Using Networking Commands in DOS

OnNet™ for Windows version 2.0 (July 1995)

Using Networking Commands in DOS

OnNet™ for Windows version 2.0 (July 1995)

Appendix B Keyboard Scan Codes

Appendix C Graphics/Color Display Attributes

Chapter 10
Backing Up and Restoring Files

When you perform regular backups of your files, you protect your data from loss and corruption. You can use the **tar** command to backup all or part of your hard disk. The **tar** command creates an archive, the .TAR file, that includes copies of your files and additional information needed to restore data to your disk. You can list the information to find out what data the .TAR file contains and when it was archived.

This chapter describes how to backup and restore files to either an attached or remote tape drive, or how to back up files to local or network mounted drives. This chapter also discusses how to make incremental backups of your system so that you do not have to back up your entire system each time.

10.1 Before You Start Backing Up or Restoring Files

If you plan to back up files on a remote host, you should ensure that

- You can use network security programs if any are installed.
- You have a password and can log in to the remote system.

On a UNIX system, you should ensure that

- You know the correct device driver (*/dev*) to use.
- Your tape is ready for use.

If you are uncertain about this information, contact the remote host system administrator.

10.2 Using a Remote Tape Drive

You can use the procedures in the following sections to back up files on your personal computer. If you want more information about how to specify files that you want to back up, turn to section 10.4, Using tar Command Syntax.

Also, if you plan to use the **rmt** command, ensure that the remote system supports it and does not rewind your tape automatically.

To back up files on a remote tape drive

1. Change directories to the root of your file system or to the subdirectory that you want to archive.

2. Use the **tar** command and include the **cvf** options, your user ID, the remote host and device for the tape drive, and the target directories and files that you want to archive.

   The **c** and **v** options create and display a .TAR file. The **f** option lets you indicate the .TAR file or remote device. By default, the **tar** command starts working at the current directory. It creates a .TAR file that contains copies of the files and an index of all directory and filenames.

   For example, user Chris specifies a tape on the remote host vienna at the device /dev/rmt0. (This device may be different on your UNIX machine.) The dot (**.**) indicates that the target is the current directory and everything below it:

   ```
   tar cvf chris@vienna:/dev/rmt0 .
   ```

3. Enter your password at the prompt from the remote host.

   If you used the **v** option in step 2, the **tar** command lists files as it archives them. The archive is complete when the listing ends.

4. Display the .TAR file to verify that it is properly archived.

   For example, Chris lists the remote tape drive device with the **t** option:

   ```
   tar tf chris@vienna:/dev/rmt0
   ```

   If the **tar** command reports anything except a file listing, you might have difficulty restoring one or more files from this archive. In this case, repeat the file backup procedure.

   If you want a record of this archive, you can redirect the listing to a file. Use the **v** option to display the date, time, protections, and size of each file in the archive. For example, to direct verbose output to the file TARLIST.TXT, Chris enters the following:

   ```
   tar tvf chris@vienna:/dev/rmt0 tarlist.txt
   ```

   Note: If you backed up files to a remote host that runs UNIX, the **tar** command displays files with the UNIX slash (*/filename*). For more information, see section 10.4.1, Choosing UNIX

or DOS File Syntax.

5. Take the remote tape off-line to ensure that no one else uses it before you remove it from the tape drive.

   For example, Chris uses the **rmt** command to take the tape off-line. The **h** option specifies the host vienna and the **f** option indicates the device to take off-line:

   ```
   rmt -h vienna -f /dev/rmt0 offl
   ```

To restore files from a remote tape

1. Ensure that your backup tape is properly mounted and ready to use.
2. Change directories to the root of your file system or to a subdirectory that you want to restore.
3. Use the **t** option to list files on the remote tape.

   –or–

   Refer to any files that you may have created that contain redirected listings of the archive.

   For example, Chris lists files from the tape on vienna at the /dev/rmt.0 tape drive device:

   ```
   tar tvf chris@vienna:/dev/rmt0

   drw-rw-rw-     0 Sept 10 16:53:32 1992 ./
   -rw-rw-rw- 10230 Sept 10 16:53:32 1992 ./aria.txt
   -rw-rw-rw-  3510 Sept 10 16:53:32 1992 ./chorus.txt
   ```

4. Use the **x** option to restore files.

   By default, the **tar** command restores the entire archive. You can use the **tar p** option to prevent the **tar** command from overwriting files that were modified on your disk after you backed them up. For example, Chris enters the following:

   ```
   tar xpvf chris@vienna:/dev/rmt0
   ```

To restore specific files or directories

Specify the file or directory name (exactly as listed with the **t** option).

For example, the following command line restores the file ./aria.txt (not aria.txt):

```
tar xpvf chris@vienna:/dev/rmt0 ./aria.txt
```

10.3 Using a Local or Network Mounted Drive

You can back up and restore files to disks or tape on a local or network mounted drive.

To back up files to a local or network mounted drive

1. Insert a formatted disk or tape in any drive of your PC, or switch to your network drive.

   Ensure that you have enough disks or tapes to hold the files that you plan to archive. If you are archiving files to a remote file system, ensure that the space allotted is sufficient. The **tar** command notifies you when disks or tapes are full so that you can continue the backup with additional media.

2. Change directories to the root of your file system or to the subdirectory that you want to archive.

   The examples in this procedure assume that the current directory is the root. The backup targets two subdirectories immediately below the root.

3. Use the **tar** command and include options, the drive and .TAR filename, and the target directories or files that you want to archive.

   For example, use the **c** option to create a new archive file, the **f** option to name the archive MY.TAR, and the **v** option to display files during processing. The device is drive A and the targets are the directories named ONE and TWO.

   ```
   tar cfv a:my.tar .\ONE .\TWO
   ```

   Do not back up to a .TAR file in your current directory or **tar** attempts to archive the .TAR file itself.

4. Insert another formatted disk or tape in the drive when or if you see the following message:

   ```
   Disk full. Insert next floppy and type space to continue or Ctrl+C to abort.
   ```

5. To continue, press the spacebar.

   –or–

   To end, press Ctrl+C.

6. Remove the disk from the local drive when you see the following message:

   ```
   End of file
   ```

To restore files from a local or network mounted drive

1. Insert the disk that contains the .TAR file in a local drive or switch to the network drive.

2. Change directories to the root of your file system or to a subdirectory that you want to restore.

The examples in this procedure assume that the current directory is the root.

3. Use the **tar** command and include options, the drive and .TAR filename, and the target directories or files that you want to restore.

   The following example uses the **x** option to extract files from the archive file MY.TAR. The device is drive A and the targets are the directories named .\ONE and .\TWO.

   ```
   tar xvf a:my.tar .\ONE .\TWO
   ```

   The **tar** command restores two subdirectories immediately below the root.

4. Remove the disk from the local drive.

Note: If you are restoring a single file, the **tar** command searches the archive and may take some time before it lists the filename. The **tar** command does not report an error when it fails to find files in the archive.

10.4 Using tar Command Syntax

Make sure that the target that you specify on the command line matches the .TAR file. For example, when you back up the file C:\TAXES\CURRENT.TXT,

If your current directory is	The default .TAR filename is
root (for example, `C:\>`)	TAXES\CURRENT.TAR
`C:\TAXES>`	CURRENT.TXT

If the specified target does not match the .TAR file, the **tar** command can fail or give unintended results.

If you want to modify the **tar** default behavior and specify a larger or smaller group of files:

Use this syntax from any directory	To back up (and restore)
Slash or backslash (\ or /)	All directories from the root: **`tar cvf chris@vienna:/dev/rmt0 /`**
Dot (**.**)	Your current directory and everything below it: **`tar cv chris@vienna:/dev/rmt0 .`**
Dot (.) and the other pathname	Your current directory and other directories: **`tar cv chris@vienna:/dev/rmt0 . /arias`**
The wildcard abbreviation ***.***	All files in your current directory on a DOS system only: **`tar cvf a:operas.tar *.*`**
A specific pathname	The file or a directory and its named subdirectories: **`tar cvf a:operas.tar \current\arias.txt`**

Use the same command syntax to create, list, and restore files. By default, the **tar** command restores the complete .TAR file into your current directory. In addition, **tar** references files according to the index in the .TAR file and attempts to restore the structure that it archives. For this reason, you should restore files into the correct directories so that the **tar** command does not

create multiple copies of directories and files. For example,

If you create with this syntax	Restore with this syntax
`c:\opera>tar cvf one.tar c:\opera`	`c:\opera>tar xv one.tar \opera\arias.txt`
`c:\opera>tar cvf one.tar .`	`c:\opera>tar xvf one.ta .\arias.txt`
`c:\opera>tar cvf one.tar *.*`	`c:\opera>tar xv one.tar arias.txt`

Note: If you use the dot (.) syntax as the target filename, do not back up to a .TAR file in your current directory or **tar** attempts to archive the .TAR file itself.

10.4.1 Choosing UNIX or DOS File Syntax

Use UNIX file syntax to restore files from a UNIX system to a personal computer. Note, however, that the **tar** command truncates long UNIX filenames to legal DOS names. This operation can create a file with the same name as a file already on your disk.

Use DOS file syntax to archive and restore files on a DOS drive.

Caution: If you are going to create a .TAR file on a DOS machine for later restoration to a UNIX system, you should not include a drive letter when specifying the target filename. The UNIX system cannot process drive letters and will in fact include the letter and colon in the restored filename.

10.5 Choosing Backup Types

Data that changes frequently needs frequent backups; data that rarely changes does not need frequent backups. Based on the importance of your data and how often it changes, you can use several **tar** command options to implement any one of the following backup types.

Use this type	To archive
Full Backup	Everything on the disk, including system and hidden files. Typically, you always perform a full backup when a system goes into service and when system software changes. You can also perform full backups at other times. Consult your system administrator for advice and specific information about backup policies at your site.For an example, see section 10.2, Using a Remote Tape Drive. **Note:** The **tar** command does not restore DOS hidden and read-only file attributes. It does uniformly give read-write permissions to user, group, and other when it restores files to UNIX systems.
Partial Backup	A subset of files on the disk. Typically, a partial backup archives only the data and system configuration files that you specify. The backup includes all files that you specify even when the data in them has not changed since the last backup. For an example, see section 10.3, Using a Local or Network Mounted Drive.
Incremental Backup	Archive only files that change between backups. An incremental backup uses **tar** options to target changed files for backup. Because each backup includes different sets of files, keep the media for incremental backups separate and do not overwrite them until the next full backup. For an example, see section 10.6, Making Incremental Backups.

10.6 Making Incremental Backups

When you create or modify a DOS file, the operating system sets an archive bit to indicate whether or not the file requires back up. At first, the bit is turned on indicating that the file requires backup. After you back up the file, the archive bit is off until you change the file.

To make an incremental backup

Assign values (0-9) known as “levels” to backups.

Except for 0, the values have no significance until you assign a meaning to each level. When you use the **0-9** option, the **tar** command stores the level and date of the archive in a date file. For example, Chris assigns level 2 to a backup of the /operas directory:

```
C:\> tar c2vf chris@vienna:/dev/rmt0 /operas
```

At the next backup, when you specify a level, the **tar** command reads the date file and selects only files that meet both of the following criteria:

- A backup level that is less than or equal to the level that you specify on the **tar** command line. If you specify 2, **tar** selects files at levels 0, 1, and 2 to archive.
- A file creation date that changed after the date of the previous backup.

Note: If you plan to make incremental backups, do so consistently.

To display the contents of the date file

Use the **ddates** command to list the dates and times of your previous backups. When you make incremental backups, **tar** keeps the dates of the backups in a separate file. The **ddates** command displays the contents of this dump-dates file. Use the `date-file=` parameter in the `[pctcp tar]` section of the PCTCP.INI configuration file to specify the name of this file.

To see the results of an incremental backup, enter the following:

```
C:\> ddates

Level 0: never
Level 1: never
Level 2: never
Level 3: never
Level 4: never
Level 5: Tue Jun 16 14:31:11 1992
Level 6: never
Level 7: never
Level 8: never
Level 9: never
```

To display the archive bit

Use the DOS **attrib** command.

To modify the archive bit

Use the DOS **backup**, **restore**, and **xcopy** commands. Ensure that the way that you use these commands is compatible with your backup strategy.

To mark files to prevent subsequent archiving

Use the **u** option.

The following command archives all files in the ONE directory that have archive bits turned on:

```
tar cuvf a:my.tar .\one
```

This command also turns off the archive bits of the files on your disk. When you next use the **tar u** command, it selects only files that changed since the previous backup. However, if you need to restore something from the .TAR file, the archive bit is on, reflecting the file status at the time of archive.

Note: If you make incremental backups with the **u** option, do not use it when you do complete backups. In this way, the **tar** command does not use the DOS archive bit and selects all files to back up.

To restore files from incremental backups

First restore the most recent files. Then work in succession back to the earliest files. Use the **p** option to prevent **tar** from replacing newer versions of files with older versions from the archive.

10.7 Configuring tar Command Line Options

You can automatically use **tar** command line options if you configure the `[pctcp tar]` section of the PCTCP.INI file. Configuring this section is useful if you routinely back up your system to the same remote system or to the same drive or remote device.

For example, your `[pctcp tar]` section may resemble the following:

```
[pctcp tar]
date-file = \etc\dates.txt
user = chris
host = 128.127.50.100
file = /dev/rmt0
```

10.8 Troubleshooting Backing Up and Restoring Files

This section provides possible solutions to situations that you can encounter when backing up and restoring files. The situation is described first, followed by the meaning of the situation and the action to take.

After using the **t** option to display that the .TAR file is properly archived, tar reports something other than a file listing.

One or more files might not have been backed up properly.

Repeat the file backup procedure.

You are unable to decompress a compressed .TAR file.

The .TAR file may have been created on a UNIX system that uses a 16-bit compression scheme. PC/TCP Network Software uses a 12-bit compression scheme that is incompatible with a 16-bit compression scheme.

You need to decompress files on a system that uses the same compression scheme that was used to compress the file.

Appendix C
Graphics/Color Display Attributes

This appendix lists the color settings for IBM personal computer CGA monitor adapters. If you have a different monitor adapter, you may need to experiment to define the appropriate color values.For more information, see the **setcolor** command in the *Command Reference*.

You can set color display attributes for terminal emulators using parameters in the `[pctcp screen]` and `[pctcp 3270]` sections of your PCTCP.INI configuration file. Refer to the following table to determine the values of colors that you want to use. For details, see Chapter 5, Customizing Terminal Emulation.

Note that colors with hexadecimal values of 80 through FF are flashing on Color Graphics and Monochrome adapters.

Note also that if you use a color labeled “high intensity” to display normal characters (the first value of the `ftp-attr=` parameter), the VT220 escape sequence for turning on the bold attribute causes these characters to return to normal intensity.

Value		**Color/Graphics Adapter**		**Monochrome Adapter**
Hexadecimal	**Decimal**	**Background**	**Foreground**	
00	000	Black	Black	No display

01	001	Black	Blue	Underline
02	002	Black	Green	Normal
03	003	Black	Cyan	Normal
04	004	Black	Red	Normal
05	005	Black	Magenta	Normal
06	006	Black	Brown	Normal
07	007	Black	Light Grey	Normal
08	008	Black	Dark Grey	No display
09	009	Black	Light Blue	High intensity underline
0A	010	Black	Light Green	High intensity
0B	011	Black	Light Cyan	High intensity
0C	012	Black	Light Red	High intensity
0D	013	Black	Light Magenta	High intensity
0E	014	Black	Yellow	High intensity
0F	015	Black	White	High intensity
10	016	Blue	Black	Normal
11	017	Blue	Blue	Underline
12	018	Blue	Green	Normal
13	019	Blue	Cyan	Normal
14	020	Blue	Red	Normal
15	021	Blue	Magenta	Normal
16	022	Blue	Brown	Normal
17	023	Blue	Light Grey	Normal
18	024	Blue	Dark Grey	High intensity
19	025	Blue	Light Blue	High intensity underline
1A	026	Blue	Light Green	High intensity

1B	027	Blue	Light Cyan	High intensity
1C	028	Blue	Light Red	High intensity
1D	029	Blue	Light Magenta	High intensity
1E	030	Blue	Yellow	High intensity
1F	031	Blue	White	High intensity
20	032	Green	Black	Normal
21	033	Green	Blue	Underline
22	034	Green	Green	Normal
23	035	Green	Cyan	Normal
24	036	Green	Red	Normal
25	037	Green	Magenta	Normal
26	038	Green	Brown	Normal
27	039	Green	Light Grey	Normal
28	040	Green	Dark Grey	High intensity
29	041	Green	Light Blue	High intensity underline
2A	042	Green	Light Green	High intensity
2B	043	Green	Light Cyan	High intensity
2C	044	Green	Light Red	High intensity
2D	045	Green	Light Magenta	High intensity
2E	046	Green	Yellow	High intensity
2F	047	Green	White	High intensity
30	048	Cyan	Black	Normal
31	049	Cyan	Blue	Underline
32	050	Cyan	Green	Normal
33	051	Cyan	Cyan	Normal
34	052	Cyan	Red	Normal
35	053	Cyan	Magenta	Normal

36	054	Cyan	Brown	Normal
37	055	Cyan	Light Grey	Normal
38	056	Cyan	Dark Grey	High intensity
39	057	Cyan	Light Blue	High intensity underline
3A	058	Cyan	Light Green	High intensity
3B	059	Cyan	Light Cyan	High intensity
3C	060	Cyan	Light Red	High intensity
3D	061	Cyan	Light Magenta	High intensity
3E	062	Cyan	Yellow	High intensity
3F	063	Cyan	White	High intensity
40	064	Red	Black	Normal
41	065	Red	Blue	Underline
42	066	Red	Green	Normal
43	067	Red	Cyan	Normal
44	068	Red	Red	Normal
45	069	Red	Magenta	Normal
46	070	Red	Brown	Normal
47	071	Red	Light Grey	Normal
48	072	Red	Dark Grey	High intensity
49	073	Red	Light Blue	High intensity underline
4A	074	Red	Light Green	High intensity
4B	075	Red	Light Cyan	High intensity
4C	076	Red	Light Red	High intensity
4D	077	Red	Light Magenta	High intensity
4E	078	Red	Yellow	High intensity
4F	079	Red	White	High intensity

50	080	Magenta	Black	Normal
51	081	Magenta	Blue	Underline
52	082	Magenta	Green	Normal
53	083	Magenta	Cyan	Normal
54	084	Magenta	Red	Normal
55	085	Magenta	Magenta	Normal
56	086	Magenta	Brown	Normal
57	087	Magenta	Light Grey	Normal
58	088	Magenta	Dark Grey	High intensity
59	089	Magenta	Light Blue	High intensity underline
5A	090	Magenta	Light Green	High intensity
5B	091	Magenta	Light Cyan	High intensity
5C	092	Magenta	Light Red	High intensity
5D	093	Magenta	Light Magenta	High intensity
5E	094	Magenta	Yellow	High intensity
5F	095	Magenta	White	High intensity
60	096	Yellow	Black	Normal
61	097	Yellow	Blue	Underline
62	098	Yellow	Green	Normal
63	099	Yellow	Cyan	Normal
64	100	Yellow	Red	Normal
65	101	Yellow	Magenta	Normal
66	102	Yellow	Brown	Normal
67	103	Yellow	Light Grey	Normal
68	104	Yellow	Dark Grey	High intensity
69	105	Yellow	Light Blue	High intensity underline

6A	106	Yellow	Light Green	High intensity
6B	107	Yellow	Light Cyan	High intensity
6C	108	Yellow	Light Red	High intensity
6D	109	Yellow	Light Magenta	High intensity
6E	110	Yellow	Yellow	High intensity
6F	111	Yellow	White	High intensity
70	112	White	Black	Reverse video
71	113	White	Blue	Underline
72	114	White	Green	Normal
73	115	White	Cyan	Normal
74	116	White	Red	Normal
75	117	White	Magenta	Normal
76	118	White	Brown	Normal
77	119	White	Light Grey	Normal
78	120	White	Dark Grey	Reverse video
79	121	White	Light Blue	High intensity underline
7A	122	White	Light Green	High intensity
7B	123	White	Light Cyan	High intensity
7C	124	White	Light Red	High intensity
7D	125	White	Light Magenta	High intensity
7E	126	White	Yellow	High intensity
7F	127	White	White	High intensity
80	128	Black	Black	No display
81	129	Black	Blue	Underline
82	130	Black	Green	Normal
83	131	Black	Cyan	Normal
84	132	Black	Red	Normal

85	133	Black	Magenta	Normal
86	134	Black	Brown	Normal
87	135	Black	Light Grey	Normal
88	136	Black	Dark Grey	No display
89	137	Black	Light Blue	High intensity underline
8A	138	Black	Light Green	High intensity
8B	139	Black	Light Cyan	High intensity
8C	140	Black	Light Red	High intensity
8D	141	Black	Light Magenta	High intensity
8E	142	Black	Yellow	High intensity
8F	143	Black	White	High intensity
90	144	Blue	Black	Normal
91	145	Blue	Blue	Underline
92	146	Blue	Green	Normal
93	147	Blue	Cyan	Normal
94	148	Blue	Red	Normal
95	149	Blue	Magenta	Normal
96	150	Blue	Brown	Normal
97	151	Blue	Light Grey	Normal
98	152	Blue	Dark Grey	High intensity
99	153	Blue	Light Blue	High intensity underline
9A	154	Blue	Light Green	High intensity
9B	155	Blue	Light Cyan	High intensity
9C	156	Blue	Light Red	High intensity
9D	157	Blue	Light Magenta	High intensity
9E	158	Blue	Yellow	High intensity

9F	159	Blue	White	High intensity
A0	160	Green	Black	Normal
A1	161	Green	Blue	Underline
A2	162	Green	Green	Normal
A3	163	Green	Cyan	Normal
A4	164	Green	Red	Normal
A5	165	Green	Magenta	Normal
A6	166	Green	Brown	Normal
A7	167	Green	Light Grey	Normal
A8	168	Green	Dark Grey	High intensity
A9	169	Green	Light Blue	High intensity underline
AA	170	Green	Light Green	High intensity
AB	171	Green	Light Cyan	High intensity
AC	172	Green	Light Red	High intensity
AD	173	Green	Light Magenta	High intensity
AE	174	Green	Yellow	High intensity
AF	175	Green	White	High intensity
B0	176	Cyan	Black	Normal
B1	177	Cyan	Blue	Underline
B2	178	Cyan	Green	Normal
B3	179	Cyan	Cyan	Normal
B4	180	Cyan	Red	Normal
B5	181	Cyan	Magenta	Normal
B6	182	Cyan	Brown	Normal
B7	183	Cyan	Light Grey	Normal
B8	184	Cyan	Dark Grey	High intensity
B9	185	Cyan	Light Blue	High intensity

				underline
BA	186	Cyan	Light Green	High intensity
BB	187	Cyan	Light Cyan	High intensity
BC	188	Cyan	Light Red	High intensity
BD	189	Cyan	Light Magenta	High intensity
BE	190	Cyan	Yellow	High intensity
BF	191	Cyan	White	High intensity
C0	192	Red	Black	Normal
C1	193	Red	Blue	Underline
C2	194	Red	Green	Normal
C3	195	Red	Cyan	Normal
C4	196	Red	Red	Normal
C5	197	Red	Magenta	Normal
C6	198	Red	Brown	Normal
C7	199	Red	Light Grey	Normal
C8	200	Red	Dark Grey	High intensity
C9	201	Red	Light Blue	High intensity underline
CA	202	Red	Light Green	High intensity
CB	203	Red	Light Cyan	High intensity
CC	204	Red	Light Red	High intensity
CD	205	Red	Light Magenta	High intensity
CE	206	Red	Yellow	High intensity
CF	207	Red	White	High intensity
D0	208	Magenta	Black	Normal
D1	209	Magenta	Blue	Underline
D2	210	Magenta	Green	Normal
D3	211	Magenta	Cyan	Normal

D4	212	Magenta	Red	Normal
D5	213	Magenta	Magenta	Normal
D6	214	Magenta	Brown	Normal
D7	215	Magenta	Light Grey	Normal
D8	216	Magenta	Dark Grey	High intensity
D9	217	Magenta	Light Blue	High intensity underline
DA	218	Magenta	Light Green	High intensity
DB	219	Magenta	Light Cyan	High intensity
DC	220	Magenta	Light Red	High intensity
DD	221	Magenta	Light Magenta	High intensity
DE	222	Magenta	Yellow	High intensity
DF	223	Magenta	White	High intensity
E0	224	Yellow	Black	Normal
E1	225	Yellow	Blue	Underline
E2	226	Yellow	Green	Normal
E3	227	Yellow	Cyan	Normal
E4	228	Yellow	Red	Normal
E5	229	Yellow	Magenta	Normal
E6	230	Yellow	Brown	Normal
E7	231	Yellow	Light Grey	Normal
E8	232	Yellow	Dark Grey	High intensity
E9	233	Yellow	Light Blue	High intensity underline
EA	234	Yellow	Light Green	High intensity
EB	235	Yellow	Light Cyan	High intensity
EC	236	Yellow	Light Red	High intensity
ED	237	Yellow	Light Magenta	High intensity

EE	238	Yellow	Yellow	High intensity
EF	239	Yellow	White	High intensity
F0	240	White	Black	Reverse video
F1	241	White	Blue	Underline
F2	242	White	Green	Normal
F3	243	White	Cyan	Normal
F4	244	White	Red	Normal
F5	245	White	Magenta	Normal
F6	246	White	Brown	Normal
F7	247	White	Light Grey	Normal
F8	248	White	Dark Grey	Reverse video
F9	249	White	Light Blue	High intensity underline
FA	250	White	Light Green	High intensity
FB	251	White	Light Cyan	High intensity
FC	252	White	Light Red	High intensity
FD	253	White	Light Magenta	High intensity
FE	254	White	Yellow	High intensity
FF	255	White	White	High intensity

Appendix C Graphics/Color Display Attributes

Chapter 5
Customizing Terminal Emulation

You can customize the default behavior of the terminal emulators in remote login applications. This chapter describes how to

- Change terminal types and screen sizes.
- Enable the exchange of data in various modes: binary mode, line mode, echo mode.
- Customize terminal characteristics and screen colors.
- Encrypt data in a Telnet session.
- Use the scrollback buffer.
- Specify a display for the X Window System.
- Troubleshoot terminal emulation.

Refer to Chapter 1, Introduction to see which terminal emulation programs discussed in this chapter are included with your networking software.

5.1 Before You Start Customizing Terminal Emulation

You should ensure that

- You understand the default behavior of the terminal emulators.
- You understand the requirements and capabilities of applications that you want to use on the remote host.
- The remote system is configured to support the terminal emulation features that you want to use.
- Your PC has a video card that is configured to support the screen size and colors that you want to use.

If you are unsure about any of this information, contact your system administrator or the remote host system administrator.

5.2 Requesting Terminal Types and Screen Sizes with tn

The tn program normally negotiates with the remote host for the most appropriate terminal type when you start a remote login session. However, you can request specific terminal types and screen sizes on the login command line.

Requesting a terminal type for a tn session does not guarantee that it will be established. Some systems may not support the requested terminal type; the remote host may reject or ignore the request.

If you want to specify a particular terminal type, you should consider

- The operating system running on the remote host (for example, the emulators support DEC VT and IBM PC terminal types if the remote host is running UNIX software, and IBM 3270 terminal types if the remote host is an IBM mainframe).

- Applications that you want to use on the remote host. Certain applications may be compatible with only certain terminal types, or may work best with specific screen sizes.

5.2.1 Requesting a Range of Terminal Types

Normally, when negotiating a terminal type, tn sends names from an ordered list in response to requests from the remote host. The tn program cycles through the list until the remote host accepts a terminal type or stops requesting terminal types. The default order in which tn negotiates for terminal types is DEC VT220, DEC VT100, DEC VT52, IBM PC, IBM 3278 Model 2 with extended attribute support, and IBM 3278 Model 2 without extended attributes. Terminals with extended attributes support more screen color and highlighting features than 3270 terminals.

To request a range of terminal types, or a different starting point in the list

Use the **-t** *ttype* option, where *ttype* is one of the following terminal type keywords:

```
vt vt220 vt100 vt52 ibmpc 3277 3278 3279
```

Terminal type keywords are case sensitive; enter them exactly as shown.

Table 5-1 summarizes the terminal types that **tn** offers based on each *ttype* keyword, and indicates the order in which they are offered. The E after IBM terminal types indicates extended attribute support.

Use this keyword	To request these terminal types
`vt`	DEC VT220, DEC VT100, DEC VT52
`vt220`	DEC VT220, DEC VT100, DEC VT52, IBM PC, IBM 3278-2-E, IBM 3278-2
`vt100`	DEC VT100, DEC VT52, IBM PC, IBM 3278-2-E, IBM 3278-2
`vt52`	DEC VT52, IBM PC, IBM 3278-2-E, IBM 3278-2
`ibmpc`	IBM PC, IBM 3278-2-E, IBM 3278-2
`3277`	IBM 3277-2
`3278`	IBM 3278-2-E, IBM 3278-2
`3279`	IBM 3279-2-E, IBM 3279-2

To shorten the negotiation list

Use the **-t** option on the tn command line.

This shortens the time that it takes to establish a connection to the remote host. The following sample command requests that tn offer only VT terminal types in negotiating for a session on remote host ball.toys.com:

```
C:\>tn -t vt ball.toys.com
```

If the remote host accepts the VT220 terminal type, negotiation ends. Otherwise, tn offers the VT100 terminal type, then VT52, if necessary.

To request an IBM 3279 model 2 terminal type for a session on remote host jacks.toys.com, enter the following command:

```
C:\>tn -t 3279 jacks.toys.com
```

The tn program first offers the terminal type with extended attributes, and then, if necessary, without them.

5.2.2 Requesting a Specific Terminal Type

When you establish a tn connection, you can request a specific terminal type for your session.

To request a specific terminal type

Use the **-x** *ttype* option on the tn command line. The same keywords apply as for the **-t** option:

```
vt vt220 vt100 vt52 ibmpc 3277 3278 3279
```

The keyword `vt` works the same as with the **-t** option. Specifying `vt` causes tn to offer all three VT terminal types to the remote host, starting with VT220. Specifying any other terminal type with the **-x** option causes tn to offer only that terminal type. The following sample command requests a VT52 terminal type for logging in to the remote host kite.toys.com:

```
C:\>tn -x vt52 kite.toys.com
```

5.2.3 Configuring and Requesting Terminal Types by Nonstandard Names

When the tn program negotiates with the remote host for a terminal type, it requests VT terminal types using names that comply with RFC 1340, *Assigned Numbers*:

DEC-VT220

DEC-VT100

DEC-VT52

A remote UNIX host searches for the specified terminal name in a database containing the profiles of all terminals that the system supports. If the database does not contain terminal type names that comply with RFC 1340, the remote host does not recognize the terminal types tn offers and is likely to establish your session using a "dumb" terminal (one with no specific type).

To configure tn to send a VT terminal name that the remote host will recognize

Use the `vt100-terminal-id=` or `vt220-terminal-id=` parameters in the `[pctcp vt]` section of your PCTCP.INI file. For each parameter, supply a VT100 or VT220 terminal type name that does exist in the remote host's terminal information database. The tn program then requests terminal types using the name that you configure instead of the RFC-compliant name.

For example, the following PCTCP.INI parameter specifies that tn should send the name `vt220` instead of DEC-VT220 when negotiating with the remote host for the VT220 terminal type:

```
[pctcp vt]

vt220-terminal-id=vt220
```

To configure tn to send an IBM PC terminal name that the remote host will recognize

Use the `ibmpc-terminal-id=` parameter in the `[pctcp ansi]` section of your PCTCP.INI file. The IBM PC terminal type has no RFC-compliant name; the tn program requests the terminal name IBMPC.

5.2.4 Requesting Extended Screen Height and Width

Most terminal types support extended screen height. The number of extra lines can vary depending on the terminal type negotiated and on your video card and monitor characteristics.

To request a screen height of more than the default 25 lines

Use the **-h** option on the login command line.

If the tn program negotiates a VT or IBM PC terminal type for you, or if you specify a VT or IBM PC terminal type on the command line, the **-h** option results in a 43- or 50-line screen. Screen height is typically 43 lines if your PC has an EGA card and 50 lines with a VGA card.

If the terminal established is an IBM 3270 type, the result of using the **-h** option varies depending on several factors, including

- The model negotiated.
- The setting of the `model-3/4=` parameter in the `[pctcp 3270]` section of your PCTCP.INI file.
- The capabilities of your video card and monitor.

All IBM 3270 terminal models have a default screen size of 24 lines by 80 columns. Some models have an alternate screen size that goes into effect when the remote host sends a request for a larger screen. Table 5-2 indicates the alternate screen sizes available with various IBM terminal models, and the combination of command line options and PCTCP.INI file parameters that you need to request a particular terminal model and screen size. A request for a terminal type with alternate screen size capability does not automatically change the screen size. The screen size does not change until tn receives a specific data sequence from the remote host.

To request this terminal type and model	With this alternate screen size	Use these command line options	In combination with this paramet the `[pctcp 3270]` section of your PCTCP.INI file
3277-2	24 x 80	**-x 3277**	
3278-2	24 x 80	**-x 3278**	
3278-3	32 x 80	**-x 3278 -h**	`model-3/4=3`
3278-4	43 x 80	**-x 3278 -h**	`model-3/4=4`
3278-5	27 x 132	**-x 3278 -w**	
3279-2	24 x 80	**-x 3279**	
3279-3	32 x 80	**-x 3279 -h**	

As Table 5-2 shows, you can request a wide screen display using the **-w** option with the IBM 3278 terminal type. The **-w** option does not apply to any other IBM terminal type, nor does it apply to VT terminal types. The DEC VT and IBM PC emulators enter 132-column mode if an application running on the remote host requests it, and if your PC's video card and monitor are capable of it.

Examples

The following sample command requests extended screen height without specifying a particular terminal type. The screen height may be 32, 43, or 50 lines, depending on the terminal type negotiated and on your video card.

```
C:\>tn -h jacks.toys.com
```

The next command requests an IBM 3278 model 4 with extended screen height (the `model-3/4=` parameter in the PCTCP.INI file is set to 4):

```
C:\>tn -x 3278 -h doll.toys.com
```

5.2.5 Requesting Use of the Bottom Line of the Screen

You can request that the VT emulator use the bottom line of the screen (the status line), thereby increasing your screen height by one line.

To request use of the bottom line of the screen

1. In the `[pctcp vt]` section of your PCTCP.INI file, specify **`use-bottom-line=on`**
2. Set the TERMCAP or TERMINFO for your VT terminal to 25 lines.

If you request use of the bottom line and the status line is in use, the status line will be disabled.

5.3 Changing VT Terminal Types Within a tn or rloginvt Session

When you are using the DEC VT emulator within a tn or rloginvt session, you can change the terminal type without leaving your session. This function emulates the ability of a VT220 terminal to change to different operating modes. Thus, the terminal type is referred to in this context as a “mode.”

To change to a new terminal mode

Enter the **m** escape command.

You see a message that indicates the current mode, and a menu that offers the following numbered options:

0: VT220, 7-bit controls

1: VT220, 8-bit controls

2: VT100, send VT100 ID

3: VT100, send VT220 ID

4: VT52

Type the number of the mode that you want to change to. If you decide to stay in the same mode, type the number of the current mode, or press the spacebar twice to return to your session.

Modes	Description
0	Is the default mode. It supports VT220 functions and complies with ANSI standards. Control codes, which specify how the terminal should behave and handle data, are in 7-bit format. All other data is in 8-bit format. This mode provides backward compatibility with software written for VT100 terminals.
1	Offers the full range of VT220 functions and complies with ANSI standards. All data, including control codes, are in 8-bit format. Not all hosts and communications environments support 8-bit controls; if you use this mode, you may get unexpected results.
2 and 3	Offer full compatibility with software written for VT100 terminals. Control codes are in 7-bit format, and functions comply with ANSI standards. The only difference between modes 2 and 3 is the ID that they send in response to an inquiry from the host (the host may periodically request that a terminal report information about itself, such as its ID and other basic attributes). Modes 2 and 3 emulate the ability of a VT220 to send an ID of either VT100 or VT220 when in VT100 mode.
4	Emulates DEC private (non-ANSI) functions supported by the VT52

terminal. Control codes are in 7-bit format.

5.4 Enabling Binary Mode

Some remote hosts support the exchange of data in binary mode. In binary mode, all data is in 8-bit format and is interpreted literally, without modification or filtering. When you are using IBM 3270 emulation, the connection is automatically in binary mode and you cannot change it. However, you can change to binary mode during a VT220 emulation session.

Before you use binary mode in a connection to a UNIX system, you may need to change some **stty** settings to ensure a full 8-bit data path to the remote host.

To request binary mode

Enter the **Ctrl+b** escape command (tn only).

–or–

Enter the **m** escape command to get a list of VT emulation modes (not valid with the IBM PC emulator). Then type `1` to choose Mode 1 (VT220, 8-bit controls).

–or–

In the `[pctcp vt]` section of your PCTCP.INI file, specify **`8-bit=on`** This requests binary mode automatically every time that you start rloginvt or tn.

Requesting binary mode for a tn session does not guarantee that it will be established. Some systems do not support the ability to change to binary mode within a session; the remote host may reject or ignore the request.

Binary mode is of limited usefulness on some remote systems. A 4BSD UNIX system equates Telnet binary mode with a mode of the UNIX terminal line discipline called “raw mode.” In raw mode, the Return (Enter) and Delete keys do not work properly because the remote host processes codes for functions such as carriage returns literally and does not interpret them as control functions.

5.5 Changing Echo Mode in tn and tnglass

The tn and tnglass programs support the ability to change echo modes. Echo mode determines how the program displays your keyboard input on your PC screen.

By default, your login session is in “remote echo mode” — every keystroke that you type makes a round trip from your PC to the remote host and back to your PC screen. Network congestion or several network “hops” between your PC and the remote host can cause this exchange to be time consuming, and may prevent you from typing as quickly as you want.

To enable local echo mode

Enter the **l** escape command.

In “local echo mode,” the software sends your keystrokes to the remote host, but the host does not echo them back. DOS is responsible for displaying the characters that you type on your PC screen.

To return to remote echo mode

Enter the **r** escape command.

Note: The ability to change echo mode is not available with the 3270 terminal emulator. Also, not all hosts support changing to local echo mode, even if you are using the VT or IBM PC emulators.

5.6 Using a Line Mode Connection to an IBM Host

Some IBM hosts establish a connection in line mode instead of 3270 mode. Line mode uses the Telnet standard Network Virtual Terminal (NVT) as an emulator. NVT implements a common definition for exchanging data and control functions across a network. It is a subset of the DEC VT220 terminal emulator, and uses the same default values. Thus, if your IBM connection is in line mode, it is using VT emulation.

The VT and IBM PC emulators send each character to the remote host as you type it.

To increase speed and more closely emulate an IBM terminal

Use the **E** escape command.

The **E** command causes **tn** to send a line of characters to the remote host only after you press the Enter key. You can then backspace to delete and change characters on a line before sending those keystrokes across the network.

5.7 Customizing VT and IBM PC Terminal Characteristics

You can customize many of the VT and IBM PC emulators terminal characteristics. Table 5-3 summarizes the escape commands that change VT terminal features in rloginvt as well as VT and IBM PC terminal features in tn. Do not type the comma; it indicates a sequence of keystrokes. First type the escape key sequence, then type the escape command.

Note: tn accepts F10 as well as Alt+F10 from the DEC VT and IBM PC emulators.

Table 5-1 Escape Commands for Creating and Managing Connections (Cont.)

Tasks	rloginvt Escape commands	tn Escape commands
Define Backspace (←) key to send backspace,Ctrl+Backspace (Ctrl+←) key to send delete	F10, B	Alt+F10, B
Define Backspace (←) key to send delete,Ctrl+Backspace (Ctrl+←) key to send backspace	F10, D	Alt+F10, D
Disable line wrap	F10, d	Alt+F10, d
Enable line wrap	F10, w	Alt+F10, w
Define Enter key to send carriage return and line-feed		Alt+F10, N
Define Enter key to send carriage return only		Alt+F10, R
Send each character as you type it		Alt+F10, e
Send a line of characters only after you press Enter		Alt+F10, E

5.7.1 Defining Backspace Key Behavior

A VT220 terminal has separate backspace and delete keys. In the VT and IBM PC emulators, these two functions are combined in the PC Backspace (←) key. When you press the Backspace key, the VT and IBM PC emulators send an ASCII delete character to the remote host. When you press Ctrl+Backspace, the emulator sends an ASCII backspace character.

To send ASCII backspace when you press the Backspace key

Use the **B** escape command.

The **B** escape command causes the Backspace key to send a backspace character and Ctrl+Backspace to send a delete character. You may need to do this if the remote system interprets the ASCII backspace character as the erase character. Alternatively, you can change settings on the remote system.

To revert to sending ASCII delete when you press the Backspace key

Use the **D** escape command.

To specify that the Backspace key send a delete character for a tn session

In the `[pctcp tn]` section of your PCTCP.INI file, specify **`back-arrow-key=del`**

To specify that the Backspace key send a backspace character for a tn session

In the `[pctcp tn]` section of your PCTCP.INI file, specify **`back-arrow-key=bs`**

The `back-arrow-key=` parameter defines the behavior of the Backspace key each time that you start tn; you can override it using the **B** and **D** escape commands.

5.7.2 Controlling Line Wrap

When automatic line wrap is on, if a line is too long for the display, extra characters appear on the next line. Line wrap is disabled in the VT and IBM PC emulators; if a line is too long for the display, extra characters overwrite the last character on the line.

To enable line wrap

Use the **w** escape command.

To disable line wrap

Use the **d** escape command.

To enable line wrap for tn and rloginvt sessions

In the `[pctcp vt]` section of your PCTCP.INI file, specify **`wrap-line=on`**

To disable line wrap for tn and rloginvt sessions

In the `[pctcp vt]` section of your PCTCP.INI file, specify **`wrap-line=off`**

5.7.3 Defining Enter Key Behavior

When you press the Enter key, the VT and IBM PC emulators in tn send the Telnet protocol sequence for carriage-return and line-feed characters.

To specify that the Enter key send a carriage return only

Use the **R** escape command.

To revert to sending carriage return and line feed when you press the Enter key

Use the **N** escape command.

5.7.4 Controlling Keystroke Buffering

The VT and IBM PC emulators in tn send each character to the remote host as you type it.

To specify that you want to send a line of characters to the remote host only after you press the Enter key

Use the **E** escape command.

After using the **E** escape command, you can erase or change a character on a line before you send it to the remote host. The **E** escape command functions only in local echo mode. If you change to remote echo mode, the terminal emulator reverts to sending each character as you type it.

To specify that you want to send each character to the remote host as you type it

Use the **e** escape command.

5.7.5 Changing the Character Set

If you are using DEC VT100 emulation within a tn session, you can use any single-byte character set (code page) that is available to you.

To change the character set for DEC VT00 emulation

1. Install the single-byte character set that you want to use.

   For information about installing and using character sets, see your Microsoft MS-DOS documentation.

2. In the `[pctcp vt]` section of your PCTCP.INI file, specify **`character-set=HFT`**

3. Establish a tn session with the remote host.

5.8 Customizing IBM 3270 Terminal Characteristics

When you log in to a remote IBM host with tn, you are using an IBM 3270 terminal emulator.

The 3270 emulator maintains a buffer of characters that you type and sends them to the host when you press a 3270 attention identifier key (such as the Enter key or a PF key). The emulator and the remote host communicate by exchanging blocks of data. The data blocks include characters, and control sequences, known as 3270 data stream orders, which affect the arrangement and display of information on your screen.

Some of the features of the 3270 terminal emulator are included for compatibility with the IBM 3270 terminal emulators produced by UC-Berkeley and Yale University. Yale functions that the emulator supports are indicated with a (Y) in the list of PC-to-IBM key mappings in Appendix A, Terminal Emulation and Character Set Tables. The emulator also supports Yale-style processing of null characters.

5.8.1 Selecting Null Processing Style

The network software supports two ways of processing null characters: Yale and IBM styles.

Yale style	Replaces null characters in a modified field with blanks before sending data to the remote host. This lets you move the cursor to a given position within a field by pressing the arrow keys instead of the spacebar.
IBM style	Preserves all null characters as null characters. The emulator does not interpret horizontal cursor movement over a null field as blank space. Consequently, text that you format by pressing the arrow keys instead of the space bar may be interpreted as left-justified at the remote host.

The 3270 emulator uses Yale-style null processing.

To disable Yale null processing

Use the **y** escape command.

To enable Yale null processing

Use the **Y** escape command.

5.8.2 Emulating a 3270 Selector Pen

A selector pen is a pointing device that is sensitive to the light emitted by characters on the screen. Some 3270 applications let a user choose items on the screen by pointing to them with the selector pen. In a tn connection to an IBM host, you can use a key combination, your mouse, or a light pen connected to your PC, to emulate a 3270 selector pen.

To emulate a selector pen using the keyboard

Move your cursor to the field or item that you want to select, and press Alt+F6.

Note: Before you can use the **M** escape command to enable and disable emulation of your mouse as a selector pen, you must install a mouse driver on your PC.

To enable emulation of your mouse as a selector pen

Use the **M** escape command.

–or–

To enable this feature every time that you start tn, in the `[pctcp 3270]` section of your PCTCP.INI file, specify **`mouse=on`**

To disable emulation of the mouse as selector pen

Use the **M** escape command.

–or–

In the `[pctcp 3270]` section of your PCTCP.INI file, specify **`mouse=off`**

To enable emulation of a light pen as a selector pen

To enable this feature every time that you start tn, in the `[pctcp 3270]` section of your PCTCP.INI file, specify **`lightpen=on`**

To disable emulation of a light pen as a selector pen

In the `[pctcp 3270]` section of your PCTCP.INI file, specify **`lightpen=off`**

5.9 Using IBM PC Terminal Characteristics

When you establish a tn session using an IBM PC terminal type, tn provides the following terminal characteristics. During IBM PC emulation, your terminal

- Displays characters from any character set installed on your system.
- Uses the 25th line of the screen.
- Accepts the following ANSI scrolling escape sequences: Esc[S, Esc[T.
- Accepts Select Graphic Rendition (SGR) escape sequences.
- Can send scan codes or ANSI escape sequences.

To use IBM PC terminal emulation

1. Install the character set that you want to use.

   For information about installing and using character sets, see your Microsoft MS-DOS documentation.

2. If you want to change your default keyboard mappings, in the `[pctcp vt]` section of your PCTCP.INI file, specify the following value:

   `vt220-keymap=` *`drive:\path\filename`*

   where *`filename`* is one of the following values:

   – ANSI-SYS.KYB contains mappings for non-character keys (such as , PageUp, and Alt). When you use these mappings in a Telnet session, a key's scan code is sent to the remote host.

   – ANSI.KYB contains mappings for non-character keys (such as , PageUp, and Alt). When you use these mappings in a Telnet session, a key's ANSI escape sequence is sent to the remote host.

3. Specify IBM PC terminal emulation in one of the following ways:

   In the `[pctcp vt]` section of your PCTCP.INI file, specify **`def-em-mode=ibmpc`** and then establish a tn session with the remote host.

   –or–

   Specify the value `ibmpc` with the tn **-x** command line option.

   –or–

   Specify the value `ibmpc` with the tn **-t** command line option.

5.10 Customizing Screen Colors for VT and 3270 Emulation

You can customize default screen colors and display characteristics for terminal emulation using either of two methods:

- Use the **setcolor** command to choose and test colors interactively. You can type and enter color values or select them with a mouse. You can then save your choices to parameters in the PCTCP.INI file.
- Use **config** or a text editor to change parameters directly in your PCTCP.INI file.

You must have the appropriate color adapter (a CGA, PGA, VGA, EGA, SVGA or XGA card) to customize screen colors. If you have a monochrome adapter, you are limited to changing display characteristics such as underlining, highlighting, and reverse video.

Three parameters in the PCTCP.INI file control screen colors and display characteristics:

Parameter	PCTCP.INI file section	Function
`ftp-attr=` *values*	`[pctcp screen]`	Defines basic screen colors and display characteristics for VT, IBM PC, and 3270 emulation (the vmail program also uses this parameter).
`ftp-sfe-attr=` *values*	`[pctcp 3270]`	Defines extended color attributes for IBM 3270 emulation.
`ftp-sfe-rv-attr=` *values*	`[pctcp 3270]`	Defines extended reverse video color attributes for IBM 3270 emulation.

Each parameter consists of a set of values separated by commas. Each value represents a foreground and background color combination for a particular type of character or field. Although applications control and define the field types that they use, you can customize the screen colors that the OnNet or PC/TCP software associates with each type.

Table 5-4 summarizes the six values in the `ftp-attr=` parameter and indicates their defaults. Color codes are in hexadecimal format, as indicated by the 0x prefix.

This value	Affects field or character type	For these terminal types	Has this default code	Representing these colors

1	Normal	VT, IBM PC, and 3270	0x07	Light gray on black
2	Underline	VT, IBM PC, and 3270	0x49	Light blue on red
3	Reverse video	VT, IBM PC, and 3270	0x70	Black on white
4	Normal unprotected (highlighted)	3270 only	0x0F	White on black
5	Normal protected (unhighlighted)	3270 only	0x07	Light gray on black
6	Normal protected (highlighted)	3270 only	0x0F	White on black

This example shows an `ftp-attr=` parameter that specifies these default values:

```
ftp-attr=0x07,0x49,0x70,0x0F,0x07,0x0F
```

The sections that follow describe the meaning of each of these values.

5.10.1 Defining Colors for VT Emulation

The first three values of the `ftp-attr=` parameter determine the colors for VT and IBM PC emulation. They correspond to the following character or field attributes, in the order listed:

Attribute	Meaning
normal	Characters that have no special display characteristics.
underline	Characters that would have an underscore beneath them on a terminal. The VT and IBM PC emulators do not display underscores. Instead, they use an alternative color to display underlined text.
reverse video	In a reverse video display, the character color becomes what is normally the background color, and the background color becomes what is normally the foreground (text) color. For example, black characters on a white background become white characters on a black background.

To change VT colors using setcolor

1. To start the program, enter **`setcolor`**

   The program displays the current colors (and their hexadecimal values) for normal, underlined, and reverse video (inverse) text.

2. If you want to change the colors, answer **`y`** to the `Would you like to change the colors?` prompt.

   –or–

   Answer **`n`** if you do not want to change the colors.

3. If you want to restore default colors, answer **`y`** to the `Would you like to restore default colors?` prompt.

   –or–

   Answer **`n`** if you do not want to restore default colors.

4. Type or select the code for a new color.

   –or–

   Press Enter to accept an existing color. The setcolor program prompts you for new colors, one at a time. The display changes to show the new colors that you have selected.

5. If you want to review or modify the colors, answer **`y`** to the `Would you like to review or modify the new color settings?` prompt.

   –or–

   Answer **`n`** if you do not want to review or modify the colors.

6. To save your changes to the PCTCP.INI file, answer **`y`** to the `Would you like to save the new color settings?` prompt.

To define VT and IBM PC colors in the PCTCP.INI file

1. Use any text editor to open your PCTCP.INI file.

2. Go to the `ftp-attr=` parameter in the `[pctcp screen]` section and type the codes for any new colors that you want to define.

   You can specify color values in hexadecimal (with the 0x prefix), octal (with a leading 0), or decimal format (with no leading 0). Specify `0` to accept the default value. If you plan to use only VT or IBM PC emulation, you need to specify only the first three values; the last three are for 3270 emulation.

3. Save your changes and close the file.

5.10.2 Defining Colors for IBM 3270 Emulation

All six values of the `ftp-attr=` parameter determine colors for IBM 3270 emulation. However, the second and third values (underline and reverse video) apply only to 3270 emulation with extended attribute support. Colors for 3270 emulation are defined on the basis of attributes, or characteristics, of fields and characters. A field is a portion of the screen defined by the application or the operating system running on the remote host. The purpose of a field is usually for displaying information or accepting input.

The values of the `ftp-attr=` parameter correspond to the following field or character attributes, in the order listed:

Attribute	**Meaning**
normal unprotected	Fields that are unprotected and that have no special display characteristics. An unprotected field is modifiable.
extended underline	Fields or characters that have an underscore attribute associated with them. Underlining is available only with extended 3270 emulation.
extended reverse video	Reverse video fields or characters. In a reverse video display, the foreground color becomes what is normally the background color, and the background color becomes what is normally the foreground (text) color. For example, black text on a white background becomes white text on a black background. Reverse video is available only with extended 3270 emulation.
normal unprotected, highlighted	Normal modifiable fields that are highlighted (the brightness of characters is intensified).
normal protected, unhighlighted	Normal fields that are not modifiable (display-only) and not highlighted.
normal protected, highlighted	Normal fields that are not modifiable (display-only) and highlighted.

If you use 3270 emulation with extended attribute support, you can use the `ftp-sfe-attr=` and `ftp-sfe-rv-attr=` parameters to define additional color values. Each parameter consists of seven values. The `ftp-sfe-attr=` parameter reflects an ordered list of default colors that applications can specify as an extended attribute of a field. The `ftp-sfe-rv-attr=` parameter reflects an ordered list of default reverse video colors that an application can specify. You can change the display of an extended color by specifying a different color in its position in the

appropriate PCTCP.INI file parameter.

Table 5-5 shows the default colors and their positions in the `ftp-sfe-attr=` parameter.

Table 5-2 Default Values for ftp-sfe-attr= Parameters

Application-defined color	**Corresponding `ftp-sfe-attr=` value**	**Default code**	**Colors Displayed**
Blue	1	0x09	Light blue on black
Red	2	0x04	Red on black
Pink	3	0x05	Magenta (pink) on black
Green	4	0x02	Green on black
Turquoise	5	0x03	Cyan (turquoise) on black
Yellow	6	0x0E	Yellow on black
White	7	0x0F	White on black

Table 5-6 shows the default reverse video colors and their positions in the `ftp-sfe-rv-attr=` parameter.

Table 5-3 Default Values for ftp-sfe-rv-attr= Parameters

Application-defined color	**Corresponding `ftp-sfe-rv-attr=` value**	**Default code**	**Colors Displayed**
Rev-vid blue	1	0x10	Black on blue
Rev-vid red	2	0x40	Black on red
Rev-vid pink	3	0x50	Black on magenta (pink)
Rev-vid green	4	0x20	Black on green
Rev-vid turquoise	5	0x30	Black on cyan (turquoise)
Rev-vid yellow	6	0x60	Black on brown (yellow)
Rev-vid white	7	0x70	Black on white

The following are sample `ftp-sfe-attr=` and `ftp-sfe-rv-attr=` parameters that specify the default extended color and extended reverse video color values, respectively:

```
ftp-sfe-attr=0x09,0x04,0x05,0x02,0x03,0x0E,0X0F
ftp-sfe-rv-attr=0x10,0x40,0x50,0x20,0x30,0x60,0x70
```

The color of a field depends on the combination of attributes that an application specifies for that field. In some cases, a color setting in the `ftp-sfe-attr=` or `ftp-sfe-rv-attr=` parameter overrides a color setting in the `ftp-attr=` parameter.

Table 5-7 indicates the color that the terminal emulation software displays in response to various combinations of extended attributes.

Table 5-4 Effect of Extended Attributes on Color Values

Application-specified extended attributes	**Corresponding OnNet or PC/TCP color value**
Color	Value in corresponding position of `ftp-sfe-attr=` parameter
Underline	Value 2 of `ftp-attr=` parameter
Reverse video	Value 3 of `ftp-attr=` parameter
Color and underline	Value in corresponding position of `ftp-sfe-attr=` parameter
Color and reverse video	Value in corresponding position of `ftp-sfe-rv-attr=` parameter
None	Value 1, 4, 5, or 6 of `ftp-attr=` parameter, depending on protection and highlighting characteristics defined for the field

To define 3270 colors using setcolor

1. To start the program, enter **`setcolor -3`**

   The **-3** option indicates that you want to set colors for 3270 emulation. The program displays the current colors, and their hexadecimal values, for all 3270 field types.

2. If you want to change the colors, answer **`y`** to the `Would you like to change the colors?` prompt.

–or–

Answer **n** if you do not want to change the colors.

3. If you want to restore default colors, answer **y** to the `Would you like to restore default colors?` prompt.

   –or–

   Answer **n** if you do not want to restore default colors.

4. Type or select the code for a new color.

   –or–

   Press Enter to accept an existing color. The setcolor program prompts you for new colors, one at a time. The display changes to show the new colors that you have selected.

5. If you want to review or modify the colors, answer **y** to the `Would you like to review or modify the new color settings?` prompt.

   –or–

   Answer **n** if you do not want to review or modify the colors.

6. To save your changes to the PCTCP.INI file, answer **y** to the `Would you like to save the new color settings?` prompt.

To define 3270 colors in the PCTCP.INI file

1. Use any text editor to open your PCTCP.INI file.

2. Go to any of the three parameters applicable to 3270 emulation and type the codes for new colors that you want to define.

   For the `ftp-sfe-attr=` or `ftp-sfe-rv-attr=` parameters, you must specify all seven values, even if you do not want to change them all. Specify 0 to accept the default value. Color values can be in hexadecimal (with the 0x prefix), octal (with a leading 0), or decimal format (with no leading 0). For information on color values, see Appendix C, Graphics/Color Display Attributes.

3. Save your changes and close the file.

5.11 Encrypting Data in a Telnet Session

Encrypting data in a Telnet session allows you to send and receive data in a format that cannot be deciphered.

Requesting encryption for a tn session does not guarantee that it will be established. Some systems do not support the ability to encrypt within a session; the remote host may reject or ignore the request.

5.11.1 Prerequisites to Encrypting a Telnet Session

Before you can encrypt data in a Telnet session, you must perform the following tasks:

- Configure Kerberos security
- Edit your PCTCP.INI file

Configuring Kerberos Security

Before you can use encryption, you must use Kerberos security. Before you can use Kerberos security, however, you must configure it.

To configure Kerberos security

Follow the directions described in *Advanced User's Guide*, Chapter 24, Network Security.

Requesting Kerberos security for a tn session does not guarantee that it will be established. Some systems do not support authentication within a session; the remote host may reject or ignore the request.

Editing Your PCTCP.INI File

Before you can use encryption, you must add several parameters to your PCTCP.INI file. The following table summarizes the parameters that you need to add and the PCTCP.INI file sections in which they appear:

Parameter	PCTCP.INI Section
all parameters	`[pctcp kerberos]`
`authentication= [enabled|required|disabled]`	`[pctcp tn]`
`encryption=[disabled|enabled|required]`	`[pctcp tn]`

If you want to encrypt data in your Telnet session, you must set the authentication parameter to one of its non-disabled states; that is, either enabled or required.

In certain cases an interdependence between the authentication and encryption parameter settings exists. This can result in ambiguous behavior during your Telnet session. Understanding the Relationship Between Authentication and Encryption

The authentication and encryption parameters in your PCTCP.INI file allow you to create nine possible combinations of settings. In most cases, these combinations make sense. There are, however, three combinations that result in ambiguity; in these cases, Telnet changes your environment so that encryption works correctly. It does so by forcing your session to behave as though your authentication variable has been set to the same value as your encryption variable. The following table summarizes these ambiguous cases:

If `encryption` is set to	And `authentication` is set to	Then Telnet operates as though `authentication` is set to
`required`	`enabled`	`required`
`required`	`disabled`	`required`
`enabled`	`disabled`	`enabled`

Prevent these ambiguous cases by setting the values in your PCTCP.INI file appropriately.

5.11.2 Using Kerberos

After you have configured Kerberos, and before you can enable encryption, you must obtain a ticket-granting ticket. You may also want to list information about the ticket or destroy the ticket when you no longer need it.

To obtain a ticket-granting ticket

At the DOS prompt, type **`kinit`**

Your ticket grants you access to a remote host for a predetermined period of time, after which your ticket expires. When your ticket expires, you must obtain a new ticket-granting ticket.

To list ticket information

At the DOS prompt, type **`klist`**

klist provides information such as when you obtained the ticket and when the ticket expires.

To destroy a ticket

At the DOS prompt, type **`kdestroy`**

You should destroy any ticket-granting tickets that have not yet expired when you have finished sending encrypted data in your Telnet session. This security precaution ensures that no one else can access your Telnet session.

For more information about using Kerberos security in a Telnet session, see section 4.3, Logging In.

5.11.3 Enabling Encryption

After you meet the prerequisites for encrypting a Telnet session, you can enable encryption. There are two methods that you can use to enable encryption:

- Permanently; that is, for all of the data in your Telnet session.

  Use this method if all the data in your Telnet session is sensitive and requires encrypting. You can ensure that all your data will be encrypted by specifying `encryption= required` in the `[pctcp tn]` section of your PCTCP.INI file. If encryption negotiation fails, your Telnet session is closed.

- Temporarily; that is, for only some of the data in your Telnet session.

  Use this method if only some of the data in your Telnet session is sensitive and requires encrypting. You can choose when to encrypt data in a Telnet session by specifying `encryption= enabled` in the `[pctcp tn]` section of your PCTCP.INI file. Then, during your Telnet session, press F10, Ctrl+e to toggle encryption: pressing F10, Ctrl+e once turns encryption off; pressing F10, Ctrl+e again turns encryption on. If encryption negotiation fails, the Telnet session remains open and your data is sent unencrypted.

  You can use the following two methods to set the encryption parameters in your PCTCP.INI file to enable encryption.

If you want to	**Then specify**	**And**
encrypt all of the data in your Telnet session	`encryption= required`	----
encrypt only some of the data in your Telnet session	`encryption=enabled`	press F10, Ctrl+e during your Telnet session to alternately disable and enable encryption.

5.11.4 Disabling Encryption

If you do not want to encrypt data in your Telnet session, you do so by disabling encryption. There are two methods that you can use to disable encryption:

- Permanently; that is, for all of the data in your Telnet session.

  Use this method if none of the data in your Telnet session is sensitive and requires encrypting. You can ensure that none of your data will be encrypted by specifying `encryption= disabled` in the `[pctcp tn]` section of your PCTCP.INI file.

- Temporarily; that is, for only some of the data in your Telnet session.

  Use this method if only some of the data in your Telnet session is sensitive and requires encrypting. You can choose when to encrypt data in a Telnet session by specifying `encryption= enabled` in the `[pctcp tn]` section of your PCTCP.INI file. Then, during your Telnet session, press F10, Ctrl+e to toggle encryption: pressing F10, Ctrl+e once disables encryption; pressing F10, Ctrl+e again enables encryption.

  You can use the following two methods to set the encryption parameters in your PCTCP.INI file to disable encryption.

If you want to	**Then specify**	**And**
Encrypt none of the data in your Telnet session	`encryption= disabled`	----
Encrypt only some of the data in your Telnet session	`encryption= enabled`	press F10, Ctrl+e during your Telnet session to alternately enable and disable encryption.

5.12 Using the Scrollback Buffer

The VT and IBM PC emulator scrollback buffers allow you to view information that has scrolled off your screen.

5.12.1 Prerequisites to Using the Scrollback Buffer

Before you can use the scrollback buffer in a remote login session, you must configure your environment by performing the following tasks:

1. Load a memory manager for DOS.

   Because the scrollback buffer uses extended memory (XMS), you must load the appropriate memory manager, such as HIMEM.SYS.

2. Edit your PCTCP.INI file.

   Before you can use the scrollback buffer, you must specify how many lines you want the buffer to contain. In the `[pctcp vt]` section of the PCTCP.INI file, specify **`scroll-lines=`** *`value`*, where *`value`* is an integer in the range 1 to 10,000.

5.12.2 Viewing the Contents of the Scrollback Buffer

After you meet the prerequisites for using the scrollback buffer, you can view the contents of the scrollback buffer in a remote login session.

Text accumulates in the scrollback buffer as it scrolls off the top of your screen. You can view the buffer line-by-line or screen-by-screen. As you view the contents of the scrollback buffer, the 25th line status indicator of your screen displays a value indicating your location in the buffer.

For example, if you specify `scroll-lines=1000` and you scroll back two screens worth of information (48 lines at 24 lines a screen), the status indicator reads:

```
scroll buffer: Line 51 of 99 (51%)
```

You can use the following methods to view the contents of the scrollback buffer:

If you want to view	**Then press**
the previous line	Alt+
the next line	Alt+↓
the previous screen	Alt+PageUp
the next screen	Alt+PageDown

5.13 Specifying a Display for the X Window System

If a remote host is running the X Window System (X) and you want to run X applications during a Telnet session, you must make the Internet address of your display hardware known to it. The IP address is used by the application to determine where to display output from your Telnet connection.

Requesting a display for a tn session does not guarantee that it will be established. Some systems do not support the X Window System; the remote host may reject or ignore the request.

5.13.1 Preparing to Run X Applications

Before you can run an X application during a Telnet session, you must prepare your environment.

Prerequisites to Specifying an X Display

Before you can run an X application during a Telnet session, an X server must be installed and running on your system.

Specifying an X Display

To specify where you want your display sent

Use the following parameter in the `[pctcp tn]` section of your PCTCP.INI file

`x-display=` *`hostname:server.screen`*

5.14 Troubleshooting Terminal Emulation

This section provides solutions to situations that you might encounter while customizing terminal emulation characteristics. The situation is described first (including any messages that you see), followed by the meaning of the situation (where applicable) and the action to take.

The remote UNIX system host does not recognize your terminal type.

If you have system management privileges, verify that the RFC 1340 standard terminal type designations (DEC-VT220, DEC-VT100, DEC-VT52) exist as aliases in the host's /etc/termcap file or /usr/lib/terminfo directory. If they do not exist, add them to the appropriate terminal definitions.

–or–

Verify that an IBM PC terminal type parameter exists in the host's /etc/termcap file or /usr/lib/terminfo directory. If it does not exist, add it to the appropriate terminal definition.

If you do not have system management privileges, you have several options: Ask the system manager on the remote host to add the appropriate aliases to the TERMCAP or TERMINFO file.

–or–

Find a VT100 or VT220 terminal ID that does exist in the remote host's terminal information file. Configure it as the value of the `vt100-terminal-id=` or `vt-220-terminal-id=` parameter in the `[pctcp vt]` section of your PCTCP.INI configuration file. Or find an IBM PC terminal ID that does exist in the remote host's terminal information file. Configure it as the value of the `ibm-terminal-id=` parameter in the `[pctcp ansi]` section of your PCTCP.INI configuration file. These parameters allow tn to pass nonstandard terminal type names when negotiating the terminal type with the remote host.

–or–

Include a **tset** command in your .login file on the remote host that sets the terminal type, or translates between the tn and UNIX terminal naming conventions. You also can enter a **tset** command after you log in to set the terminal type for the duration of that session only.

–or–

Include a command in your .login file that sets the TERM environment variable to a terminal type recognized by the UNIX system. You also can set the environment variable after you log in to last for the duration of your session.

Arrow keys do not work properly in a connection emulating a DEC VT100 or VT220 terminal.

If you have system management privileges, change the VT100 or VT220 parameters in the appropriate terminal definition file on the remote host. If the host uses a TERMCAP file, make sure the `:ks` variable looks like the following:

```
:ks=\E[?1h\E>
```

If the host uses a TERMINFO database, make sure the `smkx` variable is set to `\`

```
E[?1h\E>.
```

You use the **-h**, **-43**, or **-50** command line option to request extended screen height, but the resulting screen is normal size.

Verify that your PC has a video card that supports extended screen height. Typically, EGA cards support a 43-line screen, and VGA cards support a 50-line screen.

If the remote host is a 4BSD UNIX system:

Ensure that the TERMCAP or TERMINFO file has the appropriate `:li` variable definition to support extended screen height. If you have system management privileges, you can change the parameter yourself. If not, ask the remote system administrator to modify the parameter.

If you do not have system management privileges but know a terminal definition with extended screen height exists on the remote host, you can use a **tset** command in your .login to set the terminal type. For example, this .login parameter sets the terminal type to vt220-42 in a network connection to the host:

```
eval 'tset -s -m 'network:?vt220-42''
```

–or–
After you log in, enter a **tset** command that sets the terminal type for the duration of your session.

If you do not have system management privileges, and you do not know of a terminal definition you can use with **tset**, use the **stty rows** *n* command, where *n* sets the number of lines on the screen. You can store this command in your .login file or execute it once you have logged in.

If all else fails, the problem may be the application that you are running on the remote system. Some applications may not work properly if you use a 43- or 50-line display. For more information, consult the documentation for the application.

If the remote host is an IBM system:

The remote host may not have sent a request to enlarge the screen size. All IBM terminal types have a default screen size of 24 lines by 80 columns.

To establish a terminal type with a larger screen size capability, specify the **-h** command line option. The larger screen size does not go into effect until tn receives a request from the remote host.

The connection to a remote IBM host is established in line mode unexpectedly.

When you connect to a remote IBM host, the host typically negotiates with the tn program for a terminal type and for certain options involving the transmission of data. If the negotiations succeed, the host establishes the connection using 3270 emulation mode.

If your connection is established in line mode, the reason may be that the

negotiations failed or stopped before completing. Some hosts cease negotiations when you type ahead before the connection is established.

If you do not want to use a line mode connection, try logging in again using the **-x** or **-t** option to request a specific terminal type. Do not type until the remote host displays the login prompt.

You use the **-w** command line option to request extended screen width in tn, but the resulting screen is normal size.

Verify that your video card and monitor are capable of supporting 132-column mode.

If the `[pctcp screen]` section of your PCTCP.INI file contains a `card=vga` parameter, change it to `card=vesa`. The `vga` value does not support 132-column mode. If a `card=` parameter did not previously exist, and adding `card=vesa` still fails to produce 132-column mode, try changing the parameter to `card=autodetect`.

Use the **Alt+F10**, **Ctrl+t** escape command to verify that the terminal model is 3278 Model 5. This is the only terminal type that supports the **-w** option. (DEC VT and IBM PC terminal types enter 132-column mode only when an application running on the remote host requests it.)

If your terminal type is 3278 Model 5, but the screen still is not in 132-column mode, the reason may be that the remote host has not yet sent a request to enlarge the screen.

You receive the following message:

```
Authentication failed ...closing connection.
```

Log in to a new session using the tn **-D** option to request Kerberos debugging.

Ask the system administrator if the remote host supports Kerberos authentication.

Type **`klist`** to verify that you have a ticket-granting ticket. If you do not have a ticket-granting ticket, type **`kinit`**

If you have a ticket-granting ticket, the clocks on your PC and the remote host may not be synchronized. Log in to a new tn session specifying port 13, the time server. If the difference between the times on your PC and the remote host is greater than 5 minutes, notify your system administrator.

If you have a ticket-granting ticket, ask the system administrator if the remote host is running Sandia National Laboratories' implementation of the Telnet server. If it is, you must define the service name as **`telnet`** You can do this in one of two ways:

Log in to a new session specifying the tn **-p** command line option with **`telnet`** as the service name: **`-p telnet`**

–or–

In the `[pctcp tn]` section of your PCTCP.INI file, specify **`service-`**

name=telnet

You receive the following message:

```
Unable to encrypt data ...closing connection.
```

Log in to a new session using the tn **-D** option to request Kerberos debugging. Output from the remote host is written to a file named ENCRYPT.DBG.

Ask the system administrator if the remote host supports Kerberos encryption.

While you are connected to a remote 3270 application, characters appear on your screen at unexpected locations.

The system administrator on the remote 3270 system may have changed the default screen size to be the same as the alternate screen size.

Disconnect your Telnet session. Log in to a new session using the tn **-a** option to request the alternate screen size for the chosen terminal type.
–or–
In the `[pctcp 3270]` section of your PCTCP.INI file, specify **`alt-overrides-default=yes`**

You receive the following error message:

```
Error: Can't Open Display
```

The Telnet server does not support the X-display location.

Establish a Telnet connection; on the remote host, specify the IP address of the display hardware.

During a Telnet session in which you are using the ANSI-SYS.KYB or ANSI.KYB keyboard mapping file, the F10 escape key does not work.

Edit the keyboard mapping file to remove the mapping for the F10 key.

The Enter key does not work properly in a connection emulating a DEC VT terminal.

The server on the remote host may have established binary mode.

Log in to a new session using the tn **-b** option to request that binary mode not be negotiated.

Appendix A
Terminal Emulation and Character Set Tables

This appendix includes tables that you can refer to when you use terminal emulation. It consists of the following major sections:

- DEC VT Emulation Tables
- IBM PC Emulation Tables
- IBM 3270 Emulation Tables

These sections contain tables that are useful for understanding and customizing the VT, IBM PC, and 3270 emulation environments, respectively.

A.1 DEC VT Emulation Tables

The tables in this section contain the following information:

- PC keys that perform functions other than for VT terminal emulation, and their map values.
- Default mappings of PC keys to VT function keys, and their map values.
- Hexadecimal codes for characters in the DEC multinational character set.
- Characters that the network software substitutes for display when it receives a character from the remote host that does not have a counterpart in the PC ASCII character set.

As you customize your terminal emulation environment, be aware that not all PC keys map to a corresponding VT function key. Certain map values translate to local PC functions, and others perform functions outside of the normal scope of terminal emulation, such as escaping to a local command interpreter.

Table A-1 shows these special function keys and their map values.

Table A-1 Keys That Perform Other Than VT Emulation Functions

PC Key	Map Value	Function
F10 (or Alt+F10)	0x070A	Escapes to command interpreter
	0x5000	Sends nothing to remote host
Ctrl+Alt+Del	0x5001	Reboots system
Shift+PrtSc	0x5002	Sends the contents of the screen to the printer
Ctrl+PrtSc	0x5003	Turns continuous screen printing on or off
Caps Lock	0x6000	Turns Caps Lock on or off
Num Lock	0x6001	Turns Num Lock on or off
Scroll Lock	0x6002	Turns scrolling on or off
Shift	0x7001	Turns Shift state on
Ctrl	0x7002	Turns Ctrl state on
Alt	0x7004	Turns Alt state on
Alt+PageUp	0x553	View previous screen if scrollback buffer is enabled

Alt+PageDown	0x554	View next screen if scrollback buffer is enabled
Alt+	0x555	View previous line if scrollback buffer is enabled
Alt+↓	0x556	View next line if scrollback buffer is enabled

Table A-2 shows the default mappings of PC keys to VT function keys. For certain VT function keys (F1, F3, F4, and F5), no corresponding PC key is defined, because these keys are used for local hardware functions on a real VT terminal.

Use the “map value” column when you define an alternative PC key to emulate a VT function. Look up the hexadecimal map value of the function key that you want to emulate, then create a key map file entry to associate it with the appropriate PC key. The “escape sequence” column is useful for verifying that a key that you have redefined sends the appropriate escape sequence. The escape sequence produced when you press a key may vary depending on the terminal type and key mode. The sequences listed are for VT220 terminal emulation with 7-bit controls under normal (default) operating conditions.

Table A-2 VT Function Key Mappings (Cont.)

Press this PC key	**To emulate this VT key**	**Which has this map value**	**And sends this VT escape sequence (7-bit ASCII)**
Cursor Control Keys			
F5, or keypad 8 with Num Lock off (also up arrow on enhanced keyboards)	↑ (up arrow)	0x0241	Esc[A
F6, or keypad 2 with Num Lock off (also down arrow on enhanced keyboards)	↓ (down arrow)	0x0242	Esc[B
F8, or keypad 6 with Num Lock off (also right arrow on enhanced keyboards)	→ (right arrow)	0x0243	Esc[C
F7, or keypad 4 with Num Lock off (also left arrow on enhanced keyboards)	← (left arrow)	0x0244	Esc[D
Auxiliary Keypad Keys			

0	0	0x0710	
1	1	0x0711	
2 (with Num Lock on)	2	0x0712	
3	3	0x0713	
4 (with Num Lock on)	4	0x0714	
5	5	0x0715	
6 (with Num Lock on)	6	0x0716	
7	7	0x0717	
8 (with Num Lock on)	8	0x0718	
9	9	0x0719	
. (period)	. (period)	0x071B	
Enter (or +)	Enter	0x071C	
- (or ,)	, (comma)	0x071D	
*/PrtSc	-	0x071E	
PF Keys (VT100 and VT220 Only)			
F1	PF1	0x0150	EscO P
F2	PF2	0x0151	EscO Q
F3	PF3	0x0152	EscO R
F4	PF4	0x0153	EscO S
Function Keys (VT220 Only)			
Ctrl+F2	F2	0x05002	
Ctrl+F6	F6	0x0311	Esc[17~
Ctrl+F7	F7	0x0312	Esc[18~
Ctrl+F8	F8	0x0313	Esc[19~
Ctrl+F9	F9	0x0314	Esc[20~
Ctrl+F10	F10	0x0315	Esc[21~
Alt+Ctrl+F1	F11	0x0317	Esc[23~
Alt+Ctrl+F2	F12	0x0318	Esc[24~

Alt+Ctrl+F3	F13	0x0319	Esc[25~
Alt+Ctrl+F4	F14	0x031A	Esc[26~
Alt+Ctrl+F5	F15 (Help)	0x031C	Esc[28~
Alt+Ctrl+F6	F16 (Do)	0x031D	Esc[29~
Alt+Ctrl+F7	F17	0x031F	Esc[31~
Alt+Ctrl+F8	F18	0x0320	Esc[32~
Alt+Ctrl+F9	F19	0x0321	Esc[33~
Alt+Ctrl+F10	F20	0x0322	Esc[34~
Programmable Function Keys (VT220 Only)			
Shift+F6	Shift+F6	0x0400	
Shift+F7	Shift+F7	0x0401	
Shift+F8	Shift+F8	0x0402	
Shift+F9	Shift+F9	0x0403	
Shift+F10	Shift+F10	0x0404	
Alt+Shift+F1	Shift+F11	0x0405	
Alt+Shift+F2	Shift+F12	0x0406	
Alt+Shift+F3	Shift+F13	0x0407	
Alt+Shift+F4	Shift+F14	0x0408	
Alt+Shift+F5	Shift+F15	0x0409	
Alt+Shift+F6	Shift+F16	0x040A	
Alt+Shift+F7	Shift+F17	0x040B	
Alt+Shift+F8	Shift+F18	0x040C	
Alt+Shift+F9	Shift+F19	0x040D	
Alt+Shift+F10	Shift+F20	0x040E	
Editing Keys (VT220 Only)			
Alt+F (or Insert key on enhanced keyboards)	Find	0x0531	Esc[1~

Alt+I (or Home key on enhanced keyboards)	Insert	0x0532	Esc[2~
Alt+R (or Page Up key on enhanced keyboards)	Remove	0x0533	Esc[3~
Alt+S (or Delete key on enhanced keyboards)	Select	0x0534	Esc[4~
Alt+P (or End key on enhanced keyboards)	Previous Screen	0x0535	Esc[5~
Alt+N (or Page Down key on enhanced keyboards)	Next Screen	0x0536	Esc[6~

During a VT emulation session, certain applications that you run on the remote host cause the emulator to put the auxiliary keypad (the rightmost bank of keys) into application keypad mode. In application mode, each application can interpret the escape sequences that the auxiliary keypad keys send in its own way. Table A-3 illustrates how application keypad mode changes the function of the auxiliary keypad keys when you run the EDT editor. This table is for your information only; you cannot redefine the behavior of keys in application mode.

Table A-3 VT Auxiliary Keypad Mappings (EDT Application Mode)

PC key	**VT function**
0	Beginning Of Line
.	Select
1	Word
2	End Of Line
3	Char
4	Forward
5	Backwards
6	Cut
7	Command
8	Section
9	Replace

*	Delword
- (or ,)	Delchar
+	Enter

Refer to Table A-4 when you redefine a PC key to send an alternative DEC multinational character. Look up the hexadecimal code of the character that you want to send to the remote host, then create a key map file entry to associate it with the appropriate PC key. The column labels indicate the first digit of the hexadecimal code, and the row labels indicate the second digit.

Table A-4 DEC Multinational Character Set

Hex Digits1st → 2nd ↓	**0-**	**1-**	**2-**	**3-**	**4-**	**5-**	**6-**	**7-**	**8-**	**9-**	**A-**	**B-**	**C-**	**D-**	**E-**	**F-**
-0	NUL	DLE	SP	0	@	P	‘	p		DCS		°	À		à	
-1	SOH	DC1	!	1	A	Q	a	q		PU1	¡	±	Á	Ñ	á	ñ
-2	STX	DC2	“	2	B	R	b	r		PU2	¢	2	Â	Ò	â	ò
-3	ETX	DC3	#	3	C	S	c	s		STS	£	3	Ã	Ó	ã	ó
-4	EOT	DC4	$	4	D	T	d	t	IND	CCH			Ä	Ô	ä	ô
-5	ENQ	NAK	%	5	E	U	e	u	NEL	MW	¥	µ	Å	Õ	å	õ
-6	ACK	SYN	&	6	F	V	f	v	SSA	SPA		¶	®	Ö	æ	ö
-7	BEL	ETB	´	7	G	W	g	w	ESA	EPA	§	·	Ç		ç	œ
-8	BS	CAN	(	8	H	X	h	x	HTS		¤		È	¯	è	ø
-9	HT	EM	)	9	I	Y	i	y	HTJ		©	1	É	Ù	é	ù
-A	LF	SUB	*	:	J	Z	j	z	VTS		ª	º	Ê	Ú	ê	ú
-B	VT	ESC	+	;	K	[	k	{	PLD	CSI	«	»	Ë	Û	ë	û
-C	FF	FS	,	<	L	\	l	|	PLU	ST		1/4	Ì	Ü	ì	ü
-D	CR	GS	-	=	M	]	m	}	RI	OSC		1/2	Í	Ÿ	í	ÿ
-E	SO	RS	.	>	N	^	n	~	SS2	PM			Î		î	
-F	SI	US	/	?	O	_	o	DEL	SS3	APC		¿	Ï	β	ï	

When the DOS VT emulator receives a DEC multinational character that has no corresponding character in the PC code page in use on your PC, the emulator substitutes another character for display on your screen. The network software supports code pages 437 and 850. Table A-5 illustrates the substitutions that the VT emulator makes for DEC multinational characters that it receives but cannot display with code page 850.

Table A-5 DEC Multinational-to-PC Display Mappings (Code Page 850)

DEC multinational character	Hexadecimal value	PC ASCII character	Hexadecimal value
	0xD7	E	0x45
Ÿ	0xDD	Y	0x59
œ	0xF7	e	0x65

Table A-6 illustrates the substitutions that the VT emulator makes for DEC multinational characters that it receives but cannot display with code page 437.

Table A-6 DEC Multinational-to-PC Display Mappings (Code Page 437) (Cont.)

DEC multinational character	Hexadecimal value	PC ASCII character	Hexadecimal value
©	0xA9	c	0x63
3 (cubed)	0xB3	3	0x33
1 (unity)	0xB9	1	0x31
À	0xC0	A	0x41
Á	0xC1	A	0x41
Â	0xC2	A	0x41
Ã	0xC3	A	0x41
È	0xC8	E	0x45
Ê	0xCA	E	0x45
Ë	0xCB	E	0x45
Ì	0xCC	I	0x49

Í	0xCD	I	0x49
Î	0XCE	I	0x49
Ï	0xCF	I	0x49
Ò	0xD2	O	0x4F
Ó	0xD3	O	0x4F
Ô	0xD4	O	0x4F
Õ	0xD5	O	0x4F
	0xD7	E	0x45
Ù	0xD9	U	0x55
Ú	0XDA	U	0x55
Û	0xDB	U	0x55
Ÿ	0xDD	Y	0x59
ã	0xE3	a	0x61
õ	0xF5	o	0x6F
œ	0xF7	e	0x65

During VT emulation, when you run a graphics application or other program that uses the DEC special graphics character set, the VT terminal emulator loads that character set automatically.

The special graphics character set includes graphics symbols and short line segments, some of which do not have equivalents in the PC ASCII code pages supported by the network software. Table A-7 illustrates the substitutions that the VT emulator makes for undisplayable DEC special graphics characters that it receives.

Table A-7 DEC Special Graphics-to-PC Display Mappings

DEC special graphics character	**Hexadecimal value**	**PC ASCII character**	**Hexadecimal value**
Horizontal tab	0x62	Right arrow	0x1A
Form feed	0x63	Up-down arrow	0x17
Carriage return	0x64	Left arrow	0x1B

Line feed	0x65	Down arrow	0x19
Null	0x68	Solid block	9xFE
Vertical tab	0x69	Inverted triangle	0x1F
Not equal	0x7C	Spade	0x06
Scan line 1	0x6F	Underscore	0x5F
Scan line 3	0x70	Underscore	0x5F
Scan line 5	0x71	Scan line 5	0xC4
Scan line 7	0x72	Scan line 5	0xC4
Scan line 9	0x73	Scan line 5	0xC4

A.2 IBM PC Emulation Tables

For tables that apply to IBM PC emulation, refer to section A.1, DEC VT Emulation Tables.

An HFT character set allows you to use any code page, and therefore display any character in that code page.For example, with the HFT character set, you can install code page 865 and have access to the Nordic character set. The HFT character set in Table A-8 illustrates the characters available when it is used with code page 850.

Refer to Table A-8 when you redefine a PC key to send an alternative HFT character. Look up the hexadecimal code of the character that you want to send to the remote host, then create a key map file entry to associate it with the appropriate PC key. The column labels indicate the first digit of the hexadecimal code, and the row labels indicate the second digit.

Table A-8 HFT Character Set Using Code Page 850

Hex Digits 1st → 2nd ↓	0-	1-	2-	3-	4-	5-	6-	7-	8-	9-	A-	B-	C-	D-	E-	F-
-0	NUL	DLE	Blank (space)	0	@	P	`	p	Ç	É	á	▒	└	ð	Ó	-
-1	SOH	DC1	!	1	A	Q	a	q	ü	æ	í	▓	┴	Ð	ß	±
-2	STX	DC2	"	2	B	R	b	r	é	Æ	ó	▓	┬	Ê	Ô	=
-3	ETX	DC3	#	3	C	S	c	s	â	ô	ú	▓	├	Ë	Ò	¾
-4	EOT	DC4	$	4	D	T	d	t	ä	ö	ñ	▓	─	È	õ	¶
-5	ENQ	NAK	%	5	E	U	e	u	à	ò	Ñ	Á	┼	ı	Õ	§
-6	ACK	SYN	&	6	F	V	f	v	å	û	ª	Â	ã	Í	µ	÷
-7	BEL	ETB	'	7	G	W	g	w	ç	ù	º	À	Ã	Î	þ	¸
-8	BS	CAN	(	8	H	X	h	x	ê	ÿ	¿	©	╚	Ï	Þ	°
-9	HT	EM	)	9	I	Y	i	y	ë	Ö	®	╔	╩	┘	Ú	¨
-A	LF	SUB	*	:	J	Z	j	z	è	Ü	¬	╦	╠	┌	Û	·
-B	VT	ESC	+	;	K	[	k	{	ï	ø	½	╗	═	█	Ù	¹
-C	FF	FS	,	<	L	\	l	|	î	£	¼	╝	╬	▄	ý	³
-D	CR	GS	-	=	M	]	m	}	ì	Ø	¡	¢	╧	¦	Ý	²
-E	SO	RS	.	>	N	^	n	~	Ä	×	«	¥	╨	Ì	¯	■
-F	SI	US	/	?	O	_	o	Δ	Å	ƒ	»	┐	▫	▀	´	Blank "ff"

A.3 IBM 3270 Emulation Tables

The tables in this section contain the following information:

- Default mappings of PC keys to 3270 function keys, and their map values.
- Default ASCII and EBCDIC character sets for 3270 emulation. These two tables combined reflect the characters supported in the default translation table, XLATE327.TBL.

As you customize key mappings, be aware that Alt+F10 is the default escape key for the 3270 emulator. Its map value is 0x00CC; if you want to redefine the key that escapes to the local command interpreter, create an entry in the key map file that associates the value 0x00CC with another PC key.

Table A-9 lists default mappings of PC keys to IBM 3270 function keys and cursor motion keys. A (Y) after the 3270 key name indicates a Yale feature. The following Yale features are not emulated: Word Tab, Word BackTab, Indent, Undent, WordEnd, FieldEnd, and Clear Single ColTab.

Table A-9 IBM 3270 Function Key Mappings (Cont.)

Press this PC key	To emulate this 3270 key	Which has this map value
F1	PF1 (PSA)	0x00D8
F2	PF2 (PSB)	0x00D9
F3	PF3 (PSC)	0x00DA
F4	PF4 (PSD)	0x00DB
F5	PF5	0x00DC
F6	PF6	0x00DD
Page Up	PF7 (CMS usage)	0x00DE
Page Down	PF8 (CMS usage)	0x00DF
F9	PF9	0x00E0
F10	PF10	0x00E1
Shift+F1 (or F11 on enhanced keyboards)	PF11	0x00E2
Shift+F2 (or F12 on enhanced keyboards)	PF12	0x00E3

Shift+F3	PF13 (Red)	0x00E4
Shift+F4	PF14 (Pink)	0x00E5
Shift+F5	PF15 (Green)	0x00E6
Shift+F6	PF16 (Yellow)	0x00E7
Shift+F7	PF17 (Blue)	0x00E8
Shift+F8	PF18 (Turquoise)	0x00E9
Shift+F9	PF19 (White)	0x00EA
Shift+F10	PF20 (Black)	0x00EB
Ctrl+F1	PF21	0x00EC
Ctrl+F2	PF22	0x00ED
Ctrl+F3	PF23	0x00EE
Ctrl+F4	PF24	0x00EF
Alt+F1	PA1	0x00D1
Alt+F2	PA2	0x00D2
Alt+F3	PA3	0x00D3
Ctrl+C	Clear Yale Parameters (Y)	0x00BA
Ctrl+H	Set Yale Home (Y)	0x00B9
Ctrl+L	Redisplay Screen	0x00A5
Ctrl+M	Set Yale Margin (Y)	0x00B8
Ctrl+T	Set Yale Col Tab (Y)	0x00B6
Ctrl+F9	Reset (Keyboard Unlock)	0x00C8
Ctrl+F10	Master Reset	0x00C9
Alt+F4, Keypad +	Clear	0x00D4
Alt+F5	Test Request	0x00D5
Enter	Enter	0x00D6
Ctrl+Scroll Lock	Attention	0x00FF
Alt+F6	Cursor Sel (light pen)	0x00A3

EBCDIC Data or Control Characters Not Present in ASCII

Alt+D	Duplicate	0x00A1
Alt+F	Field Mark	0x00A2
Alt+C	Centsign	0x00A4

3270 Local Editing Keys

Esc	Erase Input	0x00A6
Keypad -	Erase to End of Field	0x00A7
Keypad Del	Delete (under cursor) (Y)	0x00A8
Ins	Toggle Insert	0x00A9
Keypad End (or Enter)	Newline	0x00B0
Backspace <-	Erase	0x00C4
Ctrl+backspace	Erase current field	0x00C6

IBM 3270 Cursor Motion Keys

Keypad 2	Down arrow	0x00B3
Keypad 4	Left arrow	0x00B5
Keypad 6	Right arrow	0x00B4
Keypad 7	Home	0x00B1
Keypad 8	Up arrow	0x00B2
Ctrl+keypad 6	Col Tab (Y)	0x00AC
Ctrl+keypad 4	Col BackTab (Y)	0x00AD
Tab	Field Tab	0x00AA
Shift+Tab	Field Backtab	0x00AB

Table A-10 shows the hexadecimal codes for the default EBCDIC character set supported by the 3270 emulator. The row labels indicate the first digit of the hexadecimal code, and the column labels indicate the second digit. The first four rows are not shown because they contain control characters.

The 3270 emulator's built-in EBCDIC-to-ASCII translation table contains ASCII character code mappings for all of the EBCDIC characters shown. In fact, Table A-10 mimics the format of the

online translation table, except that the online table contains ASCII codes for the characters instead of the actual characters shown here. You can use the blank spaces in the online table to insert additional mappings for special or multilingual characters that you expect to receive from the remote host.

Table A-10 Default EBCDIC Character Set for 3270 Emulation

Hex Digits2nd → 1st ↓	**-0**	**-1**	**-2**	**-3**	**-4**	**-5**	**-6**	**-7**	**-8**	**-9**	**-A**	**-B**	**-C**	**-D**	**-E**	**-F**
4-	SP										¢	.	<	(	+	|
5-	&										!	$	*	)	;	^
6-	-	/										,	%	_	>	?
7-		^								‘	:	#	@	‘	=	“
8-		a	b	c	d	e	f	g	h	i						
9-		j	k	l	m	n	o	p	q	r						
A-		~	s	t	u	v	w	x	y	z				[		
B-														]		
C-	{	A	B	C	D	E	F	G	H	I						
D-	}	J	K	L	M	N	O	P	Q	R						
E-	\		S	T	U	V	W	X	Y	Z						
F-	0	1	2	3	4	5	6	7	8	9						

Table A-11 shows the hexadecimal codes for the default ASCII character set supported by the 3270 emulator. The row labels indicate the first digit of the hexadecimal code, and the column labels indicate the second digit. The first two rows are not shown because they contain control characters.

The 3270 emulator’s built-in ASCII-to-EBCDIC translation table contains EBCDIC character code mappings for all of the ASCII characters shown. In fact, Table A-11 mimics the format of the online translation table, except that the online table contains EBCDIC codes for the characters instead of the actual characters shown here. You can use the blank spaces in the last two rows of the table to insert additional mappings for special or multilingual characters that you want to send to the remote host.

Table A-11 Default ASCII Character Set for 3270 Emulation

Hex Digits2nd → 1st ↓	**-0**	**-1**	**-2**	**-3**	**-4**	**-5**	**-6**	**-7**	**-8**	**-9**	**-A**	**-B**	**-C**	**-D**	**-E**	**-F**
2-	SP	!	“	#	$	%	&	‘	(	)	*	+	,	-	.	/
3-	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
4-	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5-	P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
6-	‘	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
7-	p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	DEL
8-																
9-																

Chapter 3
Transferring Files

Several DOS commands that let you transfer files between your PC and other computers (hosts) on the network. For most file transfers, you can use the **ftp** or **tftp** client commands, or you can set up a file transfer server on your PC with the **ftpsrv** or **tftp serve** commands. You can also transfer files, including directory hierarchies, with the **rcp** command.

The **ftp** command is based on the File Transfer Protocol (FTP). Most hosts support FTP. The **tftp** command is based on the Trivial File Transfer Protocol (TFTP), which provides a simple user interface with no user authentication. The **rcp** command is based on the Remote Copy Protocol (RCP), which provides Kerberos authentication, if available. Note that 4BSD UNIX hosts support RCP.

Refer to Chapter 1, Introduction to see if the DOS commands discussed in this chapter are included with the version of the network software that you have.

3.1 Before You Start Transferring Files

You should ensure that you

- Know which file transfer server programs are running on the remote host.
- Know how to log in to the remote host.
- Have a user ID and a password (if required) on the remote host.
- Are familiar with security systems installed on the remote host.
- Are familiar with filename conventions and case sensitivity rules on the remote host.
- Are familiar with wildcard syntax used by the operating system on your PC and on the remote host.

If you are unsure about this information, contact the system administrator for the remote host.

3.2 Transferring Files with ftp

The **ftp** client command lets you

- Open and close an ftp session on a remote host.
- Transfer single and multiple files.
- Transfer binary files.
- Select options during a file transfer.
- Execute DOS commands during an ftp session.
- Manage directories during an ftp session.
- Display file contents during an ftp session.

3.2.1 Managing an ftp Session on a Remote Host

To transfer files with **ftp**, you must first learn how to

- Begin and end an ftp session on a remote host.
- Get ftp online help.

To begin an ftp session on a remote host

1. At the DOS prompt, enter **`ftp`** followed by the name of the remote host.

   For example, to connect to a remote host named paris, enter

   ```
   ftp paris
   ```

2. To accept the default user ID supplied by the network software, press Enter or enter another user ID at the prompt.

   For example, if your user ID is pat, enter the following:

   ```
   Userid for logging in on paris.comp.com (default)? pat
   ```

3. Enter your password at the prompt from the remote host.

   ```
   Password for logging in as (pat) on paris.comp.com?
   ```

   If you entered an incorrect password, you are still in an ftp session. You can restart the login procedure by typing **`user`** at the prompt, or you can close the session by typing **`bye`** or **`quit`**

After you open an ftp session, you see the ftp prompt. This prompt differs in appearance depending on how you specified the remote host. In the following examples, the prompt is abbreviated to `ftp>`

To get ftp online help

To see a command list, at the ftp prompt, type a question mark(**?**).

```
ftp>?
```

–or–

Enter **`help`** followed by the **ftp** command name.

For example, to see command line usage for **get**, enter the following:

```
ftp>help get
```

3.2.2 Transferring Single and Multiple Files

Once you open your ftp session, you can

- Get a single file from the remote host.
- Get multiple files from the remote host.
- Put a single file on the remote host.
- Put multiple files on the remote host.

To get a single file from the remote host

Enter **`get`** followed by the filename of the remote file.

For example, to transfer the file BUBBLES.TXT from the remote host and store it under the same name on the local PC, enter the following:

```
ftp>get bubbles.txt
```

To transfer the file SOAP.TXT and assign it the new name BATH.TXT, enter the following:

```
ftp>get soap.txt bath.txt
```

The ftp session prompts you for these filenames if you do not supply them. (Note that case sensitivity rules on the remote host may differ from those on your PC.)

To get multiple files from the remote host

Enter **`mget`** followed by the filenames to be transferred. Specify parts of the filename common to all the needed files, and use wildcards to stand for other characters.

The remote host interprets the wildcard syntax. After transfer, the files retain their original names on your PC. For example, to transfer all files that have a .TXT extension, enter the following:

```
ftp>mget *.txt
```

Note: These examples may not work as described if the remote host's wildcard syntax is different.

To put a single file on the remote host

Enter **`put`** followed by the filename of the local file and the filename that you want to give the file on the remote host.

For example, to put SHOWER.TXT on the remote host, enter the following:

```
ftp>put shower.txt
```

To put multiple files on the remote host

Enter **`mput`**, followed by wildcard syntax for the files to be transferred from your PC. Use PC wildcard syntax, since it is your PC that interprets the syntax. The **mput** command works like the **mget** command.

3.2.3 Transferring Files in Binary Mode

The **ftp** default transfer mode for transferring files is ASCII. Some files (for example, executable files) must be transferred in binary mode rather than in ASCII. You can set binary mode as the prevailing transfer mode, or you can specify binary mode transfer for individual files. Binary modes are Binary, Image, Tenex, or Local *n* (where *n* is the byte size of the remote machine).

To transfer a single file in binary mode

Enter **`iget`** or **`iput`** followed by the filename. For example, to transfer the binary file PRINT.EXE from the remote host and store it under the same name on your PC, enter the following:

```
ftp>iget print.exe
```

To set the transfer mode to binary for all file transfers

Enter `binary`, `image`, `tenex`, or `local` *n* at the ftp prompt. You can then use the **get** or **put** command for binary files as you do for ASCII files.

To reset the transfer mode for ASCII file transfers

Enter **`ascii`** at the ftp prompt:

```
ftp>ascii
```

3.2.4 Selecting Options During a File Transfer

The **ask** option is useful when you are transferring more than one file and you want to change parts of the transfer selectively. When this option is on, ftp prompts you before each transfer and lets you specify such actions as renaming files and changing transfer mode.

To transfer multiple files selectively

1. Enter **`option ask on`** at the ftp prompt:

   ```
   ftp>option ask on
   ```

2. Enter **`mget`** at the ftp prompt.

   For example, to get all the files named ANJOU, enter the following:

   ```
   ftp>mget anjou.*
   ```

3. Respond to the prompt by typing the first letter of the options that you want.

   For example, to select the **image** option for the transfer, and then to transfer the file, enter the letters **`I`** and **`Y`**

   ```
   anjou.txt --->anjou.txt
   TRANSFER FILE?(Yes/No/Proceed/Quit/Rename/Ascii/Image/Tenex] I Y
   ```

   To rename the file, enter the letters **`R`** and **`Y`** and respond to the filename prompts by typing a filename or accepting a default.

3.2.5 Executing DOS Commands on Your PC During an ftp Session

DOS commands are useful during an ftp session if you want to view or edit files on your PC before transferring them, or if you want to create directories on the PC to receive files from the remote host.

To execute a DOS command from an ftp session

Enter an exclamation point (**!**) followed by a space, followed by the command.

For example, to request a display of the file LEMONS.TXT before sending it to the remote host, enter the following:

```
ftp>! type lemons.txt
```

To escape to a DOS session

Enter only the exclamation point:

```
ftp>!
```

Your PC displays the DOS prompt, from which you can issue any number of DOS commands.

To return to the ftp session from a DOS session

Enter **exit** at the DOS prompt.

3.2.6 Managing Directories During an ftp Session

You can display, change, create, and delete directories on both your PC and the remote host while you are in an ftp session. The commands for those actions are familiar DOS commands or variations on them. Commands to the local host are preceded by the letter l (for local), while some remote hosts may require the letter f (for foreign) before the DOS command equivalent.

Note: If you have opened your ftp session on a a remote UNIX host, be sure to use a slash (/) instead of a backslash (\) when changing directories or specifying a pathname.

To manage directories on the remote host during an ftp session

Use the following commands:

To do this on the remote host	Enter
Display a directory list.	**`dir`** or **`ls`**
Display the current working directory.	**`pwd`** or **`fpwd`**
Change the current working directory.	**`cd`** (or **`fcd`**) and the pathname
Create a directory.	**`mkdir`**
Delete a directory.	**`rmdir`**

For example, if you want to change to the /etc directory on a UNIX host, enter the following command:

```
ftp> cd /etc
```

To manage directories on your local PC during an ftp session

Use the following commands:

To do this on your local PC	Enter
Display a directory list.	**`ldir`**
Display the current working directory.	**`lpwd`**
Change the current working directory.	**`lcd`**
Change the current drive.	**`drive`** and the drive letter

Create a directory. **lmkdir**

For example, to change to your \ETC directory, enter the following command:

```
ftp>lcd \etc
```

3.2.7 Displaying File Contents During an ftp Session

You can display file contents on both your PC and the remote host while you are in an ftp session. The **option** command lets you activate special features of ftp such as the **page** feature, which controls the scrolling of information across your screen.

To display a file on the remote host

1. At the ftp prompt, enter **`option page on`** to prevent the display from scrolling off the screen:

   ```
   ftp>option page on
   ```

2. At the ftp prompt, enter **`show`** followed by the filename.

   For example, to see the contents of the LEMONS.TXT file, enter the following command:

   ```
   ftp>show lemons.txt
   ```

3. At the ftp prompt, enter **`option page off`** to reactivate the normal scrolling feature:

   ```
   ftp>option page off
   ```

3.3 Transferring Single Files Quickly with tftp

The **tftp** command, an implementation of the Trivial File Transfer Protocol (TFTP), lets you transfer single files *without any user authentication* between hosts on a network.Not all hosts implement **tftp** service. It is currently available on most networked Multics, 4BSD UNIX, DOS, and TOPS-20 machines.

To transfer files with tftp

Use the following command syntax for each file that you want to transfer:

tftp (**get** | **overwrite** | **put**) *local_filename host remote_filename* [**image**]

where

local_filename Specifies the filename on the PC issuing the transfer command; it is always the first filename argument required.

host Specifies the name of the machine running the TFTP server.

remote_filename Specifies the name of the file on the remote host running the TFTP server. You need to specify the complete pathname if it is different from the default tftp directory. For remote UNIX hosts, use the slash pathname syntax (*/path/filename*).

Use the following table to determine which option to use:

To do this	Enter
Copy a file from the server.	**get**
Place a file on the server.	**put**
Overwrite a file on the local system.	**overwrite**
Use binary mode transfer.	**image**

For example, to transfer a file named GRAPES from the remote host called garden and store it under the same filename on the local PC, enter the following:

```
tftp get grapes garden grapes
```

Or to replace in Image mode the local PC file SEARCH.EXE with the file etc/find.exe from the remote UNIX host called vex, enter the following:

```
tftp overwrite search.exe vex etc/find.exe image
```

3.4 Transferring Files and Directories with rcp

The **rcp** command is a client command based on the Remote Copy Protocol (RCP). It lets you transfer not just files but directories and hierarchies of directories. However, you cannot move between directories and display directory listings as you can with the **ftp** command.

Before you start using **rcp**, you or your system administrator should ensure that

- The UNIX remote host is running the BSD rsh or rexec server programs.
- The `user=` parameter in the `[pctcp general]` section of your PCTCP.INI configuration file matches your user ID in the UNIX .rhosts file, or that your PC's hostname appears in the UNIX host's /etc/hosts file.

To copy a file from a UNIX host to your PC

Use the following command syntax:

rcp *user@hostname:remote_filename local_filename* [**-a** | **-b**]

where

user Specifies your user ID as specified by the remote host in its .rhosts file.

hostname Specifies the name of the remote host.

remote_filename Specifies the filename of the source (remote) file that you want to copy. Use the UNIX slash pathname syntax (*/path/filename*).

local_filename Specifies the path and filename of the destination (local) file. You need to specify the complete pathname if it is different from the default directory.

-a Specifies that the file being transferred is ASCII text, and requires translation between UNIX end-of-line notation and PC end-of-line notation. This is the default transfer mode. This option cannot be used with the **-b** option.

-b Specifies binary file transfer, and disables conversion between UNIX end-of-line notation and PC end-of-line notation. This option cannot be used with the **-a** option.

For example, if your user ID on the remote host peach is pat, and you want to copy the file STRAWB.TXT from the remote directory fruit to your PC, enter the following:

```
rcp pat@peach:/fruit/strawb.txt strawb.txt
```

To copy a file from your PC to a UNIX host

Use the following command syntax:

rcp *local_filename user@hostname:remote_filename*

where

local_filename Specifies the source file on the local host.

remote_filename Specifies the destination file on the remote host. You need to specify the complete pathname if it is different from the default directory.

For example, to copy in binary mode all .EXE files in the current directory from your PC to your login directory on the host green.xyz.com, enter the following (including the colon):

```
rcp -b *.exe green.xyz.com:
```

To copy all files from a current directory and its subdirectories

Use wildcards with the **-r** and **.** (period) options.

For example, to copy all files from your current directory and its subdirectories to your login directory on the host green.xyz.com, enter the following (including the colon):

```
rcp -r *.* green.xyz.com:
```

To copy all files from your current directory and its subdirectories to your \TEST directory on the host green.xyz.com, enter the following:

```
rcp -r *.* green.xyz.com:\test
```

To copy all files from your login directory and its subdirectories on the remote host green.xyz.com to the current directory on your PC, enter the following (including the space before the final period):

```
rcp -r green.xyz.com:* .
```

3.5 Activating a File Transfer Server on Your PC

If a remote user wants to transfer files to or from your PC, you can start an FTP server on your PC. You can also use a password file to limit FTP access to your PC.

When you start a file transfer server, remote users can establish an FTP connection to your PC and enter file transfer commands. By default, they log in to the current working directory on your PC. Note that their remote FTP client command may not work the same way the OnNet or PC/TCP **ftp** command works.

While the file transfer server is running, your PC does not display a command line prompt. However, you can still get online help or request information, such as the number of connections made to your PC, and the number of files received or sent.

3.5.1 Activating a TFTP Server on Your PC

The TFTP server does not require a password from the user. Since anyone can access any disk on your PC when running **tftp serve**, use the server very carefully. Moreover, the DOS operating system is not designed for unattended use. For example, if the remote user uses the **put** command to write a file to a write-protected diskette or unreadied disk drive, DOS prompts the operator of the server PC for instructions. Until someone answers this prompt, the TFTP server is disabled.

To run the TFTP server

Enter **`tftp serve`** at the system prompt.

To get TFTP server online help

Enter a question mark (**`?`**) subcommand.

To turn off the TFTP server

Enter **`q`**

3.5.2 Activating an FTP Server on Your PC

Activating an FTP server on an unattended PC exposes it to other users who can write over and delete any of your files that are not write protected. You should create and use a password file that prevents unauthorized use of your PC as an FTP server. For a description of this procedure, see section 3.6, Using a Password File to Limit FTP Access to Your PC.

To start an FTP server on your PC

Enter **`ftpsrv`** at the system prompt:

```
ftpsrv
```

To restrict FTP access to a specified host

Start the FTP server on your PC with the **-h host** option.

For example, to restrict the server to the host paris, enter the following:

```
ftpsrv -h paris
```

To get FTP server online help

Type a question mark (**`?`**).

To get FTP server statistics

Enter **`s`**

To exit from the FTP server

Enter **`q`**

3.6 Using a Password File to Limit FTP Access to Your PC

You can restrict access to an ftp server on your PC to those users listed in a password file. You can also use this file to limit access to specified directories. Users *not* listed in this password file *cannot* open an ftp session on your PC. For the server to prompt users for a password, first give them one with the **passwd** command.

Before you execute the **passwd** command, the `pfile=` parameter in your PCTCP.INI file must point to a filename for the password file.

***Caution*:** PCs are not designed to be secure machines, even with a password file. If your PC is not physically protected, any person can use it, tamper with files (even password files) on it, or reboot it. The **passwd** command lets a user enter a new password without requesting the old password.

To create a password file

1. Edit your PCTCP.INI file and add the `pfile=` parameter to the `[pctcp general]` section to point to your password file, as in the following example:

   ```
   [pctcp general]
   pfile=C:\PCTCP\PASSWD
   ```

2. Have each user listed in your password file use the **passwd** command on your PC (or assign them a password and enter it yourself.) Passwd prompts you for the required information.

   ```
   C:\> passwd joe
   ```

   Passwd prompts you for responses in a dialog similar to the following:

   ```
   Password file C:\PCTCP\PASSWORD.TXT does not exist, create (y/n)? Y
   User joe is not in the password file, add (y/n)? Y
   New Password:
   Re-enter new password to verify:
   Enter UID for new user [-2]:
   Enter GID for new user [-2]:
   Enter full name for new user [none]: joe smith
   Enter home directory for new user [C;\]: C:\REPORTS
   Enter drive restrictions for new user [none]: C,D
   ```

The passwd program inserts the new entry in your password file with the password encrypted. This release of OnNet or PC/TCP software uses a more powerful encryption method than previous releases. When using a password file from a previous release, **passwd** first attempts to authenticate the password with the new method, and then uses the old method.

To change a user's password

Use the **passwd** command. Passwd prompts for the new password:

```
C:\> passwd cloudy

New password:
Re-enter new password to verify:
```

To restrict a user's directory access

1. Use the DOS **subst** command for each directory to which you want to restrict access.

   The command uses the syntax

   subst *drive: drive:\directory_path*

   For example, a user might create two logical drives – I that refers to the directory C:\PAT and D that refers to the directory C:\RECORDS:

   ```
   subst I: c:\pat
   subst D: c:\records
   ```

2. Modify the password file entry for each user, specifying a logical drive as the login directory and a list of logical drives that each user can access. (On the line after each user entry, press Tab and type the logical drives to which the user can have access.)

   Note: When adding a new user with the **passwd** command, you are prompted for drive access restrictions.

   For example, a user could specify the logical drive I as a login directory for Pat and restrict her to the logical drives I and D with the following entry in \PCTCP\PASSWORD.TXT:

   ```
   pat:n9yn8bX365:110::Pat J. Sawyer:I;\
      I,D
   ```

Note: Some text editors replace tabs with spaces, which cause the password file to fail.

3.7 Transferring Files During a Remote Login Session

If you need to transfer files while running a terminal emulation program such as tn or rloginvt, you can start an FTP server on your PC. (This FTP server is embedded in these programs.) Then you can start an ftp session between your PC and the terminal emulation host.

Since your PC is the FTP server, *it* becomes the FTP remote host. The host on which you are logged in for the terminal emulation session becomes the local host. Thus, at the FTP session prompt, the remote commands apply to your PC. (Note that FTP commands supported by the remote host may differ from the **ftp** commands supported by your OnNet or PC/TCP software.)

***Caution*:** The FTP server embedded in these applications supports using a password file. If you do not have this file, anyone can log in to your system while it is running the server.

To activate an embedded FTP server

From the remote host prompt, press F10, Shift+F or Alt+F10, Shift+F. (Your PC becomes an FTP server.)

To deactivate an embedded FTP server

From the remote host prompt, press F10, Shift+F (or Alt+F10 Shift+F) again.

To transfer files during a remote login session

1. Activate the embedded FTP server.
2. Start an ftp session by entering the **ftp** *hostname* command at the remote prompt.

   –or–

   Enter the remote host's equivalent FTP command.
3. Enter your login *userid* and *password*.
4. Use the remote host's ftp session commands to transfer files between your PC and the remote host.

   Most hosts use the same basic command set as that of OnNet or PC/TCP. Refer to the remote host's manuals to verify its ftp session commands.
5. Exit from the ftp session when you are done transferring files. (If you do not deactivate the embedded FTP server, users can still log into your PC.)

To restart an embedded ftp session that has stopped from inactivity

From the remote host prompt, press F10, Shift+F (or Alt+F10 Shift+F).

To change the directory on the remote host during an embedded ftp session

Use the **lcd** command.

For example, if you want to change to the \ETC directory on the remote host, enter the following:

```
ftp>lcd \etc
```

To manage directories on your PC during an embedded ftp session

Use the following commands:

To do this on your PC	Enter
Display a directory list	**dir**
Display the current working directory (not universally supported)	**pwd**
Change the current working directory	**cd**
Create a directory	**mkdir**
Delete a directory	**rmdir**

For example, to change to your \ETC directory, enter the following command:

```
ftp>cd \etc
```

3.8 Automating or Initializing File Transfers

You can use take (batch) files to automate or initialize your ftp session or your daily file transfers.

If there are **ftp** initialization commands that you enter each time that you run **ftp** (for example, **option ask on**), you can automate the process by placing these commands in a take file. Use a text editor to create this take file.

For example, to get daily files from one of two machines (VEX or VOX) running UNIX, you could type the following text into a take file called \ETC\NIGHTGET.TAK:

```
#Get my daily files
option ask on
# VEX directory
cd /trees/flowering/fruit
# VOX directory
cd /flowers/scented/roses
mget *.txt
iget start.exe
quit
```

You can configure this ftp take file in your PCTCP.INI file, or you can activate it from the ftp session prompt with the **take** *FILENAME*.TAK command. For example, to initialize your **ftp** command to use the \ETC\NIGHTGET.TAK file, list this file with the `ftpinit=` parameter in the `[pctcp ftp]` section of your PCTCP.INI file as follows:

```
[pctcp ftp]
ftpinit =C:\ETC\NIGHTGET.TAK
```

Every time that you run **ftp**, it first executes any commands in the initialized take file, skipping commands that do not work (server-specific commands such as **cd** DIRECTORY). You can then enter additional **ftp** commands or **exit** to exit from the ftp session.

To activate the \ETC\NIGHTGET.TAK file from the ftp prompt, enter the following command:

```
ftp>take \ETC\NIGHTGET.TAK
```

You can also execute this same take file from the DOS prompt, using the **-u userid password** and **command** options of the **ftp** command.

For example, if your userid is pat and your password is hushhush on the remote host vex, enter the following:

```
ftp -u pat hushhush vex take \ETC\NIGHTGET.TAK
```

When executed by **ftp** for server VEX, this \ETC\NIGHTGET.TAK take file

1. Turns on the **ask** option.

2. Changes the working directory on the remote host to `/trees/flowering/fruit`.

3. Transfers to the local host a set of files whose filenames end with .TXT.
4. Transfers the START.EXE file in binary mode to the local host.
5. Exits from the ftp session.

3.9 Troubleshooting File Transfers

This section provides possible solutions to situations that you can encounter when transferring files. The situation is described first, followed by the action to take.

When using the **get** command, there is a long wait for a response.

Use the **inet stat** command to determine if TCP retransmits packets.
–or–
Adjust the TCP window size by changing the value of the `window=` parameter in the `[pctcp kernel]` section of your PCTCP.INI file. (Unload and reload the kernel to make the change take effect.)
–or–
Increase the number of packet buffers by reloading the kernel with the **-p n** and **-s n** options of the **kernel** command.
–or–
On an IBM PS/2 or PC AT host, try turning off the DMA (direct memory access) on your network interface card. Refer to the documentation for your network interface card for instructions.

Some commands to the remote machine fail.

Upgrade the remote FTP server program.
–or–
Get a list of the commands that this server supports by running the help function on the remote host (for example, enter **`quote help`**).

Transferred binary files do not execute.

Use **image** to transfer files from remote machines with 8-, 16-, or 32-bit word size. Use **tenex** to transfer files from systems such as LISP and TOPS-20 that use another word size.

Service not available, remote server has closed connection.

Restart the embedded FTP server by pressing F10, Shift+F (or Alt+F10, Shift+F). Note that this message does not appear on its own, but only after a user attempts a command other than the **quit** sort after five minutes of inactivity.

Out of resources (memory or connections).

Unload and reload your kernel with an additional TCP connection. (Use the **-t** option of the kernel command, or the `tcp-connections=` parameter in your PCTCP.INI file.) A simple **ftp** transfer requires two connections on the client side. Use **inet tcp** to verify that one TCP connection is open between some port on your PC and port 21 on the remote host during an **ftp** transfer.

Note: Error messages that display a three-digit number at the beginning of the message originate from the server. If the message is not clear, consult the documentation of the remote

FTP server.

Chapter 1
Introduction

OvNεt™ and PC/TCP® let your PC exchange information and services with other computers that connect to a TCP/IP network.You can perform tasks and services on your PC by using either DOS commands or applications available through your Windows graphical user interface. This manual explains how to perform networking tasks using DOS commands. Refer to *Using OnNet for Windows* for information about the available Windows applications.

Because OnNetand PC/TCP are distributed in different configurations on different media, it is important to know which version you have and to understand which DOS commands are available with each configuration.

- The PC/TCP product is distributed on diskettes and includes all of the DOS commands described in this book, as well as some Windows applications.
- One version of OnNet is distributed on CD-ROM and includes all of the DOS commands listed and described in this book, and all of the Windows applications.
- One version of OnNet is distributed on diskettes. It includes a full set of Windows applications and a subset of the DOS commands, as follows:

bootp	dhcp	dos2unix	ftpver	host
idchmod	idconfig	idls	idmnt	idprint
idumnt	idutil	inet	kdestroy	kinit
klist	kpasswd	lpq	lpr	lprm
pctcpcfg	ping	rmt	tar	tftp
tnglass	unix2dos			

The following table lists the networking tasks that you can perform with this software, and the commands to use for each task:

Networking Task	**DOS Commands**
Learning about hosts and users on the network	**finger, host, inet, nicname, ping, setclock, whois**
Transferring files	**ftp, ftpsrv, passwd, rcp, rloginvt, tftp**

Logging in to a remote host, customizing terminal emulation, and remapping your keyboard	**keymap, rlogingl, rloginvt, rsh, setcolor, tn, tnglass**
Printing to a network printer	**lpd, lpq, lpr, lprm, predir, onpredir, dopredir**
Exchanging mail and network news	**nntp, pcmail, pop2, pop3, smtp, vmail**
Backing up and restoring files	**ddates, rmt, tar**
Connecting to remote networks over a modem or a serial line	**comscrpt, inet**

1.1 Before You Start Using Commands in DOS

To use your network software, you must know the names and locations of "servers," systems that provide services to other systems in a network. Your system administrator can provide information about the servers at your site.

In most cases, your PC is a "client" of the TCP/IP network servers. With your network software, you can connect to many types of servers on your network to extend your PC's computing capabilities. In addition, your PC can become a server for some applications, such as ftp, a file transfer program.

You should also ensure that you understand

- How to use wildcards.

  Some commands, such as **ftp**, take command line arguments in a wildcard format. Since the remote host interprets the wildcard syntax, you need to use the wildcard characters that the remote host interprets. For example, you can use the asterisk (*) as a wildcard, as in **ls *.doc**, only if the remote host interprets the asterisk as a wildcard.

- Case sensitivity requirements on remote hosts that you are accessing.

  Many operating systems interpret uppercase letters in files or commands differently than lowercase letters. If you are connecting to another *DOS* host, case sensitivity is not an issue; DOS is not case sensitive. However, if you connect to a *UNIX* host, be aware that the UNIX host may be case sensitive.

Note: FTP Software recommends that you do not use the DOS **append** command and that you make certain that the DOS **append** command is not in your AUTOEXEC.BAT file. The DOS **append** command is a memory resident command that can cause problems when you transfer files. If you do want to use the command, read your DOS manual very carefully and understand its proper use.

1.2 Entering Commands

OnNet and PC/TCP support both a command-line interface and a Microsoft Windows graphical user interface.

1.2.1 Using Commands from the DOS Command Line

You enter commands at the DOS prompt using the following command line syntax conventions:

Enter	Initiates the command. For a brief display of command-line options, press Enter immediately after the command name.
Esc or Ctrl+C	Aborts most DOS commands.
-*options*	Modifies the behavior of the command in the way that you choose. You generally enter a hyphen (-) before command line options. You enter one hyphen, followed by one or more options.
command -?	Displays the command syntax and a list of command-line options.
command -version	Displays the version number of the command.

The descriptions of individual commands in the *Command Reference* explain any exceptions to these conventions.

1.2.2 Using Commands In Windows

If you use Microsoft Windows, you can use DOS applications with Windows . Execute the DOS commands by one of the following methods:

- Entering the command in a DOS session.
- Using the Windows Run command from the Program Manager File menu.

1.2.3 Interactive Commands

After you enter a command, the command usually executes a task and then returns control to DOS—you immediately see the DOS prompt. Some commands, however, start an application that provides its own command-line or graphical user interface. For example, when you enter the **ftp** command, you start an FTP session—you see an **ftp** command-line prompt. Until you exit from the application, the **ftp** command interprets any command that you enter. Similarly, when you enter the **keymap** command, you start a DOS application with a graphical user interface—you work with menus and dialog boxes in the application until you exit from the application.

Appendix B
Keyboard Scan Codes

This appendix contains translated scan codes that the key mapping software uses to identify each key. It shows the scan codes for these standard IBM keyboards:

- IBM standard U.S. PC or PC XT
- IBM standard U.S. PC AT
- IBM enhanced PC AT (European)

Refer to these keyboard diagrams in Figures B-1 to B-3 when redefining key mappings for terminal emulation. If the scan codes for your keyboard are not included here, you can use the **sc** command to display the scan codes interactively for keys that you press.

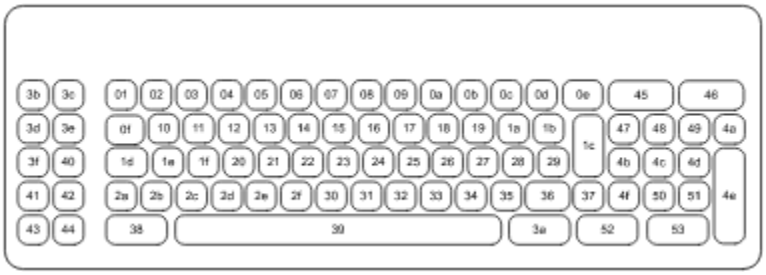

Figure B-1 IBM PC or PC XT Standard Keyboard Scan Codes

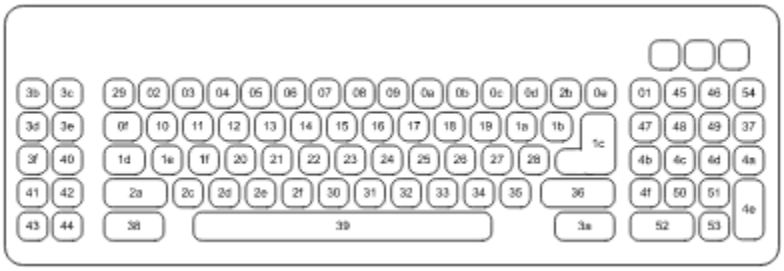

Figure B-2 IBM PC AT Standard Keyboard Scan Codes

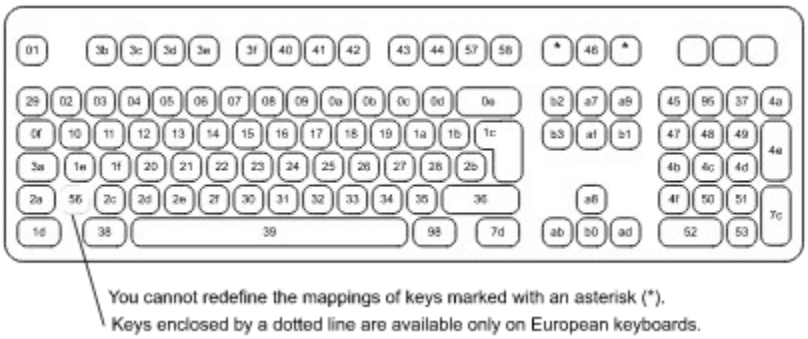

Figure B-3 IBM PC AT Enhanced Keyboard Scan Codes (European)

Appendix B Keyboard Scan Codes

Chapter 6
Customizing Your Keyboard

A major part of terminal emulation involves translating the characters that you type at your PC keyboard into characters that the remote system can use. You can customize your terminal emulation environment by redefining the character that gets sent to the remote system when you type a key.

This chapter describes the DEC VT terminal emulation environment and the IBM 3270 terminal emulation environment. Refer to Chapter 1, Introduction to see if the DOS commands discussed in this chapter are included with your version of the network software.

For related information about keyboard mapping refer to Appendix A, Terminal Emulation and Character Set Tables and Appendix B, Keyboard Scan Codes. In addition, the Keymap application provides useful online help.

6.1 Before You Start Customizing Key Mappings

If you plan to customize your keyboard for terminal emulation, make sure that you

- Understand the default key mapping behavior.
- Copy the necessary translation tables and other files from the network software distribution media (many of the files are not installed automatically).
- Have the appropriate character code tables in front of you for reference.

The software provides a number of sample VT key map files that you may be able to edit and use. Table 6-1 provides a list of the sample keymap files included with the PC/TCP software.

This sample file	Contains this
ANSI-SYS.KYB	Mappings for non-character keys (such as , PageUp, and Alt). When you use these mappings in a Telnet session, a key's scan code is sent to the remote host.
ANSI.KYB	Mappings for non-character keys (such as , PageUp, and Alt). When you use these mappings in a Telnet session, a key's ANSI escape sequence is sent to the remote host.
ESC.KYB	Mappings that swap the function of the Esc and ~ keys.
FINNISH.KYB	Finnish/Swedish key mappings.
GERMAN.KYB	German key mappings for the MFII keyboard.
GR-ANSI.KYB	German key mappings for the 8-bit ANSI character set.
GR-ASCII.KYB	German key mappings for the 8-bit ASCII and IBM Extended Character Set.
ITALIAN.KYB	Italian key mappings
SWISS-FR.KYB	Swiss French key mappings.
SWISS-GR.KYB	Swiss German key mappings.
SWISS.KYB	Swiss key mappings.
TOSHIBA.KYB	German key mappings for the Toshiba laptop T3200 keyboard.
UK.KYB	British key mappings.

If you decide to use any of these files, make sure that they are installed on your system. If they

did not install automatically into your PCTCP directory, you must copy them from the network ssoftware distribution media.

6.2 Understanding the DEC VT Emulation Environment

When you use **rloginvt** or **tn** to log in to a remote host running UNIX or VMS, you are using a DEC VT terminal emulator. Characters that you type travel to and from the remote host in the form of codes from the DEC multinational character set.

Figure 6-1 shows the path of a keystroke through the terminal emulator to the remote host and back to your PC screen.

Figure 6-1 VT Key Mapping Environment

The figure illustrates these steps:

1. When you press a key, it generates a unique value called a “scan code.”
2. The network software uses a key map table to translate the scan code to either a character in the DEC multinational character set or a VT escape sequence (the escape sequence emulates the action of a function key on a real VT terminal). You can modify the default mappings in this table by creating a custom key map file.
3. When the remote host sends a character to your PC, the VT emulator uses an internal table to translate the DEC character code to a code in the IBM PC ASCII character set.

   The translation of DEC characters to PC ASCII characters varies depending on the code page installed on your PC (the VT emulator includes support for code pages 437 and 850; the IBM PC emulator includes support for any single-byte code page). When the emulator receives a DEC character code, it searches the appropriate code page for the character’s ASCII code. If the DEC character does not have a counterpart in the code page on your PC, the emulator substitutes another character for display. If you plan to use many multilingual characters, code page 850 is best.

6.3 Understanding the 3270 Emulation Environment

When you use **tn** to log in to a remote IBM host, you are using a 3270 terminal emulator. The 3270 key mapping environment is similar to the VT environment, except that, in addition to translating from key scan codes to ASCII character codes, the emulator must translate from ASCII to EBCDIC before sending a character code to the remote system. Likewise, when the remote system sends a character, the 3270 emulator translates it from EBCDIC to ASCII.

Figure 6-2 illustrates the path of a keystroke through the terminal emulator to the remote IBM host and back to your PC screen.

Figure 6-2 3270 Key Mapping Environment

The figure illustrates these steps:

1. When you press a key, it generates a unique value called a “scan code.”
2. The network software uses a key map table to translate the scan code to either an IBM 3270 function or a character in the standard ASCII character set. You can modify the default mappings in this table by creating a custom key map file.
3. If the scan code maps to a character, another table translates the character code from ASCII to EBCDIC before sending it to the remote host. The default table contains mappings for the standard PC ASCII character set (decimal codes 0 through 127). You can edit a copy of this table to customize the mappings, or to create new mappings for special EBCDIC characters.
4. When the 3270 emulator receives a character code from the remote system, it first translates the EBCDIC code to a PC ASCII code, using the EBCDIC-to-ASCII translation table. This is the other half of the same table that translates characters on the sending side. This table is modifiable; if you add a new character mapping to the ASCII-to-EBCDIC portion of the table, you should edit the EBCDIC-to-ASCII portion to make a parallel change to the receiving side. Otherwise, the emulator will not be able to interpret the character for display.

6.4 Customizing VT and IBM PC Key Mappings

This section describes the process that you use to customize VT and IBM PC key mappings.

1. At the DOS prompt, type **`keymap`**

   The Keymap application allows you to

   – Create new key mappings.
   – Save your mappings to a file.

2. Configure the pathname of the alternative key map file in the `vt220-keymap=` parameter in the `[pctcp vt]` section of your PCTCP.INI file.

6.5 Customizing 3270 Key Mappings

This section describes the process that you use to customize 3270 key mappings.

1. At the DOS prompt, type **`keymap`**

   The Keymap application allows you to

   – Create new key mappings.
   – Save your mappings to a file.

2. If you want to map a key to an EBCDIC character that is not part of the standard ASCII character set, you need to edit the ASCII/EBCDIC translation table.

   For details, see section 6.5.1, Mapping a Key to a Special or Multilingual EBCDIC Character.

3. Configure the pathname of the alternative key map file in the `3270-keymap=` parameter in the `[pctcp 3270]` section of your PCTCP.INI file. If you edited a copy of the ASCII/EBCDIC translation table, configure its pathname in the `ascii/ebcdic=` parameter.

6.5.1 Mapping a Key to a Special or Multilingual EBCDIC Character

To map a key to an EBCDIC character that is not part of the standard ASCII character set, you need to customize the ASCII/EBCDIC translation table.

To customize the ASCII/EBCDIC translation table

1. Copy one of the following translation files from the network software distribution media:

File	Contents
INTLDOS.TBL	A sample DOS translation file using the ASCII character set.
INTLWIN.TBL	A sample Windows translation file using the Windows font FTPVTVGA.
XLATE327.TBL	Default ASCII-to-EBCDIC and EBCDIC-to-ASCII mappings that the 3270 emulator uses.

2. Determine the EBCDIC code page in use on the remote IBM host, and find out the hexadecimal code for the EBCDIC character that you want to send.

3. Use any binary editor to open the translation file.

   The table has two parts: the EBCDIC-to-ASCII portion occupies the first 256 bytes (100 hexadecimal bytes), and the ASCII-to-EBCDIC portion occupies the next 160 bytes.

4. Type **`-d 200`** to go to the ASCII-to-EBCDIC portion of the file.

   The following example shows how the debug editor displays the ASCII-to-EBCDIC portion of the table in the file XLATE327.TBL.The ASCII-to-EBCDIC portion starts at an offset of 200 (the sum of a 100 hexadecimal offset required by debug plus 100 hexadecimal bytes occupied by the EBCDIC-to-ASCII part of the table).

   Thus, the **-d 200** command causes debug to display the contents of the file starting with the portion that you want: byte 200. The second **-d** command displays subsequent rows (the remainder of the table).

```
C:\PCTCP> debug xlate327.tbl

-d 200


397C:0200 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00 ................
397C:0210 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00 ................
397C:0220 40 5A 7F 7B 5B 6C 50 7D-4D 5D 5C 4E 6B 60 4B 61 @Z.{[lP}M]\Nk`Ka
397C:0230 F0 F1 F2 F3 F4 F5 F6 F7-F8 F9 7A 5E 4C 7E 6E 6F ..........z^L~no
397C:0240 7C C1 C2 C3 C4 C5 C6 C7-C8 C9 D1 D2 D3 D4 D5 D6 |................
397C:0250 D7 D8 D9 E2 E3 E4 E5 E6-E7 E8 E9 AD E0 BD 5F 6D ..............._m
397C:0260 79 81 82 83 84 85 86 87-88 89 91 92 93 94 95 96 y...............
397C:0270 97 98 99 A2 A3 A4 A5 A6-A7 A8 A9 C0 4F D0 A1 00 ............O...
```

```
-d

397C:0280 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00 ................
397C:0290 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00 ................
```

In the far left column, debug displays the address of the beginning of each row in the table. The remaining columns display the contents of the table. If you picture those columns as having hexadecimal labels 0 through F, you will notice that the values are arranged in rows and columns based on the hexadecimal code of the ASCII character being mapped. The last two rows of the table (positions 80 through 9F) contain 0x00 values; they are empty rows that you can use for mappings of multilingual and special characters that are not part of the standard ASCII character set.

5. In one of the empty positions of the ASCII-to-EBCDIC table, place the EBCDIC code for the character that you want to send.

   For example, suppose you want to send an é character when you press the 2 key. The code page in use on the IBM system is 037, so you look up é in code page 037 and find that its EBCDIC value is 0x51. You do not want to just replace the mapping for ASCII 2 (in position 32) with the EBCDIC value 0x51, because you still want to be able to send a 2 when you press Shift+2. So create a new mapping for the é in the first open space (position 80) in the table.

   The following sample debug session illustrates this procedure:

```
C:\PCTCP> debug xlate327.tbl

-d 200

397C:0200 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00 ................
397C:0210 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00 ................
397C:0220 40 5A 7F 7B 5B 6C 50 7D-4D 5D 5C 4E 6B 60 4B 61 @Z.{[lP}M]\Nk`Ka
397C:0230 F0 F1 F2 F3 F4 F5 F6 F7-F8 F9 7A 5E 4C 7E 6E 6F ..........z^L~no
397C:0240 7C C1 C2 C3 C4 C5 C6 C7-C8 C9 D1 D2 D3 D4 D5 D6 |................
397C:0250 D7 D8 D9 E2 E3 E4 E5 E6-E7 E8 E9 AD E0 BD 5F 6D ..............._m
397C:0260 79 81 82 83 84 85 86 87-88 89 91 92 93 94 95 96 y...............
397C:0270 97 98 99 A2 A3 A4 A5 A6-A7 A8 A9 C0 4F D0 A1 00 ............O...

-d

397C:0280 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00 ................
397C:0290 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00 ................

-e 280 51

-w
```

```
-q

C:\PCTCP>
```

where

- The **-e** command inserts the hexadecimal value 51 in position 80.
- The **-w** command writes the changes to the file.
- The **-q** command exits from debug.

The ninth row of the table now looks like this:

```
397C:0280 51 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00 Q...............
```

The top two rows of the ASCII-to-EBCDIC translation table are occupied by unprintable control characters. If you fill the bottom two rows of the table with new mappings, you can overwrite some positions in the top two rows, with these exceptions:

Code	Description	Code	Description
0x03	end of text	0x0C	form feed
0x08	backspace	0x0D	carriage return
0x09	horizontal tab	0x14	device control 4
0x0A	line feed	0x1B	escape

6. In the EBCDIC-to-ASCII portion of the table, create a parallel mapping for the new character that you just mapped in the sending direction.

   This mapping allows the emulator to interpret the special character for display when the remote IBM host echoes it back.

   To define the EBCDIC-to-ASCII mapping of a character, first look up its ASCII code in code page 437 (the 3270 emulator supports only code page 437). For example, the ASCII value of the é character in code page 437 is 0x82.

   If you cannot find a match in code page 437 for the EBCDIC character that you defined in the sending direction, choose a substitute character to which to map it for display.

7. Go to the top of the translation table (the EBCDIC-to-ASCII portion). This portion is formatted in the same way as its counterpart, except that in this table, you look up a character by its EBCDIC code rather than by its ASCII code.

   The following sample debug output shows the default contents of the EBCDIC-to-ASCII

translation table (debug adds an offset of 100 hexadecimal bytes to the character codes):

```
C:\PCTCP> debug xlate327.tbl

-d

397C:0100 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
397C:0110 20 20 20 20 20 20 20 20-20 20 20 20 2A 20 3B 20 * ;
397C:0120 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
397C:0130 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
397C:0140 20 20 20 20 20 20 20 20-20 20 9B 2E 3C 28 2B 7C ..<<+|
397C:0150 26 20 20 20 20 20 20 20-20 20 21 24 2A 29 3B 5E & !$*>;^
397C:0160 2D 2F 20 20 20 20 20 20-20 20 7C 2C 25 5F 3E 3F -/|,%_>?
397C:0170 20 5E 20 20 20 20 20 20-20 60 3A 23 40 27 3D 22 ^ `:#="

-d

397C:0180 20 61 62 63 64 65 66 67-68 69 20 20 20 20 20 20 abcdefghi
397C:0190 20 6A 6B 6C 6D 6E 6F 70-71 72 20 20 20 20 20 20 jklmnopqr
397C:01A0 20 7E 73 74 75 76 77 78-79 7A 20 20 20 5B 20 20 ~stuvwxyz [
397C:01B0 20 20 20 20 20 20 20 20-20 20 20 20 20 5D 20 20 ]
397C:01C0 7B 41 42 43 44 45 46 47-48 49 20 20 20 20 20 20 {ABCDEFGHI
397C:01D0 7D 4A 4B 4C 4D 4E 4F 50-51 52 20 20 20 20 20 20 }JKLMNOPQR
397C:01E0 5C 20 53 54 55 56 57 58-59 5A 20 20 20 20 20 20 \ STUVWXYZ
397C:01F0 30 31 32 33 34 35 36 37-38 39 20 20 20 20 20 20 0123456789
```

The EBCDIC-to-ASCII table has many positions that are filled with the value 0x20 (the ASCII code for a space). These correspond to the hexadecimal codes of multilingual and special characters in the EBCDIC character set, which the network software does not map by default. You can use these positions for EBCDIC-to-ASCII mappings for special characters that you have already mapped in the sending direction.

8. In the location corresponding to the EBCDIC code of the character that you defined in the send direction, place the ASCII code for that character, or a substitute character, if necessary.

   For example, to map the EBCDIC é character (hexadecimal value 0x51) to its corresponding ASCII value from code page 437, place an 82 in position 51 of the table.

   The following sample debug session illustrates this:

```
C:\PCTCP> debug xlate327.tbl

-d

397C:0100 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
397C:0110 20 20 20 20 20 20 20 20-20 20 20 20 2A 20 3B 20 * ;
397C:0120 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
397C:0130 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
397C:0140 20 20 20 20 20 20 20 20-20 20 9B 2E 3C 28 2B 7C ..<<+|
397C:0150 26 20 20 20 20 20 20 20-20 20 21 24 SA 29 3B 5E & !$*>;^
397C:0160 2D 2F 20 20 20 20 20 20-20 20 7C 2C 25 5F 3E 3F -/|,%_>?
```

```
397C:0170 20 5E 20 20 20 20 20 20-20 60 3A 23 40 27 3D 22 ^ `:#='"

-e 151 82

-w

-q

C:\PCTCP>
```

The following describes each of the sample commands and the resulting output:

- The **-d** command displays the beginning of the table to your screen.
- The **-e** command places the value 82 (hexadecimal code for an ASCII é) in position 51 of the table (100 hexadecimal bytes are added for the debug offset).
- The **-w** command writes your changes to the file.
- The **-q** command exits from debug.

The sixth row of the table now looks like this:

```
397C:0150 26 82 20 20 20 20 20 20-20 20 21 24 SA 29 3B 5E & !$*>;^
```

9. Create or open your custom key map file, and insert an entry that records the location of the ASCII-to-EBCDIC mapping for the key that you are redefining. For the key map value, supply the address in the ASCII-to-EBCDIC translation table of the new mapping that you have created (do not include offsets).

   For example, to complete the redefinition of the 2 key from the previous steps, type the following line in the key map file:

   ```
   0, 0x03, 0x80
   ```

   where

   - The `0` indicates that the definition applies when the shift state is normal.
   - The `0x03` is the scan code for the 2 key.
   - The `0x80` is the location in the ASCII-to-EBCDIC translation table where you inserted the EBCDIC code for the é character.

6.6 Customizing Display Mappings

A display map table determines how characters that are sent from the remote host appear on your screen. You can customize DEC-to-PC ASCII mappings by editing a default copy of the display map table. Since the display map table applies to VT, IBM 3270, and IBM PC emulation, changes that you make to the display map table affect all emulators.

For more information about customizing display mappings, refer to the following sources:

- Anonymous FTP server ftp.ftp.com
- Technical Support Bulletin Board System at (508) 659-6240

6.7 Troubleshooting Keyboard Mapping

This section provides a solution to a situation that you might encounter when you remap your keyboard.

You receive the following error message:

`Line` *`n`* `of keyboard remapping file is longer than` *`x`* `bytes. Rest of line bypassed.`

Rewrite line *n* of your keyboard remapping file so that it contains *x* bytes or fewer.

You receive the following message:

`Error reading keyboard remapping file` *`filename`*`.`

If your text format key map file contains any of the hexadecimal codes 00 through 07 inclusive, remove them.

Chapter 11
Configuring a PC as a DOS LPD Server

You can set up your PC as a dedicated LPD (Line Printer Daemon) server to let remote hosts send print jobs to configured printers attached to the PC. The LPD server responds to requests from remote TCP/IP applications that require an LPD server, such as the **lpr**, **lpq**, and **lprm** commands. In brief, **lpr** sends print jobs to specific printers attached to specific servers, **lpq** displays the server's print queue, and **lprm** deletes jobs from the queue.

The LPD server

- Sends files to printers attached directly to the host running the lpd program.
- Supports multiple printers attached to the host, using standard DOS devices such as PRN and COM1.
- Spools and prints jobs in the order received.
- Allows you to access and manage print jobs and print queues using console commands.

This chapter describes how to configure and use the LPD server.

For information about using LPD services from the client side, refer to Chapter 7, Printing to a Network Printer.

11.1 Before You Start Configuring Your System as an LPD Server

FTP assumes that you are familiar with the printers that you use with the LPD server, and with the documentation for those printers.

Before you set up your PC as an LPD server, ensure that

- You are familiar with the character sequences (printer commands) that let you control fonts and modes for your printer.
- You do not configure the LPD server on a port used by a Windows print redirection program. If both programs are configured on the same port, you cannot print simultaneously to the LPD server and from a Windows application.

11.2 Configuring the LPD Server — Procedure Overview

Configuring the LPD server software consists of the following activities:

1. Adding LPD and printer sections to the PCTCP.INI configuration file.
2. Customizing printer sections to control printer output.
3. Altering or creating an authorization file. This step is optional.

11.3 Adding LPD Sections to the Configuration File

The LPD server requires configuration entries in the PCTCP.INI file. If the server cannot find the required information, it generates an error message on the monitor attached to the server.

You must add two types of configuration sections to the PCTCP.INI file for the LPD server:

- The LPD control section
- At least one printer control section

11.3.1 Adding the LPD Control Section

The general form of the LPD control section required by the lpd program is

```
[pctcp lpd]
printers= printer1 printer2 .. printerN
auth-file= pathname\filename
```

The header `[pctcp lpd]` identifies the configuration file section for LPD. Following the header, the `printers=` parameter identifies the names of the printers that you want to connect to the server.

Note the following requirements for entries in the `[pctcp lpd]` control section:

- You must list at least one printer.
- The `printers=` parameter cannot be longer than 128 characters.
- For each printer listed in the `printers=` parameter, you must have a corresponding printer control section for that printer in the PCTCP.INI file.
- The optional `auth-file=` parameter specifies a host authorization file that limits access to LPD. See section 11.5, Restricting Access to the LPD Server for more information.

11.3.2 Adding the Printer Control Section

Printer control sections provide specific information about printers connected to the LPD server. There must be at least one printer control section for each printer listed in the `printers=` parameter of the `[pctcp lpd]` section. Each printer control section must contain the following information:

```
[pctcp lpd lpd_printer_name]
dev= device
dir= drive:\pathname
```

The *`device`* specified can be one of the standard DOS devices: LPT1, LPT2, COM1, COM2, or COM3. The device PRN may also be used, although PRN is usually set by DOS to refer to LPT1. Do not configure the LPD server on a port used by a Windows print redirection program. If both are configured on the same port, you may lose print jobs on the LPD server.

To use multiple printer definitions for a printer

Set the `dev=` parameter to the same port in each `[pctcp lpd lpd_printer_name]` section for that printer, and list each *`of`* these sections in the `printer=` parameter of the `[pctcp lpd]` section. See section 11.6, Sample LPD Configuration Sections for an example.

Note: If you use multiple printer definitions to send print files to a printer connected to LPT1, you must set each `dev=` parameter to either LPT1 or PRN. The LPD server treats LPT1 and PRN as separate printer ports.

To send all output to a file instead of a printer port

Set the `dev=` parameter to a valid DOS path- and filename, instead of a printer port name. This setting redirects all characters to the specified file.

The `DIR=` *`drive:\pathname\filename`* parameter sets the directory in which the server spools files for this particular printer. If this directory does not exist when you load LPD, the server creates the directory.

11.4 Customizing the Printer Control Section

You can control many printing functions and print a variety of file types by customizing the printer control sections in your PCTCP.INI file. The following sections specify optional entries that enable you to perform such functions as disabling form feeds or header (break) pages, logging events to a file, and printing ASCII and PostScript files.

The following example shows the settings that you can make for a printer in the PCTCP.INI file:

```
[pctcp lpd lpd_printer_name]
break=[on | off]
break-init= sequence
chars-to-print= n
dev= device
dir= drive:\pathname
doscalls=yes
expand-tabs=yes
file-init= sequence
file-end= sequence
formfeed=[on | off]
log-file= drive:\pathname\filename
postscript-hdr-file= drive:\pathname\filename
printing=[on | off]
printer-init= sequence
spooling=[on | off]
```

11.4.1 Controlling Printer Output

The following table identifies general printer operations that you can control by adding entries to a printer control section in the PCTCP.INI file. See section 11.6, Sample LPD Configuration Sections for examples.

If you want to	**Enter this in** `[pctcp lpd lpd_printer_name]`	**Default**
Enable or disable header (break) pages	`break=[on|off]`	`on`
Enable or disable form feeds	`formfeed=[on|off]`	`on`
Enable or disable printer spooling at server start-up	`spooling=[on|off]`	`on`
Enable or disable printing at server start-up	`printing=[on|off]`	`on`
Expand tab characters in print files (to eight spaces)	`expand-tabs=yes`	none
Log events to a file	`log-file=` *`drive:\pathname\filename`*	none
Set the number of characters sent to a printer	`chars-to-print=` *`n`*	`500`
Use DOS write calls to communicate with the printer port	`doscalls=yes`	none

11.4.2 Using Printer Control (Escape) Sequences to Control Printer Output

You can control the output of printers through the use of the printer control sequences (also called "escape sequences") defined by a printer manufacturer's command language. These printer control sequences enable font types and sizes, boldface, underlining, page length, line spacing, tabs, and other printing characteristics.

Note: Refer to your printer manufacturer's documentation for a list of valid printer control sequences and formats. The sequences that you specify must use valid printer command language control characters, including the escape character (if required).

The LPD server uses these printer control sequences when

- The LPD server initializes a printer.
- A print job requests a header page.
- A remote user sends a print job identified as a standard LPD file type.

The LPD server uses the following `-init` and `-end` entries:

`break-init=` *`sequence`*

`filetype``-end=` *`sequence`*

`filetype``-init=` *`sequence`*

`printer-init=` *`sequence`*

The following sections identify printer control sequences that you can send to the printers connected to your LPD server. Add the parameters containing these sequences to your printer control sections in the PCTCP.INI file. See section 11.6, Sample LPD Configuration Sections for examples.

To set default printer font and mode using a printer initialization sequence

Use `printer-init=` *`sequence`* to set a default font, type size, or a general print mode (such as Portrait or Landscape mode).

The initialization sequence usually contains a reset character to ensure that the printer always starts in a predictable state. The LPD server sends the `printer-init=` control sequence when you issue the **lpd** command to start the LPD server.

To format a header (break) page

Use `break-init=` *`sequence`* to change the font and type size of header page information.

The header page lists the print job name, originating host, username, and time of printing.

To control printing of standard LPD file types

Use *filetype*-init= *sequence and filetype*-end =*sequence* to control printing of standard LPD file types.

An end user can then print the desired file type by specifying the appropriate argument to the LPD **lpr** command (or equivalent BSD UNIX **lpr** command). These arguments cause the LPD server to print using the specified file type sequence. See the documentation for your client **lpr** command for more details.

The LPD server supports the file types and sequences in the following table:

To print this file type	**Enter this in the** `[pctcp lpd` *lpd_printer_name*`]` **section of PCTCP.INI file**	**And use this command**
ASCII (generic) text files	`text-(init|end)`	**lpr**
binary files	`verbatim-(init|end)`	**lpr -v**
cifplot files	`cifplot-(init|end)`	**lpr -c**
ditroff files	`ditroff-(init|end)`	**lpr -n**
troff files	`troff-(init|end)`	**lpr -t**
tex (DVI format) data files	`dvi-(init|end)`	**lpr -d**
Unprocessed files	`verbatim-(init|end)`	**lpr -v**

Consider the following when using file types and sequences:

- You do not need to enclose a sequence in quotation marks.
- You can use spaces in a sequence.

Refer to your printer manufacturer's documentation for a list of valid printer control sequences and formats. The sequences that you specify must use valid printer command language control characters, including the escape character (if required).

When entering escape and control sequences in your PCTCP.INI file, use an editor that allows you to enter the actual sequence in the file (not characters that represent the sequence).

11.4.3 Using Files to Specify Printer Control Sequences

You can also use files to send required printer control sequences to printers, provided that you specify those files in printer control sequence entries. This feature is useful if you need to send a printer control sequence containing an end-of-file or end-of-line character.

When you specify a filename in a `filetype-(init|end)` parameter, the LPD server sends the entire contents of the specified file to the printer as the printer control sequence. To use this feature, set the `printer-init=` , `break-init=` or `filetype-(init|end)=` parameter to *`FILE:DRIVE:\PATHNAME\FILENAME,`* for example:

```
cifplot-init=file:c:\lpddir\cif.ini
```

11.4.4 Using Applications to Specify Printer Control Sequences

You can use an application to embed printer control sequences in print jobs sent from that application. You can also use an application to format a print job and direct the application's printer output to a disk file, to be printed without further printer control input from the LPD server.

If you embed printer control sequences in application printer output, those control sequences may override or conflict with printer control sequences that the LPD server sends to the printer.

To prevent the LPD server from interfering with application printer control

1. Set the `verbatim-(init|end)=` parameter in your printer's printer control section to contain as few printer control sequences as possible, except for a form-feed or page-clear command.

2. Send printer output to the LPD server using the verbatim printer option for your client **lpr** command.

11.4.5 Controlling PostScript Printer Output

You can use the LPD server to print PostScript output on printers that support the PostScript printer control environment.

When using PostScript printers, use the LPD server to precede your print jobs with a PostScript header page. You then specify the path and filename of a PostScript command file for the `postscript-hdr-file=` parameter in a printer control section of the PCTCP.INI file. This PostScript command file contains PostScript command variables that define a PostScript header page.

You can use the PS.HDR file supplied with LPD, or define your own PostScript command file. See the documentation that accompanies your PostScript printer for more details about PostScript command files.

To print a file as a PostScript header page

Add an entry in the following form to the printer control section in the PCTCP.INI file:

```
postscript-hdr-file= drive:\pathname\filename
```

The following example shows this parameter in an LPD printer control section for a PostScript printer:

```
[pctcp ps]
postscript-hdr-file=c:\etc\my_ps.hdr
```

Note these header page requirements for a PostScript printer connected to the LPD server:

- The PostScript command file used to generate a PostScript header page must specify the same variables as the sample PS.HDR file supplied with the LPD server.
- Printing a standard ASCII text header page on a PostScript printer may stop the printer. If you do not use the PostScript header file supplied with the LPD server (or an equivalent PostScript command file) to generate a header page for a PostScript printer, you should disable the header function for that printer.

11.5 Restricting Access to the LPD Server

You can restrict user access to the LPD server by creating a host authorization file. The authorization file, usually called \ETC\HOSTS.LPD, contains the hostnames or IP addresses for those users that you want to supply with print services. The LPD server regulates access to print services according to hostnames, not user IDs. If an authorization file is not specified for the `auth-file=` parameter in the configuration file, the LPD server grants print service access to all hosts.

To restrict access to the LPD server

1. Create the directory \ETC, if it does not already exist.

   Use the DOS **mkdir** command – for example,

   ```
   C:\>mkdir \etc
   ```

2. Create the file HOSTS.LPD in the \ETC directory.

   You configure the authentication file by placing one hostname per line in the file. Lines that begin with a # character are comments.

   Note: If you put an asterisk (*) in the first position of any line of this authentication file, the LPD server does not use the authentication file and allows access to all hosts.

   The following is a sample \ETC\HOSTS.LPD file:

   ```
   # Sample HOSTS.LPD file
   wesson.ftp.com
   ozymandius.superfine.org
   dbowie.rockroll.mil
   bumper.hypothetical.edu
   durandal.hypothetical.edu
   ```

When the LPD server starts, it tries to validate each host listed in the authentication file by accessing a network address for those hosts through the default name resolution techniques. If the server cannot validate a host listed in the authentication file, it displays an error message at the LPD console.

11.6 Sample LPD Configuration Sections

The following example shows how you can configure the LPD server to use different printer definitions. This example lists the parameters in the LPD control and printer control sections of the PCTCP.INI configuration file. A semicolon (;) begins comment lines.

Note: When entering escape or control sequences in `[pctcp lpd lpd_printer_name]` sections of the PCTCP.INI file, you must embed the actual escape or control sequence, not the characters that represent that sequence.

For example, in the following sample file the sequence Escape+E is shown as `^[E`. To add the Escape+E sequence to your file, use the appropriate commands for your editor that embed an escape sequence; *do not* enter the characters ^[E.

```
;LPD Configuration Example
;^[ denotes the ASCII escape character; for example, Escape-E is ^[E

[pctcp lpd]
printers=lp little big file ps
auth-file=d:\etc\our-hosts

[pctcp LPD lp]
; The device to print on: PRN, LPT1, LPT2, COM1, COM2, or filename
dev=PRN
; Directory where files are kept for the printer
dir=d:\printers\lp
; Defines that LPD will use DOS calls to send characters to printer
doscalls=yes
; Do NOT print header pages on this printer
break=off
; Expand tab characters to spaces for printing text files
expand-tabs=yes
; Send a file containing printer control sequences to the printer when LPD starts up
printer-init=c:\etc\lp_init.txt

[pctcp LPD little]
dev=COM2
dir=d:\printers\little
expand-tabs=yes
; Printer initialization code, sent at start up
printer-init=^[E
; Print the header page in Times Roman 8.5 point font
break-init=^[(8u ^[(s8.5v ^[(s5T
; Print text files in Times Roman 8.5 point font
text-init=^[(8u ^[(s8.5v ^[(s5T

[pctcp LPD big]
dev=COM2
dir=\printers\big
```

```
printer-init=^[E
; Print the header page in Times Roman 8.5 point font
break-init=^[(8u ^[(s8.5v ^[(s5T
; Print text files in Times Roman 10 point font with altered margins
text-init=^[(8u ^[(s10v ^[(s5T ^[&110E ^[&155E

[pctcp LPD file]
; Send printer output to a file instead of the printer
dev=C:\TMP\PRINTER.TXT
dir=d:\printers\file
expand-tabs=yes
; Start up with spooling off
spooling=off

[pctcp LPD ps]
dev=COM1
dir=d:\printers\ps
; Do not send form feed after printing files
formfeed=off
verbatim-init=^[D
verbatim-end=^[D
; Use this PostScript format page as the header page for this printer
postscript-hdr-file=c:\etc\ps.hdr
; Log events for this printer to a log file
log-file=d:\printer\ps\log-file
```

The following explains the printer control sections in the sample PCTCP.INI configuration file:

`[pctcp lpd]` Lists the names of printers configured for use with the LPD server, and the name and directory location of a hosts authorization file.

`[pctcp LPD lp]` Prints all files sent to it according to the printer control sequences contained in the file C:\ETC\LP_INIT.TXT, with no header page and using the DOS write calls for the printer port.

`[pctcp LPD little]`
Prints text files in Times Roman 8.5 point type on standard 8.5 x 11 inch paper.

`[pctcp LPD big]` Prints text files that contain no formatting information in Times Roman, 10 point type on standard paper with top and bottom margins wider than the default.

Note: Both `little` and `big` use the same physical printer, connected to the COM2 port, but are configured as two virtual printers with different styles of printing.

`[pctcp LPD file]` Prints all files sent to it into the file C:\TMP\PRINTER.TXT, rather than to a printer port. You must use the **>** console command to enable spooling to this file.

`[pctcp LPD ps]` Prints files sent to it on a PostScript printer connected to the COM1 port,

using the PostScript commands contained in the file C:\ETC\PS.HDR to format the header page, generating no blank page following print jobs, and logging events to a unique log file called D:\PRINTER\PS\LOG-FILE.

Use a printer definition such as this to control PostScript printers from the lpd program. For more information, see section 11.4.1, Controlling Printer Output.

11.7 Managing LPD Services from the LPD Server

This section defines procedures for controlling and effectively managing an LPD server from a server console.

11.7.1 Starting and Stopping the LPD Server

When LPD starts, the server verifies

- The list of available printers.
- The spooling directories.
- The print devices.

After the server verifies these settings, it sends initialization information to the printers. LPD also verifies that hosts that submit print requests are listed in the hosts authorization file, if configured.

If a printer is offline or unable to print for any reason, the server console displays an error message. If any jobs remain in a queue when the LPD server stops, the job is placed in the queue and printed if possible.

To start the LPD server

At the DOS prompt, enter the **lpd** command.

If you start the LPD server in message mode (the default), the program displays information similar to the following message:

```
c:\>lpd

No host table, no restrictions on users

List of printers and printer status No host table, no restrictions on users

    List of printers and printer status
#   name    directory             spooling      printing      device
1   lp      C:\printers\lp        on            on            lpt1
2   hp      C:\printers\hp        on            on            com1

Type 'q' to abort; '?' for other commands.
```

For information on displaying more detailed information about printer and spooler queue status, see section 11.7.7, Displaying Verbose Console Messages.

To stop the LPD server

At the LPD console, enter the **q** command.

The monitor displays the following message:

```
Server aborting at user request.
C:\ >
```

11.7.2 Suppressing All Header Pages on a Printer

By default, the LPD server prints a header page before each print job and a form feed after each print job. If you do not need this feature, you can stop the server from generating header pages by

- Specifying the **-h** option with the **lpr** command line to suppress the header page for any specific print job sent to the LPD server.
- Suppressing all header pages on a printer by setting a `break=off` parameter in that printer's specific section in the configuration file. If the `break=off` parameter is not found in a printer control section, the LPD server defaults to printing a header page for each job received for that printer.

11.7.3 Deleting a Print Job in the Spooler Queue

You can delete a file waiting in the LPD server's spooler queue from either the client side or from the server console. With LPD, you can identify and remove print jobs (by job number) from specific printer queues at the LPD console.

You can also delete a print job in a spooler queue using client print programs. See Chapter 7, Printing to a Network Printer.

To delete a print job from the server console

1. From the LPD console, enter **r**

   The console displays the following response:

```
List of printers and printer status
#   name    directory             spooling      printing      device
1   lp      C:\printers\lp        on            on            lpt1
2   hp      C:\printers\hp        on            on            com2

Remove job from queue of which printer?:
```

2. After the prompt, enter the number of the printer on which you want to delete a job.

```
Remove job from queue of which printer?: 1
Currently printing job # 13 (no jobname), from user nelson@rodney.comp.com.

In queue:

Job #       user           host                        jobname
14          cwtc           bowl.comp.com               mayrpt.prn
15          baldyr         valki.hypothetical.edu      elbows.out
```

3. After the prompt, enter the number of the print job that you want to remove from the print queue.

```
Job number to remove (0 to abort job currently
printing, > 0 to delete queued job)? 15

Removing job 15 from queue for printer lp
```

Note: If you configure the LPD server to use only one printer, the LPD console does not query you for printer number, and goes directly to the list of jobs in the print queue, querying for the print job to delete.

11.7.4 Deleting the Current Print Job

You can only delete a job that is currently printing from the LPD server console; you cannot use the client **lprm** command to delete a currently printing job.

To stop the currently printing job

1. At the LPD console, enter **r**

   The console displays the following messages:

```
List of printers and printer status
#   name    directory              spooling      printing      device
1   lp      C:\printers\lp         on            on            lpt1
2   hp      C:\printers\hp         on            on            com2

Remove job from queue of which printer? :
```

2. After the prompt, enter the number of the printer on which you want to delete a job.

```
Remove job from queue of which printer? : 1
printing dfA228ne as a text file
Printer lp :

Currently printing job #210:[C:\work\sheet.prn, from user nelson@rodney.comp.com

In queue:
Job #       user            host                        jobname
211         cwtc            bowl.comp.com               market.prn
212         nelson          rodney.comp.com             mainbtry.rpt
213         baldyr          valki.hypothetical.edu      netnews.out

Job number to remove (0 to abort currently
printing, >0 to delete queued job)?
```

   Enter **0** as the job number to remove, and you see the following response:

```
Aborting current job 210; deleting associated data files.
Removing datafile[C:\printers\lp\dfA228ne.
Removing queue file[C:\printers\lp\210.qur.
```

11.7.5 Deleting All Print Jobs in a Spooler Queue

You can only delete all print jobs in the spooler queue of a specific printer from the LPD server console; you cannot delete all jobs in a queue from a client **lprm** command.

To delete all print jobs from the spooler queue for a specific printer

1. At the LPD console, enter `c`

   The console displays the following messages:

```
List of printers and printer status
#   name    directory              spooling      printing      device
1   lp      C:\printers\lp         on            on            lpt1
2   hp      C:\printers\hp         on            on            com2

Clean which printer's queue? :
```

2. Enter the number of the printer on which you want to delete all print jobs.

   The monitor displays the following message:

```
Cleaning queue for printer lp
```

11.7.6 Examining Statistics on the Server

You can display kernel network and debugging information for the machine running the LPD server. Your system administrator may find this information useful in diagnosing network connectivity problems. The following sections describe the available LPD server commands and options to display statistics.

To display kernel debugging statistics

Use the **d** command at the console to display kernel debugging statistics.

These statistics include information about the server such as

- The hardware address for the network interface card installed.
- The number of packets received and transmitted.
- The number and general types of transmission errors encountered.
- The number of interrupts received and (when using an Ethernet or token-ring network interface card) address resolution protocol (ARP) statistics.

The following is an example of a kernel debugging statistics display:

```
Debugging information for interface wd8003 Addr(6): 00 00 c0 a6 a4 25

interrupts: 15672 (0 receive, 0 transmit)
packets received: 14100, transmitted: 1547

receive errors: 0, unknown types: 12533
    runts: 0, aligns: 0, CRC: 0, parity: 0, overflow: 0
    too big: 0, out of buffers: 20, rcv timeout: 0, rcv reset: 0

transmit errors: 0
    collisions: 0, underflows: 0, timeouts: 0, resets: 0
    lost crs: 40, heartbeat failed: 1547

ARP statistics:
arps received: 198 (192 requests, 6 replies)
    bad: opcodes: 0, hardware type: 0, protocol type: 0
arps transmitted: 23 (6 requests, 17 replies)
13 large buffers; 12 free now; minimum of 0 free
55 small buffers; 1 free now; minimum of 3 free
```

For an explanation of these statistics, refer to the **inet** command in the *Command Reference*.

To display kernel network statistics

Use the **n** command at the console to display kernel network statistics.

These statistics include information about the transfer of various server kernel packet types, including the following:

- Transmission control protocol (TCP)
- Internet protocol (IP)
- User datagram protocol (UDP)
- Internet Control Message Protocol (ICMP)

The following is an example of a kernel network statistics display:

```
Interface  address        subnet mask    pkts in pkts out errs in errs out
ifcust     128.127.50.80  255.255.255.0  38965   10501    0       0

Kernel TCP stats: 10443 pkts sent, 10524 pkts rcvd, 0 bad checksums
    188611 bytes sent, 1560811 bytes rcvd, 80 rexmits, 53 duplicate pkts
    0 protocol errs, 0 resets, 0 timeouts

Kernel IP stats: 10452 pkts sent, 10528 pkts rcvd, 0 frags, 0 errs
    0 protocol errs, 0 timeouts, 0 bad checksums, 0 security errs

Kernel UDP stats: 0 pkts sent, 0 pkts rcvd, 0 no port listening
    0 bad checksums, 0 truncated rcvs

Kernel ICMP stats: 4 pkts sent (0 errs), 4 pkts rcvd (0 bad
    DestUn: 0 sent, 0 rcvd, ParamProb: 0 sent, 0 rcvd
    TimeEx: 0 sent, 0 rcvd, Redir: 0 rcvd, SourceQ: 0 rcvd
```

For an explanation of these statistics, refer to the **inet** command in the *Command Reference*.

To display the status of open connections

Use the **o** command from the LPD server console.

The following example shows the display for an LPD server with one open connection:

```
TCP stats for connection from 128.127.59.11.
    1437 pkts sent, 2539 pkts rcvd, 0 bad checksums, 0 protocol errors
    299 bytes sent, 1143682 bytes rcvd, 0 retransmits, 3 duplicate pkts
```

You can display the status of any currently open client connections to the LPD server. This information is useful in debugging connectivity problems, to ensure that clients can connect to the LPD server.

To display LPD server statistics

At the LPD console, use the **s** command.

The system displays statistics like the following:

```
Server stats:
    Server has received 44 jobs, completed 41 jobs successfully
    deleted 4 jobs, and printed 36 files
    0 connections currently open, 45 connections made
```

You can display the following general LPD server statistics:

- Jobs received
- Jobs completed
- Jobs deleted
- Files printed
- Connections made
- Connections currently open

11.7.7 Displaying Verbose Console Messages

The LPD server displays messages about connections made from client machines to the server, and about the status of print jobs. When you send a job to the LPD server running in default message mode, you see process messages on the console like the following examples:

```
Connection from 128.127.50.166 (belknap.ftp.com), port 606
Adding job #611 to queue for printer lp
Cleaning TCP connection to 128.127.50.166.

Removing datafile C:\printers\lp\dfA776be.
Removing queue file C:\printers\lp\611.qur.
```

You can display longer, more informative messages on the LPD server console by using either of the following methods:

- When loading the LPD server, specify the **-d** option on the command line. This starts up the LPD server in verbose message mode.
- When the LPD server is running, use the **D** command at the console to change the logging mode back and forth from verbose to default mode.

When you send a job to the LPD server running in verbose message mode, you see process messages on the console like the following:

```
Connection from 128.127.50.166, port 606
received command: 2lp
received "subcommand"; 3 694 dfA327belknap.ftp.com
Opening data file C:\printers\lp\dfA327be..
    file written successfully.
received "subcommand"; 2 127 dfA327be
Opening file C:\printers\lp\615.qur to write control file
    dfA327belknap.ftp.com.

    file written successfully.
Adding job # 615 to queue for printer lp
printing file dfA327be as a text file.
Cleaning TCP connection to 128.127.50.166.

Removing datafile C:\printers\lp\dfA327be.
Removing queue file C:\printers\lp\615.qur.
```

To load the LPD server in verbose message mode

Use the **lpd -d** command.

The monitor displays messages similar to the following:

```
c:\>lpd -d

Debugging logging on
```

```
No host table, no restrictions on users
List of printers in config file: lp

Printer lp

    uses printer on device lpt1, will expand tabs
    spooling directory is C:\printers\lp.
    looking for .qur files.. no .qur files found.
```

To change the LPD server message mode

From the LPD console, use the **D** console command to change the debugging logging message mode.

When the verbose messages are enabled, you see the following message:

```
debugging logging on
```

The next use of the **D** command changes the verbose messages off again, as follows:

```
debugging logging off
```

11.7.8 Maximizing Server Performance

The ability of LPD to handle print requests over the network depends upon the kernel configuration. For this reason, you should consider tuning the kernel to improve performance. You may want to increase

- The number TCP connections.
- The number of hosts that can connect to LPD at one time.
- The number of packet buffers.

11.8 Troubleshooting the LPD Server

This section lists messages that may appear when running LPD. The list includes the text of each message and potential solutions for the situation.

`Can't get a network descriptor`

The kernel has run out of network descriptors or the program is out of memory.

Increase the number of kernel connections or make more conventional memory available on the host.

`Can't resolve` *`hostname`* `host, cannot add to list of authorized hosts`

The server cannot verify a hostname listed in the authorization file (usually called \ETC\HOSTS.LPD). The program attempts to resolve hostnames first with a local host table if there is one configured, then with the domain name servers listed in the `[pctcp addresses]` section of the PCTCP.INI configuration file.

If the unresolved hostname is not listed in the local table, if there is no local host table, or if the domain name server(s) cannot be accessed, LPD cannot verify the hostname. If the LPD server cannot find a valid hostname in the authorization file, the server rejects print requests.

Verify that the hostname in the authorization file is accurate. Verify that name resolution is working on your network. You may have to ask your system administrator for this information.

`could not allocate space for file info`

The LPD server has run out of conventional memory at startup. The LPD server does not accept any print requests.

Make more conventional memory available on the server PC, and ensure that the kernel is running.

`Could not allocate space for queue element`

The LPD server has run out of conventional memory at startup. The LPD server does not accept any print requests.

Make more conventional memory available on the server PC, and ensure that the kernel is running.

`Could not open file` *`filename`*`.qur to delete data files`

The program is unable to delete a queued print job because it cannot find or open the corresponding control file for the job. Every spooled print job has one or more data files with filenames like FDFA754TY and a control file with a name like 1.QUR. This message indicates one of the following conditions:

– There is a problem with DOS.

– The spooling directory is corrupted.
– The control file no longer exists.

If the control file no longer exists, it is possible that the job is already deleted. You can see the names of any data files that are missing control files by exiting from the LPD server after all jobs for that particular printer have printed. Any remaining files in the printer's spooling directory have no control file and will not print. Delete these remaining print data files.

`Couldn't create printer info structure for physical printer on device` *`device`*`, deleting printer` *`printer-name`* `from list`

The program is out of memory. The specified printer is not available for service until you correct this situation.

Make more conventional memory available on the server PC. Also, ensure that the kernel is running.

`Couldn't create printer info structure for printer` *`printer-name`*`, deleting from list of printers`

The program is out of memory. The given printer is not available to the server until you correct this situation.

Make more conventional memory available on the server PC. The kernel must be running for LPD to work.

`Couldn't create queue for printer` *`printer-name`*`, deleting from list of printers`

The program cannot allocate enough memory to rebuild the queue during startup. The program is out of memory. The given printer is not available for service until you correct this situation.

Make more conventional memory available on the server PC. The kernel must be running.

`Couldn't create spooling directory` *`directory`* `for printer` *`printer`*`, deleting from list`

The program cannot create the directory given for the `dir=` configuration parameter.

Create the directory manually.

`Couldn't find config info: device` *`name`* `for printer` *`printer`*`, deleting from list`

There is no value given for the `dev=` parameter in the configuration file entry for the given printer.

See section 11.3.2, Adding the Printer Control Section for information about the `dev=` parameter.

`Couldn't find config info for printers`

The program cannot find either the file designated by the environment variable PCTCP, or it cannot find valid configuration information listed in a `[pctcp lpd]` or `[pctcp lpd lpd_printer_name]` configuration section.

Verify the setting of the PCTCP environment variable.

`Couldn't find config info: spooling directory name for printer printer-name, deleting from list of printers`

The program cannot find the printer control section for the given printer within the PCTCP.INI configuration file, or the entry given for `dir=` is missing.

Verify that the `[pctcp lpd]` or `[pctcp lpd lpd_printer_name]` sections of the PCTCP.INI configuration file are complete and correct.

`Couldn't open device to send init string for printer printer-name`

The DOS print device is malfunctioning.

See your DOS reference manual for more information about print devices.

`Couldn't open queue file.qur to get info.`

The program cannot find or open the control file for the job and thus cannot respond to remote requests for queue information. Every spooled print job has one or more data files with filenames like FDFA754TY and a control file with a name like 1.QUR. This message indicates one of the following conditions:

– There is a problem with DOS.
– The spooling directory is corrupt.
– The control file no longer exists.

If the control file no longer exists, the job may already be deleted. You can see the names of any data files that are missing control files by exiting from the LPD server after all jobs have printed. Any remaining files in the printer's spooling directory have no control file and will not print. Delete these print data files.

`Couldn't save printer name for printer printer, deleting from list of printers`

The program is out of memory. The given printer is not available for service until you correct this situation.

Make more conventional memory available on the server PC. The kernel must be running.

`Couldn't save spooling directory name for printer printer, deleting from list`

The program is out of memory. The given printer is not available for service until you correct this situation.

Make more conventional memory available on the server PC. The kernel must be running.

`Error no printers...`

The program attempted to set up all printers listed in the configuration file but failed to initialize any of the listed printers. The LPD server does not accept print jobs until you correct this situation. The server indicates the specific problem with each printer with one of the messages listed in this section.

Verify that the `[pctcp lpd]` section of the PCTCP.INI file lists configured printers in the `printers=` entry.

`Error on connection`

A remote host is requesting print services, but the server program cannot respond. There is a problem with the network connection to the remote host.

Use the **n** command to gather information about the network statistics that relate to this problem, and see your network administrator.

`Error: Overflow in output buffer for connection to host` *`hostname`*

The program cannot send complete responses to remote hosts requesting information or service because the program's output buffers have overflowed. This error will most likely occur in response to requests for information about jobs waiting in the queue.

Contact your network administrator.

`Error writing to file..`

The program is attempting to take data out of its network receiving buffers and print the data to a DOS file for spooling. The LPD server does not accept the print request, and informs you of this.

Wait for the kernel to reset, then send the job again.

`Lpd_open_file: Couldn't open` *`file`*`.qur can't make .qur file`

The program fails to create a control file for the print job. The server does not accept the print request and informs you of this. This error indicates either a problem with the spooling directory or with DOS.

Verify that your PC has sufficient disk space to create the file.

`Lpd_srv_init: Couldn't allocate lpd connection structure to listen for next connection`

This error comes from the underlying network connection, and indicates that LPD is not accepting more print requests. Use the LPD console commands **d** and **n** to gather information about the server's network connections. The kernel may have exhausted its available network connections for the moment. The kernel

attempts to remedy the problem by itself, allowing more print requests to succeed.

`No such printer`

A printer name, given in response to a keyboard command prompt at the server or by a remote user, is not currently valid.

You must list the printer name in the configuration file for LPD and the LPD server must be able to initialize it at start-up, or the LPD server does not support the printer name given by the remote user.

Verify the PCTCP.INI configuration file entries.

Chapter 8
Exchanging Mail and Network News

With mail and network news applications, you can send and receive electronic mail, bulletin board, and network news group messages over the network. You run the client versions of these programs to send and receive messages at your PC. A corresponding server runs on a remote host in your network, exchanging messages with your mail or news client. The server works with a mail or news forwarding program to transfer messages over your network.

Refer to Chapter 1, Introduction to see if your version of the network software includes the following programs discussed in this chapter: nntp, pcmail, pop2, pop3, smtp, and vmail.

This chapter describes

- The features available in the mail and network news programs.
- What you (and your system administrator) must do before you begin to use the programs.
- How to configure the nntp, pcmail, pop2, pop3, and vmail programs.
- How to read and respond to your messages with the vmail program.
- How to troubleshoot unexpected situations that you encounter while using the programs.

8.1 Features of the Mail and Network News Client Programs

This chapter discusses the following mail clients: Pcmail client and Post Office Protocol (POP) clients, versions 2 (POP2) and 3 (POP3). To use one or more of these clients, a corresponding mail server must be installed and configured by your system administrator on a remote host of your network. The Pcmail, POP2, or POP3 servers are not included.

Also discussed is the Network News Transfer Protocol (NNTP) client, which supports posting messages to network news groups and retrieving messages from an NNTP server running on a remote host. To use the NNTP client, a NNTP server must be installed and configured on your network. The NNTP server is not included in the network software.

Use the vmail program to read your NNTP, Pcmail, POP2, and POP3 messages.

Use the mail program to view your Simple Mail Transfer Protocol (SMTP) messages. To receive SMTP mail messages, first run the mail program's server, smtpsrv, at your PC before attempting to use the mail program. This chapter does not describe the mail and smtpsrv programs in detail. Refer to Anonymous FTP server ftp.ftp.com for more information.

Table 8-1 compares the features of the mail and network news programs.

Table 8-1 Mail and Network News Client Features

Supported Feature	NNTP	Pcmail	POP2	POP3	SMTP
You use the vmail program to read your messages.	Yes	Yes	Yes	Yes	No
You use the mail program to read your messages.	No	No	No	No	Yes
You can receive your messages in more than one mailbox.	Yes	Yes	Yes	No	No
You have access to bulletin boards.	No	Yes	No	— (1)	No
You have access to network news groups.	Yes	No	No	No	No
Your client can transmit messages to the server without relying on the SMTP protocol.	Yes (2)	Yes	No	— (1)	No
You can configure more than one PC on which to read your mail.	No	Yes	No	No	No
You must enter a password when the client connects with the server on the remote host.	No	Yes	Yes	Yes (3)	No

Notes to Table 8-1

1. Not all POP3 servers support this feature.
2. If you are replying to the sender of the network news message privately, or are forwarding the message to other users, the NNTP client uses SMTP to transmit the reply or forward the message.
3. If the POP3 server uses the .rhosts file, you are not required to enter a password.

8.2 Before You Start Using Mail and Network News Programs

You must make certain that your system administrator

- Creates a valid system user ID and password on a remote host that provides mail services for your network, such as acting as a mail gateway to other networks.
- Creates a valid system user ID and password on a remote host that runs the mail or network news servers that are compatible with your mail and network news clients, so that you can log in to the remote host. (Note that this host may be a different host from the one that acts as a mail gateway.)

  If you plan to use the Pcmail client, you do not have to have an account on the host; however, your system administrator must create an parameter for you in the Pcmail server on the host.
- Configures the mail servers compatible with your mail clients to handle the client's requests on the remote host.
- Sets up the printer to which you will print your messages.
- Makes certain that the remote host on which your mail server is running can send print requests over the network to the printer.

In addition, you should be familiar with the text editor that will be configured for use with the vmail program.

8.3 Configuring nntp, pcmail, pop, and vmail

Before you can send and retrieve mail and network news messages, you must configure the vmail program and whichever mail client programs that you plan to use.

To configure each of these programs, either use the configure program from the DOS command line, as follows:

```
C:\>config
```

–or–

Use the configure program from Windows by selecting the Configure icon in the WinApps Group window.

- or you may use the:

```
[pctcp client_name ]
```

where *client_name* is any of the following: `nntp`, `pcmail`, `pop2`, `pop3`, or `vmail`.

For example, the section that is used to configure the nntp program has the following section name:

```
[pctcp nntp]
```

To configure nntp, pcmail, pop2, and pop3

After you locate the client's section in the file, proceed with the following tasks:

1. For the `toplevel-directory=` parameter, type as its value the full pathname of the directory to store received messages. For example,

   ```
   toplevel-directory = c:\mail
   ```

   When you run your mail or news client for the first time, it creates a subdirectory for its messages under the top-level directory. For example, if you configure the `toplevel-directory=` parameter for pcmail and give it the setting `c:\mail`, the Pcmail client would create a subdirectory whose pathname is C:\MAIL\PCMAIL.

2. For the `server=` parameter, type as its value the hostname or IP address of the remote host that runs the mail or network news server used by your client. For example,

   ```
   server = 128.127.50.50
   ```

3. If you are configuring pop2, pop3, or nntp, find the `[pctcp lpr]` section. For the `printer=` parameter, specify the name of the default printer on which you want to print your pop2, pop3, or nntp messages. For example,

   ```
   printer = lp
   ```

If you are configuring pcmail as your mail client, find the `printer=` parameter in the `[pctcp vmail]` section. Type for its value the name of the default printer that you will use to print pcmail messages. The default printer is defined on the remote host on which the Pcmail server is running. (The system administrator may have defined the printer in the /etc/printcap file or its equivalent on the remote host.)

For example,

```
printer = lp_1
```

Note: The next steps are optional.

4. Find the `[pctcp addresses]` section of your PCTCP.INI file. For the `mail-relay=` parameter, type as its value the hostname or IP address of the remote host that is running your network's SMTP mail forwarding program. Your system administrator can provide you with this information. For example,

   ```
   mail-relay = 128.127.50.67
   ```

5. Find the `[pctcp smtp]` section of your PCTCP.INI file. For the `default-host=` parameter, type as its value the network hostname that will be appended by default to any recipients' usernames for which you do not specify a hostname. For example,

   ```
   default-host = xyz.com
   ```

   For example, if you set the value of the `default-host=` parameter to `xyz.com`, then send a message to username `chris`, the SMTP mail forwarding program by default appends the hostname, `xyz.com`, to the username, `chris`, so that the actual recipient name becomes `chris@xyz.com`. Note that you can override the default host address by specifying a different address for a recipient when you compose a message.

To configure vmail

1. Find the section in your PCTCP.INI file named `[pctcp vmail]` . For the `client-section=` parameter, type the name of the mail client that you are using, such as POP3. For example,

   ```
   client-section = pop3
   ```

   If you do not specify a setting for the `client-section=` parameter, the default is `pcmail`. You can override this parameter at the prompt with the **vmail -c** command option.

2. For the `editor=` parameter, type the name of the executable file for the editor that you use to compose messages. Type the full pathname, followed by the `%s` variable to represent a file name. For example,

   ```
   editor= c:\e.exe %s
   ```

   Note: The next steps are optional.

3. Find the `[pctcp general]` section. For the `full-name=` parameter, type your full name as you want it to appear in the headers of mail messages. This parameter identifies the sender of mail messages from the PC. For example,

   ```
   full-name = Chris Smith
   ```

   ***Caution*:** Other programs rely on parameters in the `[pctcp general]` section, and will be affected by any changes that you make.

4. Type the domain name of your PC for the `domain=` parameter. For example, if the PC's name is first.xyz.com, type **`xyz.com`** for the domain name.

   ```
   domain = xyz.com
   ```

5. Type the hostname of your PC as the value of the `host-name=` parameter. For example, if the PC's name is first.xyz.com, type **`first`** for the hostname.

   ```
   host-name = first
   ```

6. Ask your system administrator what type of video card is installed in your PC and whether or not it is supported by the network software.

7. After you gather this information, find the `[pctcp screen]` section in your PCTCP.INI configuration file. For the `video-card=` parameter, specify as its value the type of video card installed in your PC, using one of these keywords: `Autodetect`, `VGA`, `XGA`, or the default, `VESA`.

   If your SuperVGA card is not in the list of supported video cards, and you suspect that the card is causing difficulties with your PC's display, set the value of the `video-card=` parameter equal to **`VESA`**. This causes the program to bypass attempts at identifying your video card.

   ```
   video-card = VESA
   ```

   Note: If you do not specify a setting for this parameter and you have a VGA card installed, the network software determines whether your card is a SuperVGA type and tests your system for VESA support.

   If OnNet or PC/TCP does not find VESA support, then the card type is set to VGA. The VGA card type does not support 132-column mode. If you have a card that worked previously in 132-column mode, set this parameter to

   ```
   video-card = autodetect
   ```

8.3.1 Configuring vmail for Multiple Clients, Hosts, or Users

You can specify how vmail interacts with different clients, remote hosts, servers, or users to perform such actions as

- Dividing tasks according to client. For example, you can use pop2 to provide multiple mailboxes, and nntp to provide access to network news groups. (By default, the vmail reader uses the Pcmail client for mail.)
- Receiving messages from and sending messages to mail or news servers on separate network hosts.
- Allowing two or more users to read their messages at the same PC.
- Receiving and reading your messages on two different PCs.

To use vmail with multiple clients, hosts, or users, you must use the `client-section=` parameter in the `[pctcp vmail]` section of the PCTCP.INI file to specify the default client, host, or user for vmail. In addition, you must add a section to the PCTCP.INI file that corresponds to each default or alternative client, host, or user (if it does not already exist in the file).

If it does not exist, you must create its section name with the format

`[pctcp` *`default_client_name`*`]`

where *`default_client_name`* is the name of your client, host, or user (for example, `pop2`, `machine1`, or `chris`). In addition, you have to add any configuration parameters that you need in the section manually, before you specify their settings.

You must use the **vmail -c** *config_section* option at the DOS command prompt with the appropriate command to access the alternative client, host, or user. The **-c** option allows the **nntp**, **pcmail**, **pop2**, **pop3**,and **vmail** commands to treat the alternative client, host, or user as its counterpart. When used with the **vmail** command, the **-c** option causes vmail to use the mailbox specified in the top-level directory specified in the configuration section for the client in the PCTCP.INI file.

Note: Each configuration section must specify a different top-level directory.

To configure vmail for use with multiple clients

1. Edit the PCTCP.INI file and locate the `[pctcp vmail]` section. For the `client-section=` parameter, specify the default client that you use at your PC. For example,

   ```
   client-section = pop2
   ```

2. Locate the section of the PCTCP.INI file that configures your default client (for example, `[pctcp pop2]`). For the `toplevel-directory=` parameter in that section, type as its value the unique directory under which messages for the default client will be stored. for example,

```
toplevel-directory = c:\mail\pop2
```

3. If it does not already exist in the file, create a section for your secondary client. For example,

```
[pctcp nntp]
```

4. If it does not already exist in the file, create the `toplevel-directory=` parameter and type as its value the name of the unique directory to store the messages received by the PC's secondary client. For example,

```
toplevel-directory = c:\mail\nntp
```

5. Save your changes and exit from the file before you run the programs.

To configure vmail for use with multiple hosts

1. Edit the PCTCP.INI file and locate the `[pctcp vmail]` section. For the `client-section=` parameter, specify the name of the default server from which your client receives messages. For example,

```
client-section = pop3
```

2. Find the section for your default server (for example, `[pctcp pop3]`). For the `server=` parameter, specify as its value the hostname or IP address of the host on which your default server runs. For example,

```
server = 128.127.50.01
```

3. For the `toplevel-directory=` parameter in that section, type as its value the name of a unique directory on the PC that will store the messages received from the default server. For example,

```
toplevel-directory = c:\mail\pop3
```

4. If it does not already exist, create a section for your secondary server. For example,

```
[pctcp pop2]
```

5. For the secondary server's section, add a `server=` parameter and specify as its value the hostname or IP address of the secondary host that runs the secondary server. For example,

```
server = 128.127.50.02
```

6. For the secondary client's section, create the `toplevel-directory=` parameter and type as its value the name of the unique directory to store the messages received from the PC's secondary server. For example,

```
toplevel-directory = c:\mail\pop2
```

7. Save your changes and exit from the file before you run the programs.

To configure vmail for use by multiple users at the same PC

1. Edit the PCTCP.INI file and locate the `[pctcp vmail]` section. For the `client-section=` parameter, type as its value the name of the section named for the default user of vmail, such as `chris`. For example,

   ```
   client-section = chris
   ```

   You do not have to type in the user's full name, because vmail relies on the setting of the `fullname=` parameter in the `[pctcp general]` section to get the full name of the user.

2. Create a section for the PC's default user. For example,

   ```
   [pctcp chris]
   ```

3. For the `toplevel-directory=` parameter in that section, type as its value the name of a unique directory on the PC that will store the messages received for the default user. For example,

   ```
   toplevel-directory = c:\mail\chris
   ```

4. For the `user=` parameter in that section, type as its value the name of the default user. For example,

   ```
   user = chris
   ```

5. For the `default-mbox=` parameter, type as its value the name of the default user's main mailbox. For example,

   ```
   default-mbox = chris
   ```

6. For the `reply-to=` parameter in that section, type as its value the address of the default user to which replies must be sent. For example,

   ```
   reply-to = chris@xyz.com
   ```

7. Create a section for the secondary user. For example,

   ```
   [pctcp robin]
   ```

8. For the `user=` parameter in that section, type as its value the name of the secondary user. For example,

   ```
   user = robin
   ```

9. For the `default-mbox=` parameter, type as its value the name of the secondary user's main mailbox. For example,

   ```
   default-mbox = robin
   ```

10. For the `reply-to=` parameter in that section, type as its value the address of the secondary

user to which replies must be sent. For example,

```
reply-to = robin@xyz.com
```

11. Save your changes and exit from the file before you run the programs.

8.4 Receiving Mail and Network News with vmail

The mail client that you run at your PC depends on which mail reader program you use: vmail or mail. Before you run any of these programs, review its command options and arguments in the *Command Reference* and decide which of them you want to use.

This section describes how to receive messages by running your NNTP, Pcmail, POP2, or POP3 client. It also describes how to start or exit from the vmail program, navigate through the layers of screens in vmail, and get online help while using vmail.

To run nntp, pcmail, pop2, or pop3

1. At the prompt, type the command that starts your mail or news client. For example,

   ```
   pop2
   ```

2. At the password prompt, enter your system password if you are running nntp, pop2, or pop3. For pcmail, perform one of the following:

   If this is your first time running pcmail, type the password given to you by your system administrator.

   –or–

   Type the password that you have defined in the `[pctcp pcmail]` section of your PCTCP.INI file.

   –or–

   If you have reset your password with the vmail **S** command, type the password that you have set for yourself.

The mail is copied into your mailbox subdirectory, which is below the client's unique top-level directory.

Note: The first time that you run your mail client, it creates the top-level directory defined for the mail client in its configuration section in your PCTCP.INI file. Note that each mail client whose mail you read in vmail *must* have its own, unique top-level directory.

8.4.1 Running vmail

The vmail program lets you read messages at your PC from the Pcmail, POP2, POP3, or NNTP clients. The vmail program displays the mailboxes, bulletin boards, descriptors, and messages from only one of these mail or news clients at a time. It automatically displays them for your default mail client. (You can use the **-c** command option to display them for a client that is not your default mail program.)

The vmail program displays four screen layers:

- Mailbox screen
- Descriptor screen
- Message screen
- Bulletin Board screen

(An example of a Bulletin Board screen appears in section 8.4.7, Subscribing to Bulletin Boards and Network News Groups.)

The vmail prompt appears at the bottom of each screen. If the mail client that you use supports mailboxes and bulletin boards, the Mailbox screen displays them when you start the vmail program. Your mailboxes are directories that you can use to separate and group your mail messages.

For example, as shown in Figure 8-1, you may have mailboxes named `chris`, `office`, and `projects`, and you may subscribe to your site's bulletin boards named `fun` and `staff`.

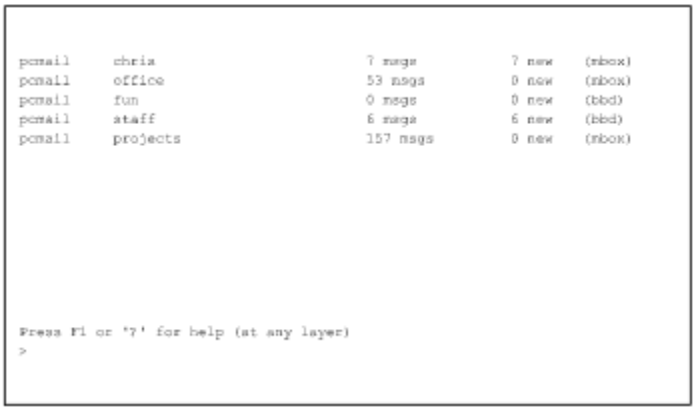

Figure 8-1 A Mailbox Screen

After entering a mailbox, you can use vmail commands to send and receive messages, reply to and forward messages, save messages to text files, copy messages to other mailboxes, and perform various other actions **.**

You can display up to 1,000 messages at a time for a single mailbox on your PC. Beyond that

number, vmail does not display the messages unless you make space for them by deleting and "expunging" (removing) other messages from the mailbox.

When you select a mailbox with the cursor and press either the space bar key or the Enter key on your keyboard, vmail displays the Descriptor screen, as shown in Figure 8-2. The Descriptor screen lists the message descriptors of all of your mail messages in that mailbox. (Descriptors are single-line summaries of messages that can be displayed in vmail.)

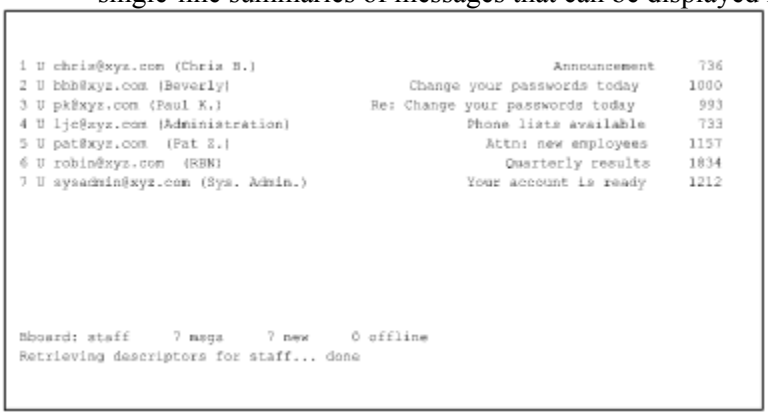

Figure 8-2 A Descriptor Screen

By selecting a descriptor with the cursor, you can display the Message screen, as shown in Figure 8-3. The Message screen lets you view the contents of a message.

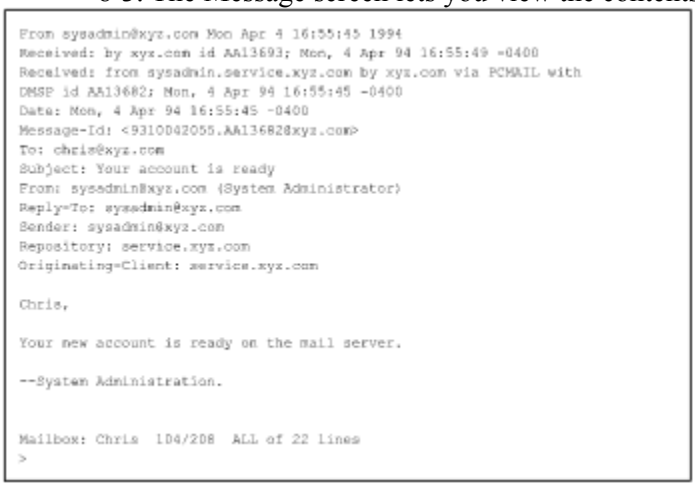

Figure 8-3 A Message Screen

If there is not enough disk space on your PC for a message that is very long, vmail retrieves only the message's descriptor. The pcmail and nntp programs flag the message with an o message flag to indicate that the message is off-line.

Note: Depending on which screen you display, the same vmail command may behave differently. For example, on the Mailbox screen, using the **p** command moves the cursor to the previous mailbox containing new messages. Once the messages in that mailbox are displayed on the Descriptor screen, using the **p** command moves the cursor to the previous undeleted message. (To move to a mailbox that does not contain new messages, use the right or left arrow keys.)

To start vmail

1. At the prompt, type **`vmail`**

   When you start the vmail program, it displays your Mailbox screen with the vmail prompt in the lower left-hand corner. The program displays your default mail client's messages.

2. Move the cursor to one of the mailboxes or bulletin boards and select it by pressing the space bar or Enter keys.

   The Descriptor screen appears.

3. To look at the body of a message, select one of the message descriptors in the list. The program displays the message belonging to that descriptor on the Message screen.

To exit from vmail

1. To exit from the Message or Descriptor screens, use either of the following approaches:

   To exit from the screen without updating the message's status, press the Esc key or type **`Q`** to cancel a vmail action.
   –or–
   To return to the Descriptor screen, type **`Q`** or **`q`**

2. To exit from the Mailbox or Bulletin Board screens, type **`q`**
   –or–
   Press the Esc key.

3. To exit from the vmail program, type **`q`**

Each time that you view a message from a mailbox or bulletin board, vmail schedules an action for your mail client to change the status of the message. Likewise, if you use a vmail command that changes a message, such as copying or deleting the message, vmail schedules an action for your mail client to change the message's status. Once you exit from the Mailbox or Bulletin Board screens with the **q** command, the status of their messages will change the next time that you run your mail client.

Once a bulletin board message's status has changed, the client permanently expunges (removes) the message when you exit with the **q** command.

To avoid removing bulletin board messages whose status has changed from unseen to seen

Exit from the Message or Descriptor screens by pressing the Esc key or using the **Q** command.

Afterwards, when you run your Pcmail client (or POP3 client that supports bulletin boards), the messages are not expunged.

To display online help in vmail

Use the following commands to get help when using the vmail program. The commands work differently, depending on which screen the vmail program currently displays. For commands that prompt for more than a yes or no answer, such as the alias command **(a**), the **F1** and **?** commands are particularly useful.

To view	**Use this command**
DOS command line usage.	**vmail -?** at the prompt
The vmail help screen. More information or a description of a procedure.	**?** or **F1** at any vmail prompt

Note: If you use a command that prompts you for an argument, and you do not want to continue, press the Esc key. If you press the Enter key, the default for that command (shown in square brackets in the prompt) is used.

To receive messages in vmail

1. At the prompt, type the command to start your mail or network news client.
2. Enter your password when you are prompted to do so.
3. At the prompt, enter `vmail` to start the vmail program.

   While you use vmail, refer to the *Command Reference* for a complete list of the vmail commands that you can use to perform such tasks as reading, copying, forwarding, and responding to your messages.
4. Use the **q** command to exit from vmail.
5. Run your mail or network news client again to carry out actions that were queued by vmail for your mail or news client, such as deleting or sending mail.

8.4.2 Sending Messages

This section describes how to send, reply to, and forward a message while using vmail. It also explains how to create your own "signature file," which can be appended to all messages that you send.

To send a message from vmail

1. At the vmail prompt on any vmail screen, type **m**

   The **m** command displays a message buffer in your text editor, with the required message header fields at the top.

   ```
   To:
   From:
   Subject:
   ```

   The `From:` field is filled in automatically by the vmail program, based on what settings you have specified for the `user=` and `full-name=` parameters in the `[pctcp general]` section of your PCTCP.INI file. The `Reply-to:` field also appears in the message header if you set the `reply-to=` or `reply-to-`*`mailbox`* `=` parameters in the `[pctcp vmail]` section, or if you enter it yourself below the `Subject:` field.

2. Fill out the header fields.

   You must type one or more addresses in the `To:` field. If you use pop2, pop3, or nntp, but do not identify an Internet address (*username @hostname*), or you have not defined a default host for the `default-host=` parameter in the `[pctcp smtp]` section of your PCTCP.INI file,vmail treats the message as "local mail." (Local mail does not leave your PC.)

   You may omit entering text in the `Subject:` field.

3. If you want to send carbon copies or "blind" carbon copies (unseen by other recipients) to other users, you can add the `Cc:` and `Bcc:` fields (pcmail only) to the message header.

   The pcmail program removes the `Bcc:` header from the message before transmitting it, so the "blind" copy is seen only by the recipients whom you have listed in the `Bcc:` field.

   The vmail program also lets you add fields to the message header required by specific sites or mail gateways. (Ask your system administrator for more information about required message header fields.)

4. Leave a blank line containing only a carriage return between the final line of the message header and the first line of the message body. (Tabs or blank spaces alone are not considered blank lines.)

5. Type your message in the space below the header fields.

   If you use a signature file (optional), vmail appends the file to the bottom of the mail

message. (For more information, refer to the procedure entitled “To create a signature file” later in this section.)

6. Save your message and exit from your text editor with the appropriate editor commands.

   The vmail program confirms that the message is written and prompts you to confirm that you want to send the message:

   ```
   c:\mail\outbound\42 written.
      Send the message (y or n)? [y]
   ```

7. To queue the message for transmission, type **y**

   –or–

   Press the Esc key or type **n** if you change your mind and do not want send the message.

   The vmail program prompts you to save the message in the C:\MAIL\OUTBOUND\DEAD.LET file:

   ```
   File for dead letter [dead.let]?
   ```

   Press the Enter key to save the letter in the “dead letter” file named DEAD.LET.

   The DEAD.LET file lets you save the text of unsent mail messages. If you have set the `ask-overwrite=` parameter to `yes` in the `[pctcp vmail]` section of the PCTCP.INI file, vmail prompts you to confirm that you want to overwrite the previous message in DEAD.LET.

   –or–

   Press the Esc key again if you do not want to save the message at all.

8. Run your mail or network news client to send the message to the server on a remote host.

   The client does not transfer the message to the server until you run the client.

To reply to a message

1. To send a reply as a response to everyone listed in the `To:` and `Cc:` fields of the message, type **r** at the vmail prompt.

   If the original message contained a `Cc:` field, or the message was sent to more than one address, vmail automatically adds the `Cc:` field to your reply. If there are `Resent:` fields, vmail sends the reply to the addresses specified in that field.

   –or–

   To reply only to the sender of the message, type **R**

   –or–

   To exit without sending your reply, press the Esc key at the vmail prompt.

Note: If you use nntp, any reply that you send using the **r** command is posted as a follow-up message. When you reply to a network news message, the reply does not include the message header or signature file. If you send the reply with the **R** command, the reply goes to the sender of the message by relying on the SMTP protocol.

The vmail program prompts you to specify whether or not you want to include the text from the original message.

2. To include the original message text, type **y** or press the Enter key.

   –or–

   To omit the original message, type **n**

   Once you include the text of the message, you can use your text editor to delete any lines of text from the included message that you do not want to include in your reply.

3. Fill out the header fields.

   When you compose a reply to a message, vmail completes the `To:`, `From:`, `Reply-to:`, and `Cc:` fields. The program also appends an `Re:` field to the `Subject:` field that identifies the subject of the original message. If there are `Resent-to:` fields, vmail sends the reply to the addresses specified in that field.

4. Leave a blank line ending in a carriage return between the final line of the message header and the first line of the message body. (Tabs or blank spaces alone are not considered blank lines.)

5. Type your reply in the space below the header fields.

   Notice that, if you use a signature file (optional), vmail appends the file to the bottom of the mail message.

   If you typed **y** at the prompt for including the text from the message that you are responding to, vmail automatically indents any included text from the left margin by four character spaces. You can override this effect by setting your own indentation style for the `indent-reply=` parameter in the `[pctcp vmail]` section of your PCTCP.INI file.

6. Use your editor commands to save and exit from the file.

   A prompt appears for confirmation to send the reply.

7. To queue the reply for transmission, type **y**

   –or–

   If you do not want to send the reply, type **n**

8. Run your client to send the reply to the server on the remote host.

   The reply is not sent until you run your client.

To forward a message

1. Select the message that you want to forward by selecting the message at the Descriptor screen, or displaying the message at the Message screen.

2. Type **`f`**

   The command displays a blank header field at the top of the screen with the message below it.

3. Fill in the `To:` field with the address of the recipient.

4. Using your text editor, add or delete text, and (if you want to) delete the forwarded headers enclosed in the message.

5. Using your text editor commands, save the message and exit from your editor.

   The vmail program prompts for confirmation to send the message.

6. To queue the message for transmission, type **`y`**

   –or–

   If you do not want to forward the message, type **`n`**

7. After you confirm that you want to forward the message, run your client to send the message to the server on the remote host.

To create a signature file

A "signature file" contains text that is appended to every message that you mail or reply to in vmail. You can make the contents of the signature file be anything that you want it to be, of any length. Typically, the file contains information about you: your name; the name, address, and phone number of your company; and your electronic mail address. Some signature files may contain personalized quotations. Signature files are typically no more than three or four lines in length.

The vmail program appends the text contained in the signature file to all messages or replies that you send, but does not append the signature file when you forward a message.

1. Using your text editor, create and name a signature file that contains the text that you want to include in your mail messages.

2. Save your changes, and exit from the file.

3. Edit your PCTCP.INI file and add the `signature=` parameter to the `[pctcp vmail]` section in the file. To provide a value for the parameter, specify the full pathname of the signature file's location, including the drive letter, as in this example:

   ```
   signature = c:\chris\my_sig.txt
   ```

4. Using your editor commands, save the changed PCTCP.INI file and exit.

The next time that you compose a message while using vmail, you should see the signature file text at the bottom of the message.

8.4.3 Using Aliases

The vmail program lets you configure aliases. An “alias” is typically a single, short address that corresponds to a long address or a list of addresses. Aliases are useful if you frequently send mail to certain users or lists of users.

You can use aliases both for individual usernames and mailing lists. A mailing list is a list of individual and/or group names; each name is treated as a single member of the list. Any message sent to the alias for the mailing list is received by each member of the list. For example, the following alias, `staff`, is the name of a mailing list:

```
staff   chr, lee, pat, alex
```

In this example, the mailing list `staff` is composed of the aliases `chr` (an alias for chris@xyz.com), `lee` (lee smith@xyz.com), `pat` (pat jones@xyz.com), and `alex` (alex@xyz.com).

To use aliases, specify the text file that contains the aliases as the value for the `aliases=` parameter of the `[pctcp vmail]` section in your PCTCP.INI file. This parameter directs the vmail program to look at the aliases in that file and include in the message headers the addresses that correspond to the aliases, before scheduling the action for the client to send the message.

To add an alias

1. Edit your PCTCP.INI file. For the `aliases=` parameter of the `[pctcp vmail]` section, specify the name of the file that contains your list of aliases. (If the file does not yet exist, the vmail program creates it.)

2. Use your text editor commands to save your changes and exit from the PCTCP.INI file.

3. At the prompt, enter **`vmail`**

4. At the vmail prompt, type **`a`**

   You are prompted for the name of the alias:

   ```
   Name of alias?
   ```

5. Type the name of the alias that you want to use and press Enter.

   For example, to use the alias `staff`, which is the name of a mailing list, enter the list’s name at the prompt:

   ```
   Name of alias? staff
   ```

   A prompt appears for the recipient list, which can be either a mailing list or a single address.

6. If you want your alias to represent the members of a mailing list, type the email address or the alias of each member, separating them with a comma. In this example,

```
Recipient list?chris@xyz.com, lee smith@xyz.com, pat jones@xyz.com,
alex@xyz.com
```

the recipient list is composed of the email addresses for four recipients. You can enter the aliases for these recipients instead of their full electronic mail addresses.

7. Press the Enter key, and the command prompts you to confirm the alias.
8. To add the parameter to the aliases file, type **y** or press the Enter key.

   –or–

   To cancel adding the alias to the file, type **n**

Note: Aliases can include other aliases, but do not nest the aliases more than three layers deep (*alias_1* includes *alias_2*, which includes *alias_3,* and so on). Nesting aliases can cause a failure in message delivery.

To use an alias

1. At the prompt, enter **vmail**
2. At the vmail prompt, type **m**

   The Message screen appears.
3. Type the name of the alias in the `To:` or `Cc:` field of the message header.
4. Compose the rest of your message.
5. Use your editor to save and exit from the message buffer.
6. Run your client to send the message.

To display the mailing list for an alias

1. At the prompt, enter **vmail**
2. At the vmail prompt, type **a**
3. To see a list of your vmail aliases, type **?** at the prompt:

   ```
   Name of alias? ?
   ```

   –or–

   If you know the name of the alias, enter the name at the `Name of alias?` prompt.
4. To return to the vmail prompt, press any key.
5. Enter the name of an alias from the list that was displayed, exactly as it appeared on the list.

The screen displays the addresses or mailing list assigned to that alias.

6. Press any key to return to the vmail prompt.

To delete an alias

Edit your ALIASES file with a text editor and remove the unwanted alias from the file.

8.4.4 Searching for, Filtering, Saving, Copying, and Printing Messages

This section describes how to search for, filter, save, copy, and print your messages while using vmail.

To search forward for a message

The **Ctrl+s** command lets you search forward at the Descriptor screen or Message screen levels for the descriptor of the message that contains in its `To:`, `From:`, or `Subject:` fields the text that you want to find. You specify the exact string of characters that is used in the search.

1. Position your cursor at the top of the list of descriptors on the Descriptor screen.

2. At the vmail prompt, press Ctrl+s.

   The `Forward Search:` prompt appears.

3. At the prompt, type the string of characters that you want to search for among your message descriptors or text. For example,

   ```
   Forward search: Meeting tomorrow
   ```

   While the search proceeds, vmail displays the message

   ```
   Retrieving descriptors for username...
   ```

   where *`username`* is your username.

   If the search succeeds, the descriptor of the first message encountered in the search that contains a match of the specified text is highlighted on the Descriptor screen, or the text of the message whose header contains the matching text is displayed on the Message screen (depending on which screen level you occupied when you started the search). Only one occurrence of the text found is displayed at a time. To look at another occurrence, use **Ctrl+s** again.

   If the search fails, vmail displays the message

   ```
   Search failed.
   ```

To search backward for a message

The **Ctrl+r** command lets you search backward at the Descriptor screen or Message screen levels for the descriptor of the message that contains in its `To:`, `From:`, or `Subject:` fields the text you want to find. You specify the exact string of characters that is used in the search.

1. Position your cursor at the bottom of the list of descriptors on the Descriptor screen.

2. At the vmail prompt, press Ctrl+r.

   The `Reverse Search:` prompt appears.

3. At the prompt, type the string of characters that you want to search for among your message descriptors or text. For example,

   ```
   Reverse search: Meeting today
   ```

   While the search proceeds, vmail displays the message

   ```
   Retrieving descriptors for username...
   ```

   where *username* is your username.

   If the search succeeds, the descriptor of the first message encountered in the search that contains a match of the specified text is highlighted on the Descriptor screen, or the text of the message whose header contains the matching text is displayed on the Message screen (depending on which screen level you occupied when you started the search). Only one occurrence of the text found is displayed at a time. To look at another occurrence, use **Ctrl+s** again.

   If the search fails, vmail displays the message

   ```
   Search failed.
   ```

To filter messages

The **h** command searches the `To:`, `From:`, and `Subject:` fields of your messages and displays a list of descriptors of only those messages that contain the specified search text. It provides a way for you to filter the messages in a mailbox, so that only those messages that contain the specified text are displayed on your screen.

1. At the vmail prompt at the Descriptor screen, type **h**

   The `Descriptor match:` prompt appears.

2. Type the text that you want to use to filter your messages. For example,

   ```
   Descriptor match: Chris Smith
   ```

   While the filtering proceeds, vmail displays the message

   ```
   Retrieving descriptors for username...
   ```

   where *username* is your username.

   If the filtering succeeds, a new list of descriptors of messages that contain the filtering text is displayed on a new screen.

   If the search fails, vmail does not display a new list or change the position of your cursor on the Descriptor screen.

3. To back out of the list of filtered descriptors or the text of one of the filtered messages, and return to the Descriptor screen, type **h** at the vmail prompt.

To save a message to a file

1. At the prompt, enter **`vmail`**

2. At the Mailbox screen, select with your cursor the mailbox whose messages you want to view, then press the space bar or Enter key.

3. At the Descriptor screen, select with your cursor the descriptor of the message that you want to save and type **`s`** at the vmail prompt.

   –or–

   Display the message at the Message screen, and type **`s`** at the vmail prompt.

4. At the `Save to file:` prompt, type a filename and press Enter. For example,

   ```
   Save to file: report.txt
   ```

   If you have specified the pathname of a directory for the `folder=` parameter in the `[pctcp vmail]` section of your PCTCP.INI file, all messages are saved into that directory automatically. If you have not set the `folder=` parameter, the vmail program saves the message in your current directory when you started vmail, unless you enter a different pathname at the `Save to file:` prompt.

   If you saved the message to a file, the program indicates where it filed the message. For example,

   ```
   Saved #250 to "c:\mail\report.txt"
   ```

   –or–

   To exit without saving the message, press the Esc key at the vmail prompt.

5. If you save another message, the vmail program displays the pathname of the file in which you saved the previous message, and prompts you to specify whether you want the current message saved in the same file. For example,

   ```
   Save to file [c:\mail\report.txt]:
   ```

   To append the current message to the other saved message in the same file, press Enter at the prompt.

   –or–

   To save the current message in a different file, type a new filename at the prompt, then press Enter. For example,

   ```
   Save to file [c:\mail\report.txt]: census.rpt
   ```

To copy a message to a mailbox

1. At the prompt, enter **`vmail`**

2. At the Mailbox screen, select with your cursor the mailbox whose messages you want to view, then press the space bar or the Enter key.

3. At the Descriptor screen, select with your cursor the descriptor of the message that you want to copy and type **`c`** at the vmail prompt.

   –or–

   Display the message at the Message screen, and type **`c`** at the vmail prompt.

4. At the `Copy to mailbox:` prompt, type the name of the mailbox to which you want to copy the message, then press the Enter key. For example,

   ```
   Copy to mailbox: reports
   ```

   The program displays a message similar to the following example:

   ```
   #274 will be copied to reports
   ```

   If you make an error entering the mailbox name, the program displays a message.

   ```
   Unknown mailbox reports
   ```

   A copied message appears in the mailbox to which it is to be copied only after you run your mail client. The original message remains in the original mailbox until you delete it and "expunge" the message from the mailbox.

Caution: Do not delete the original message that you copied until after you have run your mail client. Otherwise, the copying may fail.

To print a message

Before you can print a message directly to a printer, your system administrator must set up the printer correctly, and must make certain that the remote host on which your mail server is running can send print requests over the network to the printer.

1. Specify in your PCTCP.INI file where messages are to be printed. For the POP and NNTP clients, you must specify for the `server=` parameter in the `[pctcp lpr]` section the hostname or IP address of the print server that will send print requests to your printer.

   For pcmail, the printer must be known to the remote host on which the Pcmail server is running (such as by being listed in the /etc/printcap file on the Pcmail server's UNIX host).Specify the name of this printer for the `printer=` parameter in the `[pctcp vmail]` section of your PCTCP.INI file.

2. To request that the server print the current message, type **`P`**

   The program displays a message similar to the following example,

   ```
   Message #395 will be printed on printer.
   ```

where *printer* is the name of the printer that receives your printing request. The message is not printed until the next time that you run the client.

–or–

To save the message into a text file, type **s** at the vmail prompt, specifying a filename at the prompt. Doing so allows you to print the file later.

8.4.5 Deleting, Undeleting, Expunging, and Retrieving Messages

This section describes how to delete, expunge, locally delete, and restore a locally deleted message while using vmail. If you use the pcmail or nntp programs, and you want to save disk space on your PC without permanently removing messages, you can locally delete messages.

To delete a message

1. At the prompt, enter **`vmail`**
2. At the Mailbox screen, select the mailbox whose messages you want to view with your cursor, then press the space bar or Enter key.
3. At the Descriptor screen, select with your cursor the descriptor of the message that you want to delete and type **`d`** at the vmail prompt.

   –or–

   Display the message at the Message screen, the type **`d`** at the vmail prompt.

   Note that vmail flags the message with a `D` at the Descriptor screen, marking the status of the message to be changed by the mail client.
4. To change the status of the message, run your mail client.

   The **d** command does not remove the message from the mailbox; to remove the deleted message, you "expunge" the mailbox with the **e** command.

To undelete a message

1. At the prompt, enter **`vmail`**
2. At the Mailbox screen, select with your cursor the mailbox whose messages you want to undelete, then press the space bar or Enter key.
3. At the Descriptor screen, select with your cursor the descriptor of the message that you want to undelete and type **`u`** at the vmail prompt.

   –or–

   Display the message at the Message screen, and type **`u`** at the vmail prompt.

   Note that vmail removes the `D` message flag from the message at the Descriptor screen, marking the status of the message to be changed by the mail client.
4. To change the status of the message, run your mail client.

   The **u** command does not undelete a locally deleted message; to retrieve a locally deleted message, you must use the **g** command.

To expunge deleted messages

1. Before you expunge (remove) deleted messages from a mailbox, make certain that all unwanted messages have been deleted and flagged with a `D` in the mailbox.

2. At the prompt, enter **`vmail`**

3. At the Mailbox screen, select the mailbox whose messages you want to expunge and, at the vmail prompt, type **`e`**

   The program displays a message similar to the following example:

   ```
   The deleted messages in mbox chris will be expunged
   ```

   –or–

   At the Mailbox screen, type **`E`** at the vmail prompt to expunge the deleted messages in all of your mailboxes.

   The program displays the message

   ```
   The deleted messages will be expunged
   ```

Note: The **e** (expunge mailbox) command functions differently with different mail clients. Once a pcmail message has been expunged, it cannot be undeleted, printed, or copied to another mailbox. If you are using pcmail, and delete more messages after you issue the **e** (expunge mailbox) command, those messages are not expunged. If you are using pop2, pop3, or nntp programs, all messages flagged as being deleted are expunged, regardless of the order in which you issue these commands.

To locally delete a message

To save disk space on your PC, you may want to delete locally any pcmail or nntp messages with the **L** command, so that the contents of each locally deleted message stays "off-line" from your PC. When you locally delete messages, only the message descriptors are displayed in your mailbox, not the contents of the messages. Note that this action can be used only for pcmail or nntp messages.

1. At the prompt, enter **`vmail`**

2. At the Mailbox screen, select with your cursor the mailbox whose messages you want to view, then press the space bar or Enter key.

3. At the Descriptor screen, select with your cursor the descriptor of the message that you want to delete locally, then type **`L`** at the vmail prompt.

   –or–

   Display the message at the Message screen, and type **`L`** at the vmail prompt.

   The program displays the `Delete message` prompt, as in this example:

   ```
   Delete message #275 from this PC (y or n)? [y]
   ```

4. If you want to proceed with the local deletion, press Enter at the prompt.

   –or–

   If you want to cancel the action, type **n**

   The vmail program flags the message with an o to indicate that the message body is off-line. To indicate that the message has been locally deleted, the program displays a message similar to this example:

   ```
   Message #451 was deleted from this PC
   ```

5. For this action to take effect, run your client.

   Note that if you try to view the body of an off-line message, the vmail program displays the following message on the Message screen, below the headers of the message.

   ```
   [Message text is offline]

   Type g to queue a retrieval
   ```

Note: To prevent the accumulation on your PC of off-line messages for the pcmail program, set the `msglimit=` parameter in the `[pctcp pcmail]` section of your PCTCP.INI file . The `msglimit=` parameter takes as its value the maximum number of bytes allowed in a message. If the number of bytes of a message is larger than the value specified for this parameter, the message remains off-line (not on your PC). With a little experimentation, you can set the parameter to a number sufficiently high enough to suit your needs. As an alternative, set this parameter either to `0` for no limit, or include the parameter in the section without providing it with a value.

To retrieve a locally deleted message

This action affects only locally deleted messages or a message that is off-line because it exceeds the limit set by the `msglimit=` parameter in the `[pctcp pcmail]` section. This action can be used only for Pcmail or NNTP messages. Note that for bulletin boards, messages can expire if you do not retrieve them promptly, because messages are removed from bulletin boards once they have exceeded an expiration time set by the administrator.

1. At the prompt, enter **vmail**

2. At the Mailbox screen, select the mailbox whose off-line messages you want to retrieve and press the space bar or Enter key.

3. At the Descriptor screen, select with your cursor the descriptor of the message you want to retrieve and type **g** at the vmail prompt.

   The program displays a message similar to the following example:

   ```
   Retrieval of chris/451 queued
   ```

4. Run your client to retrieve the locally deleted message.

The retrieved message is restored on the PC.

8.4.6 Adding and Deleting pcmail or pop2 Mailboxes

This section describes how to add or delete a mailbox and/or its address for the Pcmail or POP2 clients.

Mailboxes allow you to separate and group your messages into discrete directories. The process for creating a mailbox differs, depending on whether you are using the pcmail or pop2 programs. Make certain that you display the Mailbox screen as vmail performs any of these actions.

Note: The following procedures require that you have created or changed to the appropriate file privileges on the remote host that runs your mail server. Ask your system administrator for help with this task.

To add a mailbox for the Pcmail client

1. At the prompt, enter **`vmail`**

2. When the Mailbox screen appears, at the vmail prompt, type **`A`**

   The following prompt appears:

   ```
   Mailbox name?
   ```

3. At the prompt, type the name of the new mailbox, then press Enter.

   A prompt similar to the following example appears:

   ```
   Memos is a new mailbox, do you want to add an address(y or n?) [y]
   ```

4. To accept the default address for the mailbox, press Enter.
   The default address consists of your username and your mailbox name.
   –or–
   If you do not want to use the default address, type another name when prompted.
   –or–
   If you plan to use the mailbox only as storage for mail, press Esc without specifying an address.

5. At the prompt, enter **`pcmail`** to run your Pcmail client.

   The pcmail program creates the new mailbox, and the next time that you run vmail, the mailbox will appear on the Mailbox screen.

6. Ask your system administrator to send mail to the mailbox address that you have created. For example, if there is a mailing list called `fun`, ask the system administrator to direct your mail to your mailbox, using the address that you have created, such as *`chris-fun`*, where *`chris`* is an example of a default mailbox name.

   After the system administrator has configured the mail server to direct your mail, all mail

from the mailing list is sent directly to your mailbox when you run pcmail.

To add a mailbox for a POP2 client

1. Log in to the remote host that runs your mail server.
2. Create an empty file to serve as your mailbox file.

   Make certain that you grant the file **r**, **w**, and **s** access rights with the UNIX **chmod** command. (For more information about the UNIX **chmod** command, refer to your UNIX documentation.)

   For example, to create a mailbox file named /fun for a user named Chris on a UNIX host, type the following commands at the UNIX prompt:

   ```
   >touch /users/chris/fun

   >chmod 4600 /users/chris/fun
   ```

   where `/users/chris/fun` is the full pathname of the mailbox file.
3. Log out from the remote host.
4. At the prompt, enter **vmail**
5. When the Mailbox screen appears, type **A** at the vmail prompt.

   The `Mailbox name?`prompt appears.
6. Type the name of the mailbox file that you created on the remote server. Be sure to specify the complete name and pathname as it exists on the server (for example, /users/chris/fun). When you use pop2, the vmail program does not prompt you to type the address of the mailbox. Note that while you may have specified a long pathname for the mailbox, only the name of the mailbox (preceded by a forward slash (/)) appears on the Mailbox screen.
7. At the prompt, type **pop2** to run your mail client.

   The mailbox is automatically created. Mail is then directed from the mailing list to your mailbox.
8. Ask your system administrator to direct mail from the mailing list that you choose to the file on your system account.

   For example, if there is a mailing list called `fun`, ask the system administrator to direct its mail to the /users/chris/fun mailbox file. (On UNIX mail servers, the system administrator accomplishes this through commands in the aliases file.)

To delete a mailbox and its address

1. At the Mailbox screen, select the mailbox that you want to delete.

2. At the vmail prompt, type **`d`**

   A prompt appears, similar to the following example:

   ```
   Delete the mailbox projects (y or n)? [n]
   ```

3. At the prompt, enter **`y`**

   –or–

   To cancel deleting the mailbox, type **`n`** at the prompt, press the Esc key, or just press Enter.

The mailbox will be deleted after you run your mail client.

Note: Make certain that, before you delete a mailbox, your system administrator removes the mailbox from every mailing list on which it appears; otherwise, mail messages intended for the deleted mailbox will be returned to their senders with error messages appended to them.

8.4.7 Subscribing to Bulletin Boards and Network News Groups

Bulletin board and network news group messages differ from mail messages in that the messages stored in bulletin boards and news groups can be read by many users. For example, both bulletin boards and network news groups can be used at your site to distribute public or general information on your network.

Subscribers to a bulletin board or network news group are granted read-only access to the messages in the mailbox. Only the bulletin board's or network news group's owner may remove messages from that bulletin board or news group. If you are not the owner of a bulletin board or network news group and you use the **d** command on a message displayed on the vmail Descriptor screen, the command has no effect on the actual message. (For NNTP, however, the network news group message will be deleted from your PC, not from the news group itself.) You can, however, reply to or forward bulletin board or network news group messages, using your editor and vmail in the same way that you would for mail messages.

The names of bulletin board and network news group mailboxes are unique for your system. For example, a bulletin board mailbox named `staff` may be accessed by every user of your network community. This does not preclude you from having a mailbox named `staff` unless you try to subscribe to a bulletin board by the same name.

The main differences between bulletin boards and network news groups are:

- The Pcmail or POP3 protocols are used to transmit bulletin board messages. Bulletin boards typically exist only on a site's local area network, but if that network has access to other networks, the site's system administrators may set up public access to their site's bulletin boards.

  Only the Pcmail and POP3 clients support access to network bulletin boards, but not all POP3 servers support bulletin boards. If you are using a POP3 server, your system administrator must verify that it supports bulletin boards.

- The NNTP protocol is used to transmit network news posts (messages). Network news groups are often propagated from one NNTP server to many NNTP servers throughout the Internet, but are not restricted to the Internet. Some sites use NNTP to set up their own news groups.

  The NNTP client allows you to view network news group messages, whether the messages originate on the NNTP server at your site, or on an Internet NNTP server. (The system administrators at your site determine whether or not you have access to Internet network news groups.)

You can gain read-only access to a bulletin board or news group by creating a subscription to it. You lose that access when you cancel your subscription.

You can list what local bulletin boards and network news groups are available using the vmail program. The vmail program displays the Bulletin Board screen when you enter **l** (lowercase letter L) at the vmail prompt.

The vmail Bulletin Board screen is the only screen that lists all of the bulletin boards or all of the network news groups to which you can subscribe at your site. Once you subscribe to a bulletin board or news group, a mailbox appears on the Mailbox screen with the same name as the bulletin board or news group. Note that only unread messages appear in your bulletin board mailboxes, and only messages that have not been deleted, "expunged," or expired appear in network news group mailboxes. (A news group message expires from your PC when it exceeds the time limit that you have set for messages that appear in your network news group mailbox. You can set the expiration limit in your PCTCP.INI file.) You can save these messages in text files or copy them to your other mailboxes, but you do not have to delete the messages.

Note: The pcmail program deletes all bulletin board messages up to the first unread or undeleted message; however, pcmail does not delete any messages if you exit from the Descriptor screen with the Esc key instead of the **q** command. Likewise, the nntp program removes all "deleted" network news messages from your PC unless you exit from the screen using the Esc key instead of the **q** command.

To retrieve a list of the available bulletin boards or network news groups

1. At the prompt, enter **`vmail`**

   If you want to retrieve a list of the network news groups, and NNTP is not your default client, enter

   ```
   vmail -c nntp
   ```

2. To schedule a retrieval of the bulletin boards list, at the vmail prompt, type **`B`**

   –or–

   To schedule a retrieval of a list of the network news groups, type **`b`**

   For either command, the program displays the message:

   ```
   Queued retrieve of bboard list
   ```

3. To exit from vmail, type **`q`** at the prompt.

4. Run your client (NNTP, Pcmail, or POP3) to retrieve a list of available bulletin boards or network news groups from the remote host.

To display a list of bulletin boards

1. At the prompt, enter **`vmail`**

   –or–

   If you are joining a network news group, and nntp is not your default client, type

   ```
   vmail -c nntp
   ```

2. At the vmail prompt, type **`l`** (lowercase letter L).

The program displays the Bulletin Board screen, as shown in Figure 8-4.

Figure 8-4 A Bulletin Board Screen

To join a bulletin board or network news group

1. At the prompt, enter **`vmail`**
   –or–
   If you are joining a network news group, and nntp is not your default client, enter

   `vmail -c nntp`

2. At the vmail prompt on the Mailbox or Bulletin Board screens, type **`j`** to join a bulletin board or network news group.

   The following prompt appears:

   ```
   Subscribe to:
   ```

3. Type the name of the bulletin board or network news group that you want to join and press Enter. For example,

   ```
   Subscribe to: staff
   ```

The next time that you run your mail client, the server creates a bulletin board or network news group mailbox, and the client retrieves messages for that mailbox.

To cancel a subscription to a bulletin board or network news group

1. At the prompt, enter **`vmail`**
   –or–
   If you are joining a network news group, and nntp is not your default client, enter

   `vmail -c nntp`

2. At the Mailbox screen, select a bulletin board or network news group with your cursor.

3. At the vmail prompt, type **`k`**

The following prompt appears, with the name of the bulletin board or news group enclosed in square brackets following the prompt:

```
Unsubscribe from: [name]
```

4. To cancel the subscription to the named bulletin board or network news group, press Enter.
   –or–
   Type the name of a different bulletin board or network news group and press Enter.
   –or–
   To cancel this action, press the Esc key.

Your subscription to the bulletin board or news group will be cancelled the next time that you run your mail client.

To post messages to a network news group

1. At the prompt, enter **`vmail`**
   –or–
   If you are joining a network news group, and nntp is not your default client, enter

   ```
   vmail -c nntp
   ```

2. At the vmail prompt, type **`N`**

   Your editor screen appears, displaying header fields at the top of the screen.

   ```
   Newsgroups:
   Keywords:
      Distribution:
      Subject:
   ```

3. Enter text in the message header fields.

   Type the names of the news groups to which you want to post the message in the `Newsgroups:` field, separated by commas. The `Distribution:`, `Keywords:`, and `Subject:` fields are optional.

4. Compose your message with your text editor.

   Separate the message from the message header fields by a blank space ending with a carriage return.

5. Save your message and exit from the editor.

The next time that you run nntp, the message is posted to the news group.

8.5 Troubleshooting Electronic Mail and Network News

This section describes possible solutions to situations that you may encounter while using your mail or network news clients. A description of the situation appears first, including any screen messages that you may see, and is followed by a brief explanation and a recommended course of action.

You receive the following message concerning a **pcmail** message:

```
Transmit failed, will try again later
```

The transmission may have failed because **pcmail** did not recognize a header field in the message. To resolve this situation, try one or more of these solutions:

Make certain that your text editor creates ASCII text files, not encoded word processing files.

Use your text editor to display the contents of the outbound mail file and make certain that the header fields have been filled in correctly.

Make certain that there is a blank line between the message header and the text (note that text also includes the header of a forwarded message or header material contained in a reply).

Delete any blank lines above the `To:` field before retransmission.

Note: The mail message is saved in the C:\MAIL\OUTBOUND subdirectory as `1` if it is the first message prepared to send while using vmail and your editor, `2` if it is the second message, and so on. If you can fix the problem in the numbered message file, save the file and send the message. If you do not want to fix the problem, delete the file.

You receive a message similar to the following when you run **pcmail**:

```
c:\pcmail\mbox5 has been orphaned. Should it be deleted? y or n ?
```

The message appears if you have deleted a mailbox using the **vmail d** command or the UNIX **peek** command.

If you want to delete the mailbox, type **`y`**
–or–
Type **`n`** if you do not want to delete it.

You send messages using the **pop2** or **pop3** commands, but the messages never reach their destinations, and are not returned to you.

The `default-host=` parameter in the `[pctcp smtp]` section of the PCTCP.INI file may be absent or may not be set. If you do not use this parameter, any mail sent to a username without *@hostname* appended to the name is sent by SMTP to a username that is local to your machine, so the message never leaves the PC.

Set the value of the `default-host=` parameter to be the hostname or IP address

of the remote host that runs your mail server.

A message is returned to you instead of reaching its destination.

This situation may be caused by any of the following situations, any of which may be indicated by the message appended to your returned message:

You failed to supply the `To:` field with a valid address, either by mistyping the address or by failing to include an address in the field altogether.

There may be a problem outside your network, such as with the gateway host connecting another network to your local area network. Contact the network administrator responsible for the gateway.

One of the recipients on the mailing list to which you sent the message did not receive it. Either resend the message only to the person who did not receive it, or inform the manager of the mailing list that a message sent to a specified address never reached its destination.

The vmail program fails to retrieve messages from a large directory.

The value of the `net-time-out=` parameter in your mail client's section of your PCTCP.INI file may not be set to a high enough value. Experiment by setting this value to a higher and higher number, until you have a setting that ensures that vmail has enough time to retrieve messages from a large directory. If the remote host times out, ask your system administrator to change the TIME_OUT value on the remote host.

You receive duplicate messages in vmail.

Duplicate messages are usually caused by the mail server or mail forwarding program.

Notify your system administrator.

You use the vmail **m** command to invoke your text editor to compose your message. When you attempt to send the message, vmail displays a `Send message?`prompt.

This situation may be caused by either of the following:

Your text editor may not have enough memory available to run. Refer to the documentation provided with your editor for instructions on changing the amount of memory required, or if you have several terminate-and-stay -resident (TSR) programs loaded, try removing one before starting vmail.

Verify that the value of the `editor=` parameter in the `[pctcp vmail]` section of your PCTCP.INI file matches the string that you type at the DOS command line to call the editor.

You have difficulty using vmail at the prompt, but vmail functions correctly in a Windows box.

This situation can occur if there is a SuperVGA card installed in your PC that is not supported by your network software, and the vmail program attempts to determine what kind of video adapter you have. Ask your system administrator what type of video card is installed in your PC and whether it is supported by OnNet or PC/TCP. Be sure that the parameter is listed in the `[pctcp screen]` section of your PCTCP.INI configuration file.

If your SuperVGA card is not in the list of supported video cards, and you suspect that the card is causing difficulties with your PC's display, set the value of the `video-card=` parameter equal to **`VESA`**. This causes the program to bypass attempts at identifying your video card.

```
video-card = VESA
```

Note: If you do not specify a setting for this parameter and you have a VGA card installed, the network software determines whether or not your card is a SuperVGA type and tests your system for VESA support.

If the network software does not find VESA support, the card type is set to VGA. The VGA card type does not support 132-column mode. If you have a card that worked previously in 132-column mode, set this parameter to

```
video-card = autodetect
```

The vmail program functions in DOS, but not in Windows.

Your editor may use an Extended Memory Manager (EMM). Refer to your text editor's documentation on using EMM in Windows.

Your editor may not have enough memory to run in Windows. Customize the .PIF file to provide more memory. (Refer to your Windows documentation for more information about .PIF files.)

The vmail program seems to be very slow to gain access to mail messages.

Due to limitations of DOS, you may have to remove fragmented disk space on your PC to improve how quickly the vmail program gains access to mail messages. When you delete files, fragmentation of disk storage may result, causing the vmail reader to access several places on the hard disk for an entire message.You can correct this situation by using one of these solutions:

Run a disk optimization program to reorganize the PC's hard disk into contiguous segments. (Ask your system administrator about disk optimization programs available at your site.)

Use a disk-caching program (such as SMARTDRV.SYS *)*. A disk-caching program stores the most recently used data in memory. For example, vmail frequently reads directory information. If you run a disk-caching

program (usually when you start the PC), the caching program stores that directory information in the cache. When vmail retrieves that information, it reads it from the cache instead of from the hard disk.

Use the **tar** command to back up the contents of the PC's mail directories to a tape or file. Verify the contents of the tape first, then delete the contents of the mail directories. Finally, restore the PC's mail files from the tape or file.

Chapter 2
Learning About Hosts and Users on the Network

Several DOS commands let you display information about the network. Some of these commands (**host, finger**, **whois**, and **nicname**) provide information about hosts and users on the network. Refer to Chapter 1, Introduction to see if these DOS commands are included with the version of the network software that you have.

Other commands (**inet** and **ping**) display information and statistics about your system and network, and can help diagnose and troubleshoot network problems.

This chapter summarizes each command, identifies important arguments and options for each command, and explains why and how to use each command.

2.1 Before You Start Learning About Users on the Network

Before attempting to collect network information, be aware that

- Using the **finger** or **whois** commands requires that a Finger server is running on the remote host.
- Using the **nicname** command requires that your network have access to the Internet.

If you are uncertain about this information, contact your network administrator.

2.2 Identifying Users on a Network

When you want to identify all users on a network host, use the **finger** or **whois** command to query the host. These commands are client implementations of TCP/IP protocols of the same name, and can be used with any system running the appropriate (Finger or Whois) server.

Both commands produce a display of current users (IDs and usernames) and related information, including terminal process (TTY) assignments, idle times, and office locations. Some hosts may display additional information such as the time and reason for logging in and the user's hostname.

The Whois protocol is an option of the Finger protocol that requests more information. The **whois** command may expand and reformat the displayed text to include this information. If you use either command to identify a specific user on a host, or if there is only one current user, the host may respond with expanded information about that user.

Some hosts do not respond to **whois** or **finger** requests and may either reject or not respond to the request. If there is a response, the form and contents of the display may vary between hosts.

To display users on a host

Use the **finger** command to display the usernames of people logged in to a specified host.

The **finger** command requires a hostname (or IP address) in the form *@host*. The display produced by the **finger** command may change depending on the specified host, as shown in the following examples:

```
C:\>finger @abc

[abc.xyz.com]
Login      Name                 TTY     Idle    When           Office
ckj        Chris K. Jones       p0      26      Fri 13:07      B-36
smith      Lee Smith            p1              Fri 13:28

C:\>finger @ghi

[ghi.xyz.com]
User       Real Name      What    Idle   TTY    Host       Console Location
doe        John Doe       mail           co     tunes.xyz  Office #314
cort       Fran Cort      sendmai 2:04   *p3    songs.xyz. Test room
```

To display additional user information

Use the **whois** command to display additional information about a user or host. (Note that some hosts do not display expanded information.)

As with the **finger** command, you must specify the hostname (or IP address) in the form *@host.*

```
C:\>whois jkd@vex

[vex.xyz.com]
```

```
Login name:jkd            In real life: John K. Doe
Directory: /u/jkd         Shell: /bin/csh
On since May 31 13:07:53 on ttyp0 from Drain.xyz.com
1 hour 9 minutes Idle Time
Project: To document software.
Plan: Provide required information.
```

2.3 Finding Users on the Internet

If your network interfaces with the Internet, you can use the **nicname** command to identify users or hosts on the Internet. By default, the **nicname** command automatically sends your request to RS.INTERNIC.NET (198.41.0.5). This is the host server for the InterNIC name resolution service. The **nicname** command displays directory listings from the InterNIC for the name that you request.

If the network connection fails or is not immediately available, you may get the following message:

```
net_connect
Connection reset.
```

If you receive this message, you should run the **nicname** command again. Use the **-help** option to display some hints on how to use the **nicname** command.

To search for Internet users using the InterNIC name resolution service

Use the **nicname** command to search the InterNIC name resolution service for a hostname and the coordinator of that host.

Place an asterisk (*) before the hostname to search for registered users on that host, as shown in the following example:

```
C:\>nicname *vex

Connected to 198.41.0.5
[No name] (VEX)
Hostname: VEX.XYZ.COM
Address: 128.127.50.127
System: MICROVAX running ULTRIX
Coordinator:
    Doe, John K. (JKD2) jkd##XYZ.COM
    (323) 555-1010

domain server
Record last updated on 24-Oct-90.
There is one registered user:

Doe, John K. (JKD2)  jkd##XYZ.COM   (323) 555-1010
```

To search for users with their InterNIC handles

The InterNIC “handle” lets you look up users without knowing their host(s). The InterNIC handle appears in parentheses after the user’s full name. To look up a user using a handle, prefix the specified InterNIC handle with an exclamation point (!), as shown in the following example:

```
C:\>nicname !jkd2
```

```
Connected to 198.41.0.5
Doe, John K. (JKD2)       jkd##XYZ.COM
    XYZ, Inc.
    2 Main Street
    Anywhere, MA 01845

Record last updated on 01-Jan-95.
```

If you do not use the exclamation point, the **nicname** command displays all exact occurrences of the handle as a username, hostname, or last name.

To search for users by first or last name

Use one of the following methods to search the InterNIC name resolution service for a user's first or last name (if you do not know the user's host or handle):

- Prefix the specified username with a period to display matching hostnames and last names:

```
C:\>nicname .lee

Connected to 198.41.0.5
Lee Air Force Base        APDS-II-OS107.AF.MIL          26.5.0.39
Lee, Abra (AG158)         1txlgsc##TACHOST.AF.MIL       (DSN) 555-4673
Lee, Lisa E. (LEL3)       ELee##DDN-WMS.DCA.MIL         (703) 555-9400
Lee, Maynard G. (LMG)     lee##NOSC.MIL                 (619) 555-4788
```

- Remove the period prefix to obtain a longer list of names:

```
C:\>nicname lee
```

The **nicname** command searches for and displays matching usernames as well.

- Add a period suffix to search for every username, hostname, and last name that starts with the specified name:

```
C:\>nicname lee.
```

The **nicname** command displays the longest possible list of related InterNIC entries.

To search with a specific Nicname server

Enter **nicname** followed by the **s** *address* option.

```
C:\>nicname -s 128.127.51.50
```

The **nicname** command sends the request to the server at the address that you specify.

To change your default Nicname server in your PCTCP.INI file

Add the following parameter to the `[pctcp addresses]` section of your PCTCP.INI file:

```
nicname-server= address
```

If multiple Nicname server entries are encountered, **nicname** sends a request to each address in the order listed until a valid response is received.

To override the Nicname server specified in your PCTCP.INI file

Enter **`nicname`** followed by the **`i`** option.

```
c:\>nicname -i
```

The **nicname** command sends the request to the InterNIC name resolution service.

2.4 Finding a PC's Hostname or Internet Address

The **host** command searches for the Internet address corresponding to a character string name.

To find a host's Internet address

Use the **host** command followed by the target hostname:

```
C:\>host vex

by (everything), vex: 128.127.50.127, cname is vex.xyz.com
```

The phrase `by (everything)` indicates that you did not use an option in your command line. You can also specify multiple hostnames and use command line options with the **host** command.

To find the hostname of an Internet address

Use the **host** command followed by the Internet address of the target host:

```
C:\>host 128.127.50.128

by (everything), 128.127.50.128's name is vex.xyz.com
```

On the Internet, this number-to-text database is not as well maintained as the text-to-number database. As a result, the **host** command may not display a canonical name (cname) that corresponds to the Internet Protocol address.

2.5 Displaying Information About Your Network

Use the **inet** command to monitor network traffic and to troubleshoot local network problems.

The **inet** command requires an argument, several of which are useful to the network administrator in diagnosing network performance problems: **arp**, **config**, **debug**, **route**, **stats**, **tcp, and unload**.

Specify the help argument (**inet help)** for a list of arguments to the **inet** command. Specify the version option (**inet version)** if you want to display the version number of your kernel.

Use the **inet config** command to learn about your hardware configuration, network addresses of your routers or domain name servers, and other information.

Use the **inet stats** command to learn about your network interface, IP address, total numbers of packets sent and received sorted by packet type, and other information.

The **inet** command is described more fully in the *Command Reference*.

2.6 Testing the Availability of a Remote Host

The easiest way to test the network is to use the **ping** command. **Ping** tests the connection between two hosts by sending an "echo request." An echo request is a message to the remote host, requesting a response. The **ping** command also displays the time in milliseconds for a response to arrive, and debugging information about the network interface.

If the remote host is active and sends a reply, you know that the network media and IP routers forming the path to that host are working. You can then use other TCP/IP applications on that path.

If a host fails to respond to a network request, it means there has been a failure at one of several points from your PC to the remote host. The host may not be working and is unable to respond, some network or gateway in the path from the user to the host may not be working, or the host may not implement the service that you are requesting.

To test the availability of a remote host

Use the **ping** command and specify the remote host by hostname or IP address:

```
C:\>ping 128.127.50.128

host responding, time = 25 ms

Debugging information for interface wd8003 Addr(6): 00 00 c0 05 93 15
interrupts: 1145 (0 receive, 0 transmit)
packets received: 682, transmitted: 463
receive errors: 0, unknown types: 198
    runts: 0, aligns: 0, CRC: 0, parity: 0, overflow: 0
    too big: 0, out of buffers: 0, rcv timeout: 0, rcv reset: 0
transmit errors: 0
    collisions: 0, underflows: 0, timeouts: 0, resets: 0
    lost crs: 0, heartbeat failed: 463
ARP statistics:
arps received: 13 (10 requests, 3 replies)
    bad: opcodes: 0, hardware type: 0, protocol type: 0
arps transmitted: 3 (3 requests, 0 replies)
3 large buffers; 2 free now; minimum of 0 free
3 small buffers; 3 free now; minimum of 1 free
```

After you install PC/TCP Network Software for DOS, send an echo request to yourself to make sure that the software is installed correctly. Use your IP address as an argument instead of your hostname because hostname translation introduces another variable into the test. Once you have established that the **ping** command is functional, you can send an echo request to a remote host to test your network connection.

Chapter 4
Logging In to a Remote Host

You can log in to a remote host using various communications protocols: tn and tnglass implement the TCP/IP Telnet protocol; rloginvt, rlogingl, and rsh implement the 4BSD Berkeley rlogin protocol.This chapter introduces these remote login programs and describes how to use them. Refer to Chapter 1, Introduction to see if the DOS commands discussed in this chapter are included with the version of the network software that you have.

4.1 Before You Start Using Remote Login

You should ensure that

- You have a user ID and password on the remote system.
- The appropriate login server is running on the remote system.
- You are aware of and can use any network security programs that are installed.
- Your PC hostname is in the /etc/hosts file on any system that you want to log in to using the rlogin protocol (also, although this is not required for Telnet, it can save time in establishing telnet sessions with some systems).

If you are unsure about any of this information, contact the remote host system administrator.

4.2 Deciding Which Login Program to Use

This section briefly describes each of the remote login programs and suggests when and why you might use each one.

Some remote login programs are “terminal emulators”— that is, they translate input from your PC keyboard to a format that the remote host can process. Likewise, they translate output from the remote system to a format suitable for display on your PC. This process is called “terminal emulation” because the remote host interacts with your PC as if your PC were a locally attached terminal.The programs tn and rloginvt are terminal emulators.

Note: Refer to Appendix A, Terminal Emulation and Character Set Tables for more information about using default mappings of PC keys to DEC VT and IBM 3270 keys.

Other programs do not emulate characteristics of any specific terminal and do not translate local input or remote system output. As a result, the terminal type is known as a “glass terminal” or a “dumb” terminal.The programs rlogingl, tnglass, and rsh do not emulate terminal characteristics.

Whether or not a program supports terminal emulation, and what types of terminals it emulates, are just some of the factors that you should consider before using the program.

4.2.1 Using tn and tnglass

An advantage of the **tn** and **tnglass** commands is that they implement the TCP/IP Telnet protocol, which is widely available on IBM mainframes and other systems such as UNIX and VMS hosts.

Choose the **tn** command if

- A Telnet server is available on the remote host.
- An application that you want to run on the remote host expects a DEC VT or IBM 3270 terminal type.

  The tn program negotiates with the remote host to establish the most appropriate terminal type to emulate. However, if an application that you want to use requires a specific terminal type, you can request that terminal type on the login command line. You also can change terminal types from within a DEC VT session.
- You want to create several connections to different hosts from within the same login session (tn supports as many as 10 simultaneous connections).
- You want to be able to transfer files to and from your PC during a login session.

  The tn program has an embedded FTP server that you can enable and disable from within your remote login session.
- You want Kerberos authentication.

  Kerberos adds security by requiring a trusted outside source (a Kerberos authentication server) to verify your identity before you can log in.
- You want to encrypt data.

The **tnglass** command is an implementation of the Telnet protocol that does not do terminal emulation. It establishes a glass terminal type. For reasons why you might use tnglass, see section 4.2.3, Using the Glass Programs.

4.2.2 Using rloginvt, rlogingl, and rsh

The **rloginvt, rlogingl,** and **rsh** commands are implementations of the 4BSD UNIX rlogin protocol. They provide convenient ways to establish a session or execute a command on a remote system. However, their use is limited to remote systems (usually running UNIX) that support the rlogin protocol.

The rlogin protocol has a built-in authentication system that makes it possible to log in to a remote host without supplying a username and password. When a user attempts to log in, the remote login server scans two files on the target system: /etc/hosts.equiv and .rhosts.Hostnames and account names listed in either of these two files are considered to have security levels equivalent to that of the target system, and the user can log in without supplying a password.

This is a convenient way for users and programs to execute commands on a remote system. If you are concerned about security, however, do not use the /etc/hosts.equiv or .rhosts authentication system.

If neither of these files contains information about your PC, the rlogin programs still work. The remote login server verifies your username in the /etc/passwd file (the username is either taken automatically from your PCTCP.INI `user=` parameter or specified by you on the command line). Then the server prompts you for a password.

Choose the **rloginvt** command if

- The remote host supports the rlogin protocol.
- An application that you want to run on the remote host expects a DEC VT terminal type.

  By default, the **rloginvt** command establishes a DEC VT220 terminal type. You can change to other VT terminal types from within your login session.
- You want to create several connections to different hosts from within the same login session (**rloginvt** supports as many as 10 simultaneous connections).
- You want to be able to transfer files to and from your PC during a login session.

  The rloginvt program has an embedded FTP server that you can enable and disable from within your remote login session.
- You want Kerberos authentication.

  Kerberos adds security by requiring a trusted outside source (a Kerberos authentication server) to verify your identity before you can log in. Without Kerberos, the rloginvt login procedure can be slightly less secure than with tn, depending on how you configure the files used by the rlogin software on the remote system. With Kerberos, both rloginvt and tn offer a more secure login mechanism.

The **rsh** command lets you execute a single command on a remote host from your PC. The **rsh** command does not do terminal emulation because the connection lasts only as long as it takes for

the command to execute. This command is useful if you want to accomplish simple tasks on the remote host without logging in.

The **rlogingl** command uses the rlogin protocol to establish a session with a remote host, but does not do terminal emulation unless you request it. By default, the rlogingl program establishes a glass terminal. However, you can request emulation of a DEC VT terminal type on the command line. For reasons why you might use rlogingl, see section 4.2.3, Using the Glass Programs.

4.2.3 Using the Glass Programs

The **rlogingl** and **tnglass** commands are useful when you want to

- Connect to a remote host using nonstandard display cards or other nonstandard (or unsupported) terminals.
- Redirect a Telnet connection through a serial communications port on your PC to another device (like another terminal or a line printer) with the DOS **ctty** command.
- Use a terminal emulator that loads as a DOS console driver.
- Use a commercial terminal emulator through the Interrupt 14 interface.

4.3 Logging In

To log in using **rlogingl, rloginvt**, **tn**, or **tnglass**, type a command in the form

commandname host

where

commandname is your choice of remote login command

host is the name or Internet address of the remote host.

In addition to the hostname, many other command line options are available, only some of which this chapter discusses. See the *Command Reference* for complete details on options and syntax.

With tn and tnglass, the remote host typically prompts you for a user ID and password. Supply the user ID and password for your account on the remote host. Following the appropriate password verification and negotiation of terminal characteristics, your session is established and you can begin working on the remote host.

The rloginvt and rlogingl programs do not prompt for a user ID. They automatically pass the remote host the value of the `user=` parameter in the `[pctcp general]` section of your PCTCP.INI file. If you have not configured a username in this parameter, a login prompt appears, and you can supply any valid user ID listed in the /etc/passwd file on the remote host. You also can override the `user=` parameter by supplying an alternative username on the command line.

For example, the following command requests an rloginvt session as user guest on host vex.xyz.com:

```
C:\>rloginvt vex.xyz.com guest
```

The **rlogingl** and **rloginvt** commands do prompt you for a password, unless your PC name and user ID exist in the /etc/hosts.equiv or .rhosts files on the remote host (FTP Software recommends against storing information about your PC in these files). Following the appropriate authentication checks and negotiation of terminal characteristics, your remote session is established.

4.3.1 Logging In Using a Default Command Line

The **tn** command lets you specify a default login command line as the value of the `cmdline=` parameter in the `[pctcp tn]` section of your PCTCP.INI file. Include the name of the remote host to connect to and any command line options that you want to use. Then type the **tn** command to start a session.

4.3.2 Logging In Using Kerberos Authentication

The **rloginvt** and **tn** commands support the use of Kerberos Version 4 authentication. Kerberos adds an extra level of security by verifying your identity through a trusted outside source.

Before you can use Kerberos with the remote login programs, issue the **kinit** command to obtain a Kerberos "ticket-granting ticket." Then when you use a remote login command, the remote login program contacts a Kerberos authentication server and obtains a "service ticket." The service ticket lets you run the program as a user whose identity has been authenticated.

If the remote host that you are logging in to is in a Kerberos realm outside of your default realm, you must obtain authentication from the remote host's realm. Use the **-k** *realm* option on the **rloginvt** or **tn** command line to specify the realm name. The following example command uses tn to log in to the remote host grapes.xyz.org and specifies that Kerberos authentication should be obtained from the realm fruit.xyz.org:

```
C:\>tn -k fruit.xyz.org grapes.xyz.org
```

The **tn** command lets you use PCTCP.INI file parameters to control how authentication works when you start **tn**. Use the `authentication=` parameter in the `[pctcp tn]` section to specify whether or not you will use Kerberos authentication if the remote host requests it.

Set this parameter to `enabled` if you have properly configured Kerberos; Kerberos grants a ticket-granting ticket before you start **tn**. Set this parameter to `required` if you want **tn** to attempt a normal login if Kerberos authentication fails. This setting ensures maximum security; you can log in only if Kerberos authentication succeeds.

4.4 Using Escape Commands

All of the remote login programs include a set of subcommands, or “escape” commands, that perform various management functions. To use escape commands, press an escape key to suspend the remote session, then you can enter an escape command. Escape commands consist of single characters and are case sensitive.

Program	**Escape Key**
rloginvt	F10 or Alt+F10
tn	Alt+F10 (or F10 in DEC VT mode)
rlogingl	Ctrl+6
tnglass	Ctrl+6

Note: If you use a commercial terminal emulator with rlogingl or tnglass, you cannot use the Ctrl+6 escape key. Use the escape key, if any, provided by the emulator that you are using.

4.5 Getting Online Help

To see the correct syntax and usage of any of the remote login commands while at the DOS prompt, enter a command in the format

commandname **-?**

where *commandname* is any of the remote login commands.

Once you are logged in to a remote session, you can see an online list of the escape commands.

To see	**Press**
A list of escape commands	Escape key followed by **?**
A list of Ctrl+ escape commands (rloginvt and tn only)	Escape key followed by Ctrl+h

4.6 Logging Out

The best way to end a remote login session is to enter `logout` or press Ctrl+D. Typically, the remote host then closes the connection automatically. If you have difficulty closing a connection, you can use the escape commands shown in Table 4-2. Do not type the comma; it indicates a sequence of keystrokes. First type the escape key sequence, then type the escape command.

Note: tn accepts F10 as well as Alt+F10 from the DEC VT emulator.

Table 4-1 Escape Commands for Closing Connections

	Escape commands			
Tasks	**rlogingl**	**rloginvt**	**tn**	**tnglass**
Close connection gracefully	Ctrl+6, c	F10, c	Alt+F10, c	Ctrl+6, c
Quit without gracefully closing the current connection	Ctrl+6, q	F10, q	Alt+ F10, q	Ctrl+6, q
End all connections without closing gracefully			Alt+F10, Q	

The **c** escape command causes the login program to close the connection "gracefully" (that is, the local and remote host acknowledge the closing to one another). The **q** command resets the current connection without closing it; this is not a graceful way to end your session. The **Q** command resets all existing connections without closing them gracefully. Use the **q** or **Q** command only when you cannot log out at the system prompt or by using the **c** command.

If you use the **q** or **Q** command, or if you exit from a remote session in some other abrupt way, such as by turning off your PC, the remote host may not be aware that your session has ended. If you later attempt to log in to that host from the same PC, you might encounter interference from the unclosed connection. (After a period of inactivity, the host may eventually end your session and close the connection.)

4.7 Creating and Managing Multiple Connections

With rloginvt and tn, you can open as many as 10 connections to the same remote host or to several hosts. Table 4-3 summarizes the escape commands that you can use to create and manage multiple connections. First type the escape key sequence, then type the escape command.

Note: tn accepts F10 as well as Alt+F10 from the DEC VT emulator.

Table 4-2 Escape Commands for Creating and Managing Connections

	Escape commands	
Tasks	**rloginvt**	**tn**
Create or switch to another connection	1. Press F10	1. Press Alt+F10
	2 . Type a number 09	2. Type a number 09
Switch to next active connection		1. Press Alt+F10
		2. Press Enter
Display list of open connections	1. Press F10	1. Press Alt+F10
	2. Press Ctrl+s	2. Press Ctrl+s
Display status of current connection		1. Press Alt+F10
		2. Press Ctrl+t

4.7.1 Before You Create Multiple Connections

If you plan to create multiple connections and also to use the embedded FTP server, you may need to configure more TCP connections in the TSR kernel. You must have one TCP connection for each remote login session, and at least two TCP connections to activate the embedded FTP server. This is an advanced topic that may require consultation with your system manager.

To create a new connection

1. Press the escape key.
2. At the `Command:` prompt, type any unused number 1–9.

   When you log in, your initial connection is always numbered 0. If you are unsure which numbers are in use, use the **Ctrl+s** escape command to see a list of current connections. Then enter a number that you do not see in the list.

   This message appears:

   ```
   No connection. Host to connect to?
   ```

3. Enter the name of the host to which you want to connect.

   Along with the hostname, include any command line options that you want to use for the new connection; options that you specify for the first connection do not carry over automatically to subsequent connections.

   In tn, if you have configured a default command line as the `cmdline=` parameter in the `[pctcp tn]` section of your PCTCP.INI file, press the Enter key to connect to the host that the default command line specifies.

If multiple connections exist, you also can create a new connection after logging out of an existing one. To do so,

1. Log out of your current connection.

   You see a message similar to this:

   ```
   Connection #0 closed.
                 Listing of all current connections
       Connection #                 Host connected to
              1      in 3270 mode   vex.xyz.com


   Type # of connection to switch to (or press ENTER):
   ```

2. Enter a new number to create a new connection.

   –or–

   Type the number of an existing connection to return to that one. (In this example, typing `1`

returns you to the session on vex.xyz.com.)

4.7.2 Displaying a List of Connections

Once you have established several connections, you can view a list of them. Displaying a list and selecting from the list also is an easy way to switch to an existing connection whose number you do not remember.

To see a list of existing connections

Enter the **Ctrl+s** escape command.

The following is sample output from the **Ctrl+s** escape command:

```
     Listing of all current connections
Connection #                 Host connected to
       0                     fred.xyz.com
       1      in 3270 mode   vex.xyz.com
           Active connection is connection #1
              Local FTPSERVER off
[Press SPACE to return to session, or enter another command
(? for help)]
```

4.7.3 Switching to an Existing Connection

Switch to an existing connection in one of the following ways:

- Press the escape key, then type the number of the connection that you want to switch to.
- If you do not remember the number of the connection that you want to switch to, use the **Ctrl+s** escape command to display a list of all connections. Type a number from the list; the remote login program switches to the connection with that number.
- Log out of your current connection. You see a display of remaining connections and their numbers; type the number of the connection that you want to switch to.
- In tn only, you can simply press the escape key, followed by the Enter key, to switch to the next connection in a list of open connections.

  For example, if you have connections numbered 0, 1, and 2, and you are currently at connection 1, press the escape key, then the Enter key to switch to connection 2.

  Once you are at connection 2, repeating this procedure switches you to connection 0.

4.7.4 Viewing Information About an Existing Connection

Use the **Ctrl+t** escape command to view information about the current connection. The **Ctrl+t** command displays information about a variety of session and terminal characteristics, including

- Connection number.
- Current terminal type and last requested terminal type.
- Whether the connection is in local or remote echo mode (VT only).
- Whether the auxiliary keypad is in application or numeric mode (VT only).
- Whether data is being exchanged in 7-bit or 8-bit format (VT only).
- Whether Yale-style null processing is on or off (3270 only).
- The number of the active DOS code page (tn supports code pages 437 and 850).
- Whether the embedded FTP server is enabled or disabled.
- Whether keystrokes are being sent to DOS as well as to the remote host.
- Whether an input file or output file is open.
- Whether the local host is sending encrypted or unencrypted data.
- Whether the remote host is sending encrypted or unencrypted data.

4.8 Exchanging Files and Data

The remote login programs offer several ways to transfer files and manage data during a remote login session. Table 4-4 summarizes the escape commands available for performing these tasks. Do not type the comma; it indicates a sequence of keystrokes. First type the escape key sequence, then type the escape command.

Note: tn accepts F10 as well as Alt+F10 from the DEC VT emulator.

Table 4-3 Escape Commands for Exchanging Data

	Escape commands			
Tasks	**rlogingl**	**rloginvt**	**tn**	**tnglass**
Enable FTP Server		F10, F	Alt+F10, F	
Disable FTP Server		F10, F	Alt+ F10, F	
Enable or disable Write-Protect mode on FTP server		F10, W	Alt+F10, W	
Read a file as input to the remote host command line	Ctrl+6, i	F10, i	Alt+F10, i	Ctrl+6, i
Record your session in a file on your PC	Ctrl+6, o	F10, o	Alt+F10, o	Ctrl+6, o

4.8.1 Enabling the Embedded File Transfer Server

The rloginvt and tn programs have an FTP server embedded in them. The **F** escape command enables this FTP server on your PC, letting you transfer files between your PC and a remote host without leaving the remote login session.

In the context of interactions with the embedded FTP server, your PC becomes the remote host. Thus, remote **ftp** commands apply to your PC, and local **ftp** commands apply to the host to which you are connected. For example, to transfer a file from a remote host to your PC during a remote login session, you can

1. Use the **F** escape command to enable the embedded FTP server on your PC.
2. Use the **ftp** command on the remote host to create an ftp connection to your PC.
3. Use the **ftp put** command to transfer the file from the remote host to your PC.

While the FTP server is enabled on your PC, its use is not limited to your remote login session. You can control others' ability to use the embedded FTP server by creating a password file: users whose names are not in the password file are prevented from logging in.

The **tn** command lets you control the embedded FTP server from your PCTCP.INI file.

To enable the FTP server automatically every time that you start tn

Set the `ftpsrv=` parameter in the `[pctcp tn]` section of your PCTCP.INI file to `on`.

4.8.2 Disabling the Embedded File Transfer Server

An enabled FTP server continues to run even after you change connections. Closing the last connection turns the FTP server off and terminates all existing connections. In tn and rloginvt, you also can disable a running server during a remote session by using the **F** escape command. Disabling the server prevents new connections, but does not terminate existing connections.

To prevent existing connections from writing or deleting files

Enable write protection with the **W** escape command.

The **tn** command lets you control the embedded FTP server from your PCTCP.INI file.

To specify that you do not want the FTP server to start automatically when you start tn

Set the `ftpsrv=` parameter in the `[pctcp tn]` section of your PCTCP.INI file to `off`. Once a tn session is established, you can still enable and disable the FTP server using the **F** escape command.

To prevent the server from being enabled during a tn session (for security reasons, for instance)

Set the `ftpsrv=` parameter to `never`.

4.8.3 Controlling Write-Protect Mode on the FTP Server

The **W** escape command enables or disables write protection for the FTP server (by default, write protection is disabled). Write protection means users can read files, but they cannot write or delete files. The command does not affect transfers in progress. If the FTP server is running when you turn write protection on, the write protection applies to all current and subsequent connections. If the FTP server has never been enabled, the command has no effect. In tn and rloginvt, if the FTP server was previously running and is now disabled, enabling write protection affects the remaining connected users.

4.8.4 Sending Input to the Remote Host Command Line

The rlogin and telnet programs let you send the contents of a file on your PC as input to the remote host, as if you typed the file contents there.

Using an input file is a convenient way to execute several commands or perform several tasks, in a manner similar to using a batch file on your PC.

To send a file as input to the remote host

Use the **i** escape command. Enter a filename in response to the prompt.

The contents of the file are transferred to the remote host command line exactly as if you typed and entered them there.

When the remote login program is finished transferring the contents of the input file, it displays the following message on the status line:

```
File input done
```

With rlogingl and tnglass, you must then press the Enter key to return to the remote host's command prompt. Otherwise, the remote host may continue processing your keystrokes as input even after the input file on your PC is closed.

Some hosts support redirecting the input file contents to another file on the remote host. For example, if you issue the command **cat > frommypc** while logged in to a UNIX host, then use the **i** escape command and the name of a local file TEST, you transfer the contents of TEST FROMMYPC on the remote host. Press Ctrl+D to end the input redirection on the remote host.

The **i** escape command works only with ASCII data. Also, in 3270 emulation mode, tn does not support the use of input files.

4.8.5 Recording Your Session in an Output File

The **o** escape command lets you record a transcript of your remote login session in a file on your PC. You are prompted for the name of a file in which to store the data. If you supply the name of an existing file, the output from the remote session overwrites the file's current contents. You also can specify a device such as a printer as the output destination. If you change connections while an output file is open, the file remains open and continues to create a record of subsequent connections until you enter the **o** escape command a second time.

In a session using 3270 emulation, the output file records remote system output in the form of a hexadecimal EBCDIC dump, with characters translated to printable ASCII and enclosed by asterisks in a column to the right. The hexadecimal values FF EF represent a Telnet IAC (Interpret as Command) End-of-Record (EOR) command. These codes indicate the end of a 3270 data stream (and potentially the beginning of another). The hexadecimal values that correspond to 3270 data stream orders are represented in the output file as two-character abbreviations for the order names. Table 4-5 shows the substitutions made in the output file for each hexadecimal value.

Table 4-4 Output File Substitutions

This 3270 data stream order	**With this hexadecimal value**	**Has this two-letter code in the output file**
Program Tab	0x05	PT
Graphics Escape	0x08	GE
Set Buffer Address	0x11	SB
Erase Unprotected to Address	0x12	EU
Insert Cursor	0x13	IC
Start Field	0x1D	SF
Set Attribute	0x28	SA
Start Field Extended	0x29	SE
Modify Field	0x2C	MF
Repeat to Address	0x3C	RA

Output from a session using VT emulation is in regular ASCII form. The output file does not record messages displayed by escape commands.

When you change connections or create a new connection, the output file remains open and continues to create a record of subsequent connections, until you enter the **o** escape command a second time. The output file indicates where new connections and connection changes occurred.

4.8.6 Using DOS Redirection with the Glass Programs

In addition to using the **o** escape command, you can use the DOS feature of redirecting output to a file to capture a transcript of a tnglass or rlogingl session. For example, if at the DOS prompt you enter a command in the following form,

tnglass *host >> filename*

the output from your keyboard and from the remote host goes to the file named by *filename* instead of to your screen. Your screen remains blank until you end the tnglass connection.

4.9 Managing Local Session Characteristics

In rloginvt and tn, you can use escape commands to control certain local aspects of your terminal emulation environment. Table 4-6 summarizes the escape commands that perform these session management tasks. Do not type the comma; it indicates a sequence of keystrokes. First type the escape key sequence, then type the escape command.

Note: tn accepts F10 as well as Alt+F10 from the DEC VT emulator.

Table 4-5 Escape Commands for Managing Local Session Characteristics

	Escape commands	
Tasks	**rloginvt**	**tn**
Enable status line display	F10, U	Alt+F10, U
Disable status line display	F10, u	Alt+ F10, u
Allow use of a pop-up program		Alt+F10, s
Prevent inappropriate activation of a screen saver program		Alt+F10, S

Additional escape commands are available to customize specific terminal characteristics during your remote login session.

4.9.1 Enabling or Disabling the Status Line

The rloginvt and tn programs display a status line at the bottom of your terminal screen to indicate the name of the host to which you are connected and the time of day. Other messages and codes also appear on the status line in response to certain escape commands. The status line is on by default, but you can turn it off with the **u** escape command.

To turn on a disabled status line

Enter the **U** escape command.

The **tn** command lets you use a parameter in your PCTCP.INI file to control the display of the status line.

To automatically prevent display of the status line each time that you start tn

Set the `status=` parameter in the `[pctcp tn]` section to `off`.

To display the status line automatically

Set the `status=` parameter in the `[pctcp tn]` section to `on`.

4.9.2 Using Pop-up Programs During a Remote Session

A pop-up program is a type of terminate-and-stay-resident (TSR) application that resides in your PC's memory but remains invisible until you press a key or key combination, called a "hotkey," to activate it.

To use a hotkey to enable a pop-up program from within a remote tn session

Enter the **s** escape command.

The emulator prompts you for the hotkey and sends the next key or key combination that you press to DOS only. If the key is recognized as a hotkey for a pop-up program, the program starts (pops up). If not, the emulator sends the keystroke to the remote host.

When you exit from a pop-up that you have activated, the emulator also sends the next keystroke that you type to DOS. This lets you directly start another pop-up program, or restart the same program, without having to enter the **s** command again. If the first key that you press after exiting from the pop-up is not recognized as a hotkey, the emulator resumes sending keystrokes to the remote host.

4.9.3 Using Screen Savers During a Remote Session

If you are running a screen saver program on your PC, it may activate inappropriately during a remote login session. The reason is that a screen saver detects your activity through keystrokes passed to DOS. Normally, during a remote login session, the terminal emulator does all of the processing and therefore does not pass keystrokes to DOS.

The **S** escape command enables or disables the passing of keystrokes to both DOS and the remote host. Passing keystrokes to DOS as well as to the remote host prevents inappropriate activation of a screen saver during your remote session. However, when keystrokes are being passed to DOS, pressing a key that is recognized as a hotkey for a pop-up program activates the pop-up.

To prevent unwanted activation of a pop-up

Enter the **S** escape command to disable passing of keystrokes to DOS.

Press the key that would otherwise be recognized as a hotkey, and then enter the **S** command again to resume sending keystrokes to both DOS and the remote host.

The **tn** command lets you use a parameter in your PCTCP.INI file to specify whether you want to use a screen saver during your tn session.

To prevent a screen saver from activating inappropriately during your remote login session

Set the `screen-saver=` parameter in the `[pctcp tn]` section to `yes`. This causes tn to send your keystrokes to both DOS and the remote host.

4.10 Using DOS Commands During a Remote Session

All of the remote login programs support the ability to use DOS commands without terminating the remote session. This is useful if you want to temporarily do work on your PC, then return to your remote session.

To start a nested DOS command interpreter

Type the appropriate escape key sequence followed by the **!** escape command.

To return to the remote session

Type **`exit`** at the DOS prompt.

If an embedded FTP server is running when you use the **!** escape command, it is suspended during the escape to the DOS command interpreter. When you exit from DOS, the FTP server reactivates and any transfers in progress continue.

4.11 Printing Screen Output

The tn and rloginvt programs support sending screen output to a printer connected directly to your PC. From both DEC VT and IBM 3270 terminal emulators, you can print a copy of the current screen display. In addition, the DEC VT emulator lets you enable and disable the continuous printing of each line sent from the remote host to your PC screen.Table 4-7 lists the key combinations used to print screen output.

Task	**rloginvt Key Sequence**	**tn Key Sequence**
Print current screen display	Shift+PrtSc	Shift+PrtSc (3270 or VT) or PrtSc (3270 only)
Turn continuous screen printing on or off	Ctrl+PrtSc or PrtSc	Ctrl+PrtSc or PrtSc (VT only)

4.12 Using Emulators with Glass Login Programs

This section describes how to use terminal emulators with the glass login programs. With rlogingl, you can request DEC VT terminal emulation on the login command line. Also, you can use both rlogingl and tnglass in conjunction with any commercial emulator that conforms to the IBM PC BIOS Interrupt 14 interface.

For additional information about glass terminal emulation and the IBM PC BIOS Interrupt 14 interface, see the following resources:

- Anonymous FTP server ftp.ftp.com
- Technical Support Bulletin Board System at (508) 659-6240, using a modem

4.12.1 Using VT Terminal Types with rlogingl

You can use the glass login programs with a DEC VT emulator.

To request emulation of a VT terminal type with rlogingl

Use the **-tt** option on the login command line.

Specify the option in the form **-tt** *type* where the value of *type* can be `vt220`, `vt100`, or `vt52`. Terminal type keywords are case sensitive.

The following example command requests a glass login session with VT220 terminal emulation on the remote host vex.xyz.com:

```
C:\>rlogingl -tt vt220 vex.xyz.com
```

4.12.2 Using Other Commercial Emulators with rlogingl and tnglass

You can use both the rlogingl and tnglass programs with any commercial terminal emulator that supports the IBM PC BIOS Interrupt 14 interface.

To specify the full pathname of an emulator program, together with command arguments the emulator needs at startup

Use the **-e** *emulator command_list* option on the login command line.

For example, to make a Telnet connection to the host green.xyz.com using a terminal emulator with the filename ST240.EXE in the directory \TERM, enter this command:

```
C:\>tnglass green.xyz.com -e \term\st240.exe
```

For more information on the commercial terminal emulator types available, contact FTP Software, Inc.

4.13 Executing a Single Command with rsh

The **rsh** command lets you execute a single command on a remote system from your PC without having to log in. The basic command syntax is

rsh *host commandline*

where

host is the name or Internet address of the host where you want to execute the command.

commandline is the command.

The remote command should be last on the line, after any **rsh** command line options.

Like rloginvt and rlogingl, rsh uses the rlogin authentication protocol. The **rsh** command sends the remote host the value of the `user=` parameter in your PCTCP.INI file. If you do not have a value for that parameter configured, the **rsh** command does not work. You can override the `user=` parameter with the **-l** *userid* option on the **rsh** command line.

Kerberos authentication is optionally available with the **rsh** command. If Kerberos is configured on your PC, the **rsh** command first attempts Kerberos authentication. If that fails, the command uses the rlogin protocol to verify your identity, and prompts you for a password if necessary. Because Kerberos authentication eliminates the need to prompt for user information, using the **rsh** command with Kerberos is a convenient way to execute multiple remote commands from batch files on your PC.

The following sample **rsh** command requests a listing of files from the user's home (login) directory on the remote host grapes.xyz.org:

```
C:\>rsh grapes.xyz.org ls -l
```

4.14 Troubleshooting Remote Login

This section provides solutions to situations that you might encounter when using remote login programs. The situation is described first (including any messages that you see), followed by the meaning of the situation and the action to take.

The remote login program times out when you attempt to log in.

The remote host may not be responding.

Use **ping** to confirm that the host is running and available on the network.

Make sure the appropriate server is running on the remote host.

The `Password:` prompt is truncated to `rd:` during an attempt to start an rloginvt session.

This anomaly occurs with some 4BSD UNIX hosts but does not affect the remote login session. You can still enter your password at the `rd:` prompt and continue the session.

During an attempt to create a tn session with 3270 terminal emulation, you receive the following message:

```
Could not allocate storage for 3270 emulator.
```

Not enough memory is available to use 3270 emulation. The tn program creates the new connection, but uses VT220 type terminal emulation instead of 3270 emulation. (An IBM 3270 terminal emulator requires twice as much memory as a VT220 emulator.)

The remote IBM host behaves as if the connection is using the Telnet standard Network Virtual Terminal (NVT) type. NVT implements a set of common terminal characteristics that are actually a subset of VT220 terminal emulation.

During an attempt to create a tn session with DEC VT emulation, you receive the following message:

```
Could not allocate storage for new emulator.
```

Not enough memory is available to use VT emulation, and tn cannot establish a connection.

Free some memory on your PC and try again.

Your screen updates slowly during a remote login session.

If you are printing screen output or capturing output to a file, there may be a slow disk or a congested network connection.

The situation could also be due to a difference in data capacity between your PC and the remote host. Network interfaces for many larger systems can store more data in a buffer than PC interfaces. This can result in overruns in the exchange of data between the two systems. Overruns can affect performance on a UNIX

system host because it must retransmit lost data later.

To increase the capacity of your PC to handle network data, adjust the `window=` parameter in the `[pctcp kernel]` section of your PCTCP.INI file.

You cannot print screen output with the Print Scrn or Ctrl+Print Scrn in tn.

If you are using an IBM PC, a terminate-and-stay-resident (TSR) module may be interfering with the print capability. If you cannot use the screen printing feature even when no other TSR modules are loaded, contact your OnNet or PC/TCP supplier for help.

If you are using an IBM PC-compatible machine, your hardware may not support this screen dump capability. Contact your PC supplier for help.

After pressing the Print Scrn key in a tn session, you receive the following message: `PRINTER ERROR: Abort, Retry, or Ignore?` The screen display then slows down considerably.

Enter **`A`** to abort, **`R`** to retry, or **`I`** to ignore.

The rloginvt or tn program does not display all of the multilingual characters that you expect to see during a terminal emulation session.

DOS uses a set of characters called a "code page" to determine the characters to display on your screen. If you do not see all the characters that you expect, you may need to install or change to a different code page.

To verify the code page currently in use, enter the **p** escape command. A message indicates the current code page and prompts for a new one. The rloginvt and tn programs support the use of code pages 437 and 850; code page 850 contains more special and multilingual characters than code page 437. If the code page is currently 437, enter **`850`** at the prompt.

If you still do not see the characters that you expect to be available with code page 850, exit from the program and set up the code page support using DOS commands. Changing code pages from within rloginvt or tn works only if the code pages have been previously installed and set up in DOS. See your DOS documentation for details.

Pressing the left Shift key during a tn session causes your PC's bell to sound.

This typically occurs with users who are running DOS version 5.0 and using a European keyboard. The KEY.COM program intercepts the scan code for the key and causes the bell to sound.

Set the `screen_saver=` parameter in the `[pctcp tn]` section of your PCTCP.INI file to `yes` to prevent this problem automatically every time you start tn.
–or–
Press Alt+F10, S to solve the problem for the duration of your current session.

You also can avoid this problem by replacing the DOS Version 5.0 KEYB.COM

and KEYBOARD.SYS files with 3.0 versions.

Your keyboard locks after you press an attention identifier key during 3270 emulation.

The keyboard is locked because the remote host has not replied.

Use the Reset key (by default, this is Ctrl+F9 on your PC keyboard) or the Master Reset key (Ctrl+F10) to unlock the keyboard.

In changing from one connection to another, you receive a message in the following format:

```
Could not save screen for connection #n
```

When you change from one connection to another, lack of memory sometimes prevents the tn program from saving the screen image for the current connection. The connection is still open and usable. If you change back, you see another message, in the following format:

```
Could not restore screen for connection #n
```

You are unable to see a record of activity prior to the connection change, but subsequent keyboard input or remote system output appears on the screen.

Your screen blanks or behaves strangely during an rlogingl, rloginvt, or tn session.

This can occur if you are using an unsupported SuperVGA card and the program attempts to determine what kind of video adapter you have. SuperVGA cards lack standardization in control techniques, so methods that control one card may cause another card to stop working.

This software has been explicitly certified for use with these VGA cards:

1024 VGA (Boca Research Inc.)
18800, VGAWONDER (ATI Technologies Inc.)
6400, SuperVGA (Genoa Systems Corporation)
82C452 (Chips & Technologies Inc.)
CL-GD510, CL-GD520 (Cirrus Logic Inc.)
Compaq Triton (Compaq Computer Corp.)
HT-208 (V7VGA), Vid Sev VGA 1024 (Headland Technology Inc.)
MaxVGA (MaxLogicSystems Inc.)
Poach 51 (ZyMOS Corporation)
Speedstar Plus (Diamond Computer Systems Inc.)
TVGA 8800 (Trident Microsystems Inc.)
V5000, VGA (Ahead)
VGA (TrueTech Inc.)
Viewpoint VGA (Everex Systems Inc.)
WD90C00 WD Paradise VGA 1024 (Western Digital Imaging)

If your SuperVGA card is not in the above list, and you suspect that it is giving you problems, set the card= parameter equal to vesa in the [pctcp screen] section of your PCTCP.INI file. This causes the affected application to bypass attempts at identifying your video card.

The connection to a remote host closes automatically after you have not been using it for some time.

The remote login programs do not control this behavior. Whether you are logged out automatically, and after how long, depends on the configuration of the remote host.

The remote host system administrator may be able to change this behavior.

The connection to a remote host closes unexpectedly while you are using it.

If more than one system on your network has the same address, data from the remote host can be directed to the wrong system, and this can cause your Telnet session to end.

Verify that your system’s IP address is unique.

4.14 Troubleshooting Remote Login

Chapter 7
Printing to a Network Printer

This chapter introduces options for network printing and describes how to use the printing methods available to you in DOS to send files to a printer that is not directly connected to your PC.

Printing services available with PC/TCP Network Software come in two basic categories:

- Network print commands, which send a file directly across the network to a print server system.
- Print redirectors, which intercept data that is targeted for a specific port, such as LPT1, and send the data across the network to a print server instead.

The network software includes two network print commands:

- The **lpr** command sends files to print servers running the Berkeley UNIX line printer daemon (LPD).
- The **iprint** command sends files to an IMAGEN printer. IMAGEN printers are directly connected to the network. They have their own IP addresses and are not managed by a print server system.

The DOS commands **iprint** and **predir**, which are discussed in this chapter, are not available with all versions of the network software. Refer to Chapter 1, Introduction for more information.

Note: In addition to the methods of print redirection discussed in this chapter, you can also use InterDrive client software for print redirection if you have access to Network File System (NFS) servers running PCNFSD software.

Figure 7-1 shows the path of a file that is printed using the **lpr** command.

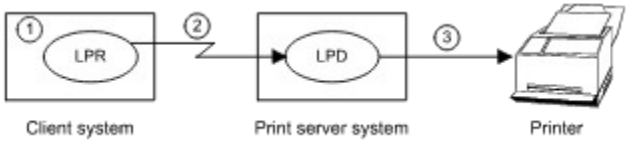

Figure 7-1 Printing with a Network Print Command

The figure illustrates the following steps:

1. On the client system, the user enters the **lpr** command at the system prompt.
2. The **lpr** command sends the file across the network to a print server system where an LPD is running.

3. The LPD queues the file to a printer that is physically connected to the server system.

Network print commands are convenient because they are easy to use and require no advance configuration. You enter a network print command each time that you want to send a file to print. You can specify any available print server and printer on the command line.

The network software offers three print redirection applications:

- The **predir** command redirects print jobs from DOS applications to most types of network printers.
- The Network Driver lets you configure and manage print redirection in Windows. It allows you to send files to an LPD print server, an NFS print server, or a print program.

Print redirectors are convenient because, once you have configured and loaded them, they are no longer visible to you. You configure print redirection by creating a logical association between a local port name and a network printer. Then, when you choose a print option from an application menu, the print redirector automatically sends the output to the network printer associated with the port to which you are printing.

You also can use **predir** and the Network Driver to redirect output to a file containing a command or series of commands. In this way, you can use the redirector to do other processing in addition to (or instead of) printing the file. For example, if you write a document using a text markup language, you can create a batch file to run a text processor on the document before sending it to the printer.

For guidelines on when and why it is appropriate to use the various printing commands, see section 7.1, Choosing a Printing Method. If you already know what printing services you want to use, go on to the remaining sections in this chapter, which describe

- How to use **lpr** and related commands for managing print jobs.
- How to redirect printing with **predir** and related commands.
- What to do when you encounter unexpected situations and how to respond to messages from the printing commands.
- Where to find more information about network printing.

See the *Command Reference* for details on using the **iprint** command.

7.1 Choosing a Printing Method

You can use the network print commands at any time regardless of whether you are using print redirection. However, if you send files frequently to a network printer, you will probably find it convenient to configure a print redirector. Choosing the best print redirection method depends on several factors, including

- Whether you most frequently print from DOS or from Windows, or a combination of both.
- What software is available on the print server.
- The number and variety of printers that you want to use.
- The disk space and memory available on your PC.

The following table summarizes the recommended use of print redirection options, based on the environment in which you normally print and the software that is available to you on the remote print server:

Primary Printing Environment	**Print Server**	**Recommended Method**
DOS	NFS (PCNFSD)	InterDrive client software
	LPD	**predir** command
Windows	NFS (PCNFSD)	InterDrive client software in combination with the Network Driver
	LPD	Network Driver
Both DOS and Windows	NFS (PCNFSD)	InterDrive client software (from DOS) or InterDrive client in combination with the Network Driver (from Windows). Print connections established in DOS are usable by Windows applications, and vice versa. Configure them using the environment that you prefer.
	LPD	**predir** to redirect one port for use by DOS applications. Use **predir** only from DOS; not from a DOS session in Windows. Network Driver to redirect other ports for use by Windows applications.

Note that if you want to alternate between a Windows environment and a pure DOS environment

(exiting from Windows) while retaining InterDrive or **predir** print connections, you must use the TSR version of the kernel and InterDrive.

With the VxD kernel and InterDrive, DOS applications and commands are available from within a DOS session in Windows only. The VxD kernel (and thus the network) unloads when you exit from Windows.

If you are able to choose what software runs on the print server, consider the features and benefits of each printing option as well.

7.1.1 Using predir

The **predir** redirector is convenient if you are primarily a DOS user. You can use it to print to the **lpr** command or to any other printing program or batch file on your system. Consider these other factors:

- The **predir** command requires about 10K of conventional memory.
- You can redirect only one port with **predir**, and it must be a parallel (LPT) port.
- Print connections that you establish in DOS are available to you only in DOS. FTP Software does not support the use of **predir** from a DOS session in Windows. Results can be unreliable, especially when you redirect other ports in Windows using the PC/TCP Network Driver.
- The **predir** redirector stores its print spool file locally, whereas InterDrive stores the spool file on the print server. This might be a consideration if you have very limited disk space and frequently print large files.

7.2 Printing with the lpr Command

Use the **lpr** command to send files directly to a print server running the Berkeley UNIX line printer daemon (LPD). A single LPD print server can control one or more printers, hold several files in a job queue, and send jobs in the order received to a printer that you specify.

In addition to the **lpr** command, other commands are available to monitor and manage print jobs.

To do this	**Use this command**
Send files to the printer	**lpr**
Monitor the status of print jobs	**lpq**
Remove a print job from the queue	**lprm**

7.2.1 Before You Start Printing with the lpr Command

Before you start printing with the **lpr** command, ensure that

- You know the hostname or IP address of the LPD server system that you want to use.
- You know the name of the printer that you want to use.
- Your PC's hostname is in the LPD server's authorization file, if one is in use. This file is typically called /etc/hosts.lpd or /etc/hosts.equiv.

7.2.2 Sending Files to the Printer

You can use **lpr** command line options to specify the name of the print server and printer where you want to print a file. You also can use the command line to specify other options, such as suppressing header pages and printing binary files.

If you use the same print server and printer for the majority of your printing jobs, configure their names, and any other commonly used options, in your PCTCP.INI file. Then you no longer have to specify that information every time that you enter the **lpr** command.

To specify a server and printer on the command line

Use the **lpr** command with the **-S** option to specify the hostname or IP address of the print server, and the **-P** option to specify the name of the printer.

For example, to send the file MYFILE.TXT to the printer lp on the print server named green.anyu.edu, enter

```
lpr -S green.anyu.edu -P lp myfile.txt
```

You can specify other options on the **lpr** command line as well. For example, you can use options to suppress the printing of header pages or to print binary files.

To suppress header pages

Use the **lpr** command with the **-h** option. For example,

```
lpr -h myfile.txt
```

To print binary files

Use the **lpr** command with the **-v** option. For example,

```
lpr -S green.anyu.edu -P ps -v myfile.ps
```

This command sends the file MYFILE.PS to the PostScript printer ps attached to the server named green.anyu.edu. The **-v** option is for use with files that contain raster images, or for files in printer-specific formats such as PostScript, IMAGEN ImPRESS, or Hewlett-Packard Printer Control Language (PCL) format.

The **-v** option does not work for all print servers; sometimes you must use the **-l** option instead. The **-l** option may work better than **-v** for printing to a Sun system. See the *Command Reference* for more detailed descriptions of the **lpr** command line options.

To print using configured information

1. In the `[pctcp lpr]` section of your PCTCP.INI file, specify the print server name, the printer name, and other parameters that you use regularly with the **lpr** command.

The following sample PCTCP.INI file section specifies the printer `lp` and the print server `green.anyu.edu`, and sets the option to suppress printing of header pages.

```
[pctcp lpr]
printer=lp
server=green.anyu.edu
banner=no
```

2. Use the **lpr** command and specify the filename only; the other information is supplied from the configuration file.

   For example, to send the file MYFILE.TXT to a previously configured printer and print server, enter

   `lpr myfile.txt`

7.2.3 Monitoring the Status of a Print Job

Use the **lpq** command to verify the status of a job that you have sent to an LPD printer.

For example, to display the job queue for the printer hp2 controlled by the print server green.anyu.edu, enter

```
lpq -S green.anyu.edu -P hp2

Trying printer hp2 on server green.anyu.edu...open
printer hp2: spooling is on, printing is on
List of queue for printer hp2.
    Job #  user    host                  jobname
    66     kris    paris.alpha.com       myfile.txt
```

7.2.4 Removing Jobs from the Print Queue

If a print job has been queued but not yet printed, you can remove it from the queue using the **lprm** command. You also can use the **lprm** command to remove all print jobs sent by a specified user.

To remove a specific print job

1. If you do not know the number of your print job, determine the number by using the **lpq** command.

2. Use the **lprm** command, specifying the number of the job that you want to remove, and the name of the print server and printer (if they are not already configured).

   For example, to remove job 13 from the printer queue for hp2 on the server green.anyu.edu, enter

```
lprm -S green.anyu.edu -P hp2 13

Trying printer hp2 on server green.anyu.edu...open
Removing job #13 from printer hp2's queue
```

To remove all jobs for a specific user

Use the **lpr** command and specify the username of the person whose jobs you want to remove.

For example, the following command removes all jobs queued for user Kris:

```
lprm kris

Trying printer lp on server green.anyu.edu...open
Removing job #15 from printer lp's queue
Removing job #17 from printer lp's queue
```

7.3 Printing with predir

The **predir** command starts a terminate-and-stay-resident (TSR) program that redirects print jobs to the network printing command or program that you specify. For example, you can configure **predir** to execute the **lpr** command. Alternately, you can configure **predir** to execute a batch file that contains one or more commands.

7.3.1 Before You Start Printing with predir

Before you start using the **predir** redirector,

- Verify that you are running the TSR version of the kernel. The TSR version is required for **predir**.
- Decide what print program or batch file you want **predir** to use and create it or configure it appropriately.
- Decide what printer port you want to redirect (LPT1, LPT2, or LPT3) and verify that it is not being used by another redirector (such as **idprint** or the Network Driver).
- If you are printing from an application, verify that the default printer port set in the application's printing options matches the port that you configure for **predir** redirection.

7.3.2 Configuring the predir Redirector

Although you can specify most **predir** options on the startup command line, FTP recommends that you configure frequently used or required options in the `[pctcp print]` section of your PCTCP.INI file. Follow these steps:

1. Use the `prog=` parameter to specify the pathname of the print program or batch file that you want to use.

   If you specify a network print command, you must also set required parameters for that command in the appropriate PCTCP.INI file section. For example, if you redirect output to the **lpr** command, set the print server name and printer name in the `[pctcp lpr]` section.

2. Use the `printer=` parameter to specify the port (LPT1, LPT2, or LPT3) whose data you want **predir** to redirect.

   If you are printing from a DOS application, this port should match the default port set in the application's printing options.

3. Specify conditions that signal when to print the job. You should configure at least one print condition; you can configure more than one. The following parameters configure print conditions:

   `hotkey=[on|off]`

   `oneof=[on|off]`

   `onexit=[on|off]`

   `timeout=` *`seconds`*

   where

`hotkey=on`	Specifies that you want to print when you press the Ctrl+LeftShift+RightShift key combination. This option is useful for sending files to the printer while you are still using the file or application. For example, the hotkey lets you print the same file at several different times, or, if multiple files are open, print the file that is currently active.
`oneof=on`	Specifies that you want to print when you close the file.
`onexit=on`	Specifies that you want to print when you exit from the application.
`timeout=` *`seconds`*	Indicates that you want to print after a period of seconds has elapsed since the last character arrived at

the redirected printer port. If your DOS application takes a long time to format a print job, set a high timeout value (for example, 300 seconds) to ensure that the entire job is formatted before **predir** starts printing it.

4. Optionally, you can configure the name of the spool file or directory to hold jobs before sending them to print, and the name of the swap file or directory that **predir** uses temporarily while it loads and runs a print program or batch file.

   The defaults for these entries are `spool=c:\predir.spl` and `swap=c:\predir.swp` respectively.

The following example `[pctcp print]` section shows how to configure **predir** to redirect LPT1 output to the **lpr** command. It accepts the default spool and swap file names. It specifies that files should be printed after a timeout of 5 minutes (300 seconds), or when you press a hotkey combination, or when you close the file. The condition for printing when you exit from the application is turned off. In addition, the `[pctcp lpr]` section specifies the hostname of the print server and the name of the printer that the **lpr** command uses.

```
[pctcp print]
prog= c:\pctcp\lpr.exe
spool= c:\predir.spl
swap= c:\predir.swp
printer=LPT1
timeout=300
hotkey=on
oneof=on
onexit=off

[pctcp lpr]
printer=c10
host=printserver
```

7.3.3 Loading and Unloading the predir Redirector

Once you configure **predir**, you can load it from the AUTOEXEC.BAT file or from the command line. You can use other commands to unload **predir** from memory and disable printing without unloading the redirector.

To load predir from the command line

Use the **predir** command:

```
predir
```

To remove predir from memory

Use the **predir unload** command:

```
predir unload
```

Note that if you have loaded other TSRs after loading **predir**, you must unload them before you can unload **predir**.

To disable print redirection

Use the **predir printer off** command:

```
predir printer off
```

7.3.4 Printing Files with the predir Redirector

The **predir** TSR must be running before you can redirect files to network printers. Use the **onpredir** command to determine if **predir** is loaded and to display the current configuration.

To display print redirector status

Use the **onpredir** command:

```
onpredir

Current loaded version: 3.0
lpt1/prn is redirected
prog=c:\pctcp\lpr.exe
spool=c:\predir.spl
swap=c:\predir.swp
print-on-hotkey is enabled
print-on-exit is disabled
print-on-timeout is enabled
print-on-eof is enabled
```

To redirect a print job to a network print program

1. Ensure that the pathname of the network print program is specified with the `prog=` parameter in the `[pctcp print]` section of the PCTCP.INI file. For example:

   ```
   [pctcp print]
   prog=c:\pctcp\lpr.exe
   ```

2. To format the file for print, use your DOS application's standard print command or print key. (If the file is already formatted for printing, you also can use the DOS **copy** command or **print** command.)

3. Initiate printing by using one of the print conditions that you set in the `[pctcp print]` section of the PCTCP.INI file.

   –or–

   If no print conditions are set, use the **dopredir** command to send the file to the printer.

To redirect a print job to a batch file

1. Create the batch file (use any filename with a .BAT extension).

   The following example shows a simple file, PRINT-IT.BAT, that uses the **lpr** command to print to a host and printer other than those configured in the `[pctcp lpr]` section of the PCTCP.INI file. It specifies the server `green` and the printer `lp1`. It also uses the **-v** option to specify printing in binary mode. The `%1` is a replaceable parameter representing the name of the current print file.

```
lpr -S green -P lp1 -v %1
```

2. Ensure that the name of the batch file is specified in the `[pctcp print] prog=` parameter in your PCTCP.INI file. For example:

```
[pctcp print]
prog=c:\print-it.bat
```

3. To format the file for print, use your DOS application's standard print command or print key. (You also can use the DOS copy command or print command.)

4. Initiate execution of the commands in the batch file by using one of the print conditions set in the `[pctcp print]` section of the PCTCP.INI file.

7.3.5 Logging predir Status Messages to a File

When you load **predir**, you can use the standard DOS command output redirection symbol (>) to send status messages to a file. This technique keeps messages from disrupting your display and is also useful for diagnosing print redirection problems. You also can disable logging of status messages by redirecting output to a nul file.

To log predir status messages to a file

Load **predir** and specify a filename for redirecting the messages, as in the following command:

```
C:\> predir > logfile.txt
```

Note also that when you use the Ctrl+LeftShift+RightShift hot key to activate printing, the print redirector automatically places three types of messages in a PREDIR.LOG file in the current working directory:

- Error messages
- Status messages
- Messages produced by any batch file commands

To disable logging of predir status messages

Load **predir** and redirect the output to nul, as in the following command:

```
C:\> predir > nul
```

7.4 Troubleshooting Network Printing

The following sections list common situations that you might encounter when using the network print commands and describe how to respond.

LPR Printing

When printing with the **lpr** command, you see the message
`Server not set`

You need to specify the hostname or IP address of the print server. Use either the **-S** option of the **lpr** command line, or the `server=` parameter in the `[pctcp lpr]` section of your PCTCP.INI file.

You cannot print binary files with the **lpr** command.

Specify binary mode with the **-v** option on the **lpr** command line.

If you are printing to a Sun system, and if the **lpr -v** option does not work, try the **-l** option instead. Some Sun systems work better with the **-l** option.

If you are printing to an HP/UX server, the problem is that HP/UX servers do not implement a Berkeley style LPD. They use a printing script instead, and the script does not interpret binary mode correctly. Call your OnNet or PC/TCP technical support organization for a workaround that you can implement on the server.

Chapter 9
Connecting to Remote Networks over a Modem or Serial Line

If you travel and need to communicate with coworkers, OnNet or PC/TCP lets you connect over a modem and phone line to programs at your office or other sites, using the Serial Line Interface Protocol (SLIP) or the Point-to-Point Protocol (PPP). Once connected, you can

- Transfer and print files.
- Send and receive mail.
- Log in to a remote host with terminal emulation.
- Execute any other network task, such as transferring files between directories.

Dedicated serial lines do not use a modem or telephone line to connect PCs. Therefore, you do not have to dial a number or use any modem commands to communicate between systems.

This chapter assumes that you have worked with modems before and that you understand basic modem configuration options.

9.1 Before You Start Networking Across a Modem or Dedicated Serial Line

You should ensure that

- Your PC is connected to a modem or a dedicated serial line.
- You have the modem documentation on hand (if you are using a modem).

You should also ensure that the Internet service provider has given you

- A phone number to dial to connect to the network.
- A description of how to respond to prompts for information from the Internet service host.
- A description of what text appears when you are successful in connecting to the Internet service.

Depending on the type of service your Internet service provider supports, your Internet service provider *may* also give you the following information:

- The username and password that identify you to the Internet service.
- An Internet (IP) address to identify your host to the Internet service.
- A hostname that identifies your host to the Internet service.
- A Domain Name System (DNS) address for resolving references to Internet host names.
- The software control setting to use (if you are using PPP). (To communicate, both the Internet service and your host must agree on the setting (on/off).)
- Your Password Authentication Protocol (PAP) or Challenge-Handshake Protocol (CHAP) user identification and password (if you are using PPP *and* if your service provider supports PAP/CHAP).
- The VJ header compression setting to use (on or off). (To communicate, both the Internet service and your host must agree on the setting.)

To define a serial network connection, you need the information that your Internet service provider gave you, as well as

- The serial line protocol to use for your connection (SLIP or PPP).
- The type of modem that you are using (for example, Hayes compatible).
- The dialing method that you are using (Touch Tone or Pulse).
- The port where your modem is attached to your PC (for example LPT1).
- The modem’s baud rate (speed) and hardware/software control settings.

Note: The Telebit T1000-PC internal card modem is incompatible with the FTP serial drivers SLP16550 and PPP16550. Use a modem compatible with the drivers instead.

If the Internet service provides both SLIP and PPP options, and you need to determine which serial protocol to use, you can use these guidelines:

SLIP networks

- Can be dial-up connections, requiring a modem and telephone system, or they can be direct connections occurring over an RS-232 null-modem cable. Direct connections are dedicated connections, that is, the connection is reserved for only that connection.
- Do not require a network interface card.
- Use the PC's standard RS-232 asynchronous serial line port to send and receive data.
- Have a greater potential for electrical interference ("noise") on the line when using a modem. Noise on the line can give less reliable data than a direct connect cable.
- Eliminate custom configuration for every new connection you make.

PPP networks

- Can be dial-up connections, requiring a modem and telephone system, or they can be direct connections occurring over an RS-232 null-modem cable.
- Eliminate custom configuration for every new connection that you make.
- Provide inexpensive access to networks from remote sites, such as from a satellite sales office or campus building.
- Use the PC's standard RS-232 asynchronous serial line port to send and receive data.
- Can occur over a modem and telephone system, allowing you the full range of network applications.
- Do not require an interface card.

9.2 Configuring and Using SLIP and PPP — Procedure Overview

The following procedure describes the steps that you take to configure and use SLIP or PPP:

1. Choose a SLIP or PPP protocol.
2. Load the SLIP or PPP packet driver and kernel. (See Section 9.2.1, Loading the SLIP or PPP Packet Driver and Kernel.)
3. Use a text editor to configure your PCTCP.INI file.
4. Run the **comscrpt** command to connect to a remote host.

Note: You must perform these steps in order because the **comscrpt** command runs only if the kernel is loaded, and the kernel runs only if the packet driver is loaded.

To display comscrpt command usage

Enter the following command at the prompt:

```
comscrpt -?
```

9.2.1 Loading the SLIP or PPP Packet Driver and Kernel

To load the SLIP packet driver and kernel

1. Disable any currently loaded packet driver and kernel.

   Unload the driver and kernel using the appropriate unload commands. For example, use the command **inet unload** to unload the TSR kernel.

   –or–

   Comment out the command lines that load the driver and kernel in your AUTOEXEC.BAT file and reboot your PC.(To comment out a line, enter a semicolon as its first character.)

2. To loadthe SLP16550.COM packet driver and the SLIPDRV.EXE kernel, enter the following commands, respectively:

   ```
   slp16550
   slpdrv
   ```

   These commands load the SLIP packet driver and kernel, and display information about the configuration.

To display data about the SLIP packet driver

Use the following command to display UART (Universal Asynchronous Receiver Transmitter) statistics:

```
inet slip
```

To load the PPP packet driver and kernel

1. Disable any currently loaded packet driver and kernel.

   Unload the driver and kernel using the appropriate unload commands. For example, use the command **inet unload** to unload the TSR kernel.

   –or–

   Comment out the command lines that load the driver and kernel in your AUTOEXEC.BAT file and reboot your PC. (To comment out a line, enter a semicolon as its first character.)

2. Enter the following commands to load the PPP16550.COM packet driver and PPPDRV.EXE kernel, respectively:

   ```
   ppp16550
   pppdrv
   ```

   These commands load the PPP packet driver and kernel, and display information about the configuration.

Note: Command line options for the packet driver are set by default, so FTP recommends that you do not use them. The packet drivers use the following default settings:

- COM1, 2400 baud rate
- Software vector 0x60
- I/O address 0x3f8
- IRQ 4
- No hardware flow control.

If these are not your desired settings, you can edit your PCTCP.INI file or use the **comscrpt** command to override any of these settings.

To display data about the PPP packet driver and kernel

To display data about the PPP packet driver and kernel, use these commands.

To display	Use this inet command
UART and HDLC statistics	**inet ppp**
LCP statistics	**inet lcp stat**
LCP configuration (initial and final)	**inet lcp conf**
IPCP statistics	**inet ipcp stat**
IPCP configuration (initial and final)	**inet ipcp conf**

9.2.2 Setting Configuration Parameters for SLIP and PPP

You can set basic and advanced configuration parameters for SLIP and PPP in the following sections of your PCTCP.INI configuration file:

- `[pctcp ifcust 0]`
- `[pctcp comscrpt connection]`
- `[pctcp serial connection]`

The network software installation program automatically creates `[pctcp comscrpt connection]` and `[pctcp serial connection]` sections for SLIP and PPP configurations.

Each connection that you define has a different `[pctcp comscrpt connection]` section. Each serial connection has a unique `[pctcp serial connection]` section. You specify the name of the appropriate [pctcp serial `connection`] configuration file section using the `serial= connection` parameter in the `[pctcp comscrpt connection]` section. You can also use the **comscrpt** command to specify the `connection` name.

You can change the `connection` field in the `[pctcp comscrpt connection]` section to any arbitrary name that is more specific to your configuration. For example, `[pctcp comscrpt PPP_from_home]`.

If you need to configure serial communication options to override those that the packet driver sets by default, make sure that you have a `serial=` parameter in the `[pctcp comscrpt connection]` section, where *connection* identifies which `[pctcp serial connection]` section to use.

For advanced configuration, you set values for the following:

- Van Jacobsen (VJ) compression
- Software interrupt
- Hardware flow control
- I/O base address number
- Interrupt request number

VJ compression can significantly reduce data transmission time for applications that use TCP (but not User Datagram Protocol) connections. By default, VJ compression is enabled for SLIP and PPP connections, but both your local site and the remote site must be properly configured. (If you turn VJ Compression off, you can gain as much as 4K conventional memory.)

9.2.3 Customizing Dial-up and Hang-up Script Files

To save you the effort of typing modem commands every time that you want to establish a serial network connection, you can (optionally) place these commands in "script files."

For example, a modem dial-up script file generally initializes the modem, dials the remote host, and logs you in with a SLIP or PPP account name and password. A modem hang-up script file generally signals the remote host, ends the connection, then resets your modem so that it is ready to receive the next dial-up sequence.

Your software distribution includes sample script files that you can customize and use to connect to and disconnect from a remote host automatically. (The installation procedures copy these files to the C:/PCTCP /ETC directory (by default).)

These are the sample script files:

Script File	**Description**
DIALUP.SCR	Connects to a remote host and works with all Hayes-compatible modems. It has a modem-dependent line (the modem initialization string). However, you can find several versions of this line in the sample script file.
HANGUP.SCR	Disconnects a remote host and works with all Hayes-compatible modems.
DLDIALUP.SCR	Connects to a remote host using a dedicated serial line, rather than a modem.
DLHANGUP.SCR	Disconnects a remote host using a dedicated serial line, rather than a modem.

You can find default modem script files (DIALUP.SCR and HANGUP.SCR) on your network software distribution disks. If you are using a dedicated line, you can use the DLDIALUP.SCR and DLHANGUP.SCR files instead.

You can then specify script filenames as "keywords" in the `[pctcp comscrpt` *`connection`*`]` sections of your PCTCP.INI file. You can also use **comscrpt** command keywords to specify the names of your script files.

You can use these basic commands to construct modem scripts:

Command	**Description**
pause *x* [*units*]	Specifies how many units of time to pause before continuing with the script. Unit values can be `secs` for seconds, `msecs` for microseconds, or `ticks` for PC clock ticks. If the *units* parameter is absent, **comscrpt** uses `secs` as the default.

send *text*	Specifies text to send to the serial port, omitting initial tabs or spaces.
changemode (**packet** | **char**)	Switches the packet driver between packet mode and character (or "raw") mode.
signal (**physical** | **lcp** | **ipcp**) (**open** | **closed**)	Sends a request to open or close a specific layer.
poll (**physical** | **lcp** | **ipcp**) (**open** | **closed**)	Pauses until a synchronization is complete before continuing to read the script file.

Type a semicolon (;) or **rem** at the beginning of lines to disable lines in a script file. If you want to send a RETURN, line-feed, or horizontal tab character, you must use special character sequences, as follows:

Character	Special Character	Hex Value
RETURN	\r	0x0D
Line-feed	\n	0x0A
Horizontal Tab	\t	0x09

For example, the following connect script uses `\r` to indicate a RETURN. The login name being sent is `chris` and his password is `hushhush`.

```
send AT&C1\r
pause 1
send ATDT9,,555-1212\r
poll physical open
pause 8
send chris\r
pause 4
send hushhush\r
pause 2
changemode packet
signal lcp open
poll lcp open
poll ipcp open
```

To configure the default DIALUP.SCR script file

Edit the DIALUP.SCR script in your C:/PCTCP directory and save it with a new name (with

a .SCR filename extension).

FTP recommends that you use a name describing your remote connection, such as PPP2WORK.SCR. (Write down the name since you will use this name with the **comscrpt** command.)

At a minimum, you must supply a new phone number, username, and password. You may also want to change other modem commands and pause times.

You can use this new dial-up script file to connect to one remote host. For each additional SLIP or PPP connection, copy the sample script file and give it a unique filename, phone number, login ID, and password where appropriate.

To configure the default HANGUP.SCR script file

Edit the HANGUP.SCR script in your C:/PCTCP directory and save it with a new name (with a .SCR filename extension). FTP recommends that you use a descriptive name, such as MYHANGUP.SCR. (Remember this name since you will need it for the **comscrpt** command.)

Note: The default HANGUP.SCR settings work for most Hayes-compatible modems, so you probably need only one hang-up script file, even if you call several remote hosts. You can edit this file to change the settings as appropriate.

To configure script files for dedicated serial lines

You can find default DLDIALUP.SCR and DLHANGUP.SCR files in your distribution disks. Dedicated-line script files do not contain modem commands. You can edit these files and rename them to customize them for your use.

9.2.4 Setting Configuration Parameters

The sections that follow describe how to set configuration parameters for SLIP and PPP.

To set basic configuration parameters for SLIP

You need to edit the PCTCP.INI file to describe your SLIP connection.

Edit this entry	To do this
`[pctcp ifcust 0]`	
`ip-address=`	Specify the IP address of the remote host.
`[pctcp comscrpt` *`connection`*`]`	Create a section to describe this network *`connection`*.
`dialup=`	Specify the full pathname of your dialup script file (for example, C:\PCTCP\MYDIALUP.SCR).
`hangup=`	Specify the full pathname of your hangup script file (for example, C:\PCTCP\MYHANGUP.SCR).
`serial=`	Identify the appropriate `[pctcp serial` *`connection`*`]` section (for example, `serial=slip2wrk)`. Remember this name since you will need it for the **comscrpt** command.
`[pctcp serial` *`connection`*`]`	Create a section to describe this serial *connection*.
`baud=`	Specify the baud (speed) setting on your modem.
`port=`	Specify the serial port on your PC.

For example, these PCTCP.INI file entries describe the connection slip`2wrk`:

```
[pctcp ifcust 0]
;IP address for SLIP connection
ip-address = 128.127.50.50

[pctcp comscrpt slip2wrk]
dialup = f:\script\mydialup.scr
hangup = f:\script\myhangup.scr
serial = slip2wrk

[pctcp serial slip2wrk]
baud = 4800
port = 2
```

Note: You can identify additional script files using *`keyword = filename`* parameters in the `[pctcp comscrpt slip2wrk]` section.

To set advanced configuration parameters for SLIP

The following sample configuration file sections set advanced configuration parameters for SLIP:

```
[pctcp ifcust 0]
; IP address for SLIP connection
ip-address = 128.127.50.50
vj-compression = on
vj-compression-auto = on
vj-max-slot = 16
vj-slot-id = on

[pctcp comscrpt slip2wrk]
dialup = f:\script\mydialp.scr
hangup = f:\script\myhangup.scr
swint = 0x62
serial = slip2wrk

[pctcp serial slip2wrk]
baud = 4800
port = 2
hardware-flow-control = on
io-addr = 0x2f8
irq = 3
```

To set basic configuration parameters for PPP

You need to edit the PCTCP.INI file to describe your PPP connection.

Edit this entry	To do this
`[pctcp ifcust 0]`	
`ip-address=`	Specify the IP address of the remote host.
`[pctcp comscrpt` *`connection`*`]`	Create a section to describe this network *`connection`*.
`dialup=`	Specify the full pathname of your dialup script file (for example, C:\PCTCP\MYDIALUP.SCR).
`hangup=`	Specify the full pathname of your hangup script file (for example, C:\PCTCP\MYHANGUP.SCR).
`local-ip-address=`	Specify 0.0.0.0 or a local IP address to use for IPCP synchronization.
`remote-ip-address=`	Specify 0.0.0.0 or a remote IP address to use for IPCP synchronization.
`serial=`	Identify the name of the appropriate `[pctcp serial` *`connection`*`]` section (for example, `serial=ppp2work)`. Remember this name since you will need to use it with the **comscrpt** command.

`[pctcp serial connection]` Create a section to describe this serial *connection*.

`baud=` Specify the baud (speed) setting on your modem.

`port=` Specify the serial port on your PC.

For example, these PCTCP.INI file entries describe the connection `ppp2work`.

```
[pctcp comscrpt ppp2work]
dialup = f:\script\ppp2work.scr
hangup = f:\script\hangup.scr
serial = ppp2work
local-ip-address = 128.127.50.125
remote-ip-address = 0.0.0.0

[pctcp serial ppp2work]
baud = 4800
port = 2
```

Note: You can identify additional script files using *`keyword = filename`* parameters in the `[pctcp comscrpt ppp2work]` section.

To set advanced configuration parameters for PPP

The following sample file sections set advanced configuration parameters for PPP:

```
[pctcp ifcust 0]
ip-address = 128.127.50.49
vj-compression = on
vj-compression-auto = on
vj-max-slot = 16
vj-slot-id = on

[pctcp comscrpt ppp2work]
dialup = f:\script\ppp2work.scr
hangup = f:\script\hangup.scr
serial = ppp2work
accm = 0x000A0000
addr-ctrl-field-comp = on
identity = chris
local-ip-address = 128.127.50.125
mru = 1500
password = alias
prot-field-comp = on
remote-ip-address = 0.0.0.0

[pctcp serial ppp2work]
baud = 4800
port = 2
hardware-flow-control = on
```

```
io-addr = 0x2f8
irq = 3
```

Note: UNIX systems require that you manually log in and give a password despite what is in the PCTCP.INI file. Do not confuse PPP link-level authentication with the UNIX login and password prompts.

9.2.5 Establishing a Serial Line Connection

Once you have configured your script files and updated your PCTCP.INI file, you can use the **comscrpt** command to establish a serial line connection over a modem or dedicated line. The output of this operation varies, depending on the

- Make and model of the modem.
- Remote host's communication hardware.
- Contents of the dial-up script file.

As the commands execute, the session displays output from the serial line on your screen.

Note: If you use a modem, make sure that you have adjusted your modem speaker so that you can hear the dial tone.

To establish a serial line connection manually

1. Enter a command line similar to the following, where **ppp2work** represents the name of the appropriate `[pctcp comscrpt connection]` section from your PCTCP.INI file:

```
comscrpt ppp2work

Packet Driver found at vector 0x65
    name: SLP16550
    version: 2.20, class: 18, type: 2, functionality: 2
Serial Port parameters:
    Serial Port: COM1
    I/O Address: 0x3f8
    Hardware IRQ: 4
    Baud Rate: 9600
    UART Type: 16550
    Hardware Flow Control: on

Operating modem under manual control
Press Ctrl-C to Exit
```

2. Press Ctrl+C to exit.

3. Enter any modem commands at the DOS prompt to finish connecting your PC to the network.

You can now use other applications to transfer files, send and receive mail, log in to remote hosts, or do other network transactions.

To establish a serial line connection with a script file

1. Enter a command line similar to the following, where **ppp2work** represents the name of the appropriate section from your PCTCP.INI file:

```
comscrpt ppp2work dialup
```

```
Packet Driver found at vector 0x65
    name: SLP16550
    version: 2.20, class: 18, type: 2, functionality: 2

Serial Port parameters:
    Serial Port: COM1
    I/O Address: 0x3f8
    Hardware IRQ: 4
    Baud Rate: 9600
    UART Type: 16550
    Hardware Flow Control: on

Operating modem under control of script: c:\pctcp\dialup.scr
Press Ctrl+C to Exit
AT&C1
OK
ATDT555-1212
RING
CONNECT 2400
Link is opened
XXX.xxx.com [modem program vers XX.XX running]

login: chris
Password:

Packet mode enabled
```

2. If you hear a busy signal or you want to cancel the call before the connection is made, press Ctrl+C to return to the DOS prompt.

When packet mode is enabled and your cursor is back at the system prompt, your PC is connected to the network. You can now use other applications to transfer files, send and receive mail, log in to remote hosts, or do other network transactions.

To disconnect from the remote host

1. Ensure that background network activity, such as a file transfer, is not in progress when you execute the hang-up script. Such an activity will stop executing when you close the connection.

2. Enter a command similar to the following, where **`ppp2work`** is the name of the appropriate section in the PCTCP.INI file:

```
comscrpt ppp2work hangup

Packet Driver found at vector 0x65
    name: SLP16550
    version: 2.20, class: 18, type: 2, functionality: 2
Serial Port parameters:
```

```
    Serial Port: COM1
    I/O Address: 0x3f8
    Hardware IRQ: 4
    Baud Rate: 9600
    UART Type: 16550
    Hardware Flow Control: on
Operating modem under control of script: c:\pctcp\hangup.scr
Press Ctrl-C to Exit
OK
ATH0
NO CARRIER
```

(You need only one hang-up script file, even if you call several remote hosts.)

9.3 Tuning Your Serial Line Connection

You can tune your serial connection to improve performance. Specifically, you can

- Reconfigure the Communications port, or hardware flow control.
- Adjust Van Jacobson (VJ) compression.
- Increase your TCP window size.
- Determine the optimal transmission speed.
- Improve performance in a multitasking environment such as Windows.

To reconfigure the communications port, or hardware flow control

1. Open your PCTCP.INI file with a text editor.
2. Locate the `[pctcp comscrpt connection]` section for the appropriate connection.
3. Make sure that the `serial= connection` parameter identifies the appropriate `[pctcp serial connection]` section.

   For example, the `serial=ppp2work` parameter identifies the `[pctcp serial ppp2work]` section.

4. In the `[pctcp serial connection]` section, move your cursor down to the appropriate parameter and change the value.

For example, you might have the following sections in your PCTCP.INI file:

```
[pctcp comscrpt ppp2work]
dialup     =f:\script\ppp2work.scr
hangup     =f:\script \hangup.scr
serial     =ppp2work

[pctcp serial ppp2work]
baud       =4800
port       =2
hardware-flow-control=on
io-addr    =0x2f8
irq        =3
```

To adjust Van Jacobson (VJ) compression

1. Open your PCTCP.INI file with a text editor.
2. Locate or create the interface section `[pctcp interface n]` and replace the remaining variables with an appropriate value.

VJ compression can significantly reduce data transmission time for applications that use TCP (but not UDP) connections. By default, VJ compression is enabled for SLIP and PPP connections, but

both your local site and the remote site must be properly configured. (If you turn VJ Compression off, you can gain as much as 4K conventional memory.)

For example, you might have the following section in your PCTCP.INI file:

```
[pctcp ifcust 0]
vj-compression           =on
vj-compression-auto      =on
vj-max-slot              =16
vj-slot-id               =on
```

To increase your TCP window size

1. Change the `window=` value of the `[pctcp kernel]` section in your PCTCP.INI file to the maximum segment size (964 for SLIP, 1460 for PPP), or a multiple thereof.

2. Unload and reload the kernel to make the change take effect.

Note: Specify the maximum segment size if you communicate via a SLIP or PPP link with a remote host that uses a different interface (such as Ethernet).

To determine the optimal transmission speed across a serial line

1. Transmit data at a low baud rate, such as 2400.

2. Use the **inet stat** or **inet ppp** command to display the `Kernel TCP stats` and `Kernel IP stat` sections.

3. Increase your baud rate if you receive bad checksum values of 0 in these sections.

4. Retransmit data at the new baud rate.

5. Repeat steps 2, 3, and 4 until you receive nonzero values for the bad checksum entries.

6. (Bad checksum values other than 0 mean that communications errors cause the network software to retransmit data, which degrades performance. You can tune your baud rate for optimal speed in both a DOS environment and a Windows environment.)

7. Decrease your transmission speed one level (back to where you got 0 for the checksum value); for example, change 19,200 baud to 9600 baud.

9.4 Running PPP Over a Null-Modem Cable

You can directly connect your PC to a server port, using an RS-232 null-modem cable. To run PPP over a null-modem cable, your configuration must include two PCs connected as shown in Figure 9-1.

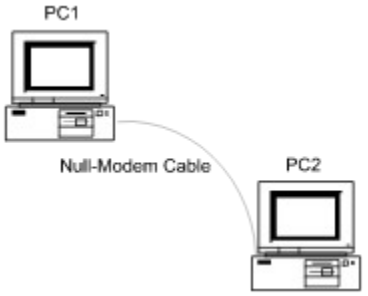

Figure 9-1 Null-Modem Configuration

The following procedures describe how to configure PC1 and PC2 to run PPP over a null-modem cable.

To set up PC1

1. Edit the script file so that it has the following entries:

```
changemode packet
pause 2
signal lcp open
pause 2
poll lcp open
poll ipcp open
```

2. Edit the `[pctcp comscrpt connection]` section of the PCTCP.INI file so that it has the following parameters:

```
local-ip-address = some IP address
remote-ip-address = some IP address other than the above
```

3. Edit the `[pctcp serial connection]` section of the PCTCP.INI file so that it has the following parameter:

```
hardware-flow-control = off
```

   If you must use hardware-flow-control, then add the following parameters to the `[pctcp serial connection]` section:

```
ignore-cts = [ off | on ]
ignore-dsr = [ off | on ]
```

   `Off` means that COMSCRPT monitors the RTS/CTS lines or the DSR (Data Set Ready) line. `On` means that it ignores the lines. For example, a typical combination might be:

```
hardware-flow-control = on
ignore-cts = on
ignore-dsr = off
```

To set up PC2

1. Edit the script file so that it has the following parameters:

   ```
   changemode packet
   pause 2
   signal lcp open
   poll lcp open
   poll ipcp open
   ```

2. Edit the `[pctcp comscrpt connection]` section of the PCTCP.INI file so that it has the following parameters:

   ```
   local-ip-address = 0.0.0.0
   remote-ip-address = 0.0.0.0
   ```

3. Edit the `[pctcp serial connection]` section of the PCTCP.INI file so that it has the following parameter:

   ```
   hardware-flow-control = off
   ```

   If you must use hardware-flow-control, then add the following parameters to the `[pctcp serial connection]` section:

   ```
   ignore-cts = [ off | on ]
   ignore-dsr = [ off | on ]
   ```

   `Off` means that COMSCRPT monitors the RTS/CTS lines or the DSR (Data Set Ready) line. `On` means that it ignores the lines.

   After you configure PC1 and PC2, try to **ping** the PCs. If you get the message `host unreachable hardware error`, recheck your configurations to ensure that they are as described in the procedures above.

9.5 Frequently Asked Questions About SLIP and PPP

What is the difference between synchronous and asynchronous PPP?

Synchronous is generally simpler and runs at faster speeds, but it requires a synchronous modem, which is more expensive than an asynchronous modem. Also, synchronous boards have an SCC chip (Serial Communications Controller), which has a clock to synchronize transmission and thus optimize the speed of transmission. Asynchronous boards have a UART chip, which does not have this feature.

What does asynchronous PPP offer that SLIP does not?

Several features, including:

- Multiprotocol support
- Data link level frame check sequence
- Standardized authentication capability
- Capability to escape control characters in the data stream
- Standardized IP address synchronization capability

Does the PPP16550 packet driver support synchronous mode?

No, it communicates with the 16550 UART and not the synchronous communication controller chips.

Can PPP handle XREMOTE traffic?

No, they are different protocols.

Can I set up my PC with SLIP or PPP so that another user can dial into it?

Yes, follow these steps:

1. Set your modem for autoanswer mode.
2. Load the SLIP or PPP packet driver and kernel.
3. Run the **comscrpt** command using a dial-up script file with the following contents:

```
signal lcp open
```

After you perform these steps, another PC can dial into your PC and connect through your modem.

Can I make two simultaneous calls through the slpdrv and pppdrv kernels, and slp16550 and ppp165550 packet drivers?

No, FTP's serial kernels and packet drivers are only capable of maintaining one connection at a time.

Can I assign an IP address dynamically when I dial in to my remote host using SLIP?

There is not a standard method; therefore, the industry does not have a well-defined guaranteed solution. Some system administrators create methods for doing this, but these methods vary widely, are highly non-standard, and work only with the system administrator's site.

Does the 16550 UART perform better than the 8250 UART?

The typical 8250 UART generates one interrupt per byte sent or received over the serial line. This is equivalent to one interrupt per character. This puts too much of a load on the typical 286 or 386 processor.

The 16550 UART generates one interrupt per 8 bytes sent or received (thus 1 interrupt per 8 characters). The 16550 also features a 16-byte FIFO (First In First Out) queue, configurable trigger levels, and support for clock rates up to 460 kbps. In view of this, it should boost performance in most cases. However, on a 286 class machine, the improvement in performance may be marginal.

Do SLIP and PPP support hardware flow control?

Yes, the maximum speed handled is 56K baud.

How do you let another host set up a PPP connection to your PC?

To let another host set up a PPP connection to your PC, run **comscrpt** on both PCs. Otherwise, you cannot determine whether the modem has a connection and should initiate a PPP session.

9.6 Troubleshooting Your Serial Line Connection

This section describes situations that may occur. When possible, the reason for the situation is provided and a possible solution.

The PCTCP.INI configuration file could not be found.

> The PCTCP.INI file may not exist or the drive and pathname may not be correctly specified.
>
> Verify that you have set the PCTCP environment variable to point to an existing configuration file. Make sure that you have fully and correctly specified the drive and pathname.

The `[pctcp comscrpt]` section could not be found.

> The `[pctcp comscrpt` *`connection`*`]` section for the particular *`connection`* may not be in your PCTCP.INI file.
>
> Verify that the section that you specified with **comscrpt** is in your PCTCP.INI file and is correctly spelled.

The dial-up script file was not found in the PCTCP.INI configuration file.

> The `dialup=` parameter may not point to a script file.
>
> In the `[pctcp comscrpt` *`connection`*`]` section of your PCTCP.INI file, verify that the `dialup=` parameter points to a script file.

The COM port was not found.

> You may have defined your serial port to be used by another device.
>
> Configure you serial port to an unused port. For example, if you use COM1 for your mouse, you could configure your serial port to COM2.

LCP or IPCP fails to reach an open state.

> You may be missing LCP or IPCP parameters in your PCTCP.INI file.
>
> Check the `[pctcp comscrpt` *`connection`*`]` section of your PCTCP.INI file to ensure that LCP and IPCP parameters are defined.

Everything is configured correctly, but you cannot make a connection.

> Your dial-up script file may be faulty or your modem may not be functioning properly.
>
> Verify that your dial-up script file has the correct commands in the correct order. Also, verify that your modem functions properly. (Refer to your modem documentation for possible configuration problems.)

You cannot send data to the serial port.

The `hardware-flow-control=` parameter in your PCTCP.INI file may be set to on or your hardware might be misconfigured.

Set the parameter `hardware-flow-control=off` in the `[pctcp serial connection]` section of your PCTCP.INI file. If the error message still appears, there is some hardware misconfiguration that must be resolved in either the serial board installation (IRQ conflict) or in the RS-232 cable between the PC and the modem.

You cannot ping other machines.

The `router=` line may be missing from your PCTCP.INI file.

Verify that the section pointed to by the `interface=` parameter in the `[pctcp kernel]` section of your PCTCP.INI file is present (that is, the `[pctcp ifcust 0]` section). A `router=` parameter must also be present that specifies as a value the IP address of your server.

You have two Ethernet subnets joined by a SLIP subnet. When you try to send a large packet (greater than 1006 MTU for SLIP), it gets dropped.

COMSCRPT automatically lowers its MTU to fit the smallest link it has to go over. That may not be working properly.

Try setting `mtu-discovery=no` in the `[pctcp kernel]` section of your PCTCP.INI file. After you do this, any data transfer to a host that is not on the local net uses a default TCP MSS of 536.

The MTU discovery entry in the PCTCP.INI file is only for outgoing TCP data. The MSS on Ethernet with MTU discovery on or off is 1460.

When strings are sent to the remote modem, more characters end up being sent than should be.

COMSCRPT may be generating extra characters.

Use COMSCRPT in manual mode up to the point where you get the message `Hit Ctrl+C...` At this point you could invoke the script file with the following:

comscrpt *connection* **dialup**

The script file contains just the following entries:

```
changemode packet

signal lcp open

poll lcp open

poll ipcp open
```

When COMSCRPT is used, the serial port speed has to be 9600 bps. Anything higher results in errors.

The `baud=` parameter in your PCTCP.INI file may be specified as a decimal value.

Verify that the `[pctcp comscrpt connection]` section in the PCTCP.INI file has a `serial= connection` parameter. The value you specify identifies the name of the [pctcp serial `connection`] section that describes the characteristics of the particular serial network connection.

In the `[pctcp serial connection]` section, make sure that the `baud=` parameter is not specified as a decimal value. For example, make sure it specifies:

`baud=19200` and not `baud=19.2`

When using PPP, you get an LCP open stat but timeout with IPCP.

The address the server assigned to you might be the same as the address defined by `local-ip-address=` in your PCTCP.INI file.

The items that are synchronized at the IPCP layer are the IP addresses and the extent of support for VJ compression. In view of this, verify whether or not you have a `local-ip-address= parameter` specified in the `[pctcp comscrpt connection]` section. The address assigned to you by the server must be different from this one.

You can further investigate connection problems by putting your modem into echo mode. A modem in echo mode sends back to your screen all commands that it receives, so you can see the commands sent to the modem as they are processed. On a Hayes-compatible modem, you

- Turn on echo mode with the **AT E1** command.
- Turn off echo mode with the **AT E0** command.

If you run the **comscrpt** command with echo mode enabled and see nothing on your screen, then your modem or connection is causing the problem. Otherwise, you see both the modem commands as they are sent to your modem and your modem's responses. In many cases, the responses reveal what is wrong. Refer to your modem's documentation for hardware-related troubleshooting instructions.