Anonymous FTP file transfers initiate a chroot() call, so the new root directory is the home directory for the anonymous ftp user.

In this case, as with "secure TFTP" above (see Section 3.1.3.3), you must understand how these security mechanisms affect the entry of the HDSware path on the ViewStation. Your path on the ViewStation must take into account the new anonymous ftp root directory.

3.1.3.6 TFTP File Transfer Protocol on IBM RS6000 Systems

The IBM RS6000 does not start TFTP in its default configuration.

It is easy to start the TFTP protocol with the SMIT tool. If you use the fast path mechanism with the SMIT tool, this is very simple. Type:

```
smit inetd.conf
```

This points the tool to the inet daemon configuration file and gives you a menu for the daemon’s processes, (list, add, change, and delete). If you “list” the processes, you will see that TFTP is absent. Using the “add” command, you can click on TFTP and SMIT adds it to the running daemon processes.

The TFTP daemon does not run in secure mode by default, so it is ready to load the ViewStation’s files from any directory.

3.1.4 FTP

FTP is normally included with the host operating system software, but it is often not started (with a Sun installation, for example); refer to the */etc/inetd.conf* file for FTP as above. You should check to see if the FTP daemon is running; check for a comment character on the FTP line in the */inetd.conf* file. The following line should be present in the */etc/inetd.conf* file.

```
ftp  stream  tcp  nowait  root    /usr/etc/in.ftpd    in.ftpd
```

Follow the example above if you need to restart the inetd process.

FTP requires a valid username and a real password to run, so the appropriate accounts should be set up on the Sun (normal login accounts and passwords are sufficient, but they must be entered in the ViewStation’s Setup Mode Remote Hosts fields to be used for file loading).

FTP also verifies the user’s shell with the *getusershell()* query to the */etc/shells* file. Sun does not create this file in normal installation. Unix System V Release 4 and Solaris 2.x replace the Bourne shell (*sh*) with the Korn shell (*ksh*) as the standard shell. If the Korn shell is not added to the */etc/shells* file, or this file doesn’t exist, the query detects the Korn shell as invalid and the FTP request is denied. If you are using the Korn shell, you must make these changes.

3.1.4.1 Anonymous FTP File Transfer

Anonymous FTP file transfers do not require a password, but have other security limitations. All files to be transferred must be in a special anonymous FTP directory. You must set up a special anonymous FTP account if you intend to boot the ViewStation using the FTP protocol. Since FTP requires a username and password, and these can’t be entered from Monitor Mode, anonymous FTP is needed to boot.

Refer to your man pages for details about setting up an anonymous FTP account. In summary, you must enter a “anonymous ftp” user in the password file (*/etc/passwd*) with appropriate group and ownership limitations, and then use that anonymous ftp user’s home directory as the root directory for file transfers.

4. Restart the inetd process. Find the process identification number (PID) from the following command:

```
ps -aux | grep inetd
```

Then issue this command:

```
kill -1 <PID>
```

This restarts the inetd process which starts the TFTP daemon.

TFTP in "Secure Mode" on HP Systems

TFTP on HP/UX systems operates with security limitations. Access to the file system is limited by the TFTP configuration. There are three possibilities for setting the TFTP security.

1. File access is limited by the filenames or directories specified on the TFTP startup line in */etc/inetd.conf*, as described in the previous section.

```
tftp   dgram   udp   wait   root    /etc/in.tftpd    tftpd\
     /usr/lib/uxinstlf.700\
     /usr/lib/uxinstkern.700\
     /usr/lib/HDSware
```

In this case, TFTP file transfers are permitted for the two .700 files and any files in the */usr/lib/HDSware* directory. You could add other file names or directories as needed. Symbolic links are permitted in this path.

2. File access is limited to the home directory of the pseudo-user "tftp". In general, the "tftp" user is identified in the */etc/passwd* file as follows:

```
tftp:*:510:guest:tftp server:/usr/tftpdir:/bin/false
```

where tftp is the username, * is the password, guest is the membership, */usr/tftpdir* is the home directory, and the default shell is bogus since there is never a login to the tftp user's shell.

A TFTP file transfer initiates a chroot() call so it changes its root directory to the home directory of the tftp pseudo-user, which is */usr/tftpdir* in this case. All files transferred must be in this directory, and the file paths you enter must take this into account. Symbolic links are not permitted in this directory. This security mechanism for TFTP simulates the behavior of "TFTP secure mode" found in other operating systems.

3. You can specify both of these TFTP security variables. When you request a TFTP file transfer, TFTP first looks for the file using its home directory (which is */usr/tftpdir* in this example) as the root directory of its search. If the requested file is not found, it searches from the "root" directory specified in the TFTP startup line in */etc/inetd.conf*, which in the example above is */usr/lib/HDSware*.

Check the man pages on your HP system for the TFTP arguments and options for your system. Check the relevant files to see what the current TFTP configuration is on your system.

```
cd /usr/tftpboot
ln -s /usr .
```

Now a file access to /usr/tftpboot/foo is successful.

2. Do not use secure TFTP - Remove "-s /tftpboot" from the TFTP line and restart the inetd process, as described above. This means that TFTP is not secure and will move files from or to any directory on the system. This is convenient, but you may want to keep the security features.

3. Use a file Link - Link your files to */tftpboot*. For instance, you could create a tftpboot directory in your */usr* partition, */usr/tftpboot*, and link it to */tftpboot*, as follows:

```
cp -r /tftpboot /usr
rm -rf /tftpboot
ln -s /usr/tftpboot /tftpboot
```

3.1.3.5 TFTP on Hewlett Packard Systems

Typical HP installations do not start the TFTP daemon. When TFTP is started, various security mechanisms limit file access. These security mechanisms are discussed below.

On HP systems there is a startup line for TFTP present in the */etc/inetd.conf* file, but it is usually commented out. With the comment character removed, the TFTP protocol must be restarted. Note that TFTP can read only from directories available through the security mechanisms.

If you want to run TFTP as your file transfer protocol for the ViewStation, you must start it or verify that it is running, and then add the appropriate HDSware directory to the TFTP access list.

To start your TFTP service on the HP and add the HDSware directory (you must be root user to do these steps):

1. Check to see if TFTP is running; check for a comment character on the TFTP line in the */etc/inetd.conf* file. The line looks like this:

```
#tftp  dgram  udp  wait  root  /etc/in.tftpd  tftpd\
/usr/lib/uxinstlf.700\
/usr/lib/uxinstkern.700
```

2. Remove the comment character (#) from the beginning of the line.

3. Add the appropriate HDSware directory (in this case: */usr/lib/HDSware)* to the TFTP access list.

```
tftp  dgram  udp  wait  root  /etc/in.tftpd  tftpd\
/usr/lib/uxinstlf.700\
/usr/lib/uxinstkern.700\
/usr/lib/HDSware
```

Note the backslash character as a designator of line continuation.

you want to transfer files from other directories, you will have to make some changes.

You have several options:

- **Use secure TFTP**

This means that all your files must be located in the */tftpboot* directory. This partition is usually fairly small, so check the available storage space with the "df" command if you want to use this location. The HDSware tape requires about 60 MB for a complete installation, or about 15 MB for a minimal installation.

Note that the file transfer operation pre-pends */tftpboot* to whatever directory you specify in your paths, so take this into account when you enter your HDSware path in the HDSware menu of Setup Mode or in your configuration file.

- **Use unsecure TFTP**

Remove "-s /tftpboot" from the TFTP line. This means that TFTP is not secure and can move files from or to any directory on the system. This is convenient, but you may want to keep the security features.

- **Link your files to */tftpboot***

You could create a tftpboot directory in your */usr* partition, */usr/tftpboot*, and link it to */tftpboot*, as follows:

```
cp -r /tftpboot  /usr
rm -rf  /tftpboot
ln -s  /usr/tftpboot  /tftpboot
```

3.1.3.4 TFTP in Secure Mode on Sun Systems

If the TFTP process is in secure mode (check for the "-s /tftpboot" at the end of the line), it must change to the */tftpboot* directory to move requested files. If your files are not in that directory, or you don’t want to put them there, or you want to transfer files from other directories, you will have to make some changes. Note that this change to the */tftpboot* directory pre-pends that directory to your path, so enter your HDSware path accordingly.

You have several options:

1. Use secure TFTP - this means that all the files you want to transfer must be located in the secure directory, which is */tftpboot* by default; it can be any directory you specify on the tftp startup line. This partition is usually fairly small, so check the available storage space with the "df" command. The HDSware tape requires about 21 MB for a complete installation, or about 9 MB for a minimal installation.

Example #1: If the secure path is /tftpboot, then

```
cd /tftpboot
ln -s . tftpboot
```

Now a file access to /tftpboot/foo is successful.

Example #2: If the secure path is /usr/tftpboot, then

/host3/usr3/lib/Asterix/fonts/WPfonts

3.1.3 TFTP

TFTP is Trivial File Transfer Protocol. It is the default file access protocol for the HDS ViewStation. If TFTP doesn’t work, the simplest thing is to select another file transfer protocol, either FTP or NFS. This is selectable for each host in the Remote Hosts menu of Setup Mode.

Some host computers (such as Sun and HP) do not start TFTP automatically. This is the ViewStation’s default protocol.

3.1.3.1 Using TFTP

TFTP operates invisibly, since it requires no passwords or user identification. You can use TFTP manually by typing “tftp” at your user prompt. If it is running, you will get a “tftp>” prompt and you can do “?” to get information about TFTP commands.

Note that TFTP has a file size limitation of 16 MB. This prevents its use in loading the filesystem file for the ViewStation’s hard disk and may also limit its utility with moving other large files.

3.1.3.2 Starting TFTP on your Host

A startup line for TFTP is present in the */etc/inetd.conf* file on most host systems, but is usually commented out. With the comment character removed, the TFTP protocol is often run in "secure" mode. If you want to run TFTP as your file transfer protocol for the ViewStation, you must verify that it is running, and then decide if you want to use it in secure mode or not.

To start your TFTP service on a host (you must be root user to do these steps):

1. Check to see if TFTP was started. Look in the */etc/inetd.conf* file to see if the TFTP line has a comment character. The line looks like this:

```
#tftp   dgram   udp   wait   root   /usr/etc/in.tftpd   in.tftpd   -s   /tftpboot
```

2. Remove the comment character (#) from the beginning of the line.

3. Restart the inetd process. Find the process identification number (PID) from the following command:

```
ps -aux | grep inetd
```

Then issue this command:

```
kill -1 <PID>
```

This restarts the inetd process and starts the TFTP daemon.

3.1.3.3 TFTP in Secure Mode

If the TFTP process is in secure mode (check for the "-s /tftpboot" at the end of the line), the TFTP process must change to the */tftpboot* directory to move requested files. If your files are not in that directory, or you don’t want to put them there, or

For example, if the Local Mount Directory specifies “/fonts” (the leading slash is necessary), then a Mount Point is created in the ViewStation. The fontpath is specified as “/fonts/100dpi,/fonts/misc”. The Remote Mount Directory for that host is “/usr2/lib/X11/HDS/hds-fx/fonts”. Thus, when a font is requested, the ViewStation finds the /fonts mount point and the fontpath, strips off the mount point, prepends the Remote Mount Directory, and locates the desired font in the reconstructed path “/usr2/lib/X11/HDS/hds-fx/fonts/100dpi”, etc.

This file structure provides additional functionality for using the ViewStation on your network.

For instance, if you want to have a backup font host, you could specify “/fonts” as Local Mount Directories on both Host1 and Host2. The ViewStation’s mount point would first go to Host1, and if that file open failed, it would go on to the mount point on Host2, and so on. The Remote Mount Directory could be different for Host1 and Host2, but as long as those were correctly specified on the Remote Hosts menus, the files would be found.

Another example of customization for the ViewStation would be defining different fontpaths for different hosts. If you had one host that needed OPEN LOOK fonts and another host that needed word processing fonts, but you didn’t want to load all fonts on all hosts, you could use this configuration to handle the special fontpaths.

1. Set the ViewStation’s fontpath as follows (on the User Preferences Menu):

   /fonts1/100dpi,/fonts2/Xol,/fonts3/WPfonts

2. On the Remote Hosts Menu, set:

For Host 1

Local Mount Directory: /fonts1

Remote Mount Directory: /usr/libX11/hds-fx/fonts

which results in a full fontpath of:

/host1/usr/lib/X11/hds-fx/fonts/100dpi

For Host 2

Local Mount Directory: /fonts2

Remote Mount Directory: home/openwin/MITXol/fonts

which results in a full fontpath of:

/host2/home/openwin/MITXol/fonts/Xol

For Host 3

Local Mount Directory: /fonts3

Remote Mount Directory: /usr3/lib/Asterix/fonts

which results in a full fontpath of:

Note that this line sets "read-only" permission, and has a "-d" comment line argument.

- Check the transfer block size. The ViewStation uses a 8192 byte block size by default. If 8192 is too large for your network environment, you must set the correct value in the ViewStation's configuration file, which is */hds-fx/config/config.fx*. The ViewStation resource is:

  HDSsetup.NFS.block.size: 8192 *(permitted values are 128 to 8192)*
- Finally, run the command to export the filesystem:

  shareall

Check your system NFS man pages for more details and arguments.

3.1.2.3 Setting Up the ViewStation for NFS

1) Open the Setup Mode window

2) Click on the Setup Options icon

3) Select the Remote Hosts line

4) Select Remote Host 1 (or the host you want)

5) Enter the Host Name, Network Address (IP), and Host Type

6) Set the Access Protocol to NFS

7) Set both the Remote Mount Directory and the Local Mount Directory to the HDSware directory on exported file system on the host computer.

3.1.2.4 Using NFS for ViewStation File Access

The HDS ViewStation uses an internal file system that closely resembles the NFS file system, using mount points to establish local and remote path specifications. Local and Remote Mount Directories are entered in the Remote Hosts menu of Setup Mode, for each different host if desired. Individual paths, such as for fonts or clients, are accessed by means of the information the mount points provide.

A Local Mount Directory defines an internal ViewStation location for the server to look for things. The file system maintains an internal list of these Local Mount Directories and searches that list when it opens a file. (The list contains all the specified internal file locations, like HDS$$ROM, HostNames, Local Mount Directories, ViewStation device names like /dev/flash or /dev/tty1, etc.) If the Local Mount Directory is specified, then it is used as the mount point. If no Local Mount Directory is specified, the Host Name is prepended with a leading slash and it becomes the mount point.

A Remote Mount Directory defines a location on the remote host as a starting place for the ViewStation to look for things. The Remote Mount Directory is typically a directory location where the HDSware tape was loaded or some special fils are located. The Mount Point is the main directory, with subdirectories specified by the path itself. The Remote Mount Directory is prepended to the path (after the mount point is stripped off) to give the complete file location.

3.1.2 NFS

NFS (Network File System) is a file transfer protocol from Sun Microsystems. NFS allows the HDS ViewStation to access fonts and/or local clients as if they were on a local disk drive. Note that support for NFS is not present in the ViewStation's bootprom, so NFS is not available for first-time booting of the ViewStation.

Setting up NFS on your host system involves decisions about security and file system management. Consult your system administrator.

NFS allows the ViewStation to perform transparent file access over the network. The ViewStation dynamically mounts the filesystem and then transfers the file; it does not use a static mount. The HDSware tape may be loaded on any filesystem on any host available to the ViewStation.

There are two ways to handle NFS processes - one for Sun OS 4.1.x (or BSD types) and one for Solaris 2.x (or Sys V R4.x types). The NFS functions are the same, but the syntax and file names are different.

3.1.2.1 For Sun OS 4.1.x and BSD type UNIX:

To use NFS, you must export the filesystems and/or directories the ViewStation requires. For example, suppose you loaded the HDSware tape in the */home/HDS* filesystem.

- First, verify that the */home/HDS* directory is listed in the */etc/exports* file.
- If filesystem access needs to be restricted to the ViewStation, add the ViewStation's name to the access list for the desired filesystem. For example (in the */etc/exports* file):

  ```
  /home/HDS                    -access=hdssun5:hdsfx2
  ```

  Thus, only hdssun5 and hdsfx2 have mount privileges to the */home/HDS* filesystem. A read-only flag may also be added for these hosts' access permission.

  ```
  /home/HDS                    -access=hdssun5:hdsfx2, ro
  ```

- Check the transfer block size. The ViewStation uses a 8192 byte block size by default. If 8192 is too large for your network environment, you must set the correct value in the ViewStation's configuration file, which is */hds-fx/config/config.fx*. The ViewStation resource is:

  `HDSsetup.NFS.block.size: 8192` *(permitted values are 128 to 8192)*

- Finally, run the command to export the filesystem:

  ```
  exportfs -a
  ```

Check your system NFS man pages for more details and arguments.

3.1.2.2 For Solaris 2.x and Sys V R4.x type UNIX:

To use NFS, you must export the filesystems and/or directories the ViewStation requires. For example, suppose you loaded the HDSware tape in the */home/HDS* filesystem.

- First, add this line to the */etc/dfs/dfstab* file.

  ```
  share -F nfs -oro -d “For HDS X Terminals” /home/HDS
  ```

File Transfer Operations

This section discusses file transfer operations and three file transfer protocols, TFTP, FTP, and NFS that the ViewStation uses to load files from the host.

3.0 Section 3.0 - Network and Host System Operations

3.1 Network File Transfer Operations

Many of the ViewStation's operations depend on getting files from the host computer. These include its loading its server code for booting, loading font files, downloadable clients, and so on. The ViewStation knows the paths to these files but depends on the host's file transfer protocols to move them.

3.1.1 ViewStation File Transfer Protocols

There are several file transfer protocols that can move files to the ViewStation. These are NFS, TFTP (ViewStation's default), and FTP.

These processes are all configured and run on the host computer. The ViewStation depends on the availability and correct operation of these protocols.

3.1.1.1 Selecting a File Transfer Protocol

The ViewStation uses the file transfer protocol selected for a given host by the entry in the Remote Hosts menu of Setup Mode. This menu defines the protocol for each host, so you can communicate with one host via TFTP and another via NFS, for instance.

Other selections on the menu are also important for file transfer operations, such as access parameters (usernames and passwords), if applicable, and local and remote mount directories.

Note that NFS is available for booting the ViewStation with version 3.2 of HDSware. Earlier versions don't support NFS in the bootprom.