represented by the `$` prompt; and the C shell, `/usr/local/bin/csh`, which is often represented by the `%` prompt.

Glossary

D

daemon

A background process which waits for each occurrence of a certain set of conditions before performing a given task.

DARPA Internet name

A name for a host computer on a network that consists of the mode name and a domain name separated by a period(.).

default

A default is a value that is selected for you by the system unless you specify a different value.

default printer

The default printer is the **destination** that automatically receives all print requests, unless you request a different printer.

destination

A destination is a printer to which a print request can be sent.

device

Any electronic or electromechanical machine or component. Device always refers to hardware. Device driver refers to software that controls the hardware.

device file

A file containing configuration information used to identify the location of a particular device.

dialing sequence

A dialing sequence is what a **modem** on one system uses to reach another modem on another system. Additional digits besides the phone number may be used in a dialing sequence, such as a digit to acquire an outside line or to cause a delay. See also **modem** and **telephone link**.

direct link

A direct link refers to a cable that runs directly from a **port** on your system to a port on another system. One possible use is the exchange of electronic mail.

directory

A directory is a place where a collection of files reside in the system. If one of the files in a directory is itself a directory, it is called a subdirectory of the first directory. When you log in to the system you are placed in a directory called your home directory.

disk

A disk is a device on your system for storing large amounts of data. Two kinds of "on-board" disks for an S/Series system are ST506 5 (14-inch disks, and SCSI (small computer system interface) disks. SCSI disks are available in both 5 ¼-inch and 3 ½-inch size. Another disk that can be used in some S/Series systems is the Storage Module Drive (SMD). An SMD usually holds more data than an ST506 disk. To use an SMD, your system must have VME (Virtual Memory Expansion) capability.

domain

A domain is a logical grouping of **host** computers on a **network**. The grouping is made for administrative and addressing purposes.

domain mount table

The domain mount table is a data structure containing information about what remote **hosts** have mounted **resources** that the local machine advertised. Use of the **rmntstat(1)** command displays all of the resources or any chosen subset.

E

Ethernet link

The term Ethernet refers to a type of network that uses special communications protocols and supporting hardware. An Ethernet link may be used between systems to exchange electronic mail.

Glossary

F

file system

A file system consists of CTIX files and directories, and the data structures required to support them. File systems help you organize a disk. One form of file system is contained within a disk partition.

H

hardware tabs

Hardware tabs are a method for implementing printer tab stops with the hardware, rather than with the software. Not all printers have the capability to implement tab stops, in which case the software can implement them.

homogeneous network

A **network** on which all the machines are of the same type.

host

A host is a computer installed as a member of a **network**. This term is used in relation to the **Remote File Sharing** facility.

host mount table

The host mount table is the data structure of the remote resources currently available on the local machine. The **mount** command with no options displays this table.

I

internet name

See DARPA Internet name.

J

job

A unit of work running in the computer. A job may be a single program, or a group of programs that are required to work together.

L

line printer

A line printer is technically a printer that prints an entire line at a time. However, the term “**lp**” is used to represent any type of printer, as in the phrase “**lp system**,” which refers to the general printer population. Not all printers in the **lp** system are in fact line printers.

local advertise table

A local advertise table is a data structure of the local resources currently advertised. It can be displayed by the **adv** command with no options.

login terminal

The **lp** system considers a login terminal to be a hardcopy terminal, which more closely resembles a teletype machine than a terminal with a screen display.

lp system

Print spooler and commands and configuration files used to coordinate and execute print requests and print jobs.

Glossary

M

machine equivalence

Condition where users on a remote machine are allowed the same permissions as users on the local machine who have the same login name, excepting the root login. For example, if remote machine *flashy* is made equivalent to local machine *stormy*, then user *margie* on *flashy* can read and write to files created by equivalent user *margie* on *stormy*.

main menu

The main menu is the top of the administration tools menu hierarchy, providing access to the major functions within the administration tools.

main swap partition

Primary area of memory on disk, used by memory management system.

mapping

Mapping is the means of defining how **resource** requests from users and groups are handled.

memory

Memory consists of integrated circuits on an S/Series processor that store information or instructions for the system to execute.

menu

A menu is a list of choices from which you make a selection. Menus can take up an entire screen or they can be parts of a form. On certain forms, pop-up menus can be displayed by pressing \hat{C} .

mode

The mode of a file represents its security level: the security level concerns who can read, write, and/or execute a particular file. Modes are displayed in two forms, alphabetic (*drwxrwxrwx*) and numeric (*40777*).

model

A model is a program that the **lp** system uses to interact with a printer; a model contains the characteristics of a particular printer.

modem

A modem is a device connected to a computer and a telephone that translates the signals coming over a telephone line into data signals the computer understands. See also **phone link** and **dialing sequence**.

mount

Mount announces to the system that a file system or a remote resource is available. You must specify a **mount point** when using this command to mount a resource. If you use this command without specifying a mount point, the system will give you a list of available resources. Once a file system or remote resource is mounted, it looks to the user as if it resides on the local machine.

mount path

A mount path is the **pathname** indicating where a **file system** or remote **resource** is to reside in the directory structure. See **mount point**.

mount point

A mount point is a **pathname** indicating where a **file system** or remote **resource** is to reside in the directory structure; If you are using the **adman** program, the directory you specify to serve as the mount point must be empty. The full pathname of the mount point is prefixed to all files and directories mounted onto that point.

N

name server

A name server is a **host** computer which is designated to handle the responsibilities of maintaining the information about the **network** organization (passwords, mappings, etc.)

named pipe

A named pipe is a pipe which is listed in the system name space.

Glossary

neighboring domains

Two RFS domains, each of which is aware of the other. Each primary name server has information concerning the existence of the other domain.

network

The administration tools consider a network to be a group of systems using a particular communication protocol. A network can also refer to the entire community of systems that your system can communicate with, through any type of link.

network address

A unique address which identifies the network to which the host is connected and the logical location of the host on the network.

Network File System

(NFS) This system allows network computer users to share resources.

network gateway

A computer (host) that passes data from one network to another network. A gateway computer is connected to more than one network and generally has more than one network address.

network service

A program running on a networked computer that provides a service to users of that computer or other users on the network. Network services are sometimes called **daemons**; their names often end with the letter **d**.

node name

In a network, the name of a node, usually a **host** computer. The term node is taken from graph theory. A node is a junction point of links, areas, or edges. A network node serves as a junction point for communication of data.

nonprivileged user

Nonprivileged users may read or modify their own files, but require express permission to read or modify another user's files.

O

operating system

The operating system is the basic software that is installed on a computer to support other programs, such as the administration tools. It allows you to enter commands and perform tasks on the computer, it controls access to the system through security mechanisms, and it allocates resources among the users on a system.

P

parallel connection

A parallel connection is a type of connection between a computer and a printer which transmits data from a computer to a printer in groups of bits.

parallel printer

A parallel printer is a printer connected to a computer with a **parallel connection**.

parity

Parity is a method of checking for communication errors.

partition

A partition is a section of a disk. Partitions are synonymous with slices.

password

A password is a unique set of characters (stored by the system in encrypted format) that give a user access to a system.

pathname

A pathname is the way to designate a file's location in the directory structure. When the pathname starts with a slash, it is called the full pathname, because it shows each directory level starting from root. For example, if user john's home directory is `/u/john` and he has a file named **todo** in his subdirectory named **work**, the full pathname of **todo** is `/u/john/work/todo`.

Glossary

peripheral device

A **peripheral device** is a device, such as a terminal or printer, distinct from the S/Series system that provides additional facilities to the system (such as outside communication or hardcopy output).

pop-up menu

A screen display which shows a number of selections from which to choose. In **adman**, some tools provide pop-up menus which you can display by pressing ^C.

port

A **port** is a connector on your S/Series system into which a cable (for a terminal, printer, or other device) is plugged. You cannot use a terminal that is physically connected to the system until you enable the associated port; this allows a login to occur on the port.

primary name server

A **primary name server** is the **host computer** designated to be the major maintainer of the information about the **network** organization (**passwords**, **mappings**, etc.)

print job

Consists of instructions for the **printer** and information to be printed, and is created at the time a user initiates a **print request**.

print request

Spooling of a file by the user for printing.

print scheduler

The **print scheduler** is the part of the **lp** system that directs certain files to be printed on certain printers.

printer

A **printer** is a physical **device** used to print documents. See also **serial printer**, **remote printer**, **parallel printer**, and **login terminal**.

programmer's shell

The CTIX programmer's shell is one of the command interpreters for the CTIX operating system. There are two standard programmer's shells: the Bourne shell, `/bin/sh`, which is often represented by the `$` prompt; and the C shell, `/usr/local/bin/csh`, which is often represented by the `%` prompt. See also **shell**.

Q

queue

On the **lp** system, the queue is where print requests are held until the printer is ready to print them.

R

raw partition

A **partition** which does not have a file system on it. A raw partition is sometimes referred to as an uninitialized partition. It can be used for **swap space**, a new **file system**, or to **cpio** files into.

remote I/O processor

A remote I/O processor (RIOP) is a cluster (RS-422) device that supports RS-232 communication. RIOPs are connected in a daisy-chain fashion to an RS-422 line, and each RIOP can support up to 15 devices.

Remote File Sharing (RFS)

This facility allows users of a computer on a network to share resources.

remote printer

A remote **printer** is a printer you can access from your system, which is not directly connected to your system.

remote system

A remote system is another system linked to your system over a telephone line, directly, or through a **network**.

Glossary

resource

A resource is a file, **directory**, **device**, or **named pipe** which, using RFS, can be shared among **host** computers on a **network**.

resource name

A resource name is the name by which other **host** computers on the **network** reference a **resource** to be shared.

restore

A restore is the act of returning the system to a previous state, by copying the contents of a **backup** tape onto the system. You can either restore an entire system by means of a backup tape, or certain files from a backup tape.

root

Root has two meanings: it can refer to the superuser account, which has superior privileges and may read or modify any file on the system; root is also the name of the **directory** at the top of the directory tree, designated by a slash (/). Full **pathnames** always start from the root, for example, **/u/john/testfile**.

root file system

The file system containing the root directory. The root file system is located in Partition 1.

run level

The level of operation of the system. The run level can be set to single-user mode or multi-user mode. The run level is frequently referred to as an **init** state. For more information on the various **init** states see the *S/Series CTIX Administrator's Guide*.

S**scheduler**

Part of the operating system which initiates or terminates jobs, allocates system resources as required or directs certain files to be printed on certain printers.

secondary name server

A secondary name server is one of a number of possible host computers which has been designated as an alternate maintainer of network organization information (in case the primary name server is unable to perform the maintenance).

serial connection

A serial connection is a type of connection between the computer and the peripheral device that transfers data from the computer to the peripheral device one bit at a time.

serial port

A serial **port** is a place on the system to connect a single terminal, serial printer, or modem.

serial printer

A serial printer is a **printer** connected to the computer with a serial connection.

shell

The shell represents your working environment and how you interact with the operating system. Your shell is reflected by what you see after you log into the system. If you see a \$, #, or % prompt, and you have not changed the default prompt string, your shell is one of the programmer's shells. See also **programmer's shell**.

single-user mode

A system run level that allows the system administrator to perform administration tasks while limiting access to the system. Other users cannot log in while the system is in this mode.

Glossary

slice

A slice is a unit of disk partitioning. Disks are divided into slices. See also **partition**.

sockets link

A link established between two processes to exchange information. One possible use is to establish a link between mail processes.

spooler

The spooler queues print requests and sends them to the printer.

stop bits

Stop bits are used to inform the system when one character ends and the next one begins.

superblock

A set of information describing the file system located in the current partition. The superblock is always located in slice 0 (the first slice) of the partition containing the file system it describes.

superuser

The superuser has the privilege to act as root. The superuser acquires complete access to the system by giving the system the root password and entering superuser mode. The superuser may turn the system on or off, view any file on the system, or reconfigure the system.

swap space

Area of memory used by the **memory** management system. This consists of the **main swap partition** and any **add-on swap space**.

T**TCP/IP**

Transmission Control Protocol/Internet Protocol. TCP is a transparent level, connection-orientated protocol, that provides reliable end-to-end message transmission over an internetwork.

terminal download image

A terminal download image is the software necessary to operate a PT or GT on a cluster **channel** or in RS-232 download mode.

TLI link

Transport Layer Interface link. A link that provides services for the transport of data between **network** elements, for example between hosts. One use of TLI is to enable systems to exchange mail.

telephone link

A telephone link is a method used by the electronic mail system to exchange mail over telephone lines. See also **modem** and **dialing sequence**.

troubleshooting

The act of isolating and correcting problems (problem solving).

U**unadvertise**

Unadvertising is the process by which a **resource** is removed from the local **advertise tables**, thereby making it inaccessible to other host computers. A resource can be unadvertised by calling the **unadv** command.

UNIX

A multiuser, multitasking operating system which can run on a wide variety of computer systems.

unmount

the reverse of mount.

Glossary

user equivalent

Condition where a specific remote user is allowed the same permissions as a specific local user.

UUCP

UNIX to UNIX copy. This process is used to send information from one unix system to another unix system.

V

volume

A peripheral storage unit, such as a hard disk, or tape cartridge.

volume home block

A set of information describing the structure of this volume. The volume home block is always located in slice 0 (the first slice) of the first partition of volume it describes.

W

wild card

A wild card is a character used by your shell for pattern-matching in file searches. When a wild card is used in a file name, the system searches for all files that match the characters in the file name except the wild card. For example, if you want to print all the files that have the characters tmp without listing each one individually, you could instruct the system to print ***tmp*** and it would print **today.tmp**, **tmp.old**, and **thistmp**, for example. The asterisk wild card (*) matches any number of characters; the question mark (?) wild card matches one character.

window

A window represents the information displayed on the screen for a particular function.

X

XON/XOFF handshaking

XON/XOFF handshaking is a type of protocol between a device and the S/Serial system: the device sends a special character to inform the computer when the computer should stop sending data and when it should restart. XON/XOFF handshaking is required because devices cannot output as fast as the computer can send them information.

—

—

—

Index

/dev/dsk/c#d##s# 5-27
/dev/rdisk/c#d##s# 5-27
/etc/checklist 5-27
/etc/fstab 5-27
/etc/fumount 11-39
/etc/fuser 11-39
/etc/group 2-13
/etc/hosts.equiv 10-25
/etc/hosts 8-6, 10-25
/etc/inetd.conf 10-13, 10-25
/etc/inittab 7-21
/etc/log/confile 3-11
/etc/master 11-40
/etc/mountd 12-19
/etc/networks 10-25
/etc/passwd 2-13
/etc/protocols 10-25
/etc/rcopts/KSCSI 6-10
/etc/rcopts/LP 8-21
/etc/rcopts/NODE 9-14
/etc/riop/rtab 7-21
/etc/rmount 11-40
/etc/shadow 2-13
/etc/system 6-10
/etc/ttytype 7-22
/inetd 10-13
/install/RiopRel 7-14
/tmp 4-21
/unix 5-2
/usr/adm/acct 3-11
/usr/adm/sa 3-11
/usr/bin/passmgmt 2-13
/usr/bin/pwconv 2-13

Index

- `/usr/bin/unpwconv` 2-13
- `/usr/hosts/loopback` 10-25
- `/usr/lib/adman/compexcl.l` 4-21
- `/usr/lib/adman/incexcl.l` 4-21
- `/usr/lib/adman/lastcomp` 4-21
- `/usr/lib/adman/lastinc` 4-21
- `/usr/lib/adman/logxx` 4-20
- `/usr/lib/uucp/Devices` 9-14
- `/usr/lib/uucp/Dialers` 9-14
- `/usr/lib/uucp/Permissions` 9-15
- `/usr/lib/uucp/Systems` 8-6, 9-15
- `/usr/spool/lp/model` 8-21

A

- `accept` 8-20
- access modes A-7
- `acct` 3-10
- add a printer 8-4
- add a SCSI tape drive 6-4
- Adding A System to an Existing Domain 11-11
- Adding an Entry for a Primary from a Different Domain 11-17
- adding groups 2-7, 13-5
- adding printers 8-11
- Adding Secondary Name Servers 11-20
- adding tape drives 6-5
- adding users 2-5, 13-4
- Additional Domain Configuration Functions 11-16
- `adman` 11-1, 12-1
- `adman` 1-1
- Admin Mode 5-26
- administration
 - disk 5-1
 - file system 5-1
 - printers 8-1
 - system backup 4-1
 - system restore 4-1, 4-11

- system status 3-1
- tape drives 6-1
- terminal 7-1
- user 2-1, 10-1
- user problems 13-4
- UUCP 9-1
- administrator 11-5
- advertise 11-3
- Advertising Your Resources 11-29
- asterisk 1-10

B

- Back-Tab** 1-13
- backups 4-1
 - accidental interruption 13-7
 - complete 4-4
 - contents unreadable 13-8
 - failed messages 13-7
 - function of 4-3
 - incremental 4-6
 - maintenance 4-10
 - overwriting tapes 13-7
 - partial 4-7
 - problems 13-6
 - scheduling of 4-3
 - status messages 4-9
 - tapes 4-11
 - viewing contents of 4-13
 - user 4-8
- barring users 2-12, 13-5
- baud rate 7-8
- blocks 5-2
 - logical 5-2
 - physical 5-2
- boot device 5-2

Index

C

- cancel** 8-20
- change mode A-8
- changing passwords 2-4, 2-9
- changing user information 2-8
- Changing Your RFS Password 11-36
- channels 7-1, 7-11, 8-10
- cluster boards 7-1
 - tuning 7-1
- cluster devices
 - configuring of 7-10
- cluster lines
 - configuring of 7-10
 - enabling of 7-17
- cluster ports 7-1
- cluster terminals 7-1, 7-12
- communication links 9-6
- Completing the Addition: Non-Primary Administrator Procedures 11-13
- connectors 8-10
 - determining correct 7-6
- console
 - resetting of 3-8
- console log 3-6
 - monitoring of 3-6
 - viewing contents 3-7
- controllers 5-1
 - SMD 5-1
 - ST506 5-1
- cpio** 4-20
- CPU
 - main 7-3
 - S/80 7-5
- Creating a New Domain 11-6
- CTIX operating system A-1 to A-2
- cursor control 1-10, 1-13 to 1-14

D

- daemons** 10-12
- default** 2-5
 - home directory 2-7
 - remote login 9-4
 - swap space 5-20
- default printer** 8-3
- default values** 1-10
- Deleting a Specific System from Your Domain** 11-22
- Deleting All Systems from Your Domain** 11-23
- deleting users** 2-10 to 2-11, 13-5
- destination** 8-1
- df command** 13-25
- direct links** 9-7
- directories**
 - /bin** A-5
 - /dev** A-5
 - /etc** A-5
 - /u** A-5
 - /usr** A-5
 - home A-4 to A-5
 - root A-5
- directory structure** A-3 to A-4
- disable** 8-20
- disabling a login** 7-1
- disk description** 5-3
- disks** 5-1
 - administration 5-1
 - administration problems 13-14
 - configuring 5-5
 - distinguishing between 5-8, 5-17
 - number of partitions 5-2
 - on board 5-1
 - problems 13-14
 - SCSI 5-1
 - SMD 5-1
 - ST506 5-1

Index

- swap space 5-3
- system 5-2, 5-4, 5-20
- viewing description of 5-3, 5-5
- Displaying the Current Primary Name Server 11-38
- download
 - how to D-1
- download images 5-4
- drops 7-10 to 7-11
- du command 13-25

E

- electronic mail
 - adding entries 9-4
 - administration 9-1
 - networks 9-1
 - phone links 9-12
 - remote systems 9-1
- emulation mode D-1
- enable** 8-20
- enabling a login 7-1
- entries
 - changing of 9-11
 - deleting of 9-12
- equivalent machines
 - adding 10-11
 - deleting 10-12
- equivalent users
 - adding 10-9
 - deleting 10-10
- error log 3-4
 - resetting of 3-6
- error messages
 - how to proceed 5-8, 5-17
 - VHB unreadable 5-8, 5-17
- error report
 - detailed 3-5

- summary of 3-4
- Ethernet Combo boards 7-6
- Ethernet links 9-7
- exiting 1-6
- export 12-3
- Exporting Your Resources 12-13

F

- fields 1-1
 - edit 1-10
 - menu 1-10
 - multi selection menu 1-10
 - text 1-11
- file system administration 5-19
- file systems 5-2
 - administration 5-1
 - checking program 5-26
 - mounting of 5-2
 - orphaned 5-12
 - out of space 13-6
 - problems 13-14
 - structure of A-3
- find** 4-20
- fingerd** 10-14
- forms 1-1
 - moving between 1-8
 - moving within 1-8
 - selecting of 1-8
- fsck** 5-26
- fsstat** 5-26
- ftpd** 10-13
- fuser** 5-20

Index

G

- groups
 - adding of 13-5
- GT 5-4
 - downloading D-1
 - modes D-1

H

- hardware inventory 3-2
- help 1-7
- hinv** 3-10
- home directory 2-3
 - default 2-7
- host entries 10-16, 10-18
 - adding 10-16
 - changing 10-18
 - deleting 10-18
- hosts 9-1, 10-2
 - database 10-2
 - entries 10-2
 - host name database 10-16
 - host name resolution 10-16
- how to reboot 7-18

I

- I/O expansion boards 7-5 to 7-6
- inetd** 10-13
- Internet address 10-16
- Interrupt** 1-16
- iv -d** 5-9
- iv -u** 5-9

K

- kernel 5-8, 5-17, 7-1
- keyboards 1-11
 - PT 1-13, D-3
 - TO-250 1-13
 - TO-300 1-13
- keys
 - a-z 1-15
 - Backspace** 1-14
 - Back** 1-14
 - Cancel** 1-6, 1-15
 - control sequence 1-16
 - Control** 1-16
 - Delete Character** 1-14
 - Down** 1-14
 - Enter** 1-15
 - Exit** 1-15
 - Forward** 1-14
 - Help** 1-16
 - moving cursor between fields 1-13
 - moving cursor within fields 1-14
 - Page** 1-16
 - performing an action 1-15
 - performing other movements 1-16
 - Return** 1-14
 - Roll Down** 1-17
 - Roll Up** 1-17
 - Shift-Page** 1-16
 - Tab** 1-13
 - Up** 1-14

L

- labelit 5-11
- line printers 8-1
- Listing Secondary Name Servers 11-19
- load 10-5

Index

- login 2-3
- logins
 - cluster terminals 7-12
 - serial 7-2, 7-9
- lp**
 - status incorrect 13-10
- lpmove** 8-20
- lpsched** 8-20
- lpshut** 8-20
- lpstat** 8-21
- lp** 8-1
 - scheduling 8-15
 - starting 8-15
 - stopping 8-15
 - status 6-3, 8-3

M

- mail systems
 - adding entries 9-4
- mailx** 9-15
- mail** 9-15
- main menu 1-6
- main processor 7-3
- Managing Secondary Name Servers 11-19
- Mapping or Excluding Users and Groups 11-33
- maximum transmission unit 10-20
- mbufs 10-23
- menus 1-1
 - backup and restore 4-2
 - console log functions 3-6
 - disk and file system administration 5-3
 - error log functions 3-4
 - moving between 1-8
 - moving within 1-8
 - network administration 10-5
 - pop-up 1-10

- printer administration 8-2
- SCSI tape drive administration 6-2
- selecting of 1-8
- system status 3-1
- terminal administration 7-2
- user administration 2-2
- UUCP administration 9-2
- mkfs** 5-26
- models 8-8
 - selecting of 8-8
- modems 9-8
 - adding to a port 9-12 to 9-13
 - deleting from a port 9-14
- modes
 - administrative 5-26
 - multi user 5-16
 - read-only A-6
 - run level 5-16
 - single user 5-7
 - superuser A-6
 - terminal D-1
 - emulate D-1
 - RS-232 D-1
 - RS-422 D-1
 - viewing of A-8
- monitoring system 3-1
- mount 11-3, 12-3, 13-19
- mount** A-3
- mount path 5-19
- mount point 5-2, 5-11
- Mounting Remote Resources 11-32, 12-16
- mount** 5-2, 5-27
- moving
 - between fields 1-13
 - between forms and menus 1-8
 - cursor 1-13 to 1-14
 - within forms and menus 1-8
- Mtu 10-20

Index

N

- neighboring domains 11-17
- netstat** 10-26
- network administration 10-5
- network services
 - adding 10-12
 - descriptions 10-13
 - full list 10-13
 - security 10-12, 10-14
- networks 9-1, 10-2
 - administration of 10-9
 - host address 10-16
 - host entries 10-2
 - host name 10-16
 - host name resolution 10-16
 - hosts 10-2
 - I/O packets 10-20
 - Internet address 10-16
 - machine status 10-5
 - memory requests 10-23
 - security risks 10-9
 - servers 10-12
 - services 10-12
 - statistics 10-5, 10-19
 - active connections 10-19
 - interface 10-20
 - memory usage 10-23
 - protocol 10-23
 - routing tables 10-21
 - users statistics 10-7
- NFS 12-1
 - devices 12-1
 - directories 12-1
 - export 12-2
 - files 12-1
 - hard-mounted files 13-19
 - network 12-2

soft-mounted files 13-19
troubleshooting 13-21, 13-23
NFS Administration Procedures 12-3
node name 9-4 to 9-5
nodes 10-7
nuucp 9-4, 9-9

O

operating system A-1
ouucpd 10-13

P

partitions 5-1
 boundaries 5-6
 configuring 5-5
 creating 5-12
 determining uses 5-17
 raw 5-9, 5-18
 removing overlapping 5-9
passwd 2-13
passwords A-6
 changing of 2-4, 2-9
pathname 2-7, 5-19, A-4
phone links 9-8, 9-12
PID 7-18
pop-up menus 1-10, 7-8
ports 7-1, 8-10
 adding a modem to 9-12 to 9-13
 cluster 7-1
 deleting a modem from 9-14
 determining type 7-8
 enabling of 7-1
 serial 7-1
 disabling of 7-9
 enabling of 7-2, 7-8

Index

- numbering of 7-20 to 7-21
- viewing status of 7-18
- print system
 - scheduling 8-15
 - starting 8-15
 - stopping 8-15
 - status 8-3
- printer administration
 - problems 13-10
- printer description files 8-16
- printer models 8-8, 8-16
 - making of 8-16, 8-18
 - selecting of 8-16
 - serial 8-17
- printers
 - adding of 8-4, 8-11
 - administration of 8-1
 - changing status of 8-13
 - connecting of 8-10, 8-17
 - connections 8-5
 - default 8-3, 8-15
 - jobs 8-4
 - models 8-8
 - names 8-7
 - parallel
 - connecting of 8-5
 - printing failure 13-10 to 13-12
 - problems 13-10 to 13-11
 - queue 8-4
 - redirecting jobs 8-14
 - remote
 - connecting of 8-6
 - remote access of 10-10
 - removing of 8-14
 - requests 8-4
 - self test 8-5
 - serial
 - connecting 8-6

setting default 8-15
status 8-2
testing 8-13
privileges A-6
 execute A-8
 group A-7
 other A-7
 read A-7
 user A-7
 write A-8
process accounting
 disabling of 3-9
 enabling of 3-9
 monitoring of 3-9
process identification number 7-18
processor boards 6-5, 8-10
processors
 determining correct 7-3
 main 7-3
programmers shells A-2
protection A-6
PT 5-4
 downloading D-1
 modes D-1

Q

QIC tape 4-1
 installation 4-6
 write protect arrow 4-5
queue status
 incorrect 13-10

R

rcmd 8-6
re-admitting users 2-12

Index

- readmitting users 13-6
- rebooting 7-18
- redirecting print jobs 8-14
- Registering a System On the Primary: Primary Administrator Procedures 11-11
- reject** 8-21
- remote entries
 - deleting of 9-12
- remote I/O processor 7-1
- remote systems 9-2 to 9-3
 - adding entries 9-4
 - changing of 9-11
 - direct links 9-7
 - Ethernet links 9-7
 - listing of 9-1
 - modems 9-8
 - networks 9-1
 - phone links 9-8
- Removing an Advertised Resource 11-31
- Removing an Exported Resource 12-14
- removing overlapping partitions 5-9
- Removing Secondary Name Servers 11-21
- removing users 2-10 to 2-11
- renaming your system 9-4
- resources 11-3
- restores
 - accidental 13-8
 - complete 4-14
 - failed message 13-9
 - function of 4-12
 - incorrect 13-8
 - partial 4-15
 - problems 13-8
 - status messages 4-19
- rexecd** 10-14
- RFS 11-1
 - advertise 11-1
 - devices 11-1
 - directories 11-1

- domain 11-2
- files 11-1
- network 11-1
- Primary Name Server 11-2
- secondary name server 11-2
- troubleshooting 13-17
- RFS Administration Procedures 11-3
- RIOPs 7-1
 - channel numbers 7-6
 - configuration example 7-15
 - connecting of 7-5
 - unique ID 7-13
- rlogind** 10-13
- root** A-5 to A-6
- routes 10-21
- routing tables 10-21
- RS-232
 - mode D-1
 - port 7-1
 - terminals 7-1
- RS-422
 - mode D-1
 - port 7-1
 - terminals 7-1
- rshd** 10-13
- ruptime** 10-25
- rwhod** 10-13
- rwho** 10-26

S

- S/640
 - rear inside view 7-3
- S/80
 - CPU 7-5
 - port numbers 7-6
- sar** 3-11

Index

screens

- adding users 2-6
 - changing passwords 2-4
 - configure a disk 5-10
 - configure cluster lines and devices 7-16
 - confirm adding remote system 9-10
 - disk description 5-5
 - disk usage 5-23
 - display of other systems 9-3
 - hardware inventory 3-2
 - layout 1-9
 - Ip status** 8-3
 - make a printer model 8-19
 - network interface activity 10-20
 - network protocol statistics 10-24
 - network routing tables 10-22
 - network users 10-8
 - partial restores 4-18
 - print system status 8-3
 - proposed state of the disk 5-10
 - remote machine statistics 10-6
 - SCSI Tape Changing Entry Screen** 6-7
 - SCSI Tape Connection Information Screen** 6-5
 - SCSI Tape** status 6-3
 - Select a SCSI Tape to Delete Screen** 6-9
 - serial printer and connector information 8-9
 - terminal and connector information 7-7
 - user list 2-3
 - view port status 7-19
 - view tape contents 4-14
 - view/change partition uses 5-19
 - viewing only 1-11
- SCSI 5-1
- SCSI Tape
- changing entry information 6-8
 - connection information 6-6
 - deleting a SCSI tape 6-9
 - status 6-3

- SCSI tape drive
 - adding of 6-4
 - testing 6-7
- SCSI tape drives
 - deleting 6-8
- scsimap** 6-10
- security 2-1, 2-7, 2-9, 9-4
- Security 11-2
- security A-5 to A-8
- serial logins 7-2, 7-9
- serial ports 7-1
- serial terminals 7-1
- Set Up Your Machine to Run RFS 11-4
- Sharing Resources 11-26, 12-9
- shells 2-3, A-1
 - C A-2
 - default 2-4
 - designations 2-4
 - System V A-2
- slice 13-19
- slices 5-1
- slots 7-5
 - numbering of 7-5
- SMD 5-1
- ST506 5-1
- Starting and Stopping RFS 11-23
- super service 10-13
- superuser mode 1-5, A-6 to A-7
- swap 5-3
 - add on 5-20
 - calculating 5-20
 - main 5-20
- swap** 5-27
- system
 - monitoring status of 3-1
 - console log 3-6
 - error log 3-4
 - hardware inventory 3-2

Index

- process accounting 3-9
- system activity 3-8
- system activity reporting
 - disabling of 3-8
 - enabling of 3-8
- system backups
 - problems 13-6
- system disk 5-2, 5-20
- system restores 4-1
 - problems 13-8
- system status
 - problems 13-6

T

- talkd** 10-14
- tape drive
 - adding of 6-5
 - self test 6-5
- tape drives
 - administration of 6-1
 - status 6-2
- tape drive** 6-1
- tapes 4-11
 - viewing contents of 4-13
- tapeset** 6-10
- telephone links
 - nonfunctioning 13-15
- telinit** 7-22
- telnetd** 10-13
- terminals
 - administration 7-1
 - cluster 7-1
 - download images 5-4
 - dumb** 5-4, 7-8
 - enabling of 7-12
 - graphic 5-4

- intelligent 5-4
- keyboards B-1
- problems 13-9
- programmable 5-4
- serial 7-1
- unable to log in 13-9
- ftpd** 10-14
- tracks 5-1
- Transparency 11-2
- troubleshooting 13-1
 - NFS 13-19
 - preventive maintenance 13-24
 - RFS 13-17, 13-19
- tuning cluster lines 7-10

U

- Unmounting Remote Resources 11-33, 12-17
- usage
 - adman** 1-1
 - nonprivileged functions 1-4
 - user accounts
 - listing of 2-2
 - user administration 2-2
 - problems 13-4
 - user modes A-7
 - user restrictions 2-9
- users
 - accidental deletion of 13-5
 - adding of 2-5, 13-4
 - backups of 4-8
 - barring of 2-12, 13-5
 - changing information of 2-8
 - deleting of 2-10 to 2-11, 13-5
 - re-admitting of 2-12
 - readmitting of 13-6
 - removing of 2-10 to 2-11

Index

- restricting of 2-9
- uucp**
 - problems 13-15
- UUCP administration 9-1
 - node name 9-4 to 9-5
 - problems 13-15
- uucpd** 10-14
- uucp** 9-15
 - phone links 9-12
- uux** 8-6

V

- vertical scroll bar 1-11
- VHB 5-8
- Viewing Advertised Resources 11-28
- Viewing Exported Resources 12-11
- Viewing Mounted Remote Resources 11-28, 12-11
- Viewing the Remote Resources You Can Use 11-28, 12-12
- VME 5-1

W

- who** 10-7
- wild cards 4-16