HP FTAM/9000 User's Guide

Edition 4

B1033-90024
HP 9000 Networking
E0597

Printed in: U.S.A.

Legal Notices

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

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

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

Restricted Rights Legend. Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

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

Use of this manual and flexible disk(s) or tape cartridge(s) supplied for this pack is restricted to this product only. Additional copies of the programs may be made for security and back-up purposes only. Resale of the programs in their present form or with alterations, is expressly prohibited.

Printing History

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

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

First Edition: April 1991 (HP-UX Release 8.0)

Second Edition: November 1992 (HP-UX Release 9.0)

Third Edition: January 1995 (HP-UX Release 10.0)

Fourth Edition: May 1997 (HP-UX Release 10.30)

Preface

Purpose

This guide provides the information you need to use HP FTAM/9000 interactively.

This guide does not supply information for installing or configuring HP FTAM/9000 on your local system. For that information, refer to the Installing and Administering HP FTAM/9000 manual.

NOTE

This guide assumes that HP FTAM/9000 is correctly installed and configured for use. This includes locally configuring the address and alias of each remote host you need to work with.

This guide also does not supply information for programmatic use of FTAM. For programmatic use, refer to the *HP FTAM/9000 Programmer's Guide* (B1033-90014) and the *HP FTAM/9000 Reference Manual* (B1033-90004).

Audience

Both new and experienced users of FTAM will want to use this manual to make full use of FTAM features.

New FTAM programmers may also want to review chapter 5 to learn the basic concepts of file protection under FTAM. Programmers will also want to refer to the *HP FTAM/9000 Programmer's Guide* and the *HP FTAM/9000 Reference Manual* for detailed programming information.

Terms

The following terms are used in this guide:

Initiator	The person, process, or system that requests an FTAM transaction is called the initiator.
Responder	The process or system to which an FTAM request is directed is called the responder.
Shadow file	Every HP FTAM/9000 file has an associated shadow file, which contains attribute information not stored by the HP- UX file system.
Local host	The system you are logged into is the local host.
Remote host	Every system on the network (except the local host) is a remote host.
Access control	FTAM provides additional access control mechanisms over those inherent in HP–UX. FTAM access control governs the actions that are permitted on a file, granting different users different subsets of the available actions.
Concurrency control	Concurrency control governs whether and how multiple users can access the file. This helps maintain data integrity.
Connection	FTAM transactions between different hosts require a connection between the hosts. This connection is analogous to a telephone connection, over which two people can communicate.
File store	Every computer system has a system for storing information, which is called its file store. Different systems use different file stores, depending on the vendor and model.
Virtual File Store	FTAM defines a generic, abstract file store, which is shared by all FTAM implementations. This generic file store is called FTAM's Virtual File Store, or VFS .

Conventions

The table below explains the typographic conventions used in this manual.

Notation	Description
`computertext` or **`computertext`**	Computer font is used for on-screen prompts and messages, for responses to user commands, and what you type in.
Boldface	Boldface type is used when a term is defined.
italics	Italic type is used for emphasis and titles of manuals and publications, and to represent a variable in a syntax statement, such as *target_file*.
[ ]	An element inside brackets in a syntax statement is optional. When elements inside brackets are separated by a vertical bar (|), you can select any one or none of these elements; vertical bars are omitted for multiple command options.
. . .	A horizontal ellipsis in a syntax statement indicates that a previous element may be repeated. For example: [*options*][*filename*]...
Key	This font is used to indicate a key on the computer's keyboard. When two or more keys appear together with a dash between them, such as **CTRL-C**, press those keys simultaneously to execute the command. Note that most user commands end with an implied **Enter** or **Return** keystroke. If there is no user entry at a prompt, the **Enter** or **Return** key indicates that no other keys are pressed.

Contents

Contents

Contents

Contents

1 A Foundation for Using FTAM

Computer networks rank among the most complex systems ever invented. These networks are especially complex when they involve systems from many different computer manufacturers. To make multi-vendor networks feasible, the Open Systems Interconnection (OSI)

Reference Model has been adopted by many computer manufacturers. The OSI Reference Model identifies many different aspects of intercomputer communication.

The FTAM (pronounced *eff' • tam*) service was defined by the International Organization for Standards (ISO). FTAM conforms to the OSI reference model.

The FTAM acronym stands for File Transfer, Access, and Management. You will usually use FTAM as a file transfer service. However, FTAM also allows you to access (read) and manage (delete) remote files.

The next section introduces you to the HP-UX implementation of FTAM.

HP FTAM/9000

The HP-UX FTAM product has three complimentary interfaces:

- **Interactive**. This is described in Chapter 2, “Using Interactive FTAM.”
- **Command-line**. This is described in Chapter 3, “Using Command-Line FTAM.”
- **Programmatic**. This is described in the *HP FTAM/9000 Programmer's Guide.*

Interactive FTAM

You use HP-UX FTAM interactively by entering the ftam command at your system prompt:

```
$ ftam
```

This command starts an interactive session with FTAM, which lasts until you return to the system prompt by entering bye at the ftam> prompt:

```
ftam>bye
```

The interactive interface to HP-UX FTAM is patterned after a similar ARPA networking service called ftp. Interactive FTAM is covered in Chapter 2, “Using Interactive FTAM.” When you need to perform several file transfers, or when you need to manipulate remote directories, the ftam interactive interface is a good choice.

Command-Line FTAM

There are several FTAM commands you can enter at the system prompt. These commands allow you to transfer or manage remote files without entering an interactive ftam session. This is an example of an FTAM command called fcp, used at the system prompt:

```
$ fcp FY91data chicago:FY91
```

This example copies FY91data to a host called chicago, where its name is FY91.

The command-line interface to HP-UX FTAM is patterned after a similar ARPA networking service called rcp. Command-line FTAM is covered in Chapter 3, “Using Command-Line FTAM.” For simple file transfers, command-line FTAM is frequently the best approach.

Programmatic FTAM

This interface is for programmers only. It is used to develop applications that use FTAM services during their execution. The programmatic FTAM interface comes from the Manufacturing Automation Protocol (MAP), an industry-defined protocol specification that includes FTAM. It is extremely flexible, and is rather complex because it exposes all the features of FTAM.

Programmatic FTAM is described in a separate manual, the *HP FTAM/9000 Programmer's Guide*. Only experienced programmers will be interested in programmatic FTAM .

2 Using Interactive FTAM

This chapter describes how to use the ftam program to transfer, access, and manage files. This program transfers files between hosts (both UNIX [1]–based and other systems alike) that support FTAM services. It can also be used to perform remote file management operations.

The ftam program is patterned after ftp, an Internet service that allows you to copy files between hosts on a network. Note, however, that there are differences between ftp and ftam , such as changing file attributes, and optional directory support. These differences will be apparent to users already familiar with ftp.

1. UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Limited.

Chapter Overview

This chapter describes how you can use the ftam program to do the following:

- Establish, end, and manage ftam sessions.
- Get help with ftam.
- List, create, and remove remote directories.
- Perform file transfers over the network.
- Delete FTAM files.

Basic Steps for Using ftam

A typical ftam session consists of the following steps:

1. Invoke ftam.
2. Get connected to the remote host.
3. Use ftam commands.
4. End the ftam session.

This section describes steps 1, 2, and 4. Step 3 is covered in later sections of this chapter, titled “Managing an ftam Session,” “Performing Remote Directory Operations,” “Performing Local Operations,” and “Performing File Transfers.”

Step 1: Invoking ftam

You start a session by entering ftam at your system prompt. This command initiates an interactive session with the ftam program. The system prompt is replaced with the ftam program prompt:

```
$ ftam
ftam>
```

After the ftam prompt appears on your screen, you enter various commands to establish connections, transfer files, read directories, and control the behavior of the ftam program itself.

Step 2: Connecting to the Remote Host

Use the open Command

To interact with a particular remote host, enter the open command followed by the name of the host to which you want to connect, as shown here:

```
$ ftam
ftam> open chicago
```

This tells ftam you want to be connected to the remote host chicago.

Provide Login Information to the Remote Host

For security reasons, you must provide valid login information for the remote host you specified in step 2. At the prompts that ftam provides, you must supply the remote host with a login name and password it recognizes.

The following example illustrates these steps. Alan Martin starts an ftam session, requests a connection to the remote host chicago, and logs into the remote host with his name and password:

```
$ ftam
ftam> open chicago
Username (chicago:alan): amartin
Password (chicago:amartin):
Connected to chicago as user amartin.
ftam>
```

(Alan's password is not echoed to the screen.)

Notice the part of the Username and Password prompts in parentheses. This part of the prompt has this form:

(hostname : username)

The *hostname* is the name of the remote host you want to connect to. The *username* is the login name of the user who is invoking ftam. Interactive FTAM provides you this information to help you understand what data it is using as it establishes the connection.

Unless you specify otherwise at the Username prompt, a remote host will use your local login name [1]. Notice in the above example that the Username prompt shows alan as the current user. Because his response to the first prompt is amartin, the prompt for Password uses amartin as the username.

To save time, you can specify the name of the host to which you want to connect when you first invoke ftam. For example, the following command, issued at the system prompt, bypasses the need to use ftam's open command :

```
$ ftam chicago
Username (chicago:alan): amartin
Password (chicago:amartin):
Connected to chicago as user amartin.
ftam>
```

Alan's password is not echoed to the screen.

---

1. Using an FTAM startup file can give you a different default. See “Streamlining ftam with a Startup File” later in this chapter.

To make login even easier, you can create a special FTAM–related file called.ftamrc in your home directory. This file is used to automate the login procedure. See “Streamlining ftam with a Startup File” later in this chapter.

Set a Default Working Directory (Optional)

The default working directory for the remote host is assigned by the remote FTAM implementation. If the remote responder is HP-UX FTAM, the default directory is the “home” or default directory for the login used in the previous step.

If you want to change the current default to a different directory, use ftam's cd command. The cd command is described in more detail later in this chapter.

The following example illustrates all the steps Alan uses to start up an ftam session with a remote HP-UX host, including setting his working directory:

```
$ ftam
ftam> open chicago
Username (chicago:alan): amartin
Password (chicago:amartin):
Connected to chicago as user amartin.
ftam> cd /users/management/amartin/salaries
/users/management/amartin/salaries is the current working
directory
ftam>
```

Alan's password is not echoed to the screen.

Step 3: Using ftam Commands

Using ftam commands is the topic of all sections in this chapter that follow step 4.

All FTAM commands can be abbreviated to include just enough characters to uniquely identify the command you want to execute. For example st is a valid abbreviation for status, and g is a valid abbreviation for get.

Step 4: Ending an ftam Session

To close the current ftam connection, but remain in ftam, enter close at the ftam prompt. If you want, you can then use the open command to open a connection to a different remote host.

```
ftam> close
Released connection to denver.
ftam> open madrid
```

To end an ftam session altogether and return to your system prompt, enter quit at the ftam prompt.

```
ftam> quit
Released connection to denver.
$
```

Obtaining Help

To get a complete list of all the ftam commands, enter ? at the ftam prompt. To get help about a specific ftam command, enter ? followed by the ftam command. For example:

```
ftam> ?
```

or

```
ftam> ? open
```

Notes About Remote File and Directory Names

Note the following important points about remote file names:

- Directory names are legal only in ls, dir, and cattr commands. Directory names are not legal as source or destination file names.
- Wildcard characters are not legal. This applies to both source and destination names.
- Remote file names must be specified with the native syntax, notation, and conventions of the remote host. FTAM cannot translate or negotiate file names between different hosts, so any name you provide has to be valid on the system that uses it.
- All names are relative to the remote working directory, unless you provide an absolute pathname for a file or directory (in whatever way the remote system defines “absolute pathname”).

- The initial remote working directory for file transactions is determined by the FTAM implementation on the remote host. HP FTAM/9000 responders set the initial working directory to be the home directory for the user noted in the “Connected to ...” message during ftam startup (See “Step 2” in the previous discussion). Other (non-HP-UX) FTAM implementations are apt to use different conventions.

Managing an ftam Session

This section discusses how to use ftam commands to control various aspects of your ftam session. Table 2-1 explains the session-control commands you can use at the ftam> prompt :

Table 2-1 Commands for Controlling Your ftam Session

Command	Function
`bell`	When bell is on, a bell (or beep) sounds after each file transfer. Enter bell at the ftam prompt to toggle the bell setting.
`bye` or `quit`	Terminates your ftam session.
`close` or `release`	Terminates the connection to the current remote host.
`connect` [*hostname*] or`open` [*hostname*]	Establishes a connection to a remote host. If you do not specify a host, ftam prompts for one. Example: `ftam> connect denver`
`help` [*command*] or`?` [*command*]	Requests help for using ftam. If you specify a command, the help you receive is specific to that command. Example: `ftam> help open`
`status`	Requests a summary of the current status of ftam, including the current host, the local and remote (if known) working directories, bell mode, overwrite mode, verbose mode, and filestore.
`set` *options*	Set FTAM parameters. Valid options are:`f` specifies the remote filestore type (`f ux` or `f other`).`o` controls overwrite mode.`v` controls verbose mode.`y` satisfy file protection on destination file.`z` satisfy file protection on source file. Specifying `f ux` means that HP-UX (UNIX) conventions in path names (such as "." and "..") are valid on the remote file system. The default is "ux". The `y` and `z` options require an action/ concurrency string as a parameter. See chapter 5 for details.
`unset` *options*	Unset file (y and z) options. See set command (above).
`user` *user* [*password*] [*account*]	Reconnect to the current remote host as *user*. If you omit the password (and it is not available in your .ftamrc file), ftam will prompt you for it.

Example:

You can display the status of your local ftam settings by entering status at the ftam prompt. The display will show you the activated commands as well as the remote host.

This example shows a simple ftam session during which Sue modifies some local settings using the bell and prompt commands before transferring files.

```
$ ftam denver
Username (denver:sue): sue
Password (denver:sue):
Connected to denver as user sue.
ftam> status
Connected to denver as user sue.
Verbose mode on.
Bell mode off.
Filestore is ux.
Overwrite mode on.
Current working directory is /users/sue
Name of default working directory on denver is unavailable
ftam> set f other
Filestore is other.
ftam>
```

Sue establishes a connection to denver

She checks her local settings with the status command. The response shows Sue that she is connected to denver, and the status of various FTAM parameters. She then uses the set command to tell FTAM that the remote host has a file system unlike that of HP-UX.

Making ftam More Informative

You can obtain more detailed error information from ftam by using a command-line option when you start ftam. The option is described in Table 2-2:

Table 2-2 Command Line Option to Make ftam Responses More Informative

Option	Description
-v	Causes ftam to start up in verbose mode (see the -v option under `set` in Table 2-1). By default, verbose mode is off when you do not specify this option. Example: `$ ftam -v chicago`

Performing Remote Directory Operations

The ftam program allows you to manipulate the remote host's file system. You can change your current working directory at the remote host; delete, rename, and change the attributes of remote files; and create, rename, and delete directories on the remote host (however, see the following section on directory support). Table 2-3 lists commands that allow you to work with remote files. See "Notes About Remote File and Directory Names" earlier in this chapter for guidelines on specifying remote names.

The exact effect of the commands in Table 2-3 may depend on the level of support the responder provides for directories. See "Directory Support in FTAM Implementations" later in this chapter.

Table 2-3 ftam Directory Operations Commands

Command	Function
`pwd`	Prints the name of the current remote working directory. The resulting name uses the syntax and conventions of the remote host. Example: `ftam> pwd`
`cd` *directory*	Changes the current remote working directory. This example shows proper syntax for a remote HP-UX host. Example: `ftam> cd project7/datafiles`
`ls` [`-a`] [*name*] [*file*]	If the name argument is a directory, ls lists the files it contains; the default is the remote working directory. If the name argument is a file, ls displays the file name if it exists. If the file argument is given, the output from the command is placed in a file by the specified name.The -a option generates a complete listing of all the FTAM attributes of the file or files (see example following this table).

Command	Function
`dir` [*name*] [*file*]	If the name argument is a directory, dir shows a "summary" listing of the files the directory contains; the default is the remote working directory. If the name argument is a file, dir displays a summary listing of the file if it exists. If the file argument is given, the output from the command is placed in a file by the specified name. The listing includes the file name(s), and several important attributes for each file (see example following this table).
`rename` *from to*	Changes the name of a remote file. Example: `ftam> rename tmp1 save`
`delete` *file*	Removes a remote file. Example: `ftam> delete junkfile`
`mdelete` *files* (Multiple-delete)	Removes multiple remote files. "Wildcard" file specification is not allowed. Example: `ftam> mdelete tmp1 tmp2`
`mkdir` *directory*	Creates a directory on the remote host. Example: `ftam> mkdir newdir`
`rmdir` *directory*	Deletes a remote directory. The directory must be empty. Example: `ftam> rmdir tempdir`
`cattr` *remote_file* `-dfilnsv` *new-attr* [`-dfilnsv` *new-attr*] ...	Change the FTAM attributes of a remote file. See the section called "Using the cattr Command" following this table. The following example uses cattr to rename a file. Example: `ftam> cattr currentfile -n historyfile`

File Listings from FTAM

The following example illustrates the different kinds of file listings that are available.

```
$ ftam
ftam> open chicago
Username (chicago:alan): donald
Password (chicago:donald):
Connected to chicago as user donald.


ftam> pwd
Name of default working directory on chicago is unavailable.
ftam> cd /users/donald/reports
/users/donald/reports is the current working directory.
```

```
ftam> ls
fn_1gfs
fn_1gnl
fn_1gns
fn_2m
fn_2s
fn_3m
fn_3s
ftamdir
ftam> ls -a fn_1gns
Filename:                           /users/donald/reports/fn_1gns
Permissions:                        R-PXEACD---
File type:                          text (FTAM-1)
Storage account:                    no value available
File creation:                      no value available
Last file modification:             Apr 21 19:49
Last read:                          May 18 15:36
Last attribute modification:        no value available
Identity of creator:                donald
Identity of modifier:               no value available
Identity of reader:                 no value available
Identity of attribute modifier:     no value available
File availability:                  deferred availability
Filesize:                           1100
Access Control:                     other           R-PXEACD
                                    group           R-PXEACD
                                    user            R-PXEACD
Legal qualification:                no value available

ftam> dir
/users/donald/reports:
Permissions   Owner    File type      Filesize   Access date
Filename
-------------------------------------------------------------------
-----
R-PXEACD---  donald   text (FTAM-1)        1920 Apr 21 19:49
fn_1gfs
R-PXEACD---  donald   text (FTAM-1)      250000 Apr 21 19:51
fn_1gnl
R-PXEACD---  donald   text (FTAM-1)        1100 Apr 21 19:49
fn_1gns
RI--EACD---  donald   text (FTAM-2)       20020 Apr 21 19:50 fn_2m
RI--EACD---  donald   text (FTAM-2)        3001 Apr 21 19:50 fn_2s
R-PXEACD---  donald   binary (FTAM-3)     39999 Apr 21 19:50 fn_3m
R-PXEACD---  donald   binary (FTAM-3)      5000 Apr 21 19:50 fn_3s
R----ACD---  donald   dir (NBS-9)          1024 May 09 12:13
ftamdir
ftam>
```

Permissions are described in the first table of chapter 5 (Table 5-1).

Using the cattr Command

The FTAM specification defines many attributes that describe an FTAM file. The cattr command gives you the ability to modify many of these attributes for a file. To change the attributes of a file, you must at least have FTAM *change_attribute* permission on the file.

The cattr command can perform the actions in Table 2-4. Use the associated cattr command option to request an action.

Syntax of the cattr Command

The syntax for the cattr command is as follows:

```
cattr -dinflsv new_attribute [-dinflsv new_attribute] ... file
```

The cattr command always works on files in the remote filestore you are connected to. You can use one or more options in a command (one at a time, each followed by its argument). See Table 2-4 and the examples that follow it.

Table 2-4 cattr Actions and Command Options

Action	Command Option	Option Argument
Delete an element from the file's access control list. (File protection is discussed in chapter 5.)	-d	For HP-UX responders, this must be user, group, or other.
Insert an element into the file's access control list. (File protection is discussed in chapter 5.)	-i	For HP-UX responders, this must be user, group, or other, followed by a comma, followed by an "action/concurrency string" (see chapter 5).
Change the name of the file	-n	New file name (Character string)
Change maximum permitted size of the file*	-f	New size (integer, octets) (Numeric string)
Change the file's legal qualification*	-l	New legal qualification (Character string)
Change the file's storage account*	-s	New account (Character string)
Change the file availability*	-v	-v I or -v i :Immediate -v d or -v D :Deferred

* HP FTAM/9000 does not keep track of this attribute for local files. The option is for use with other FTAM responders.

Examples:. This example illustrates how to rename a remote file using cattr. The file called oldfile is renamed to newfile.

```
ftam> cattr oldfile -n newfile
```

This example adds access control for the file's owner, allowing all actions. It also allows group members to have read and read_attribute permissions:

```
ftam> cattr /ftamfiles/report -i user,RPXEACD -i group,RA
```

This example removes the access control placed on the file in the previous example:

```
ftam> cattr /ftamfiles/report -d user -d group
```

This example changes the account to region1sales and future filesize to 2,000,000

```
ftam> cattr atlanta:marketing.sales -s region1sales -f 2000000
```

Directory Support in FTAM Implementations

The behavior of some directory commands depends on the remote system. [1] Some remote FTAM implementations might not support the concept of directories, but others, like HP FTAM/9000, do. Table 2-5 explains the effect of different levels of support for directories:

Table 2-5 Effect of Directory Support on ftam Commands

Command	If remote system supports the concept of directories, ...	If remote system does not support the concept of directories, ...
cd	Works as described previously. Invalid directory names are detected as soon as you issue the cd command.	The directory name you supply to the cd command becomes a prefix, which ftam attaches to subsequent file names before it relays them to the remote host. If the directory name is invalid at the remote host, the error is not detected until you attempt to access a remote file.
pwd	The command returns the current working directory for the remote system. If you have not yet used cd, ftam can not obtain the name of the current working directory.	The command returns the name you specified in your last cd command. This name could be invalid. If you have not yet used cd, ftam can not obtain the name of the current working directory.
ls dir mkdir rmdir	These commands work as describ-ed previously. Invalid directory names are detected as soon as you issue the command.	These commands do not work. You receive an error message.

1. The concept of directories is represented by FTAM's NBS-9 document type.

Performing Local Operations

The ftam command allows you to change the local working directory . You can also execute HP-UX commands, or start an interactive shell using customary HP-UX syntax. Table 2-6 illustrates the ftam commands to do this:

Table 2-6 Performing Local Operations

Command	Description
`lcd` *directory*	Changes the local working directory. Note that the directory parameter is literal; environment variables (like $HOME) are not recognized.
! [*command*]	Executes a command to the local operating system. If no command is specified, ftam escapes to a local interactive shell. Use **CTRL**–**D** or exit to exit the shell and return to ftam. Example: `ftam> ! ps -ef`

Performing File Transfers

The ftam commands in Table 2-7 let you copy files to and from the remote host:

NOTE See "Notes About Remote File and Directory Names" earlier in this chapter for guidelines on specifying remote names.

Table 2-7 ftam Commands for Transferring Files

Command	Description
`append` *local_file* [*remote_file*]	Transmit the local_file to the remote host, and append it to remote_file. If remote_file does not exist, append is identical to put. If remote_file is unspecified, ftam assigns the local_file name to the remote_file name. Example: `ftam> append data1 alldata`
`get` *remote_file* [*local_file*] or `recv` *remote_file* [*local_file*]	Copy remote_file to local_file. If local_file is unspecified, ftam uses the specified remote_file name as the local_file name. Example: `ftam> get denverdata`
`mget` *remote-files* (Multiple-get)	Copy remote-files from the remote system to the local system. The new local files have the same names as the remote files. "Wildcard" file specification is not allowed. Example: `ftam> mget tmp1 tmp2`
`mput` *local-files* (Multiple-put)	Copy local-files from the local system to the remote system. The remote files have the same names as the local files. "Wildcard" file specification is not allowed. Example: `ftam> mput new1 new2`
`put` *local_file* [*remote_file*] or `send` *local_file* [*remote_file*]	Copy local_file to remote_file. If remote_file is unspecified, ftam assigns the local_file name to the remote_file name. Example: `ftam>send myreport report.june`

Example

In this example, Sue uses the get command to copy the report.dat file from the remote host denver to her working directory on the local host. Note how ftam reports the successful transfer:

```
$ ftam denver
Username (denver:Sue): Sue
Password (denver:Sue):
Connected to denver as user Sue.
ftam> get report.dat
Received file /users/marketing/sales/sue/report.dat (23749 bytes)
ftam>
```

Streamlining ftam with a Startup File

You can have ftam skip the password request and automatically set up a connection to a remote host. To automate your ftam connections, you create an FTAM "startup" file (called .ftamrc) in your home directory. This file contains login information for specific remote hosts.

Once login information is available in .ftamrc, ftam does not prompt you for passwords during connection establishment. This feature can be useful if you routinely use ftam with particular remote hosts, or use programs that need to perform ftam operations unattended.

NOTE FTAM startup files are discussed in more detail in Chapter 4, "Special FTAM Files."

The following example illustrates using automatic remote login. Note that an entry in .ftamrc has this basic form:

```
machine host_name login user_name [password user_pass] [account
account_name]
```

A startup file can contain multiple entries like this. Each one identifies a remote host, and a valid user name on that host. A startup file provides FTAM with customized default information for your convenience.

When you start an ftam session, it scans the startup file looking for the host name you specified. The information in the first entry that matches becomes the default information for the login sequence.

You can accept the default by pressing [Enter]; ftam then uses the password from that entry to log in to the remote. Also, you can specify a different user name at the Username prompt. If the startup file has an entry for that user on the specified host, ftam uses the password from that entry to access the remote.

CAUTION A startup file that contains password information is a potential security hazard . This may be an unacceptable risk in some situations. In such cases, startup files should not contain password information.

Example

Sue has the following entries in her .ftamrc file:

```
machine denver  login don   password shadowy
machine denver  login sue   password mystery
machine atlanta login kelly
```

In this example, Sue connects to each host with ftam to show the effect of these entries.

```
$ ftam
ftam> open denver
Username (denver:don): [Return]
Connected to denver as user don
ftam> close
Released connection to denver
ftam> open denver
Username (denver:don): sue
Connected to denver as user sue
ftam> close
Released connection to denver
ftam> open atlanta
Username (atlanta:kelly): [Return]
Password (atlanta:kelly):
Connected to atlanta as user kelly.
ftam>
```

Sue had two entries in her .ftamrc file, listing different login names and passwords for denver. The first (for don) is the default whenever Sue connects to denver. Because both entries for the host denver contain passwords, she is never prompted for a password when she connects as either sue or don. However, when she connects to atlanta, the startup file entry for kelly does not contain a password. Therefore, if the user kelly has a password, Sue must provide that password at the prompt.

Quick ftam Command Reference

Table 2-8 ftam Command Summary

Command	Abbreviation	Function
!	N/A	Execute a local command or new shell.
?	N/A	Request help.
append	a	Append to a remote file.
bell	be	Toggle file transfer bell.
bye	by	End an FTAM session.
cattr	ca	Change FTAM file attributes.
cd	cd	Change the current remote working directory.
close	cl	End the current connection.
connect	co	Establish a connection.
delete	de	Remove a file.
dir	di	Get a summary file or directory listing.
get	g	Copy remote file to local file.
help	h	Request help.
lcd	lc	Change the current local working directory.
ls	ls	Get a file or directory listing.
mdelete	md	Remove multiple files.
mget	mg	Copy multiple remote files to local files.
mkdir	mk	Create a remote directory.
mput	mp	Copy multiple local files to remote files.
open	o	Establish a connection.
put	pu	Copy local file to remote file.

Command	Abbreviation	Function
pwd	pw	Get current remote working directory.
quit	q	End an FTAM session.
recv	rec	Copy remote file to local file.
release	rel	End the current connection.
rename	ren	Change the name of a file.
rmdir	rm	Delete a remote directory.
send	sen	Copy local file to remote file.
set	set	Set FTAM parameters.
status	st	Request a status report.
unset	un	Unset file options.
user	us	Reconnect as a different user.

3 Using Command-Line FTAM

This chapter describes how to use the FTAM service directly from the HP- UX system prompt, rather than through the ftam program described in Chapter 2, “Using Interactive FTAM.” There are several commands that implement FTAM:

Table 3-1 FTAM Commands

Command	Function
`fcp` *source target*	Copies an FTAM file between systems. The contents of *source* are unaffected; its attributes might be updated.
`fmv` *source target*	Moves an FTAM file between systems. The *source* is deleted in the process.
`fls` [*name*]	Lists an FTAM directory (or file), named *name*.
`fdel` *file*	Deletes an FTAM file.
`fcattr` *file*	Changes the FTAM attributes of a file.

Chapter Overview

- Each of the above commands has, as a parameter, a file or directory name. The next section shows how to specify file and directory names.
- The remainder of this chapter describes how to use each of the commands listed above, along with its options and parameters.
- Some of the above commands can take command options. These options are discussed separately for each command.
- The above commands can use the -X or -z command options to satisfy file protection requirements. Using these options requires knowledge of the FTAM file protection mechanisms. FTAM file protection is the subject of Chapter 5, “FTAM File Protection.”

Specifying File and Directory Names

This section covers the way you specify both local and remote file and directory names.

Specifying Local Names

Specify local file and directory names with the usual HP-UX syntax and conventions.

Specifying Remote Names

Remote file and directory names have three elements, as described in Table 3-2.

Table 3-2 Name Elements

Element	Description
user	The login name that will be used to access the remote host.
host	The name of the remote host. This can take one of three forms: • An alias, which is easiest and most common; • A directory distinguished name; or • A presentation address. Because the second two are used infrequently, this guide does not examine them; refer to the online man pages for additional information.
name	The file or directory name. See “Notes About Remote File and Directory Names” following this section for important details.

These three elements are arranged in the following form:

```
user@host:name
```

Notice the punctuation between elements. This is an example of a legal file name:

```
betty@denver:memos/mymemo
```

The local host uses the login name `betty` to access the remote HP-UX host named `denver`. You are prompted to supply betty's password. The file name (`memos/mymemo`) accesses a file called `mymemo` in the `memos` subdirectory of betty's home (default) directory. Notice that this example file name uses normal HP-UX syntax; other vendors' responders require the native syntax and conventions of the host.

Notes About Remote File and Directory Names

Note the following important points about remote file names:

- Directory names are legal only in `fls` and `fcattr` commands. Directory names are not legal as source or destination file names.
- Wildcard characters are not legal. This applies to both source and destination.
- For all FTAM commands, remote file names must be specified with the native syntax, notation, and conventions for the remote host. FTAM cannot translate or negotiate file names between different hosts, so any name you provide has to be valid on the system that uses it. This may require you to "escape" HP-UX metacharacters (like ">") if they appear in the remote file name. To "escape" a metacharacter, precede it with a backslash, or enclose the whole file (or directory) specification in quotation marks. Example: `"fairbanks:rush>gold"` or `fairbanks:rush\>gold`
- All names are relative to the remote working directory, unless you provide an absolute pathname for a file or directory (in whatever way the remote system defines "absolute pathname").
- The default remote directory for file transactions is determined by the FTAM implementation on the remote host. HP FTAM/9000 responders set the default directory to be the home directory for the user involved in the transaction. Other (non-HP-UX) FTAM implementations are apt to use different default directories.

Shortcut Remote Names

You can omit the `user@` portion of a remote name if your ftam startup file contains an appropriate entry (see Chapter 4, “Special FTAM Files,” for information about the ftam startup file).

For example, suppose you are logged in as `betty` on the local system, and issue an fcp command with `denver:myplan` as the remote target file name (rather than `betty@denver:myplan`):

```
$ fcp plan denver:myplan
```

This example command works under the following conditions:

- Your `.ftamrc` startup file contains a valid entry for host `denver`, and user `betty`.
- If that entry also contains a password, the fcp command executes the copy immediately.
- If that entry does *not* contain a password, you are prompted to supply it; then fcp executes the copy.

In any case, the working directory on `denver` is determined by the remote FTAM implementation; HP-UX FTAM would use betty's home directory.

Copying Files with fcp

The fcp command can transfer a remote file to the local host, or a local file to a remote host. From your local host, you can also use fcp to copy files between two remote hosts, or make a local copy.

About fcp

The fcp command is patterned after rcp, a Berkeley service that copies files between UNIX hosts on a network. With fcp, you can create a copy (either local or remote) of an existing file (either local or remote). When fcp completes a copy operation, your local host redisplays its prompt.

When you work with remote files, the working directory for fcp on the remote host is a default directory that depends on the remote FTAM implementation. For HP-UX FTAM responders, it is your remote home directory.

Using fcp

The syntax for the fcp command is as follows:

```
fcp source_file [-X | -z source_access] dest_file [-X | -z
dest_access]
```

The *source_file* is the file to be copied, and *dest_file* is the destination to which the file is to be copied. If you are familiar with the HP-UX cp command, you will notice the similarity. However, for fcp, the source and destination files can be either local or remote.

The options manage file protection. The `-X` option gives you exclusive access to the file during the copy. The `-z` option can be used to satisfy more stringent file protection requirements. File protection is the subject of Chapter 5, “FTAM File Protection.”

NOTE Whether a file is local or remote depends on how you specify the file name. See “Specifying File and Directory Names” earlier in this chapter.

Example:

In this example, a user known as `betty` uses fcp to create a copy of the local file `localplan` in her home directory on a remote HP-UX host called `chicago`:

```
$ fcp localplan chicago:localplan
Password (chicago:betty):
$
```

Note that you are prompted for betty's password at chicago. Creating a `.ftamrc` file may allow you to bypass this prompt.

In fcp file transfers, you must explicitly specify both the source and destination file names. Directory names and wildcards are not allowed for either source or destination.

Moving Files with fmv

The fmv command can move a remote file to the local host, or a local file to a remote host. From your local host, you can also use fmv to move files between two remote hosts, or move files locally. The fmv command can also be used to rename a file, leaving it in its original place.

About fmv

With fmv, you can move an existing file (either local or remote) to a new location (either local or remote). The file in the new location is an exact copy of the original, and the original file (including any shadow file [1]) no longer exists. When fmv completes a move operation, your local host redisplays its prompt.

When you work with remote files, the working directory for fmv on the remote host a default directory that depends on the remote FTAM implementation. For HP-UX FTAM responders, it is your remote home directory.

Using fmv

The syntax for the fmv command is as follows:

```
fmv source_file [-X | -z source_access] dest_file [-X | -z
dest_access]
```

The *source_file* is the file to be moved, and *dest_file* is the destination to which the file is to be moved. If you are familiar with the HP-UX mv command, you will notice the similarity. However, for fmv, the source and destination files can be either local or remote.

The options manage file protection. The `-X` option gives you exclusive access to the file during the move. The `-z` option can be used to satisfy more stringent file protection requirements. File protection is the subject of Chapter 5, “FTAM File Protection.”

NOTE Whether a file is local or remote depends on how you specify the file name. See “Specifying File and Directory Names” earlier in this chapter.

1. See Chapter 4, “Special FTAM Files,” for information about shadow files.

Example:

In this example, a user known as `betty` uses fmv to move the local file `localplan` to her home directory on a remote HP-UX host called `chicago`:

```
$ fmv localplan chicago:localplan
Password (chicago:betty):
$
```

Note that you are prompted for betty's password at chicago. Creating a `.ftamrc` file may allow you to bypass this prompt.

In fmv file transfers, you must explicitly specify both the source and destination file names . Directory names and wildcards are not allowed for either source or destination.

Deleting Files with fdel

The fdel command can delete remote or local FTAM files.

About fdel

With fdel, you can delete existing FTAM files (either local or remote). When you use this command, the original file or files no longer exist. When fdel completes, your local host redisplays its prompt .

When you work with remote files, the working directory for fdel on the remote host is a default directory that depends on the remote FTAM implementation. For HP-UX FTAM responders, it is your remote home directory.

Using fdel

The syntax for the fdel command is as follows:

`fdel [-i] file[-X | -z access] [file [-X | -z access] ... ]`

The *file*s are one or more FTAM the files to be deleted. If you are familiar with the HP-UX rm command, you will notice the similarity. However, for fdel, the files can be either local or remote.

The `-i` option causes FTAM to request confirmation before it deletes a file.

The other options manage file protection. The `-X` option gives you exclusive access to the file during the deletion. The `-z` option can be used to satisfy more stringent file protection requirements. File protection is the subject of Chapter 5, “FTAM File Protection.”

NOTE Whether a file is local or remote depends on how you specify the file name. See “Specifying File and Directory Names” earlier in this chapter.

For each specified file, the fdel command deletes both the data file and the FTAM shadow file, if it exists (see Chapter 4, “Special FTAM Files,” for information about FTAM shadow files).

Example:

In this example, a user known as `betty` uses fdel to delete a local file–`localplan`. She also deletes a remote file–`regionplan`–in her home directory on the host called `chicago`:

```
$ fdel -i localplan chicago:regionplan
Password (chicago:betty):
Remove “localplan” (y/n): y
Remove “chicago:regionplan?“? (y/n): y
$
```

Note that you are prompted for betty's password at `chicago`. Because of the `-i` option, you are also requested to confirm the deletion request.

Listing Directories with fls

The fls command lists directories or files.

About fls

With fls, you can list existing either local or remote directories or files.

NOTE If the remote FTAM implementation does not support the concept of directories (i.e., NBS–9 type documents), fls does not work; you will receive an error message.

When fls is finished, your local host redisplays its prompt. When you work with remote directories, the working directory for fls on the remote host is a default directory that depends on the remote FTAM implementation. For HP-UX FTAM responders, it is your remote home directory.

Using fls

The syntax for the fls command is as follows:

`fls [-al] [`*`name`* `[-z` *`access`*`] ] ...`

The *name*s are one or more directories or files to be listed. If you are familiar with the HP-UX ls command, you will notice the similarity. However, for fls, the directories can be either local or remote.

NOTE Whether a file is local or remote depends on how you specify the file name. See “Specifying File and Directory Names” earlier in this chapter.

Command Options for fls

The following table summarizes the two unique command options (excluding –z) for the fls command:

Table 3-3 Command Options for fls

Option	Description
–a	Requests a complete listing, including information about every FTAM file attribute for each file listed.
–l	Requests a "summary" listing of the directory. Files are listed with their most important FTAM attributes: name, permissions, contents–type, file size, time of last modification, and identity of creator.

Example:

The following example illustrates the different kinds of file listings that are available. The example continues on the next page.

```
$ fls donald@chicago:/users/donald/reports/fn_1gns

/users/donald/reports/fn_1gns

$ fls -l donald@chicago:/users/donald/reports

/users/donald/reports:

Permissions   Owner    File type      Filesize   Access date
Filename
-------------------------------------------------------------------
-----
R-PXEACD---  donald   text (FTAM-1)        1920 Apr 21 19:49
fn_1gfs
R-PXEACD---  donald   text (FTAM-1)      250000 Apr 21 19:51
fn_1gnl
R-PXEACD---  donald   text (FTAM-1)        1100 Apr 21 19:49
fn_1gns
R-PXEACD---  donald   text (FTAM-1)        2015 Apr 21 19:49
fn_1gvs
R-PXEACD---  donald   text (FTAM-1)       30000 Apr 21 19:50
fn_1iam
RI--EACD---  donald   text (FTAM-2)      150038 Apr 21 19:51 fn_2l
RI--EACD---  donald   text (FTAM-2)       20020 Apr 21 19:50 fn_2m
RI--EACD---  donald   text (FTAM-2)        3001 Apr 21 19:50 fn_2s
R-PXEACD---  donald   binary (FTAM-3)     39999 Apr 21 19:50 fn_3m
R-PXEACD---  donald   binary (FTAM-3)      5000 Apr 21 19:50 fn_3s
R----ACD---  donald   dir (NBS-9)          1024 May 09 12:13
reportdir

$ fls -a donald@chicago/users/donald/reports/fn_1gns

Filename:                          /users/donald/reports/fn_1gns
Permissions:                       R-PXEACD---
File type:                         text (FTAM-1)
Storage account:                   no value available
File creation:                     no value available
Last file modification:            Apr 21 19:49
Last read:                         May 18 15:36
Last attribute modification:       no value available
Identity of creator:               donald
Identity of modifier:              no value available
Identity of reader:                no value available
Identity of attribute modifier:    no value available
File availability:                 deferred availability
Filesize:                          1100
Access Control:                    other           R-PXEACD
                                   group           R-PXEACD
                                   user            R-PXEACD
Legal qualification:               no value available
$
```

Permissions are described in Chapter 5, “FTAM File Protection,” (Table 5-1).

Changing File Attributes with fcattr

The fcattr command is similar to the HP-UX chmod command.

About fcattr

The FTAM specification defines many attributes that describe an FTAM file. The fcattr command gives you the ability to modify many of these attributes for a file. To change the attributes of a file, you must have at least FTAM *change_attribute* permission for the file.

The fcattr command can perform the actions in Table 3-4. Use the associated fcattr command option to request an action.

Using fcattr

The syntax for the fcattr command is as follows:

`fcattr` *`file`* `-dinflsv` *`new_attribute`* `[-dinflsv` *`new_attribute`* `...]`

You can use one or more options in a command (one at a time, each followed by its argument). See Table 3-4 and the examples that follow it.

Table 3-4 fcattr Actions and Command Options

Action	Command Option	Option Argument
Delete an element from the file's access control list. (Access control is discussed in chapter 5.)	-d	For HP-UX responders, this must be user, group, or other.
Insert an element into the file's access control list. (Access control is discussed in chapter 5.)	-i	For HP-UX responders, this must be user, group, or other, followed by a comma, followed by an action/concurrency string (see chapter 5).
Change the name of the file.	-n	New file name (Character string)
Change maximum permitted size of the file.*	-f	New size (integer, octets) (Numeric string)

Action	Command Option	Option Argument
Change the file's legal qualification.*	-l	New legal qualification (Character string)
Change the file's storage account.*	-s	New account (Character string)
Change the file availability.*	-v	-v I or -v i :Immediate -v d or -v D :Deferred

*HP FTAM/9000 does not keep track of these attributes for local files. The option is for use with other FTAM responders.

Examples:

This example illustrates how to rename a file using fcattr. The local file called `oldfile` is renamed to `newfile`.

```
$ fcattr oldfile -n newfile
```

The next example renames the remote file `current.dat` on the host called `chicago`. The new name is `history.dat`, on the same remote host.

```
$ fcattr chicago:current.dat -n history.dat
```

This example adds access control for the file's owner (`lisa`), granting all permissions. It also allows group members to have *read* and *read_attribute* permissions:

```
$ fcattr lisa@chicago:/ftamfiles/report -i user,RPXEACD -i
group,RA
```

This example removes the access control placed on the file in the previous example:

```
$ fcattr lisa@chicago:/ftamfiles/report -d user -d group
```

This example changes the account to `region1sales` and future filesize to `2,000,000`.

```
$ fcattr atlanta:marketing.sales -s region1sales -f 2000000
```

The remote host access methods are described under “Specifying Remote Names” earlier in this chapter.

4 Special FTAM Files

This chapter discusses certain files that FTAM uses for special purposes.

Chapter Overview

FTAM uses three types of special files for distinct purposes:

- Maintaining FTAM file attributes and access control information that HP-UX does not inherently support.
- Simplifying routine FTAM operations, like establishing connections.
- Maintaining the configuration information necessary to permit connections between hosts. FTAM users do not generally need to read or change the local configuration.

This chapter discusses the first two types of FTAM special files.

FTAM Shadow Files

The FTAM Virtual File Store (VFS) is defined by the FTAM ISO standard, and provides a common file system abstraction for all FTAM implementations to use. Each vendor independently maps the FTAM VFS to their real file system.

The FTAM VFS defines several file attributes—including access control mechanisms—that are not native to HP-UX. (See Chapter 5, "FTAM File Protection.") To implement these attributes and mechanisms, HP-UX FTAM uses supplemental files called **shadow files**.

When FTAM creates or modifies an HP-UX file, it creates a shadow file for the HP-UX file. The shadow file has the same name as the HP-UX file, prefixed by a period and underscore ("._"). The shadow file is located in the same directory as the HP-UX file.

For example, suppose you use the fcp command to copy a file named "mydata" from a remote host to your home directory. If you list the whole directory (use $ ls -a), you will find both of the following files:

```
._mydata    mydata
```

The file named `._mydata` is the FTAM shadow file for the file named `mydata`.

FTAM must be able to handle new files, which have no shadow file, as well as existing files.

- If FTAM attempts to create or modify a file for which there is a shadow file, it applies the attributes and access control settings noted in the shadow file.
- If FTAM attempts to create or modify a file for which there is no shadow file, it applies the default attributes and access control settings noted in Chapter 7, "FTAM File Details." FTAM creates a new shadow file, which contains these defaults.

Precautionary Notes about Shadow Files

An HP-UX file together with its FTAM shadow file forms a logical unit, which should be maintained. This logical unit can be thought of as "an FTAM file," and is distinct from an ordinary HP-UX file. The two HP-UX files are paired, based on their related names. However, the underlying HP-UX system does not enforce this logical matching.

As a result, common HP-UX utilities like cp, mv, rm, or chmod can inadvertently cause inconsistencies when applied to FTAM files.

For example, consider the previous case, which discussed two files: one called `mydata`, and its shadow file, `._mydata`. If you use mv to rename `mydata` to `junedata`, the contents of the file are unchanged. However, the complementary shadow file `._mydata` is not automatically renamed to become `._junedata`. Consequently, the FTAM shadow file information it contains is no longer linked to the matching data file.

Of course, FTAM can still be used with the `junedata` file, but it will apply *default* attribute information as noted previously. If the shadow file `._mydata` contained other (non–default) information, such as access control, that information is effectively lost. It is possible, in this example, to use mv to also rename `._mydata` to `._junedata`. This restores the logical pairing between the shadow file and the data file.

However, the best approach is to use ftam or fcattr-n to rename the file. These FTAM utilities will automatically update any existing shadow files. Likewise, you will want to use FTAM utilities like fcp and fmv to copy or move FTAM files.

You should also use fdel or ftam to delete FTAM files. If you use rm instead, the shadow file will continue to exist. Over time, you could accumulate a clutter of unused shadow files. In the worst case, you could create a new file with the same name as an outdated shadow file. The information in the shadow file may not match the real attributes or access control you expect or desire for the new file.

The FTAM Startup File

If you want to simplify your day–to–day use of FTAM, you can create a "startup" file called `.ftamrc`, usually in your home directory. The .ftamrc file contains two types of information:

- The logins and passwords for connecting to remote hosts.
- Special default settings for FTAM operation.

CAUTION A startup file that contains password information is a potential security hazard . This may be an unacceptable risk in some situations. In such cases, startup files should not contain password information.

General Rules about .ftamrc

There are two general rules to follow when setting up your `.ftamrc` file:

1. Use the chmod command to set the permissions on `.ftamrc` as follows:

```
   user   group  other
  r * *   - - -   - - -
```

   The file owner must have read access. Permissions marked by '*' can be set as you wish. All other permissions *must* be off.

2. The HP-UX environment variable FTAMRC specifies the full pathname for the FTAM startup file. If FTAMRC is not set, FTAM looks for `.ftamrc` in your $HOME directory.

Automating Logins with .ftamrc

For each host you want to connect to, you can create a line in `.ftamrc` like this:

`machine` *`hostname`* `login` *`login_name`* `[password` *`pswd`*`] [account` *`acct_name`*`]`

For example, examine the following line from a `.ftamrc` file:

```
machine chicago login betty password sesame
```

Having this line in `.ftamrc` can simplify using FTAM with the host named `chicago`. FTAM uses the login name `betty`, and the password `sesame` to gain access to chicago. The default directory on the remote host (chicago) depends on the FTAM implementation there.

Each item on the line is separated from its neighbors with “white space” (tabs or spaces).

Alternative Hostname Forms

The *hostname* entry is commonly an alias for a remote FTAM responder, such as `chicago` in the above example.

The *hostname* can also be the Presentation Address for the remote FTAM responder, or its Directory Distinguished Name . Both of these are more complicated than an alias, and prone to typing errors. All the examples in this guide use the alias form; see the online man pages for more information about the other two forms.

Setting Overwrite Mode with .ftamrc

When you copy or move a file, there is always the possibility that a file by the target name already exists. In this case, FTAM has to decide whether or not to overwrite the existing file.

You can use your `.ftamrc` file to set a default overwrite mode. To do this, insert only one of the following lines in your `.ftamrc` file:

```
o y
```

This line means “*o*verwrite *y*es”. It directs FTAM to overwrite existing files that have the same name as the one FTAM is trying to create.

or

```
o n
```

This line means “*o*verwrite *n*o.” It prevents FTAM from overwriting existing files. Instead, it issues an error message and averts potential data loss.

NOTE

FTAM (like HP-UX itself) ordinarily defaults overwrite mode to “yes”. Therefore, if you do *not* explicitly set overwrite to “no” in your `.ftamrc`, you can accidently overwrite files using FTAM file transfer commands. Note also that you can have only one “overwrite” entry in your `.ftamrc` file.

5 FTAM File Protection

The FTAM Virtual File Store (VFS) is defined by the FTAM ISO standard, and provides a common file system abstraction for all FTAM implementations to use. Each vendor independently maps the FTAM VFS to their real file system.

The FTAM VFS defines several file protection mechanisms that are not native to HP-UX. This chapter discusses these attributes and mechanisms and how to work with them.

NOTE

Many people only need to know about the –X option (for exclusive access). This option is covered later in this chapter.

Chapter Overview

This chapter has these main sections:

- Introduction to FTAM File Protection.
- Concepts of FTAM File Protection.
- Action/Concurrency Strings.
- Using FTAM File Protection.

Introduction to FTAM File Protection

One of the key FTAM features is its sophisticated file protection scheme. FTAM provides two related mechanisms to protect files from undesirable or unauthorized use:

- The first—called **access control** —controls the actions that users can perform on the file. A file has a list of permissions (permitted actions), which specify the actions that are allowed to be performed on the file (see Table 5-1). It is also possible to limit individual users (or classes of users) to some subset of a file's permissions. For example, one user may be allowed to read—but not modify—a certain file, while another user can do both.
- The second—called **concurrency control** —controls access to a file by multiple users (see Table 5-2). For example, a user may be allowed to modify the file only if no one else is using it. For example, consider the user who is not allowed to modify a file, but is allowed to read it. To obtain a “snapshot” of the file at a given moment, the user still needs to obtain exclusive access to the file as he reads it. Therefore, in the command to read the file, this user must request exclusive access—a function of concurrency control. This chapter shows to do this.

To summarize, **access control** governs the actions that are permitted on a file, granting different users different subsets of the available actions. **Concurrency control** governs whether and how multiple users can access the file. Access control and concurrency control were designed and implemented to help ensure that data remains secure and uncorrupted.

NOTE

Vendors implement an FTAM access control scheme appropriate to the host system. Because of this, using access control is apt to cause complications.

For example, HP-UX FTAM can apply access control to a file according to the three HP-UX ownership classes: user, group, and other. Other FTAM implementations may apply access control to individual users, different classes of users, or elect to not implement file protection *at all*. You must have considerable knowledge about the access control scheme that a remote FTAM host uses before you can effectively use FTAM access control.

In general, HP recommends using FTAM access control only if you have strict file protection requirements.

Application of File Protection

There are three aspects to using FTAM file protection mechanisms:

- Setting (or removing) file protection for a file. This is similar to putting a padlock on a building's door. You can set file protection on a file in either of two ways:
  - At the system prompt, use the fcattr command.
  - At the ftam> prompt, use the cattr command.

Usually, a file's owner will set appropriate access control (and, optionally, concurrency control) on a file. Note that if you do not explicitly apply file protection to a file, it is open to general use (within the constraints of the underlying HP-UX file system).

- Satisfying file protection conditions on a file which has had access control applied to it. This is similar to using a key to open the padlock and gain access to the building. You satisfy file protection conditions one of two ways:
  - At the system prompt, use the `-z` option on FTAM commands. This option is explained later in this chapter.
  - At the ftam> prompt, use the set `-y` or set `-z` command. This command is explained in Chapter 2, “Using Interactive FTAM,” and with specific file protection details later in this chapter.

If a file has FTAM access control applied to it, the only users who can perform a given action on a file are those users who have been explicitly granted permission to perform that action with the file.

- Locking a file during access, to ensure the integrity of the data. Many common activities can corrupt data if multiple users are permitted simultaneous access. Therefore, HP-UX FTAM provides ways to "shut-out" other users during critical operations.

For maximum flexibility in setting up or satisfying file protection on a file, HP-UX FTAM uses a syntactic element called an "action/concurrency string." The form of an action/concurrency string is concise, and uses specialized notation. Action/concurrency strings are described later in this chapter.

To obtain exclusive access to a file (that is, to lock the file during your access), HP-UX FTAM provides a "shortcut" for command–line operations, the –X option. This option locks a file during the requested operation. This option is also described later in this chapter.

Terms and Notation for FTAM File Protection

This section introduces the terminology surrounding FTAM file protection. There are two key areas to understand:

- Permissions
- Concurrency control locks

These are covered in the next two subsections.

Permissions

The following table lists the name of each possible permission (or "file–action"), an associated code letter, and an explanation of its meaning. The code letters appear in action/concurrency strings [1], and in extended and summary listings from fls and ftam:

Table 5-1 Possible File Actions

Action Name	Code Letter	Explanation: A user with this permission is allowed to ...
Read	R	... read the file.
Insert	I	... insert new data anywhere in the file.
re**P**lace	P	... replace the file with a new version.
e**X**tend	X	... insert new data at the end of the file.
Erase	E	... erase all data in the file, leaving an empty file.
read **A**ttributes	A	... read the FTAM attributes of the file.
Change attributes	C	... change the FTAM attributes of the file.
Delete	D	... delete the file entirely, leaving no trace of it.

1. See "Action/Concurrency Strings" and "Using FTAM File Protection" later in this chapter.

Concurrency Control

The following table lists each valid concurrency control value (or "lock") which can be applied to a file action, and its associated code for use in action/concurrency strings:

Table 5-2 Concurrency Control Locks

Lock Name	Code Letter	Explanation	You perform the action	Others perform the action
Shared	S	Use *shared–access* when you need to perform the action, and would not experience conflict if other users simultaneously perform same action.	Yes	Yes
e**X**clusive	X	Use *exclusive–access* when you need to perform the action, and would experience conflict if other users simultaneously perform same action.	Yes	No
No access	N	Use *no–access* when you do not need (or are not allowed) to perform the action, but you would experience conflict if other users perform that action on the file while you use it.	No	No
not required	#	Use *not–required* access when you do not need (or are not allowed) to perform the action, and would not experience conflict if other users perform that action on the file while you use it.	No	Yes

Concepts of FTAM File Protection

As noted before, there are two related concepts in FTAM file protection: access control, and concurrency control. Access control governs the actions that are permitted on a file, granting different users different subsets of the available actions. Concurrency control governs whether and how multiple users can access the file. Concurrency control is applied independently to each action, as will be described later.

All the following controls and passwords are set (or satisfied) by using an "action/concurrency string" as an argument in an FTAM command. These are discussed later in this chapter.

Access Control

The following example illustrates the concepts involved in FTAM access control.

```
$ fls -a donald@chicago:/users/donald/earlydata
Filename:
/users/donald/earlydataPermissions:
R-PXEACD---File type:                          text (FTAM-1)
Storage account:                    no value available
File creation:                      no value available
Last file modification:             Jan 12 19:49
Last read:                          Jan 18 15:36
Last attribute modification:        no value available
Identity of creator:                donald
Identity of modifier:               no value available
Identity of reader:                 no value available
Identity of attribute modifier:     no value available
File availability:                  immediate availability
Filesize:                           1100Access
Control:                      other
R-------                      group      R--X-A--
user           R-PXEACDLegal qualification:              no value
available
```

Examine the italicized line labelled Permissions. The permissions stated on that line are the only actions that anyone can perform on the file. Notice that the "I" permission is missing; this means that no one has or can be given Insert permission for this file. [1]

1. Actually, the Insert action does not apply to FTAM-1 files.

Now examine the italicized entry labelled Access Control. Each user in this category is granted different permissions:

- The owner of the file, user, has full permission (excluding **I**nsert, as just noted).
- Co-workers in the owner's group can **R**ead, e**X**tend, and read the **A**ttributes of the file; they are excluded from any other activity that involves this file.
- Other users on the system can only **R**ead the file; they are excluded from any other activity that involves this file.

File protection constraints like this are placed on the file using the fcattr -i command, or the cattr -i command within ftam. Once the file has file protection (access control) on it, users must use the -z option (for command-line FTAM), or ftam's set (-y or -z) command, to do anything with the file. See “Using FTAM File Protection” later in this chapter for details.

File-Action Passwords

The FTAM specification makes it possible to apply a password to each file action. Then a user must know the password before he can perform the action.

Note, however, that HP-UX FTAM does not keep track of file–action passwords. There is no effect if you attempt to set (or satisfy) file–action passwords for files stored by an HP-UX FTAM host, either local or remote. However, you can satisfy (i.e., supply) a file–action password when a remote FTAM host requires one, via the –z option and an action/concurrency string. These are discussed in the next section.

Concurrency Control

As noted previously, concurrency control is applied independently to each action. Concurrency control governs whether and how multiple users can perform a given action with the file.

Once again, examine the shaded Access Control entry in the previous example. Concurrency control can be associated with each of the actions listed for the users in the Access Control list.

For example, for the users in the example file owner's group, it is possible to limit e**X**tend access to occur only when a single user has access to the file. This is called “exclusive” access . The other actions for a group user

(**R**ead and read **A**ttributes) could be given “shared” access , which allows multiple users to perform these actions simultaneously. Possible concurrency controls are listed in Table 5-2.

Note, however, that HP-UX FTAM does not keep track of concurrency control applied to file–actions. There is no effect if you attempt to set (or satisfy) file–action concurrency control on files stored by an HP-UX FTAM host, either local or remote. However, you can satisfy (i.e., supply) a concurrency control code when a remote FTAM host requires one, via the –z option and an action/concurrency string. These are discussed in the next section. Furthermore, you can obtain exclusive access to an HP-UX FTAM file by using the –X option, described next.

Obtaining Exclusive Access

HP-UX FTAM also provides a “shortcut” when you need exclusive access to an FTAM file. Whenever you need exclusive access to a file and can use command-line FTAM, the –X option is the right choice.

For example, the following command obtains a “snapshot” copy of a file which may have multiple users:

```
$ fcp michael@nairobi:/users/reservations/june.reserv -X
june.bookings
```

As noted at the start of this chapter, the only thing most people need to know about FTAM file protection is how to use the –X option. Unless a remote file has a passwords associated with file actions, your use of FTAM's file protection scheme will probably only involve using the –X option to obtain exclusive access to certain files.

Action/Concurrency Strings

As noted throughout this guide, action/concurrency strings are used as arguments to options for two commands within ftam, and as arguments to options for several command–line FTAM commands. The exact usage of an action/concurrency string in each of these commands is covered in the section "Using FTAM File Protection" later is this chapter. However, the syntax of the action/concurrency string is the same regardless of where it appears.

As an example, the following fmv command uses the –z option to satisfy access control and concurrency control on the source and target files. Each use of the –z option is followed by an action/concurrency string, which conveys the necessary information to FTAM.

```
$ fmv myplan -z D=X.PassMeBy denver:FY91plan -z P=X.SupercedeMe
```

The meaning of the action/concurrency strings in this example will become clear as you progress through this section.

The general syntax for an action/concurrency string is as follows:

```
action(s) [=conc_access|=.password|=conc_access.password]
     [,action(s) [=conc_access|=.password|=conc_access.password]]
...
```

The periods, commas, and equal–signs in the above syntax are mandatory delimiters. As usual, the brackets ("[" and "]") indicate information that may be optional, depending on the situation. The vertical bar ("|") separates valid choices within an optional argument.

Table 5-3 describes the elements of the action/concurrency string .

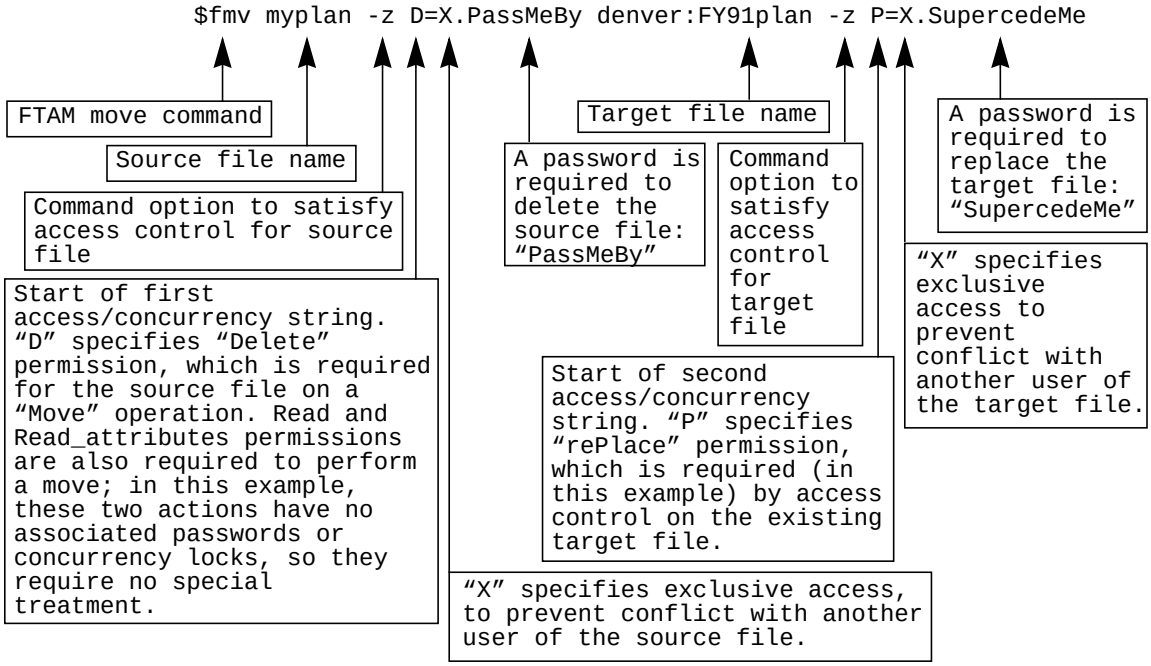
Table 5-3 Elements of an Action/Concurrency String

Element	Description
action(s)	A valid file action code (or codes) from Table 5-1.
conc_access	A valid concurrency control lock code from Table 5-2. You can specify more than one lock code when inserting an access control element; however, you can only specify one lock code in an action/concurrency string used to satisfy access control.

Element	Description
password	A password associated with the file action; there may be no password. HP-UX FTAM does not store passwords for file actions; this field is only provided for users whose remote responders do support action passwords.

The previous example is reproduced below. Each element is labelled to indicate its function in the command.

Figure 5-1



In this example, both the source and target files require the application of the –z option to satisfy access control.

The source file (which is to be deleted during the move operation) is protected against accidental deletion by having the password (PassMeBy) required on a delete action.

The target file (which is to be replaced during the move operation) is protected against unauthorized replacement by having the password (SupercedeMe) required for a replace action

Using FTAM File Protection

The tables in this section describe the syntax and use of HP-UX FTAM's action/concurrency strings. Action/concurrency strings are always and only used as arguments to certain command options, as noted in the following tables.

NOTE The syntax for action/concurrency strings is abbreviated to "a/c" in these tables. The previous section contains details about action/concurrency strings.

Table 5-4 shows the use of action/concurrency strings with interactive FTAM commands. Note that unless a file has passwords or concurrency control associated with actions, you do not need to use the y or z option to satisfy access control. You either have permission to perform the desired action, or you do not.

Table 5-4 Interactive ftam Commands with Options Using Action/Concurrency Strings

Command	Option	Syntax	Comments
set	y	set y a/c	Used (when necessary) to satisfy access control and/or concurrency control on target files in subsequent commands.
set	z	set z a/c	Used (when necessary) to satisfy access control and/or concurrency control on source files in subsequent commands.
cattr	–i	cattr –i *file user*,a/c	Used to set file protection on a *file*. The *user* is the user being granted permissions (and associated concurrency control, if any). For HP- UX filestores, *user* must be `user`, `group`, or `other`.

Table 5-5 shows the use of action/concurrency strings with command-line FTAM commands. The option (and its argument) apply to the immediately preceding file name in each command.

Note that unless a file has passwords or concurrency control associated with actions, you do not need to use the –z option to satisfy access control. You either have permission to perform the desired action, or you do not.

To obtain exclusive access to a file, use the –X option, which does not require an action/concurrency string argument.

Table 5-5 Command-Line FTAM Commands with Options Using Action/Concurrency Strings

Command	Option	Syntax	Comments
fcattr	–i	fcattr –i *file user*,a/c	Used to place file protection on a file. The user is the user being granted permissions (and associated concurrency control, if any). For HP-UX filestores, user must be user, group, or other.
fcp	-z	fcp *source* –z a/c *target* –z a/c	The command option is used (when required) to satisfy access control and/or concurrency control on the file that immediately precedes the command option.
fmv	–z	fmv *source* –z a/c *target* –z a/c	The command option is used (when required) to satisfy access control and/or concurrency control on the file that immediately precedes the command option.
fls	–z	fls *name* –z a/c	The command option is used (when required) to satisfy access control and/or concurrency control on the file that immediately precedes the command option.
fdel	–z	fdel *file* –z a/c	The command option is used (when required) to satisfy access control and/or concurrency control on the file that immediately precedes the command option.

Examples

The following examples illustrate correct use of the -z and -i option for several different situations.

To restrict access for others to read and read_attributes on the file JuneData, enter the following command:

```
$ fcattr JuneData -i user,RPXEACD -i group,RPXEACD -i other,RA
```

The following examples illustrate correct use of the -z and –i option for several different situations.

This allows the user and group members full access to the file, while other users have only read and read attribute access. To delete the access control for this file enter the following command:

```
$ fcattr JuneData -d other -d group -d user
```

Now, consider this case. First, access control is put on the file, using the following command:

```
$ fcattr MarchData -i user,RPXEACD=XS -i group,RPXEACD=XS
```

This grants the user and all group members full permissions, and allows a user to request either eXclusive or Shared access on any action. Suppose two people want to copy MarchData to their own directories, but one requests exclusive access during the copy and the other requests shared access, which is the default access method. The first person enters the following command to copy the file with shared access:

```
$ fcp /source/MarchData marchdata
```

A moment later, while the first copy is under way, the second person enters the following command to copy the file with exclusive access:

```
$ fcp /source/MarchData -X MyMarchData
```

Because the first request was for shared access (the default), the second person's request will fail; he can not get exclusive access at present. If the order of the commands were reversed, the first person would be allowed exclusive access, and the request for shared access would fail due to the current exclusive user.

The next example uses the -z option to gain access to a file on the paris host. The user requires read permission, which uses shared access and has a password associated.

```
$ fcp henri@paris:datafile -z R=S.ReadPass,A=S.RattrPass
HenrisData
```

This example shows a user setting access control on a remote file that she owns. Note that she retains all permissions, and gives group users only read and read_attribute permission.

```
$ fcattr tokyo:memos/salesmemo -i user,RPXEACD -i group,RA
```

In the next example, the file owner sets special permissions which permit multiple users to simultaneously read or read the attributes of the directory (providing they know the password). However, a user will require knowledge of a different passwords to delete, or change the attributes of, the directory. Notice that the remote host in this example (dublin) is not an HP- UX system, since it maintains concurrency and passwords on file–actions, and the specified user for access control (sales) is not a legal value for an HP-UX FTAM system.

Table 5-6

```
$ fcattr mike@dublin:MemoDir -i sales,RA=S#.ReadPass,D=X#.DelPass,C=X#.ChngPass
```

The last example shows how to use the -z option to delete a file which has access control applied to it. The access control for file deletion includes a password, and requires exclusive access to the file, so that the deletion will not affect another user's operations.

```
$ fdel giovanni@rome:italy.data -z D=X.DeletePass
```

6 Resolving FTAM Problems

This chapter is intended to help you resolve any difficulty you encounter while using HP FTAM/9000.

Chapter Overview

There are essentially two kinds of problems you can encounter when using FTAM:

- User errors
- Network/Resource errors

This chapter has two main sections to cover these two types of errors.

User Errors

A user error occurs when you make an invalid request that FTAM can not fulfill. Errors in this category include typing errors, non-existent source files, file protection errors, and so on.

The message you receive when FTAM detects a user error should be straightforward, and the remedy should normally be self-evident.

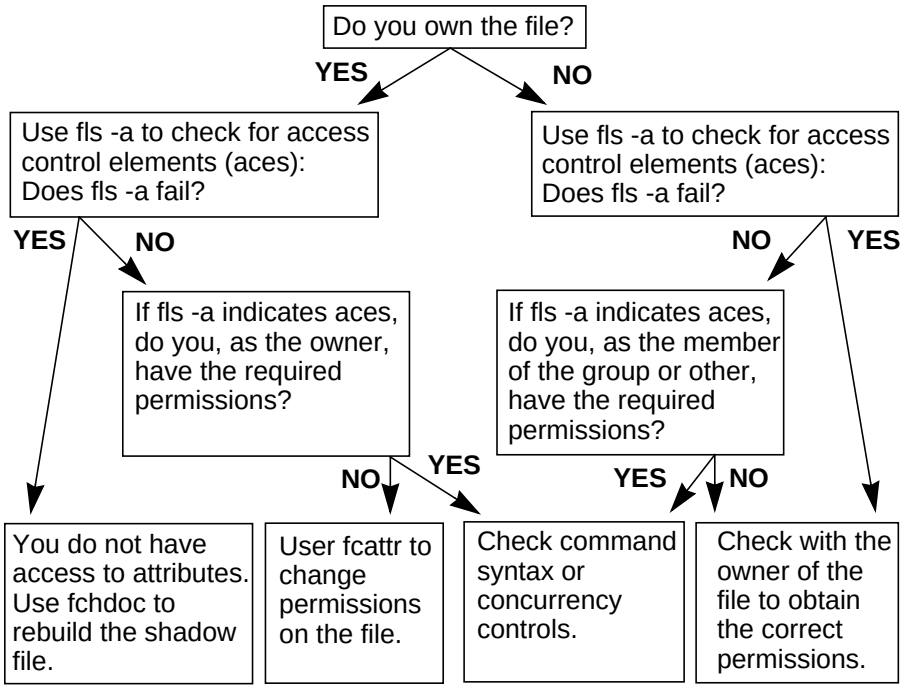
The cause of file protection errors may be less obvious; see the next section for details.

Resolving File Protection Errors

If you attempt an FTAM operation and experience an access control or concurrency error, follow the chart on the next page to resolve the problem.

Steps to Resolving File Protection Errors

Figure 6-1



Network and Resource Errors

Network and resource errors occur when some aspect of the network which supports FTAM fails to operate correctly. Errors in this category include hardware failures and resource exhaustion. For example, if the network cable is damaged or disconnected, all network operations (including FTAM) will fail. Likewise, if the lower layers of the network are not running, FTAM failures will occur. Local failures can sometimes be attributed to resource constraints.

Network and resource errors are typically more involved than user errors, and require more time and expertise to analyze and correct. A system as complex as an OSI network has many potential points of failure. However, these all show up at the FTAM user interface as one of the following problems:

- "Attempted operation failed."
- "Connect attempt aborted."
- "FTAM service provider unavailable."
- "Ftam command: out of memory"
- "No address for *hostname*."
- "Datatransfer cancelled."

If you are in "verbose mode" you will also get the additional message "check log file with log instance *log_instance_value*". Log instances are discussed in "About FTAM Troubleshooting" later in this chapter.

What To Do with a Network or Resource Error

Hewlett-Packard recommends the following steps for troubleshooting network errors detected by FTAM:

1. If you receive one of the errors listed above, retry the command that failed. Occasionally a transient problem will be cleared up by the time you retry the command. If the command continues to fail, you will have to initiate troubleshooting by following the next step.

2. Turn on verbose mode (ftam> setv), reproduce the error, and write down the “log instance” number that appears in the error message. This number will be important as you begin further troubleshooting. See the section following for a general overview of troubleshooting.
3. Turn to the *OSI Troubleshooting Guide*. That document contains detailed information about troubleshooting the network. Troubleshooting is easiest when performed by an experienced person.

About FTAM Troubleshooting

The information in this section is general. The *OSI Troubleshooting Guide* (part number: 32070-90020) provides more detailed information.

Troubleshooting a network error can be difficult and time-consuming, so Hewlett-Packard's OSI products (including HP FTAM/9000) provide substantial troubleshooting aids. When a network error occurs (say a cable gets accidently disconnected), some lower layer of the software detects the problem. It assigns the error a unique identifying number, called a “log instance ”.

The error, and its log instance, are noted (or “logged”) in a special file. Then the error is passed to the next layer in the network. As the error propagates up through the network layers, each layer logs the problem, and passes the error along. Eventually, the error appears at the interface as an error message with an associated log instance.

The log instance returned by the FTAM interface you are using directly corresponds to an FTAM error recorded in the product log files. By using this log instance to reference the log files, you can track the problem back through successive lower layers of the network, eventually to the source of the problem. The steps to accomplish this are covered in the *OSI Troubleshooting Guide*.

API Tracing. API tracing allows FTAM programmers and users to get detailed information about the interaction of an FTAM program with the HP FTAM API (Application Programmatic Interface) without having to access any source code. API tracing is of primary interest to FTAM programs and is explained in detail in the “Handling Errors” chapter of the *HP FTAM/9000 Programmer's Guide*. API tracing can be enabled or disabled during an interactive FTAM session as follows:

- Setting the API to 0 disables API tracing.
- Setting the API to 1 causes procedure entry and exit to be traced.

- Setting the API to 2 causes input parameters, as well as procedure entry and exit, to be traced.

The following example causes procedure entry and exit to be traced:

```
set api 1
```

7 FTAM File Details

This chapter discusses FTAM document types, the default attributes applied to FTAM files, and manual control of FTAM file attributes.

Document Types

The FTAM Virtual File Store (VFS) defines several document types. Document types generally correspond to file types on actual computer systems. Files are classified into various document types based on their structure and the interpretation of their contents.

HP FTAM/9000 currently supports five FTAM document types:

Table 7-1 FTAM Document Type Definitions

FTAM-1	FTAM-1 documents are unstructured text files. This is the default type that HP-UX FTAM applies to a file.
FTAM-2	FTAM-2 documents are record-oriented text files. This file type has little if any use for HP-UX FTAM. However, other vendors might use FTAM-2 files.
FTAM-3	FTAM-3 documents are unstructured files of binary data. This corresponds to executable files, scanned images, and similar non-textual data.
INTAP-1	INTAP-1 documents are record files.
NBS-9	NBS-9 documents are used to describe file directories, rather than files. Not all vendors support the NBS-9 document type.

NOTE In general, the casual user of FTAM does not need to be concerned with FTAM document types. Whether you are using FTAM to transfer text files or to remotely store executable files, FTAM will generally perform correctly. The document type information for a file is coded in its shadow file.

Default FTAM File Attributes

When HP-UX FTAM creates a shadow file, it applies the default FTAM attributes noted in the following table:

Table 7-2 Default FTAM File Attributes

Attribute	Default Value
Document type	FTAM-1
Access control	None
Permissions	Read, eXtend, rePlace, Erase, read_Attributes, Change_attributes, Delete. (That is, all actions are permitted.)
Filename	HP-UX file name
Future file size	Not stored by HP-UX FTAM
Legal qualification	Not stored by HP-UX FTAM
Storage account	Not stored by HP-UX FTAM
File availability	Not stored by HP-UX FTAM

Manual File-Attribute Control

HP-UX FTAM provides a special tool for direct control of a file's FTAM attributes. This tool , the fchdoc command, can be used to modify or reconstruct a shadow file for an FTAM file. It is only in unusual circumstances that you may need to use the fchdoc command to deliberately override the default or defined attributes for a file.

Refer to the online man pages for information on the fchdoc command.

Index

Index

Index