APPENDIX B

Configuring TFTP

As part of the CiscoWorks installation, you must configure your workstation to use the Trivial File Transfer Protocol (TFTP). TFTP enables you to transfer files to and from remote systems. With TFTP, the files belonging to the CiscoWorks applications Configuration Management, **nmconfig**, AutoInstall Manager, Software Library Manager, Device Software Manager, and Sync w/Sybase can be accessed, copied, modified, and downloaded.

You must verify that the TFTP daemon is enabled, the TFTP environment variable is set correctly, and a *tftpboot* directory exists. Instructions for these tasks are provided in this chapter. Refer to the section specific to your platform. For SunOS, refer to "Enabling TFTP on Sun Systems." For HP-UX, refer to "Enabling TFTP on HP-UX Systems."

Enabling TFTP on Sun Systems

As part of the SunOS and Solaris installation, you had the option of configuring TFTP. If you chose not to set up the TFTP boot files and directory during the installation, you must complete all the tasks in this section to enable TFTP on your Sun workstation.

Enabling the SunOS TFTP Daemon

If you are using the standard Sun software, verify that the TFTP daemon is enabled by completing the following steps:

Step 1 Log in as the superuser.

Step 2 Use a text editor such as **vi** to edit the */etc/inetd.conf* file by removing the pound sign [#] if it appears at the beginning of the tftp line. Depending on your system, the line that invokes the TFTP daemon should look similar to the following after you have removed the pound sign:

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

Step 3 Save the changes and exit your text editor.

Step 4 Display the process identification number for the *inetd* configuration by entering the following command:

On SunOS and HP-UX:

```
# ps  -ax | grep  -v grep | grep inetd
```

On Solaris:

```
# ps  -ef | grep  -v grep | grep inetd
```

The system response is similar to the following:

```
119  ?   S   0:05 inetd
```

The first number in the output is the process ID of the *inetd* configuration.

Step 5 Enable your system to read the edited */etc/inetd.conf* file by entering the following command:

```
# kill  -HUP process_ID_number
```

Replace the *process_ID_number* with the number displayed on your system as a result of Step 4. In this example, the process ID number is 119.

Step 6 Verify that TFTP is enabled by entering the following:

```
# netstat -a | grep tftp
```

The output should be similar to the following:

```
udp 0 0  *.tftp *.*
```

If there is no output, TFTP is not enabled. Check the */etc/inetd.conf* file for errors and repeat the previous steps.

For additional information on TFTP, refer to the UNIX manual pages on **tftp** and **tftpd**.

Setting the SunOS TFTPTYPE Environment Variable

TFTPTYPE is an environment variable used by the **cwconfigure** script to indicate which type of TFTP is being used. The Sun TFTP daemon requires that files being transferred must first exist as "dummy" files on the destination system. Other implementations require that the files do not exist on the destination system.

TFTPTYPE can take the value OVERWRITE (the file must exist and is overwritten) or NOOVERWRITE (the file must not exist and cannot be overwritten). If you are using the standard Sun TFTP daemon, no action is required to set the *TFTPTYPE* variable. Otherwise, you must set *TFTPTYPE* accordingly. For example, use **setenv TFTPTYPE NOOVERWRITE**.

Creating the SunOS tftpboot Directory

You can use the */tftpboot* directory to save and store device configuration files when you use CiscoWorks applications supported by TFTP. For example, the SNMP device configuration file is saved in the form of a TFTP boot file.

Creating and using the */tftpboot* directory on your system is required only if you want to take advantage of all CiscoWorks applications. The */tftpboot* directory is accessible by all users. To protect the security of your system and limit access to it, you can choose not to create this directory. However, without a */tftpboot* directory, you cannot use the CiscoWorks AutoInstall Manager, Configuration Manager, and Software Management applications.

Note If you want to use the CiscoWorks Software Library Manager or Device Software Manager applications, allocate at least 4 MB of space to the /*tftpboot* partition.

Timesaver If you upgraded from an earlier version of CiscoWorks, the */tftpboot* directory may already exist on your system. In that case, you need not perform these steps.

Creating the SunOS or Solaris TFTP Home Directory

To create the */tftpboot* directory, perform the following steps:

Step 1 As the superuser, create the */tftpboot* directory if it does not exist by entering the following command :

```
# mkdir /tftpboot
```

Step 2 Modify the permissions for the */tftpboot* directory by entering the following command:

```
# chmod 777 /tftpboot
```

Now all users accessing the */tftpboot* directory have read, write, and execute permissions. This is a CiscoWorks requirement.

Enabling TFTP on HP-UX Systems

As part of the HP-UX installation, you had the option of configuring TFTP. If you chose not to set up the TFTP boot files and directory during installation, you must complete all the tasks in this section to enable TFTP on your HP-UX system.

Configuring the HP-UX TFTP Daemon

To set up the TFTP daemon, perform the following steps:

Step 1 Log in as the superuser.

For information on how to become the superuser, refer to the section “Becoming the Superuser” in the “Installing and Configuring CiscoWorks” chapter.

Step 2 Use a text editor to add the following line to the */etc/services* file:

```
tftp    69/udp    # Trivial File Transfer Protocol
```

Step 3 Add the following line to the */etc/inetd.conf* file:

```
tftp    dgram udp wait     root /etc/tftpd    tftpd
```

Step 4 Reconfigure the TFTP daemon by entering the following at the UNIX command prompt:

```
# /etc/inetd -c
```

Step 5 Add the user *tftp* to the */etc/passwd* file with a new line similar to the following:

tftp:*:510:10:Trivial FTP user:*directory name***:/bin/false**

In this line, *directory name* is the TFTP home directory.

Step 6 Verify that TFTP is enabled by entering the following command:

```
# netstat -a | grep tftp
```

The output should be similar to the following:

```
udp 0 0  *.tftp *.*
```

If there is no output, TFTP is not enabled. Check the */etc/inetd.conf* file for errors and repeat the previous steps.

For additional information on TFTP, refer to the UNIX manual pages on **tftp** and **tftpd**.

Setting the HP-UX TFTPTYPE Environment Variable

TFTPTYPE is an environment variable used by the **cwconfigure** script to indicate which type of TFTP is being used. Other implementations require that the TFTP file does not exist on the destination system.

TFTPTYPE can take the value OVERWRITE (the file must exist and is overwritten) or NOOVERWRITE (the file must not exist and cannot be overwritten). Otherwise, you must set *TFTPTYPE* accordingly. For example, use **setenv TFTPTYPE NOOVERWRITE**.

Creating the HP-UX TFTP Home Directory

The TFTP home directory temporarily holds files that are being transferred between your system and devices on your network.

Creating the TFTP home directory is optional, because the TFTP home directory is accessible to all users. To protect the security of your system, you may choose not to set up this directory. However, without a TFTP home directory, you will be unable to use the CiscoWorks AutoInstall Manager, Configuration Manager, and Software Management applications.

Note If you want to use the CiscoWorks Software Library Manager or Device Software Manager applications, allocate at least 4 MB of space for the TFTP home directory.

To create the TFTP home directory, perform the following steps:

Step 1 Log in as the superuser.

For information on how to become the superuser, refer to the section "Becoming the Superuser" in the "Installing and Configuring CiscoWorks" chapter.

Step 2 Create the directory by entering the following command:

```
# mkdir directory_name
```

Specify the correct path for the new directory, or make sure you are already in that directory.

Step 3 Change the ownership of the directory to *tftp* by entering the following command:

```
# chown tftp directory_name
```

For example, on HP-UX the TFTP directory may be */usr/tftp*.

Step 4 Change the group ownership of the directory to *guest* by entering the following command:

```
# chgrp guest directory_name
```

Step 5 Give all users *tftp* read, write, and execute permissions by entering the following command:

```
# chmod 777 directory_name
```

Now all users using the TFTP boot directory have read, write, and execute permissions.