Command Reference

OnNet™ for Windows version 2.0 (July 1995)

Command Reference

OnNet™ for Windows version 2.0 (July 1995)

Chapter 2 DOS Commands Used by OnNet and PC/TCP

lprm
lwpe
netbios
nicname
nntp
onpredir
passwd
pcmail
pctcpcfg
ping
pop2, pop3
predir
rcp
rlogingl
rloginvt
rmt
rsh
setclock
setcolor
smtp
snmpd
tar
tftp
tn
tnglass
unix2dos
vmail
vxdinit
whois
ypcat
ypmatch

bootp

Usage

bootp [**-fnvw**] [**-d** *address*] [**-r** *retries*] [**-t** *seconds*] [*pctcp.ini_file*]
bootp [**-?** | **-version**]

Description

The **bootp** command runs the Bootstrap Protocol (Bootp) client program on your PC to obtain network configuration information from a remote server. The **bootp** command does *not* boot DOS on your PC. You can type the **bootp** command at the DOS prompt, or you can put the **bootp** command in your AUTOEXEC.BAT file so it runs each time that you start your PC.

When the **bootp** command starts, it sends a request for configuration information to a server on which Bootp server software is running. After the Bootp server software receives the request, it searches the Bootp database on the server to find the configuration needed by your PC. After the server locates the correct information, it returns a reply packet containing the PC's IP address and information from the server's database back to the bootp program on your PC.

The **bootp** command uses the information it receives to update the kernel that is running on the PC, but by default it does *not* enter the information in the PC's PCTCP.INI file. You must use the **-w** command line option if you want to write the information to the PCTCP.INI configuration file.

Command Line Options

-d *address* Specifies the IP address of the server to which the Bootp client sends its request. The address specified with this option overrides the `server-address=` parameter's setting in the `[pctcp bootp]` section of the PCTCP.INI file. If the servers's address is not set, the Bootp client broadcasts its request to the network and ignores this option.

-f Forces the **bootp** command to replace your PC's current IP address with a new one from the Bootp server. (Typically, a server does not give an IP address to a client that already has one.) If the server does not reply with a new IP address, the old address stays in use. The **bootp** command ignores this option if you also use the **-n** option.

Caution: If you use the **-f** option when you have TCP/IP applications running on your PC, you may cause the applications to terminate.

-n Does not update your PCTCP.INI file or the kernel. Use this option with the **-v** option to view the information retrieved from the server without changing your kernel parameters.

pctcp.ini_file Specifies the complete path of a PCTCP.INI file from which **bootp** reads information and to which **bootp** writes information (if the **-w** option is used). This optional setting overrides the PCTCP= environment variable setting.

-r *retries* Retries sending a **bootp** request the number of times specified by *retries*. The default number of retries is 4.

-t *seconds* Times out the **bootp** command process after waiting *seconds* seconds for the **bootp** reply to be sent from the server. The default timeout is 60 seconds.

-v Displays detailed (verbose) information about the server's reply.

-w Writes configuration information received from the server to the PCTCP.INI configuration file.

-? Displays and explains the usage line of the command.

-version Displays the version and patch level of this command. Refer to this information if you call Technical Support.

Example

To retrieve the PC's IP address and other network configuration information, timing out if no reply is received within 15 seconds, enter

```
C:\>bootp -t 15
```

See Also

dhcp

RFCs 951, 1531, 1533, 1534

bootp

Chapter 2
DOS Commands Used by OnNet and PC/TCP

This chapter describes in detail the following DOS commands:

bootp	**idnet**	**lprm**	**rmt**
comscrpt	**idprint**	**lwpe**	**rsh**
cookie	**idrive**	**netbios**	**setclock**
ddates	**idumnt**	**nicname**	**setcolor**
dhcp	**idutil**	**nntp**	**smtp**
dopredir	**inet**	**onpredir**	**snmpd**
dos2unix	**iprint**	**passwd**	**tar**
finger	**kdestroy**	**pcmail**	**tftp**
ftp	**kernel**	**pctcpcfg**	**tn**
ftpsrv	**keymap**	**ping**	**tnglass**
ftpver	**kinit**	**pop2**	**unix2dos**
host	**klist**	**pop3**	**vmail**
idchmod	**kpasswd**	**predir**	**vxdinit**
idconfig	**lpd**	**rcp**	**whois**
idls	**lpq**	**rlogingl**	**ypcat**
idmnt	**lpr**	**rloginvt**	**ypmatch**

comscrpt

Usage

comscrpt *connection* [**dialup** | **hangup** | *keyword*]
comscrpt [**-?** | **-version**]

Description

The **comscrpt** command opens or closes a serial line connection to a network using the PPP or SLIP packet driver and kernel. You then run PC/TCP applications over this connection. You can manually connect to a remote host using the **comscrpt** command, in which case you do not need to specify a script name in your PCTCP.INI file.

Command Line Options

dialup Opens the configured serial line connection with a dial-up script file. The word **dialup** is the recommended keyword for referring to a dial-up script file named in your PCTCP.INI file.

hangup Closes the configured serial line connection with a hang-up script file. The word **hangup** is the recommended keyword for pointing to a hang-up script file named in your PCTCP.INI file.

connection Specifies the name of the section in your PCTCP.INI file (like `[pctcp comscrpt PPP_from_home]`) that describes your serial connection.

keyword Specifies a unique script file keyword (other than **dialup** and **hangup**) from your PCTCP.INI file. You can create as many as 50 unique keywords that refer to 50 unique script files. You can also specify as many of these keywords on a **comscrpt** command line as you need.

-? Displays and explains the usage line of the command.

-version Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Examples

The following examples use the values in the `[pctcp comscrpt newyork]` section of the PCTCP.INI file to activate the script referred to by the dialup or hangup keyword.

In the first example, the script dials the remote host and connects to it, displaying a `CONNECT 9600` message.

```
comscrpt newyork dialup

Packet Driver found at vector 0x65
           name: SLP16550
           version: 2.30, 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
Press Ctrl+C to Exit
AT&C1
OK
ATDT555-1212
RING

CONNECT 9600
Link is opened
VEX.xyz.com [modem program vers 02.30 running]
login: pat
Password:

Packet mode enabled
```

In the second example, the script closes the remote connection, displaying a `NO CARRIER` message as the last line, indicating that the connection has been broken.

```
comscrpt newyork hangup

Packet Driver found at vector 0x65
    name: SLP16550
    version: 2.30, 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
Press Ctrl+C to Exit
OK
ATH0
NO CARRIER
```

See Also

inet, kernel

comscrpt

cookie

Usage

cookie [*server*]
cookie [**-?** | **-version**]

Description

The **cookie** command requests a fortune cookie message (Quotation of the Day) from a network fortune cookie server. Set the designated network fortune cookie server by specifying its IP address for the `cookie-server=` entry in the `[pctcp addresses]` section of your PCTCP.INI file. Otherwise, you must use the *server* argument with the command.

If you get an error message instead of a quotation, make certain that you specify the correct server, or see your system administrator. If the network fortune cookie server is running a Berkeley-derived version of UNIX, its Quote service must be enabled in the INETD.CONF file. The system administrator remove the comment character from the beginning of the line containing the Quote service in the INETD.CONF file. The internet daemon **inetd** then starts a miscellaneous daemon, **miscd**, which provides quoted service when requested.

Command Line Options

server	Specifies the hostname or IP address of the network fortune cookie server.
-?	Displays and explains the usage line of the command.
-version	Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Example

To display a fortune cookie message from the server vex.xyz.com, enter

```
C:\> cookie vex.xyz.com

Repeal the law of gravity!
```

See Also

RFC 865

cookie

ddates

Usage

ddates [**-?** | **-version**]

Description

The **ddates** command shows the dates and times of previous incremental backups of your files.

If you use the **0–9** option of the **tar** command to control the dump level, **tar** makes incremental backups and 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=` entry in the `[pctcp tar]` section of the PCTCP.INI configuration file to specify the name of this file.

Command Line Options

-? Displays and explains the usage line of the command.

-version Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Example

To display an incremental backup you made to a diskette (**tar cvz5f a:test.tar .**), enter

```
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
...
```

See Also

tar

ddates

dhcp

Usage

dhcp [**-nuvw**] [**-l** *seconds*] [**-r** *retries*] [**-t** *seconds*] *pctcp.ini_file*]
dhcp [**-?** | **-version**]

Description

The DHCP client for DOS includes a terminate-and-stay-resident (TSR) module that provides automatic DHCP lease renewal functionality. You can use this module only with the PC/TCP TSR kernel; you cannot start or unload this module from a DOS box in Windows.

The **dhcp** command runs the Dynamic Host Configuration Protocol (DHCP) client program on your PC to obtain network configuration information from a remote server. You can type the **dhcp** command at the DOS prompt, or you can put the **dhcp** command in your AUTOEXEC.BAT file so it runs each time that you start your PC.

When the **dhcp** command starts, it sends a request for configuration information to a server on which DHCP server software is running. After the DHCP server receives the request, it searches its database to find the configuration for your system. After the server locates the correct information, it returns an IP address and network parameters. DHCP can assign either a temporary or a permanent IP address, depending on the configuration of the server.

The **dhcp** command updates the kernel that is resident on the PC, but it does *not* update the PCTCP.INI configuration file by default. You must use the -w command line option if you want **dhcp** to write the configuration information to the PCTCP.INI file.

The **dhcp** command can get information from both DHCP and Bootp servers.

Command Line Options

-l*seconds* Specifies the length of the lease requested by the client in seconds. A lease is the length of time a client can keep an IP address. Note that it is the responsibility of the DHCP server to decide the lease duration, and a DHCP server may return a lease time different from that specified by the client, depending on how the server is configured.

The lease duration specified with this option overrides the “lease-time= ” option in the PCTCP.INI file. If neither is specified, the DHCP server sets the lease time.

-n Does not update your PCTCP.INI file or the kernel. Use this option with the **-v** option to view the information retrieved from the server without changing your kernel parameters.

pctcp.ini_file Specifies the complete path of a PCTCP.INI file, from which **dhcp** reads information and to which **dhcp** writes information. This optional setting overrides the PCTCP= environment variable setting.

-r *retries* Retries sending a **dhcp** request the number of times specified by *retries*. The default is 4.

-t *seconds* Times out the **dhcp** command process after waiting *seconds* seconds for the **dhcp**

reply to be sent from the server. The default is 60.

-u Unloads the DHCP module and releases the current IP address being leased. The kernel reverts to using the IP address that was in use before the DHCP TSR module was installed.

Note: The **dhcp -u** command does not function from a DOS box in Windows.

-v Displays verbose information about the server's reply.

-w Writes configuration information received from the server into the PCTCP.INI configuration file.

-? Displays and explains the usage line of the command.

-version Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Example

To set the PC's IP address and other network configuration information with a one hour lease (3600 seconds), timing out if no reply is received within 15 seconds, enter

```
C:\>dhcp -l 3600 -t 15
```

See Also

bootp

RFC 1531 for DHCP definition

RFCs 1532, 1533, and 1534 for DHCP and Bootp operation

dhcp

dopredir

Usage

dopredir [**-?** |**-version**]

Description

The **dopredir** command initiates printing of files that have been redirected to a spool file using the **predir** command. The **dopredir** command works only if the **predir** print redirector is loaded and running.

Command Line Option

-? Displays and explains the usage line of the command.

-version Displays the version and patch level of the command. Refer to this information if you call Technical Support.

See Also

onpredir, predir

dopredir

dos2unix

Usage

dos2unix [*source* [*destination*]]
dos2unix [**-?** | **-version**]

Description

The **dos2unix** command converts ASCII text files created on an MS-DOS system to a format that displays properly on a UNIX system. MS-DOS files contain end-of-line characters that can be interpreted incorrectly on a UNIX system. The **dos2unix** command replaces MS-DOS end-of-line characters in the named *source* file with UNIX new-line characters and stores the result in the named *destination* file. The *source* and *destination* filenames must be different.

Command Line Options

destination	Specifies a UNIX filename. If you do not specify a destination, the command displays the formatted output on your screen.
source	Specifies a DOS filename. If you do not specify a source, the command takes input from your keyboard.
-?	Displays and explains the usage line of the command.
-version	Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Example

To translate the DOS file JANUARY.DOS to the UNIX file january.uni, enter

```
C:\> dos2unix january.dos january.uni
```

See Also

unix2dos, idrive

dos2unix

finger

Usage

finger [*user*] *@host*
finger [**-?** | **-version**]

Description

The **finger** command displays directory information about a registered user of another network host.

Some hosts do not respond to finger requests. They either ignore the request (in which case **finger** displays the message `...host not responding`) or they reject it (in which case **finger** displays the message `Closed: foreign reset`). The Berkeley 4.2 Finger server does not send its responses in NETASCII; thus, its response may be poorly formatted. PC/TCP accepts server output in both formats.

Command Line Options

host	Specifies the name or Internet address of the remote host. You must prefix the hostname with the at-sign (@) character.
user	Specifies the character-string name of a registered user at the target host. If you omit *user*, some hosts respond with a list of currently logged-in users. If the target host is not forthcoming with a response, **finger** gives up after approximately 20 seconds.
-?	Displays and explains the usage line of the command.
-version	Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Example

To display the user IDs, usernames, terminal process (TTY) assignments, idle times, and office locations for users logged in to host vex.xyz.com, enter

```
C:\> finger @vex

[vex.xyz.com]
Login      Name           TTY     Idle    When          Office
rkd        Robin K. Doe   p0      26      Fri 13:07     B-36
lee        Lee Smith      p1              Fri 13:28
```

See Also

nicname, whois

finger

ftp

Usage

ftp [**-d**] [**-u** *userid password*] [**-p** *port_no*] [*host*] [*command*]
ftp [**-?** | **-version**]

Description

The **ftp** command transfers text (ASCII) files and binary files between hosts on a network.

It implements the client TCP/IP standard File Transfer Protocol (FTP) on a PC. If you specify a single command, **ftp** executes that command and quits. Otherwise, it starts up a command interpreter known as an **ftp** session. During this session, you can execute interactive **ftp** commands, such as directory commands and file transfer commands.

The default transfer mode is ASCII text. To send or receive binary files, you log in to the remote host and set the transfer mode for the session by using the **binary**, **tenex**, or **image** interactive command. Then you use the **get** or **put** command for each file you transfer.

You must choose the file mode based on the byte size of the system to or from which you are transferring the file. If the system has the same word size as the IBM PC (8, 16, or 32 bits), you can use **image**. If it does not, you should probably use **tenex** (binary) mode. The most common systems in use that do not have the same word size as the PC are LISP and TOPS-20 systems.

To transfer a single binary file, you can log in to the remote host and use the **iget**, **tget**, **tput**, or **iput** command for each binary file you transfer.

Command Line Options

command Performs the specified operation. See the “Interactive ftp Commands” section that follows.

-d Displays all **ftp** network commands and responses that are sent over the **ftp** control connection. This option displays your password after you enter it.

host Specifies the name of the host on which to open an **ftp** connection.

-p *port_no* Specifies the number of the remote port that the FTP server monitors.

-u *userid password* Automatically logs you in to the remote host using your username and password.

-? Displays and explains the usage line of the command.

-version Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Interactive ftp Commands

During an **ftp** session, you can use a large number of interactive commands. Unambiguous abbreviations of these commands often work in place of the full command name. For example, **di** is the same as **dir**, but **d** is ambiguous; it could mean **debug**, **delete**, **dir**, or **drive**.

Some older systems may support FTP servers that do not implement certain commands like

mkdir, **rmdir**, **pwd**, and **parent**. You should upgrade the FTP server program on these systems.

When you get the **ftp** session prompt, you can enter any of the following interactive commands:

! [*command*]	With no argument specified, switches to a command interpreter. Otherwise it executes the specified DOS command and returns your **ftp** prompt. You can run any network program while the command interpreter runs, and you can return to the **ftp** session with the **exit** command. **Note:** You must place a space between the **!** and the DOS command.
? [*command*]	With no argument specified, displays a list of available commands. Typing `?` and a command (like `acct`) displays a brief help message for the specified command.
abort	Causes the server to abruptly stop the previous FTP service command.
acct [*account_name*]	Switches to the specified account. Most FTP servers do not support or require this command, but if required, the server requests an account name.
allocate *n*	Allocates storage on a server for a file transfer. Specify the number of bytes to set aside.
append [*local_file remote_file*]	Adds a local file to a remote file on the remote host in the current mode (ASCII, Image, Tenex, or Local *n)*.
ascii [**nonprint** | **telnet** | **carriage**]	Enables the transfer of ASCII text files. Specify **nonprint**, **telnet**, or **carriage** to enable one of these modes.
binary	Synonymous with **image**.
bye	Synonymous with **exit**.
cd	Synonymous with **fcd**.
close	Disconnects from the FTP server without exiting from the FTP client program.
debug (**on** | **off**)	Sets debugging either on or off. This command is not normally needed.
delete *filename*	Deletes a specified file on the remote machine. To delete a directory, use the **rmdir** *remote_directory* command.
dir [*argument*[*filename*]]	Lists the current directory on the remote machine. You can use the first option, *argument*, to specify a pathname, filename, or argument for the server to use as it gets a directory listing. If you specify *filename*, the information normally displayed on the screen is saved to that file.
disconnect	Disconnects from the FTP server without exiting from the FTP client program.
drive *drive letter*	Changes the current drive on the PC to the specified drive.

exit Exits from the **ftp** session and returns your PC's DOS prompt.

fcd [*path*] Changes the current working directory on the remote machine. Not all servers support this command.

fdir Synonymous with **dir**.

fpwd Shows the name of the current working directory on the remote machine. Not all servers support this command.

get [*remote_file local_file*] Copies a file from the remote machine to the PC in the current mode (ASCII, Image, Tenex, or Local *n*). If the remote filename has a space in it, you can enter that filename only in response to the filename prompt. Note that when transferring files on a CMS system, you can substitute periods for spaces in filenames.

hash [**on** | **off** | *integer*] Displays a number sign (hash mark #) every time **ftp** sends or receives a specified number of bytes. Set how often number signs are displayed by specifying an integer value in the range 512– 65536 bytes. The default value is 4096 bytes. You can set a value for this with the `hash_mark_size=` entry in the [`pctcp ftp`] section of your PCTCP.INI file.

help Lists commands supported by **ftp**. Synonymous with **?**.

iget [*remote_file local_file*] Like **get**, but transfers a remote file to a local directory using Image (binary) mode (for just this one transfer).

image Enables the transfer of binary files between similar machines. Use the **local** *n* command to transfer files correctly between two different kinds of machines.

iput [*local_file remote_file*] Like **put**, but copies *local_file* to *remote_file* using Image (binary) mode. (Subsequent transfers revert back to the default ASCII mode.)

lcd [*local_directory*] Changes the current working directory on the PC to the specified directory. (Typing a drive letter in the directory name does not change the current drive. Use the **drive** command to change the current drive.)

ldir [*path*] Displays a local directory listing. Specify *path*, to view the contents of a specific directory. You can specify any of the drives on your PC as part of the filename path.

lmkdir [*local_directory*] Creates a new directory on the PC with the specified name. You must return to the DOS session to remove the directory. (There is no **lrmdir** command.)

local *n* Enables the transfer of binary files to and from a host that uses a different byte size than your PC uses, where *n* is the byte size (such as 8) of the local machine or of the passive side of a connection.

login *user* Sets your username to *user* on the remote machine. Use this command if

the login failed (perhaps due to a mistyped password), or if the remote machine supports changing usernames in the middle of a session.

lpwd Shows the name of the current directory on your PC.

ls [*argument* [*filename*]] Like **dir**, but does a short listing of the current directory on the remote machine. You can use the first option, *argument*, to specify a path or filename, for the server to use as it gets a directory listing. If you specify *filename*, the information normally displayed on the screen is saved to a file of this name.

mdelete *wildcard_name* Deletes multiple files on the remote machine. If you first specify the **option ask on** command, **mdelete** prompts you for confirmation before deleting each file. Valid responses are

- **n** No. Do not delete this file.
- **p** Proceed. Delete this file an all remaining ones without asking.
- **q** Quit. Stop immediately.
- **y** Yes. Delete this file.

mget *wildcard_name* Transfers multiple files to the local machine using wildcard syntax. If you first specify the **option ask on** command, **mget** prompts you for confirmation before transferring each file. Valid responses are

- **a** ASCII. Make all transfers from this point in ASCII mode.
- **i** Image. Make all transfers from this point in Image (binary) mode.
- **n** No. Do not transfer this file.
- **p** Proceed. Complete this transfer and all remaining ones without asking.
- **q** Quit. Stop immediately.
- **r** Rename. Prompt for a new name for the local filename.
- **t** Tenex. Make all transfers from this point in Tenex mode (Local byte size 8).
- **y** Yes. Transfer this file.

mkdir *remote_directory* Creates a new directory on the remote machine. Not all servers support this command.

mount *pathname* Changes the server's file system mount information. The syntax for the pathname is determined by the operating system on the FTP server.

mput *wildcard_name* Transfers multiple files to the remote machine using wildcard syntax. If you first specify the **option ask on** command, **mput** prompts for confirmation before transferring each file. Valid responses are the same as for the **mget** command.

open [*host_name*] [*port_no*] Opens an **ftp** connection. Use this command after the **ftp** client has been started without a connection, or after disconnecting from an FTP server.

option [*option_name* (**on** | **off**)] With no argument specified, **option** displays the current option settings. You can turn each option on or off. Options are as follows:

ask on	Prompts you for file transfer instructions. For examples, see the description for **mget** or **mdelete**.
casehack off	Uses the case you specify to generate filenames. If this is a wildcard transfer, **ftp** generates uppercase default names. Use **option casehack off** for transferring files to case-sensitive operating systems.
hash on	Displays a number sign (hash mark #) every time **ftp** sends or receives a specified number of bytes. Set how often number signs are displayed by specifying an integer value range of 512–65536. The default value is 4096 bytes.
page [**on** | *n*]	Prevents the results of a command (such as **dir**) from scrolling off the screen. The display pauses after 23 lines. If you specify a number (*n*), the display pauses after the specified number of lines.
pathhack off	Uses the path you specify to generate filenames. Otherwise, when **ftp** generates a default filename, it tries to strip off the path for the output file.
prompt [**on** | **off**]	Makes ftp prompt the user for file transfer instructions. For examples, see the description for **mget** or **mdelete**.

parent Changes the current directory on the remote machine to the parent directory. Not all servers support this command.

passive Executes the next transfer in passive mode (instead of the server opening the data connection, the PC opens the data connection). Not all servers support this command.

prompt [**on** | **off**] Makes **ftp** prompt the user for confirmation of actions to be taken on each file. For examples, see the description for **mget** or **mdelete**.

put [*local_file remote_file*] Copies *local_file* to *remote_file* in the current mode (ascii, image, tenex, or local *n*). If the local filename has a space in it, you can enter that filename only in response to the filename prompt. Note that when transferring files on a CMS system, you can type periods in place of spaces in filenames.

pwd Synonymous with **fpwd**.

quit Synonymous with **exit**.

quote *command* Sends an **ftp** command directly to the remote machine's server. For example, you can send a command that changes the remote directory to a directory with spaces in its name (`quote cd my new directory`). The complete command and argument are sent together after the **quote** command, which reads the spaces as actual characters.

Caution: Be careful not to send a command that breaks or hangs your ftp session.

reinit Reinitializes the connection to the startup state following an in-progress transfer.

rename [*old_name new_name*] Renames an existing filename to a new filename on the remote host. You can rename files on the PC by using the **!** command to escape to a command interpreter.

retrieve [*remote_file local_file*] Synonymous with **get**.

rmdir *remote_directory* Deletes a specified directory on the remote machine. Not all servers support this command.

send [*local_file remote_file*] Synonymous with **put**.

server *command* Synonymous with **quote**.

show *filename* Displays the text of a specified file (from the remote machine only) on your screen.

site free Returns the number of bytes available on the FTP server.

stat Returns the current state of the remote machine's server. Not all servers support this command.

store [*local_file remote_file*] Synonymous with **put**.

sunique [**on** | **off**] Causes the server to use a unique filename when storing a file.

take *local_file* Reads commands for **ftp** from a local file. Prompts and password responses still come from the keyboard. This command is useful for those cases where you transfer a standard set of files between hosts on a regular basis. The **ftp** command treats command lines starting with the number sign (#) as comments and does not execute them.

tenex Enables the transfer of binary files to or from a TOPS-20 machine and from most LISP machines. The Tenex mode is equivalent to Local 8.

tget [*remote_file local_file*] Like **get**, but transfers a remote file to a local directory using tenex (binary) mode (for just this one transfer).

tput [*local_file remote_file*] Like **put**, but transfers a local file to a remote directory using Tenex (binary) mode (for just this one transfer).

type *type* Displays the current file transfer mode. Set the transfer mode by specifying type. The command accepts the following transfer mode types: **image**, **ascii**, **tenex**, **local** *n*, **ascii_nonprint**, **ascii_telnet**, or **ascii_carriage**. For example, the command **type image** is equivalent to **image**.

user *name* Synonymous with **login**.

verbose (**on** | **off**) Synonymous with **debug**.

version Displays the version and patch level of the command. Refer to this information if you call technical support.

Examples

In the following examples, user Pat (password is dogwood) opens an **ftp** connection on host vex.xyz.com.

To get quickly a copy of the remote file \DESSERTS\CAKE.TXT, Pat enters the following:

```
ftp -u pat dogwood vex.xyz.com get \desserts\cake.txt cake.txt

FTP Trying...Open
220 vex.xyz.com FTP server ready.
331 Password required for pat.
Login successful.
Transferred 1315 bytes in 1 seconds (10520 bits/sec, 1315 bytes/sec)
226 Transfer complete.
```

To open an **ftp** session on the remote host, Pat enters

```
ftp vex.xyz.com

FTP Trying...Open 220
vex.xyz.com FTP server ready.
Userid for logging in on peach.comp.com(pat) pat
331 Password required for (pat).
Password for logging in as (pat) on vex.xyz.com
```

```
230 User pat logged in.
ftp:vex.xyz.com>
```

To change to the remote subdirectory DESSERTS, Pat enters

```
ftp:vex.xyz.com> cd desserts
```

To display a listing of the directory DESSERTS, Pat enters

```
ftp:vex.xyz.com> dir desserts
```

To change the PC's current working directory to the subdirectory DESSERTS, Pat enters

```
ftp:vex.xyz.com> lcd desserts
```

To transfer all files whose suffix is .TXT from the remote machine's current directory to the PC's current directory, Pat enters the following. The example assumes that Pat's machine understands the asterisk (*) wildcard.

```
ftp:vex.xyz.com> mget *.txt
```

To close the **ftp** session, Pat enters

```
ftp:vex.xyz.com> exit
```

See Also

ftpsrv, passwd, rcp, tftp

ftp

ftpsrv

Usage

ftpsrv [**-h** *host*] [**-l**] [**-t**] [**-w**]
ftpsrv [**-?** | **-version**]

Description

The **ftpsrv** command starts a File Transfer Protocol (FTP) server on your PC. Other hosts can then connect to your PC to initiate file transfers.

While the FTP server is running, you cannot run other applications on the PC. To turn off the FTP server, use the **q** command. If a file transfer is already in progress when you quit, the FTP server shuts down immediately and does not notify any logged-in hosts. Before quitting, you can use the **s** command to determine if someone is using the server. (See the section "Interactive ftpsrv Commands" for more information.)

You can control access to a PC running **ftpsrv** by setting up a password file on your PC.

DOS transfers files to and from the current working directory. The user on the remote machine, however, can specify a full pathname; users may *need* to use full pathnames in a command if the colons and backslashes appearing in fully qualified DOS filenames are also special characters (with different meanings) on the remote host. Note that the FTP server accepts both slashes (/) and backslashes (\) as local path delimiters.

This version of **ftpsrv** lets several users transfer files to and from the PC at the same time, provided you set a sufficient number of TCP connections. You can set TCP connections in the `[pctcp kernel]` section of the PCTCP.INI file, or on the command line when you load the kernel (for example,**`ethdrv -t 20`**).

Caution: An FTP server is embedded in the remote login programs: tn and rloginvt. The FTP server in these applications supports using a password file; if your system does not have a password file, anyone can log in while the server is running.

Command Line Options

-h *host* — Restricts access to the FTP server on your PC to the specified host. You can use either the hostname or the IP address to specify the host.

-l — Sets error-only logging, displaying only error messages.

You can redirect logging information to a file using standard I/O redirection. For example, a command in the following form logs all information in the FTP.LOG file:

```
ftpsrv > ftp.log
```

Since output is redirected to the file, the usual information is not displayed; however, you can still use the interactive **ftpsrv** commands.

-t — Disables connection idle time-out. The server does not stop if idle.

-w — Enables write-protect mode, which prevents a user from writing files to your PC.

If you type **`ftpsrv -w`**, users can only retrieve files (not copy files to your PC).

-? Displays and explains the usage line of the command.

-version Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Interactive ftpsrv Commands

While you are running **ftpsrv**, you can issue commands to obtain logging statistics that are useful for debugging. There are three logging levels:

Use this level	To display
Error-only logging	Minimal logging information.
Normal logging (default)	Information about **ftp** connections and users.
Debug logging	Maximum logging information.

Use the following commands to perform these functions:

C Closes a log file.

D Displays debugging information.

d Sets debug logging, displaying the most data about **ftp** sessions, including **ftp** command requests and information about connections.

F Sends logging messages to a file; **ftpsrv** prompts you for a filename.

l Sets error-only logging, displaying only error messages.

N Displays configuration information.

n Sets connection and login logging, displaying information about **ftp** connections and users. The information includes connections being established and broken, as well as users logging in and out.

q Exits from the FTP server.

S Displays kernel statistics.

s Displays FTP server statistics, including the number of connections made to the PC, the number of open connections, the number of files received and sent, and the number of bytes received and sent.

T Displays TCP statistics.

t Turns on a trace level debugging log.

w Turns on and off write-protect mode.

? Displays a list of available commands.

Example

To start the FTP server running on your PC, enter

```
ftpsrv
```

Your PC displays information about the server as well as directions on how to exit from the server (**q)** and how to get help (**?)**.

See Also

ftp, passwd, rloginvt, tn

ftpsrv

ftpver

Usage

ftpver *filename*
ftpver [**-?** | **-version**]

Description

The **ftpver** command invokes the DOS program FTPVER.EXE, which displays version information for any executable program that runs in Windows, including dynamic link library (.DLL), executable (.EXE), and driver (.DRV) files. Some executable files may not contain or display version information.

When information is available, **ftpver** displays it in the following order:

```
Program Name:
CompanyName:
File Description:
Version:
```

Some of the preceding items are not displayed if not available to **ftpver**. When the file itself is not available or is not a Windows executable, **ftpver** displays a message to that effect.

You can use wildcard characters and specify multiple filenames on the command line. If you do not specify a filename (when using the **ftpver** *filename* command), **ftpver** displays a `No file specified` message followed by the required syntax and command options.

Command Line Options

filename	Specifies the executable file or files for which you want information.
-?	Displays and explains the usage line of the command.
-version	Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Examples

To display information about the PCTCPAPI.DLL program for Windows, enter

```
C:\> ftpver pctcpapi.dll

Program Name: PCTCPAPI.DLL
File Description: FTP Software Windows Application DLL v3.0
```

To display program names and versions of all .EXE Windows programs in a directory, enter

```
C:\> ftpver *.exe

Program Name: CALC.EXE
CompanyName: Microsoft Corporation
File Description: Windows Calculator application file
Version: 3.10
```

```
Program Name: CALENDAR.EXE
CompanyName: Microsoft Corporation
File Description: Windows Calendar application file
Version: 3.10
.
.
.
MSD.EXE is not a Windows executable.
.
.
.
Program Name: WINHELP.EXE
CompanyName: Microsoft Corporation
File Description: Windows Help Engine application file
Version: 3.10.425
```

To display information for specific, multiple files, enter filenames using DOS conventions:

```
C:\> ftpver wping.exe wnet386.dll

Program Name: WPING.EXE
File Description: FTP Software Windows Ping Utility v2.31

Program Name: WNET386.DLL
File Description: FTP Software Windows Application DLL v3.0
```

ftpver

host

Usage

host [**-dhntACHMNPSTW***] [**-a** | **-s** *server*] *host1 ... hostn*
host [**-?** | **-version**]

Description

The **host** command displays the Internet address that corresponds to the name of the host.

The **host** command uses all available name resolution protocols to translate an Internet address to a hostname. The **host** command searches for the specified name in a host table, if set, then tries domain name servers. The **host** command is useful for troubleshooting when you suspect that name tables may be inconsistent or incorrect.

Command Line Options

Most of the following options define domain queries that you can specify with the host command. These queries use the Domain Name System (DNS) library, not the kernel. Use the fully qualified domain name for *host* in the command line. By default, **host** requests class Internet records.

-*
Queries the host for all types of related records.

-A
Queries the host for A (address) records.

-a
Tries all of the known name resolution methods. The **host** command invokes this option by default. Note that the **-a** and the **-s** options are mutually exclusive.

-C
Queries the host for CNAME (canonical name) records.

-d
Tries all of the configured domain name servers.

-H
Queries the host for HINFO (host information) records.

-h
Queries the host for class HESIOD records.

host1 ... hostn
Specifies the hostname or hostnames to be resolved. You must leave a space between each hostname. You can also specify a series of IP addresses.

-M
Queries the host for MX (mail exchanger) records.

-N
Queries the host for NS (name server) records.

-n
Prevents recursive attempts at name resolution.

-P
Queries the host for PTR (pointer) records.

-S
Queries the host for SOA (start of authority) records.

-s *server*
Tries the specified domain name server. Note that the **-a** and the **-s** options are mutually exclusive.

-T
Queries the host for TXT (random text information) records.

-t
Tries the configured host table.

-W Queries the host for WKS (well-known services) records.

-? Displays and explains the usage line of the command.

-version Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Examples

To query your configured host table (using the `host-table=` entry in the `[pctcp kernel]` section of PCTCP.INI *)* for the IP address and canonical name of username val, enter

```
C:\> host -t val

by host-table, val: 128.127.50.135, cname is val.xyz.com
```

To display any information in the HINFO records for hostname chris.xyz.com, enter

```
C:\> host -H chris.xyz.com

Query id 1281: 1 Questions, 1 Answers, 0 Name Servers, 0 Additional
flags: <RESPONSE><AUTHORITY><CAN_RECURSE><DO_RECURSE>
INFO (13) type Resource Record: chris.xyz.com, class: Internet (1)
Valid 24.00 hr (86400 sec): HINFO Host: Compaq286, OS: DOS
```

See Also

ping

RFCs 882, 883, 973, 1034, and 1035

host

idchmod

Usage

idchmod *mode filename*
idchmod [**-?** | **-version**]

Description

The **idchmod** command sets file access privileges on file systems that are mounted with the InterDrive client.

NFS file permissions are UNIX-like: permissions are represented by digits that indicate some combination of read, write, and execute access for each of three classes of users.

This class	Consists of these users
Owner	The user who creates the file.
Group	A defined set of users who share the group access rights.
World	Any user of the system.

An optional additional digit sets the UNIX setuid, setgid, and sticky bit. The setuid bit is the only optional bit that has meaning in NFS; it translates to the DOS hidden file attribute.

Command Line Options

filename Specifies a filename or directory on the mounted drive. Wildcards are acceptable. If the file whose permissions you are changing has a name that is invalid in DOS, you must specify the file's mapped name.

mode Sets file permissions, in the format [*n*] *nnn*. The first digit is optional and, if specified, can consist of one or the sum of the following possible values:

4 Sets the setuid bit on execution. This bit translates to the DOS hidden file attribute.

2 Sets the setgid bit on execution. This has no meaning in NFS.

1 Sets the sticky bit. This has no meaning in NFS.

The three subsequent digits are required and set permission attributes for the owner, group, and world classes, respectively. Possible values for each digit are as follows:

0 Not readable (hidden).
1 Execute.
2 Write.
3 Write and execute (2 + 1).
4 Read.
5 Read and execute (4 + 1).
6 Read and write (4 + 2).
7 Read, write, and execute (4 + 2 + 1).

Note: The execute privilege, which allows a user to run a program, has no effect on files in DOS.

A DOS user must have read access to an executable file in order to be able to run it.

-? Displays and explains the usage line of the command.

-version Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Examples

Enter the following command to grant read, write, and execute permissions to the owner; read and write permissions to the group; and world read-only permission for the file WORKFILE.TXT:

```
G:\> idchmod 764 workfile.txt
```

To set the same permissions when the file WORKFILE.TXT resides on a different drive and directory (in this example, G:\LETTERS), enter

```
K:\> idchmod 764 g:\letters\workfile.txt
```

To use your system's wildcard feature in setting permissions for a group of files (in this example, all files ending with a .TXT extension), enter

```
K:\> idchmod 764 *.txt.
```

See Also

idls, idconfig, idmnt, idumnt

idchmod

idconfig

Usage

idconfig (**-g** *drive:* [*GID*] | **-l** *seconds* | **-p** [*drive:*] [*n*] *nnn* | **-q** [*drive:*] *value* |
-r *drive: value* | **-t** [*drive:*] *value* | **-w** *drive: value* | **-z** *timeout*)
idconfig [**-?** | **-version**]

Description

The **idconfig** command sets configuration parameters for InterDrive while the TSR is loaded and running. You can change only one parameter at a time, and parameters change for the current session only. Changes to a specific file system last only as long as the file system is mounted. Use corresponding entries in the PCTCP.INI file to set values that last across mounts and across InterDrive sessions.

Note: InterDrive sets the most appropriate defaults for most of these parameters based on PC/TCP kernel configuration, network capacity, and other factors. You should not change these parameters unless you are an aware of the dependencies between the kernel, InterDrive, and the network. Making unnecessary changes can degrade performance.

Command Line Options

-g *drive:* [*GID*] Specifying only *drive:* displays the list of groups that the user is a member of on the mounted drive.

Specifying *drive:* and *GID* changes the user's primary group identifier to the value specified. The new value must be one of the GIDs listed as a result of the **idconfig -g** *drive:* command. Only PCNFSD version 2 servers support this option.

-l *seconds* Sets the look-up cache timeout, in seconds. The InterDrive client maintains a cache of the file and directory names it has looked up recently. By default, InterDrive deletes entries after they have been cached 30 seconds.

Setting the cache timeout higher speeds performance when you want to return to a file or directory repeatedly, but not frequently. Decreasing the The minimum timeout value is 1 second; the maximum is 300 seconds. Specifying 0 causes InterDrive to cache the information indefinitely (until the cache is full and newer information replaces older information).

You can use the `cache-timeout=` entry to set this value in the `[pctcp idrive]` section of your PCTCP.INI file.

-p [*drive:*] [*n*] *nnn* Sets the NFS file permission mask for all drives to be mounted subsequently, or for the specified drive. All files that you create or copy to the drive receive these default permissions. The first digit is optional and sets the setuid, setgid, and sticky bit. (The setuid bit, with a value of 4, translates to the DOS hidden file attribute; the other bits have no equivalent DOS or NFS meaning.) The next three digits apply to owner, group, and other permissions for directories and files. Possible values for these digits are as follows:

0 Not readable; not seen by DOS commands.
1 Execute.
2 Write.
3 Write and execute.
4 Read.
5 Read and execute.
6 Read and write.
7 Read, write, and execute.

Note: Granting only the execute privilege has no effect for DOS users. A DOS user must have read access to an executable file in order to be able to run it.

You can use the `umask=` entry to set this value in the `[pctcp idrive]` section of your PCTCP.INI file.

-q [*drive:*] *value* Sets the streaming value for all drives to be mounted subsequently, or for the specified drive. The *value* argument specifies the number of packets. "Streaming" is the process of sending additional packets without waiting for a response from the server. By default, the streaming value is 2 packets. Setting the value to 0 turns off streaming and causes InterDrive to wait for a response to each packet before sending another.

Note: FTP recommends that you use the autotune feature and allow InterDrive to establish the most appropriate value for streaming. Autotuning is enabled by default.

-r *drive: value* For the specified drive, sets the largest User Datagram Protocol (UDP) packet size readable by the InterDrive client, in bytes. The maximum varies depending on the transaction size at the server, the maximum transmission unit (MTU) for your network, and the value of the `huge-packets=` entry in the `[pctcp kernel]` section of your PCTCP.INI file.

Note: FTP recommends that you use the autotune feature and allow InterDrive to establish the most appropriate value for read size. Autotuning is enabled by default.

-t [*drive:*] *value* Sets the maximum number of seconds the InterDrive client spends trying to resend unacknowledged packets before aborting its current operation. You can set this timeout for a specific drive or for all drives to be mounted subsequently. The default value is 30 seconds. InterDrive may time out on several operations before you see a DOS system error message indicating that the operation is unsuccessful. Typically, you see an `Abort, Retry, Fail?` message. If you choose to abort, you must repeat any operations that did not complete before the timeout.

Setting this value to 0 disables the timeout. This is useful when you execute InterDrive commands in batch files. However, if no timeout is set in interactive mode, you must manually abort operations that do not succeed.

You can use the `timeout=` entry to set this value in the `[pctcp idrive]` section of your PCTCP.INI file.

-w *drive: value* For the specified drive, sets the largest packet size that the InterDrive client can write, in bytes. It may be helpful to set this value to the block size of the NFS server. The maximum size you can set is 8192.

Note: FTP recommends that you use the autotune feature and allow InterDrive to establish the most appropriate value for write size. Autotuning is enabled by default.

-z *timeout* Sets the amount of time, in seconds, that the InterDrive client spends negotiating with a server for file locking. The minimum is 1 second; the maximum is 15; and the default is 3. This option has no effect when file locking is off. Setting the timeout to 0 causes InterDrive to keep trying to negotiate file locking until the server responds.

You can use the `lock-timeout=` entry to set this value in the `[pctcp idrive]` section of your PCTCP.INI file.

-? Displays and explains the usage line of the command.

-version Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Examples

To set a default file permission mask of 744 for files created on or copied to the mounted file system on the F drive, enter

```
C:\> idconfig -p F: 744
```

To change your primary group identifier (GID) to 17 for the file system mounted on drive E, enter

```
idconfig -g E: 17
```

See Also

idrive, idchmod, idutil

idconfig

idls

Usage

idls [*filename*]
idls [**-?** | **-version**]

Description

The **idls** command lists names and information about files on a mounted NFS file system. The UNIX-like output of this command provides a different view of mounted files than the DOS **dir** command, which displays information about files in typical DOS style. Without options, the **idls** command lists file and directory names, dates, sizes, and permissions.

Because files on the NFS file server are usually case sensitive, the **idls** command is also case sensitive. Therefore, you must use the appropriate case when you enter the filename. For example, the filename ABcd.doc does not refer to the same file as abcd.doc.

Command Line Options

filename	Specifies a filename or directory in the format native to the remote file server. You can use either slash (/) or backslash (\) as delimiters, depending on the naming conventions supported by the file server. The asterisk (*) wildcard character is valid.
-?	Displays and explains the usage line of the command.
-version	Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Technical Notes

The following special characters in a directory listing convey additional information:

Character	Meaning
`l` in the first position	The file is a symbolic link.
`h` in the first position	The file or directory is hidden.
`h` in the first position and `s` in place of the `x` in the owner permission position	The file or directory is hidden because the setuid bit is set.
`H` in the first position	The filename starts with a leading dot (by default, InterDrive treats these as hidden files).
`S` in place of the `x` in the group permission position	The setgid bit is set.

Examples

To display the names and permission information for all files on the F: drive in UNIX-style format, enter

```
F:\> idls

drwxr-xr-x          512             Sep 15 14:55:09 .
drwxrwxrwx          1024            Sep 13 16:01:49 ..
-rw-rwSr--          23555           Jun 17 10:25:50 reports.xls
-rw-rw-r--          274716          Jul 16 14:41:06 sort_rec.out
```

See Also

idutil, idchmod

idls

idmnt

Usage

idmnt [*filesys* | **-a**]
idmnt [*filesys host path drive authentication user*]
idmnt [*drive* *host**path*]
idmnt [*host path drive*]
idmnt [**-?** |**-version**]

Description

The **idmnt** command makes a file system on a remote NFS server available for use locally. The process of connecting to the remote file system and associating a local PC drive with it is called "mounting." Entering the **idmnt** command without options produces a list of currently mounted file systems.

Typically, you mount a file system by configuring it first in a `[pctcp idrive filesys]` section of your PCTCP.INI file, then by specifying its configured name on the **idmnt** command line. You also can mount a file system by specifying all parameters on the command line.

Command Line Options

-a Mounts all file system(s) named in the `default-drives=` entry in your PCTCP.INI file.

authentication [**/r**] Specifies the type of user authentication supported by the server. Currently the only valid keyword is **pcnfs**. If you want to mount a file system as read-only, add **/r** to the keyword, for example, **pcnfs/r**.

drive Specifies a drive letter to associate with the mounted file system. The drive must be within the range specified by the `lastdrive=` entry in the CONFIG.SYS file. Each network drive that you mount requires a drive letter that is not already in use. A drive letter followed by an asterisk (for example, **G***) indicates that you want to mount the drive using the specified drive letter or, if that drive is already in use, the next available drive letter.

filesys Specifies a unique, user-assigned name of 11 characters or less, to be used as the volume label for the mounted drive. If you are mounting a previously configured file system, this is the name of a `[pctcp idrive filesys]` section in your PCTCP.INI file.

host Specifies the hostname or IP address of the NFS file server.

path Specifies the complete pathname of the file system to mount. You must use the path syntax of the server's operating system; for example, `/usr/abc/public` illustrates the correct path syntax for a UNIX server. The pathname you specify represents the root of the mounted file system on your local PC. You cannot change to a directory above it.

user Specifies your username for logging in to the file server. This name and any associated password must be listed in the password file on the server. Specify

user **nobody** if you want to mount a file system without entering a password, or if you want to mount file systems on hosts that are not running PCNFSD. Many hosts grant the user nobody the same permissions granted to an anonymous guest.

-? Displays and explains the usage line of the command.

-version Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Examples

To see a list of all currently mounted file systems, enter

```
G:\> idmnt

File system "finance1" is mounted on drive f:
```

To mount the file system apollo, which is defined in the configuration file, enter

```
F:\> idmnt apollo
```

To mount all of the default file systems defined in the configuration file, enter

```
C:\> idmnt -a
```

To mount the /etc/sys file system from host vex.xyz.com on drive F: enter

```
C:\> idmnt f: \\vex.xyz.com\/etc/sys
```

See Also

idumnt, idnet, idrive

idmnt

idnet

Usage

idnet [**login** [*username* [*password*]] | **logout** [**drives** | **printers** | **all** | **none**] | **show**]
idnet [**help** | **-?** | **-version**]

Description

The **idnet** command without any arguments starts a menu-driven application that lets you mount and unmount network file systems and printers and set default login information. If you enter the command with arguments, you can set, display, or change default login information; or you can log out of network connections.

Once you set a default username and password with **idnet**, you are no longer prompted for that information when mounting file systems and printers from either DOS or Windows. A change in the login information is also reflected in both DOS and Windows.

Command Line Options

help Synonymous with the **-?** option.

login [*username* [*password*]]

Sets the default NFS username and password . If you do not specify a username or password, the command prompts for them. The **idnet** command derives a default username from the `[pctcp idrive]` section of your PCTCP.INI file, or if none is specified there, the `[pctcp general]` section.

Note: When a file system or print session definition in your PCTCP.INI file includes a `user=` parameter, that value takes precedence over the username that you set with this command.

logout [**drives | printers | all | none**]

Clears your username and password from memory, and optionally closes connections. Entering **logout** with no arguments causes the command to prompt you for a keyword. Keywords are as follows:

drives	Close connections to all mounted file systems.
printers	Close connections to all mounted NFS printers.
all	Close connections to all mounted file systems and NFS printers.
none	Clears your username and password from memory but retains existing connections.

show Displays the current settings for **idnet**.

-? Displays and explains the usage line of the command.

-version Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Example

To log in to the network, enter

```
idnet login

Username (default is blue)? blue
Password for blue?
Your default username and password have been set.
Your default username is blue
```

To log out of the network and close all connections, enter

```
idnet logout all

Your username and password have been flushed from memory

Unmounting file system "apollo" from drive g: ...
Drive G: unmounted

Unmounting remote NFS priner from device LPT1 ...
Device LPT1 unmounted
```

To display your current **idnet** settings, enter

```
idnet show

Your default username is blue
Your default password is set
```

See Also

idrive, idprint, idmnt

idnet

idprint

Usage

idprint (*option* | *command* [*subcommand argument(s)*])
idprint *device \\host\printer*
idprint help [**edit** | **file** | **job-queue** | **mount** | **options** | **printer** | **server** | **unmount**]
idprint [**-?** | **-version**]

Description

The **idprint** command works together with the InterDrive client to redirect printing from your local PC to NFS printers. By associating a local printer port with a network printer, you can print files directly from an application or command line to the network printer. The set of characteristics that define a print connection is known as a print session. You can define a print session in one of two ways:

- Configure it in a `[pctcp idprint print_session]` section of your PCTCP.INI file; then specify the session name on the **idprint mount** command line. This is the way you should typically mount printers that you plan to use frequently.
- Specify all print session parameters on the command line. The InterDrive client does not retain the definition of these print sessions after you unmount them.

You can reconfigure an existing print connection by using the **idprint edit** command. These changes are for the current print session only and do not get saved to the PCTCP.INI file.

You can abbreviate any of the **idprint** commands by using the first one or more letters in the command name. For example, the commands **idprint h** and **idprint help** are equivalent.

Command Line Options

-comment Turns on or off the display of comments generated by the remote host.

device \\host\printer Mounts a printer by specifying the LPT or COM port to redirect, the hostname or IP address of the print server, and the printer name.

-list Displays information about mounted print sessions. You can use the **idprint edit** command to change the values for the current session.

-printlog Displays a record of three phases of the remote printing process: redirection of the file from the local printer port, occurrence of the condition indicating that the file should be sent to print, and transfer of the file to the remote server.

-trace Displays debugging information, which you can save in a file.

-? Displays and explains the usage line of the command.

-version Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Commands and Subcommands

Use the **idprint** commands and subcommands to control the mounting and unmounting of

printers, set or change print configurations in memory, and control functions associated with print services on the remote host. The following sections list the **idprint** commands and subcommands and their syntax. In general, you enter commands and subcommands in the following form:

idprint *command* [*subcommand argument(s)*]

The following is a description of each command and subcommand.

idprint edit *subcommand argument(s)* (*print_session* | *device*)

Sets or changes the configuration of an existing print connection. The command makes changes in memory only and does not save them to the PCTCP.INI file. The *print_session* name can be the name of a `[pctcp idprint print_session]` section of the PCTCP.INI file, or the name of a connection configured by a command line. Use either the print session name or the *device* name (for example, LPT1, COM3) to specify the connection that you want to change.

Valid subcommands and their arguments are as follows:

file *filename*	Specifies the name of the print spool file on the print server.
jobid *n*	Sets or changes the identifier for the job on the print server.
mine (**yes** | **no**)	Specifies whether you want to display only your jobs or all users' jobs in the queue.
number *n*	Sets or changes the number of copies to print.
options *option*	Sets or changes printer command options.
printer *printer*	Sets or changes the remote printer name.
qpos *n*	Sets or changes a job's position in the print queue.
timer *seconds*	Sets or changes the number of seconds before the **timeout** print condition takes effect.
when *condition(s)*	Sets or changes conditions that indicate when to send a file to print. Specifying a print condition that is already set disables it. Specifying a condition that is not set enables it. The following are valid keywords: **timeout**—Print when the specified period has elapsed since the last character arrived at the redirected printer port. The default timeout period is 30 seconds; use the **timer** subcommand to change that value. **hotkey**—Print when you press Ctrl+LeftShift+RightShift.

eof—Print when you close the file.

exit—Print when you exit from the DOS application from which you chose to print the file.

Separate multiple keywords with commas or spaces.

idprint file *filename* (*print_session* | *device*)

Prints the named file using the specified print connection. Arguments and their meaning are as follows:

filename	The name of the file to print. Wildcard characters are not valid (you can print only one file at a time).
print_session	The name of a preconfigured `[pctcp idprint print_session]` section in your PCTCP.INI file, or the name of a connection that was configured by command line.
device	The name of the local port associated with the print connection you want to use.

idprint help [*command-argument*]

Gives online syntax help for **idprint** commands. Entering **`idprint help`** without any arguments causes **idprint** to display an introductory help topic. Enter one of the following for *command-argument*:

edit	**options**
file	**printer**
job-queue	**server**
mount	**unmount**

idprint job-queue *subcommand* (*arguments* [*comment*] | *print_session* | *device*)

Manages the status of a job in a print queue on the remote host. Note that these commands are available only with PCNFSD Version 2, and not all servers support all functions.

The following are the valid subcommands and their functions. See the **idprint edit** command for an explanation of subcommand arguments.

cancel Cancels a print job.

Usage: **idprint job-queue cancel** (*host printer user*

jobid [*comment*] | *print_session* | *device*)

free Resumes printing of a job that was suspended.

Usage: **idprint job-queue free** (*host printer user jobid* [*comment*] | *print_session* | *device*)

hold Suspends printing of a job.

Usage: **idprint job-queue hold** (*host printer user jobid* [*comment*] | *print_session* | *device*)

list Lists jobs in the print queue. A value of **yes** for *mine* specifies that you want to list only your jobs; **no** specifies that you want to see all users' jobs.

Usage: **idprint job-queue list** (*host printer user mine* [*comment*] *print_session* | *device*)

requeue Changes the priority of a print job in the queue.

Usage: **idprint job-queue requeue** (*host printer user jobid qpos* [*comment*] *print_session* | *device*)

start Sends the file to the print spool directory on the remote host without waiting for print conditions to take effect.
Usage: **idprint job-queue start** (*host printer user file* [*options*] [*number*] [*comment*] *device* | *print_session*)

idprint mount (*host printer device* | *print_session* | **all**)

Redirects print output from a local port to a remote printer . The following is a summary of valid arguments:

host The hostname or IP address of the print server.

printer The name of the remote printer.

device The name of the local port whose output you want to redirect (valid ports are LPT1 through LPT3 and COM1 through COM4).

print_session A preconfigured *print_session* name from a `[pctcp idprint print_session]` section of your PCTCP.INI file.

all All printers preconfigured in `[pctcp idprint print_session]` sections of your PCTCP.INI file.

When you use the *host printer device* syntax to mount a printer, **idprint** assigns a

print session name based on the port you are redirecting: for example, p1 for LPT1, p3 for LPT3, p4 for COM1, and so on. You can use this session name in subsequent **idprint** commands.

idprint printer *subcommand* (*host printer* [*comment*] |*print_session* |*device*)

Performs printer related functions over the specified print connection. Note that these commands are available only with PCNFSD Version 2, and not all servers support all functions. Valid subcommands are as follows:

admin	Issues a printer-specific administrative operation.
init	Determines remote spool directory in preparation for printing.
status	Gets printer status.

idprint server *subcommand arguments*

Gets NFS server information. The following are valid subcommands and their arguments. Note that only PCNFSD Version 2 supports comments.

alert

Sends a *message* from *user* to the system administrator of *host*, the NFS server that controls the *printer* named in either /etc/printcap or /pcnfsd.conf on the server.

Usage: **idprint server alert** *host printer user message*

info

Lists the PCNFSD functions supported on the specified remote host.

Usage: **idprint server info** *host* [*comment*]

list

Lists available printers on the specified remote host. Note that the list may be truncated if the size of the printer data exceeds 1K.

Usage: **idprint server list** *host*

mapid

Displays the ID associated with the specified username or group name, or the username or group name associated with the specified ID. The *request* field indicates to the server what information to return for the specified name or ID. Legal values include **0** (for UID), **1** (for GID), **2** (for username), and **3** (for group name).

Usage: **idprint server mapid** *host request id* [*comment*]

idprint unmount (*print_session* | *device* | **all**)

Disconnects an existing print session and removes it from memory. Specify either the print session name or the redirected port. Specify **all** to disconnect all mounted printers.

Examples

To configure a print session where the redirected port is COM1, the host is london and the printer is hpljII, enter

```
idprint com1 \\london\hpljII
```

To mount a printer that is configured in the `[pctcp idprint jet]` section of your PCTCP.INI file, enter

```
C:\> idprint mount jet
```

To unmount an existing print session named jet, enter

```
C:\>idprint unmount jet
```

To view a list of mounted printers, enter

```
C:\> idprint -list
```

To list the PCNFSD subcommands supported on the remote host paris,

```
C:\> idprint server info paris
```

See Also

idrive, idutil

idprint

idrive

Usage

idrive [**-a** *n*] [**-c** *n*] [**-e**] [**-k** *n*] [**-m** *n*] [**-n** *n*] [**-p** *n*] [**-t** *n*]
idrive [**-min**]
idrive [**-?** | **-version**]

Description

The **idrive** command starts the InterDrive client software, which lets you use files and printers on a remote NFS server as if they were local.

By default, if a memory manager that provides access to upper memory is present, InterDrive tries to load into an upper memory block. If not enough upper memory is available, InterDrive loads in the conventional memory area. When InterDrive loads, it also tries to detect the presence of an expanded memory manager (EMM). If an EMM is running, InterDrive allocates the maximum allowable number of print entries, look-up cache buffers, name-mapping cache buffers, and read-write cache buffers in expanded memory, overriding any existing settings for these in your PCTCP.INI file.

You can specify InterDrive operating parameters in either of two ways:

- Set parameters in the `[pctcp idrive]` section of your PCTCP.INI file before you start the InterDrive client.
- Set parameters with **idrive** command line options.

FTP Software recommends that you configure parameters in the PCTCP.INI file and use command line options only to temporarily override the configured parameters.

Note: To unload the InterDrive client, use the **idumnt -u** or **idutil -u** command.

Command Line Options

-a *n* — Specifies the number of file lock entries. The minimum value is 1; the maximum is 2048; and the default is 20.

-c *n* — Specifies the maximum number of buffers InterDrive uses to retain the names of directories accessed during a directory search operation. The minimum value is 1 buffer; the maximum is 128; and the default is 6.

-e — Enables use of an expanded memory manager (EMM) for caching and print buffering. By default, if an EMM is present and running, InterDrive automatically uses it. You do not need to use this option unless you want to override the `use-emm=` entry in the `[pctcp idrive]` section of your PCTCP.INI file.

-k *n* — Specifies the number of the look-up cache buffers, which speed the retrieval of frequently used data. The minimum value is 9 entries; the maximum is 512; and the default is 0, which disables look-up caching. If InterDrive loads when an EMM is running, and if the **-k** option specifies a value other than 0 (disabled), InterDrive ignores the value specified and sets the number of lookup cache

buffers to the maximum. InterDrive calculates the maximum value based on several factors; it is usually about 500.

-m *n* — Specifies the number of file systems users can mount concurrently. The minimum is 1 file system; the maximum is 16; and the default is 2.

Note: Make sure that the value of the `lastdrive=` entry in your CONFIG.SYS file is high enough to accommodate the number of mounted drives you want to use.

-min — Loads InterDrive using a default minimum configuration. This configuration permits one mounted file system and no print connections and occupies the minimum amount of memory. Streaming, read-write caching and lookup caching are disabled. If EMM and high memory are available and InterDrive's use of them is enabled, InterDrive loads into an upper memory block and uses expanded memory.

Note: You cannot use any of the other command line options when you use the **-min** option.

-n *n* — Specifies the number of name-mapping cache buffer entries. The minimum value is 32 entries; the maximum is 2048; and the default is 32. If InterDrive loads when an EMM is running, it ignores this option and sets the number of entries to the maximum value of 2048.

-p *n* — Specifies the number of printers users can mount concurrently. The minimum value is 0; the maximum is 7; and the default is 1. Specify **-p 0** if you are not planning to use a remote NFS printer and want to save conventional memory. If InterDrive loads when an EMM is running, and if the **-p** option specifies a value other than 0, InterDrive ignores this option and sets the number of print connections to the maximum value of 7.

-t *n* — Specifies the number of transaction buffers. The minimum value is 1; the maximum is 8; and the default is 3. InterDrive uses transaction buffers in its internal functions. Transaction buffers are related to streaming: the number of transaction buffers must be at least one greater than the stream value, which you can set with the **idconfig -q** command.

-? — Displays and explains the usage line of the command.

-version — Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Examples

The following command loads InterDrive and allows for the concurrent use of six file systems:

```
C:\> idrive -m 6
```

The following command loads InterDrive with 100 look-up cache buffer entries and 2 print entries (an expanded memory manager is not in use):

```
C:\> idrive -k 100 -p 2
```

See Also

idchmod, idconfig, idls, idmnt, idprint, idumnt, idutil

idrive

idumnt

Usage

idumnt (*drive:* | **-a** | **-u** | *filesys*)
idumnt [**-?** | **-version**]

Description

The **idumnt** command disconnects a mounted NFS file system. This command is useful if you have mounted the maximum number of drives and want to mount another. It can also unmount all file systems at once and unload the InterDrive software. You can enter the **idumnt** command from any drive, including the one that you want to unmount.

Command Line Options

-a	Unmounts all drives.
drive:	Specifies the drive you want to unmount.
filesys	Specifies the name of the file system you want to unmount. This can be a name in your PCTCP.INI file or a name assigned when you mounted the file system from the command line.
-u	Unmounts all drives and printers and unloads InterDrive.
-?	Displays and explains the usage line of the command.
-version	Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Examples

To unmount a drive G, enter

```
idumnt g:
```

To unmount a file system called finance1, enter

```
idumnt finance1
```

To unmount all mounted drives, enter

```
idumnt -a
```

To unmount all mounted drives and printers and unload InterDrive, enter

```
idumnt -u
```

See Also

idmnt, idrive, idnet

idumnt

idutil

Usage

idutil (**-d** | **-f** | **-h** | **-l** [*drive:*] | **-p** *drive: nfsname* | **-s** | **-t** | **-u** | **unload** | **-y**)
idutil [**-?** | **-version**]

Description

The **idutil** command displays InterDrive client statistics and settings and lets you change certain settings while the client is running. Use the **idutil** command to map filenames, to display statistics and status information, to enable or disable file locking, or to unmount all file systems and printers and unload InterDrive.

Command Line Options

-d Displays the contents of the name mapping cache. This cache changes dynamically and may contain mappings for filenames that are not in your current working directory. An asterisk next to a name denotes a mapping that you set as permanent with the **idutil -p** command or with a configuration file entry.

-f Displays current settings for each mounted file system.

-h Enables or disables the display of UNIX files beginning with a dot, such as .cshrc or .login files, when you use the **dir** command. By default, these files are hidden. In a directory listing, the dot is converted to a tilde (~) or to an alternative mapping character that you specify in the PCTCP.INI file.

-l [*drive:*] Enables or disables file locking for all files, or if you specify a drive, for files on the mounted drive, restricting any other client with file locking enabled from writing to those files. By default, file locking is enabled; use the **idutil -f** command to see the current locking status for mounted file systems. You can control how long InterDrive waits for responses to file locking requests with the **idconfig -z** command.

-p *drive: nfsname* Indicates that you want a mapped name for the specified NFS filename to remain the same (permanent) for the duration of the InterDrive session. Filename mappings that you do not specify as permanent may change several times during the course of a session, depending on the number of names InterDrive has to map and the size of the name mapping cache.

Note that you cannot specify what you want the mapped name to be, only that you want it to remain the same. You must set permanent filename mappings individually; you cannot use wildcards. You can also establish permanent filename mappings with the `mapping=` entry in the `[pctcp idrive]` section of your PCTCP.INI file.

-s Displays performance statistics.

-t Displays current global settings for InterDrive client connections.

-u | **unload** Unmounts any mounted drives and printers and unloads InterDrive.

-y Enables or disables symbolic link processing. You can also do this by setting the `symbolic-link=` entry in the `[pctcp idrive]` section of your PCTCP.INI configuration file. Do not disable symbolic link processing when your current directory is one that you accessed through a symbolic link. (The **idls** command displays a `l` next to symbolically linked files.)

-? Displays and explains the usage line of the command.

-version Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Examples

To display InterDrive statistics, enter

```
idutil -s

----------------------InterDrive Statistics------------------------

9696 RPC requests sent
9650 RPC replies received
119 retries sent
73 bad XIDs received

174 NFS errors (these can be ignored)
0 stale filehandle errors
0 send errors
0 receive errors

Last net I/O error = 0 (No error)
Last NFS error = 248 (Unexpected end of file or directory)
Last DOS error = 18 (No more files)
```

To display statistics about mounted file systems, enter

```
idutil -f

---------------- Filesystem Statistics ----------------


File system "finance" is mounted on drive F:
Remote file system path = /finance
Remote host = 255.255.50.107
uid = 1150
gid = 15
No additional groups
NFS transport protocol = UDP
NFS port = 2049
Mount port = 682
Lock port = 1027
FAT = NO (upper and mixed case filenames mapped)
Server transfer size = 8192
Current round trip time = 0.06 seconds (accuracy is within 0.06 seconds)
```

```
"Base" round trip time = 0.06 seconds (accuracy is within 0.06 seconds)
Autotuning = ON
Read size = 1024 Streaming = 4
Write size = 8192 Streaming = 4
Stream = 2
I/O timeout value = 30
Local permission mask = 664
File sharing/locking = YES
CD-ROM name processing = NO
```

To unmount all drives and unload InterDrive, enter

```
idutil -u

Unmounting remote NFS printer from device LPT1 ...
Device LPT1 unmounted
Unmounting file system "reports" from drive F: ...
Drive F: unmounted
InterDrive TSR is now unloaded.
```

See Also

idconfig, idrive

idutil

inet

Usage

inet [**arp**] [**debug**] [**pap**] [**ppp**] [**route**] [**slip**] [**stats**] [**tcp**] [**version**] [**unload**]
inet [**config** [**advanced** | **security**]]
inet [**ipcp** (**stats** | **config**)]
inet [**lcp** (**stats** | **config**)]
inet [**-?** | **-version**]

Description

The **inet** command displays network statistics from the TSR kernel, and can unload the TSR kernel.

Command Line Options

advanced Displays information about advanced kernel configuration parameters such as time to live, type of service, precedence, and so on. You must supply the **config** option when using **advanced**.

arp Displays the current contents of the kernel's address resolution protocol (ARP) cache.

config Displays the date and time the current kernel began running, the hardware configuration used by the kernel, network addresses, current connections, and other configuration information.

debug Displays information about packet receipt and transmission, interrupts, ARP statistics, and so on. For Ethernet and 802.5 interfaces, the debug argument also displays the physical address of the interface. This argument is useful when troubleshooting network performance, tuning the kernel, and analyzing remote transfers.

ipcp (**stats** | **config**) Displays information about the Internet Protocol Control Protocol (IPCP) layer. You must supply one of the following arguments:

stats Displays the IPCP layer statistics. The IPCP layer is part of the Point-to-Point Protocol (PPP) kernel. It handles IP addresses and Van Jacobson Compression for a PPP link.

config Displays the IPCP layer configuration, including the initial, intermediate, and final working values.

lcp (**stats** | **config**) Displays information about the Layer Control Protocol (LCP) layer. You must supply one of the following arguments:

stats Displays the LCP layer statistics. The LCP layer is part of the PPP driver; it handles link parameters for a PPP link.

config Displays the current LCP layer configuration, including the LCP option initial, intermediate, and final working values.

pap Displays the Password Authorization Protocol (PAP) layer statistics. The PAP layer is a link-level authentication protocol in the PPP driver.

ppp Displays 16550 UART statistics in PPP drivers, plus the PPP encapsulation framing statistics.

route Displays the current contents of the kernel's routing cache. The routing cache contains the information learned through ICMP Host Redirect packets. The routing cache holds 16 entries.

security Displays information about the kernel's basic and extended security configuration and IP security ports. You must supply the **config** option when using **security**.

slip Displays 16550 UART statistics in Serial Line Interface Protocol (SLIP) drivers, plus SLIP encapsulation framing statistics.

stats Displays network statistics about the network interface. The statistics include the name of the interface, its network (IP) address, the subnet mask, and the total number of packets sent out and received on this interface.

The **inet stats** command also displays a number of TCP, IP, ICMP, and UDP counters, including bad incoming packets and messages broken down by type.

tcp Displays the contents of the kernel's TCP connection table. The connection table contains a set of statistics for each active connection.

unload Unloads the TSR kernel from memory. If you use **inet unload**, you must use the **kernel** command to reload the PC/TCP kernel TSR into memory. See the **kernel** command for details.

version Displays the version number of the active kernel, not the version number of the **inet** command.

-? Displays and explains the usage line of the command.

-version Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Examples

To display configuration information about your PC/TCP kernel, enter

```
C:\> inet config

Kernel active since: Sat Mar 05 14:41:53 1994
0 TCP connections open/listening, of 6 allowed
2 UDP connections in use, of 6 allowed
3 IP connections in use, of 7 allowed
```

```
1 Global and 0 local network descriptors active
Using 255.255.255.255 as IP broadcast address.
Domain: xyz.com
Hosttable file: c:\pctcp\hosts
Router(s): 128.127.50.10
Domain name completion list(s): <None Configured>
Domain name server(s): 128.127.50.105
Default TCP window size: 2048
Default low window size: 0
Chain vector: 0xb
MAC Address: 00 00 f6 18 50 46
Packet Driver Class: 1
```

To display advanced configuration information, enter

```
C:\> inet config advanced

Time to live: 64
Type of service: Normal
Precedence: Routine
Will do lax precedence matching.
Maximum Transmissions Unit (MTU): 1480
Round trip time multiplier: 1
Kernel is not using expanded memory.
```

To display security configuration information, enter

```
C:\> inet config security

Basic security: <Not configured>
Extended security: <Not configured>
IP security ports: <None configured>
```

To display the current contents of your kernel's ARP cache, enter

```
C:\> inet arp

ARP cache:
    128.127.50.137:    00de200037ff    expires:  773 sec.
    128.127.50.105:    08004c002c6a    expired
```

To display statistics about the network interface, enter

```
C:\> inet stats

Interface   address        subnet mask   pkts in pkts out errs in errs out
ifcust0     128.127.50.141 255.255.255.0 157057  2555     0       0
Kernel TCP stats: 2530 pkts sent, 1869 pkts rcvd, 0 bad checksums
    943197 bytes sent, 138587 bytes rcvd, 56 rexmits, 52 duplicate pkts
    0 protocol errs, 0 resets, 0 timeouts
Kernel IP stats: 2537 pkts sent, 137419 pkts rcvd, 0 frags, 5 err
    5 protocol errs, 0 timeouts, 0 bad checksums, 0 security errs
```

```
Kernel UDP stats: 6 pkts sent, 6 pkts rcvd, 0 no port listening
    0 bad checksums, 0 truncated rcvs
Kernel ICMP stats: 1 pkts sent (0 errs), 1 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
```

See Also

kernel, ping

inet

iprint

Usage

iprint [**-n**] [**-q**] [**-b** [*port*]] *file*
iprint [**-?** | **-version**]

Description

The **iprint** command sends a text or ImPRESS file to an IMAGEN printer. The command specifies a default format that simulates an 80-character, 10-pitch line printer. Depending on the IMAGEN printer configuration, **iprint** can also print a header or cover page.

Command Line Options

-b [*port*] — The **-b** option alone specifies that the file to print is in binary format. The option in conjunction with a port number specifies a Transmission Control Protocol (TCP) port that connects to a serial printer. Always use the **-b** option when printing ImPRESS files; an ImPRESS file is in binary format by default. The printer interprets any Ctrl+Z characters as indicating the end of the file.

file — Specifies the file to print.

-n — Suppresses printing of a header line at the top of each page.

-q — Suppresses status messages unless an error occurs.

-? — Displays and explains the usage line of the command.

-version — Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Example

To print the binary file MANUAL.IMP without any headers on the configured IMAGEN printer, enter

```
C:\> iprint -n -b manual.imp
```

iprint

kdestroy

Usage

kdestroy [**-f** | **-q**] [**-l** *userid*]
kdestroy [**-?** | **-version**]

Description

The **kdestroy** command deletes a Kerberos ticket-granting ticket or a service ticket that you no longer require. The command overwrites the file that contains your active Kerberos authorization tickets, then removes the file from the system. If you do not destroy unexpired tickets, unauthorized users can gain access to them.

You cannot restore Kerberos tickets after you use the **kdestroy** command. If successful, **kdestroy** displays the message `Tickets destroyed.` If **kdestroy** is unable to destroy the ticket file, the PC it emits a tone (beep) and displays the message `Tickets NOT destroyed.`

Command Line Options

-f Runs **kdestroy** without displaying the status message. The ERRORLEVEL is set to 0 if **kdestroy** is successful, or 1 if it is not successful. This option is useful in batch or command files.

-l *userid* Specifies the Kerberos principal. If **-l** *userid* is not specified, **kdestroy** uses the `user=` entry in the `[pctcp general]` section of the PCTCP.INI configuration file as the Kerberos principal for the transaction.

-q Turns off your terminal beep if the command fails to destroy the tickets. This option is useful in batch files.

-? Displays and explains the usage line of the command.

-version Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Example

To destroy a Kerberos ticket-granting ticket or service ticket, enter

```
C:\> kdestroy

Tickets destroyed.
```

To use the ERRORLEVEL in a batch or command file, type these lines:

```
kdestroy -f
if ERRORLEVEL 1 echo ticket was not destroyed
```

See Also

kinit, klist

kdestroy

kernel

Usage

kernel [**-B**] [**-b** *broadcast_addr*] [**-i** *interrupt*] [**-m**]
[**-p** *lg_pkt_count*] [**-s** *sm_pkt_count*] [**-t** *max_tcp_conn*] [**-u** *max_udp_conn*]

kernel [**-?** | **-version**]

Description

The **kernel** command loads the TSR kernel into memory. Use **inet unload** to unload the TSR kernel from memory.

Do *not* load or unload the TSR kernel while you run Microsoft Windows.

The kernel is the central part of the network software. Loading the TSR kernel lets you use network applications.

The network kernels support several network interface cards and drivers. When you install the networking software, you select the specific kernel that is compatible with your network environment.

To load a TSR kernel enter one of the following **kernel** commands:

depca	**ibanyan**	**ltdrv**	**tokdrv**
ebanyan	**ibmtr**	**pppdrv**	**x25drv**
ethdrv	**ieeedrv**	**slpdrv**	

The TSR kernel supports upper memory (UMB) and expanded memory loading options that you can specify on the command line or in the `[pctcp kernel]` section of the PCTCP.INI configuration file. (The kernel loads its code and data segments into upper memory by default.)

The size of kernel varies, depending on the driver, the command line, and configuration options you select. When you load the kernel, it displays a report of its memory usage. Using the **kernel** command without arguments results in a configuration that uses a moderate amount of memory, and is adequate for most users.

Kernel command line options override configuration parameter settings in the `[pctcp kernel]` and `[pctcp interface n]` sections of the PCTCP.INI file.

Command Line Options

-B Specifies that Berkeley UNIX-type urgent pointers are used. Use this type of out-of-band urgent pointer when communicating with Berkeley UNIX hosts. Without this option selected, RFC 1122 urgent pointers are used; this is the default.

-b *broadcast_addr* Specifies an address other than 255.255.255.255 as the broadcast address. Other useful values include

net_addr.**255**
net_addr.subnet_addr.**255**
net_addr.**0**
net_addr.subnet_addr.**0**

where *net_addr* and *subnet_addr* are your network and subnet addresses. (Broadcast addresses that use the **0** value are unusual; they are generally used by older networks.)

-i *interrupt* Specifies a different software interrupt in hexadecimal. The default is 61 (this corresponds to 0x61 using standard hexadecimal notation). The network software automatically determines which interrupt to use. If your TSRs or other applications experience interrupt conflicts, you may need to change the software interrupt. (This option overrides the `kernel-int=` setting in the `[pctcp kernel]` section of your PCTCP.INI file.)

-m Allows the kernel to use expanded memory if a properly configured expanded memory manager is also running. This option overrides the default `use-emm=no` parameter in the `[pctcp kernel]` section of your PCTCP.INI configuration file.

-p *lg_pkt_count* Specifies the number of large packet buffers to reserve when loading the kernel into memory. The size of a large packet is equivalent to the Maximum Transmission Unit (MTU) allowed in your network. The maximum number of packet buffers is variable because the size of the MTU changes on networks other than Ethernet or StarLAN. Default: 5 or the number of TCP connections plus 1 (whichever is larger).

This option overrides the `large-packets=` setting in the `[pctcp kernel]` section of your PCTCP.INI file.

-s *sm_pkt_count* Specifies the number of small packets to reserve when loading the kernel into memory. Typically, small packets carry protocol or other handshaking data between systems, and large packets carry application data. Default: 5 or the number of TCP connections plus 1 (whichever is larger).

This option overrides the `small-packets=` setting in the `[pctcp kernel]` section of your PCTCP.INI file.

-t *max_tcp_conn* Specifies the maximum number of simultaneous TCP connections to allow. The maximum number of TCP connections is 64. Default: 4.

-u *max_udp_conn* Specifies the maximum number of simultaneous UDP connections to allow. Default: 4.

-? Displays and explains the usage line of the command.

-version Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Examples

To unload the TSR kernel, enter

```
C:\> inet unload
```

To load the DIX Ethernet TSR kernel TSR into conventional memory with 8 TCP and 8 UDP connections, enter

```
C:\> ethdrv -t 8 -u 8
```

To load the IEEE 802.3 kernel into expanded memory enter

```
C:\> ieeedrv -m
```

See Also

inet, vxdinit

kernel

keymap

Usage

keymap [**-t** *ttype*] [*filename*]
keymap [**-?** | **version**]

Description

The **keymap** command provides a character-based window interface you can use to customize key mappings for a terminal emulation session.

Command Line Options

filename Specifies the name of a key map file from which **keymap** reads your keyboard mappings. You can save this file for use when you log in to a remote host (for example, when you use the **tn** command). The remote host then uses the keyboard mappings you created with **keymap**.

-t *ttype* Specifies the terminal type for which you are remapping your keyboard. You can specify one of the following values:

vt vt320 vt220 vt100 vt52 3270 3277 3278 3279 ibmpc sco-ansi

The values are case sensitive; that is, you must type them as shown. If you specify no value, **keymap** highlights **vt**.

-? Displays and explains the usage line of the command.

-version Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Examples

To start **keymap** with the IBM 3270 terminal type preselected, enter

```
C:\> keymap -t 3270
```

To specify a key map file from which **keymap** can read your keyboard mappings, enter

```
C:\> keymap myvtkeys.map
```

To specify a key map file from which **keymap** can read your keyboard mappings, and to start **keymap** with the IBM 3270 terminal type preselected, enter

```
C:\> keymap -t 3270 my3270keys.map
```

See Also

tn

keymap

kinit

Usage

kinit [**-i***instance*] [**-r** *realm*] [**-v**] [**-l**] [*username*]
kinit [**-?** | **-version**]

Description

The **kinit** command obtains a Kerberos ticket-granting ticket, your credential for Kerberos services. Note that only registered Kerberos users can use the Kerberos system.

The **kinit** command prompts for your Kerberos password, and tries to authenticate your login with the local Kerberos server. The **kinit** command obtains your realm name from the KRB.CON file on your system.

Note: Kerberos name and password entries are case sensitive.

If Kerberos authenticates the login attempt, **kinit** retrieves your initial ticket and puts it in the ticket file. The **klist** command shows you the name and location of this ticket file.

Use the **kdestroy** command to destroy any active tickets before you end your login session. Although your tickets expire in 8 hours, deleting them gives you added security.

Command Line Options

-i *instance* Specifies a Kerberos instance. The instance is an identifier that provides additional information about the user. Typically the instance is set to null for general users. If the instance does not match the instance registered in the Kerberos database for this principal, you receive the error message

```
kinit: Principal unknown
```

If you receive this error message, verify that you are registered in the Kerberos server database.

-l Prompts you for a ticket lifetime in minutes. Due to protocol restrictions in Kerberos Version 4, this value must be 5–1275 minutes. The default is 8 hours (480 minutes).

-r *realm* Specifies a Kerberos realm name. This option lets you authenticate yourself with a remote Kerberos server outside the default realm.

username Specifies the Kerberos username. If *username* is not specified, the system prompts you for your Kerberos name.

-v Displays the realm and a status or error message. Indicates the success or failure of your login attempt.

-? Displays and explains the usage line of the command.

-version Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Example

To start a Kerberos session, user Chris with the username chrisb types

```
C:\> kinit

Kerberos name: chrisb
Password:
```

If Kerberos authenticates the login attempt, **kinit** gets the initial ticket and puts it in the ticket file. Chris can verify this authentication with the **klist** command.

See Also

kdestroy, klist, rcp, rloginvt, rmt, rsh, setclock, tar, tn

kinit

klist

Usage

klist [**-s** | **-t**] [**-l** *userid*] [**-file** *filename*]
klist [**-?** | **-version**]

Description

The **klist** command lists currently held Kerberos tickets by displaying

- The name and path of the ticket file.
- The name of the principal the tickets are for (as listed in the tickets file).
- The principal names of all Kerberos tickets currently held by the user, along with the issuance and expiration time for each authenticator. (Principal names are listed in the form *name.instance@realm*, with the period and instance omitted if the instance is null.)

The presence of a ticket file verifies a successful Kerberos authentication.

Command Line Options

-file *filename* Specifies the name of the ticket file.

-l *userid* Specifies the Kerberos principal. If you do not specify **-l** *userid*, **klist** uses the `user=` parameter in the `[pctcp general]` section of the PCTCP.INI configuration file as the Kerberos principal for the transaction.

-s Displays only the tickets within the ticket file. It does not display the issuance and expiration times, the ticket filename, or the identity of the principal.

-t Scans the ticket file for an unexpired ticket-granting ticket. If one is present, it exits with status 1; otherwise it exits with status 0. With this option **klist** does not generate output. The option is useful in batch or command files.

-? Displays and explains the usage line of the command.

-version Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Examples

To show ticket information and verify a successful Kerberos authentication, enter

```
C:\> klist

Ticket file: C:\kerb\chrisb.tkt
Principal:         chrisb.XYZ.COM
Issued             Expires               Principal
Jan 10 09:21:57    Jan 10 17:21:57       krbtgt.XYZ.COM@XYZ.CCOM
```

To list the contents of the ticket file C:\KERB\CHRISB.TKT, enter

```
C:\> klist -file \kerb\chrisb.tkt
```

```
Ticket file: C:/kerb/chrisb.tkt
Principal:         chrisb.XYZ.COM
Issued             Expires               Principal
Jan 10 09:21:57    Jan 10 17:21:57       krbtgt.XYZ.COM@XYZ.CCOM
```

To use the ERRORLEVEL in a batch or command file, enter these lines

```
klist -t
if ERRORLEVEL 1 echo No ticket-granting ticket
```

See Also

kinit, kdestroy

klist

kpasswd

Usage

kpasswd [**-i** *instance*] [**-n** *username*] [**-r** *realm*] [**-u** *fullname*]
kpasswd [**-?** | **-version**]

Description

The **kpasswd** command changes a password on the Kerberos server.

Note: Kerberos name and password entries are case sensitive.

Command Line Options

-i *instance*	Specifies the Kerberos instance. If the instance does not match the instance registered in the Kerberos database for this principal, an error message appears.
-n *username*	Specifies the Kerberos principal. If you do not specify the username or full name and **kpasswd** does not find the ticket granting ticket using the **kinit** command, the **kpasswd** command prompts you for the Kerberos principal name.
-r *realm*	Specifies a Kerberos realm name. This option lets you authenticate yourself with a remote Kerberos server outside the default realm.
-u *fullname*	Specifies the full username. If you do not specify either the username or full name, and **kpasswd** does not find the ticket granting ticket using the **kinit** command, the **kpasswd** command prompts for the Kerberos principal name.
-?	Displays and explains the usage line of the command.
-version	Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Example

To change a Kerberos password on a Kerberos server, user Chris with the username chrisb types

```
C:\> kpasswd

Old password for chrisb:
New password for chrisb:

Verifying, please re-enter new password for chrisb:
Password changed.
```

See Also

kdestroy, kinit, klist

kpasswd

lpd

Usage

lpd [**-d**]
lpd [**-?** | **-version**]

Description

The lpd program (the LPD server) lets you set up your system as a dedicated source of network print services for remote users who connect to the server using TCP/IP protocols. The LPD server responds to requests from three other remote host programs: lpr, lpq, and lprm. 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 lpd server console commands.

Command Line Options

-d Loads the lpd program with the debugging logging option on.

-? Displays and explains the usage line of the command.

-version Displays the version and patch level of the command. Refer to this information if you call Technical Support.

LPD Server Console Commands

Once the program is running, the following server console commands are available:

- (hyphen) Prompts for a printer name, and then turns off printing for the specified printer. The printer will still spool jobs.

+ Prompts for a printer name, and then turns on printing for the specified printer.

< Prompts for a printer name, and then disables print spooling for the specified printer. All attempts to send a print job to that printer will fail.

> Prompts for a printer name, and then enables print spooling for the specified printer.

! Loads a DOS command shell. Type **`exit`** to return to the **lpd** console. The lpd program does not accept files for printing while a DOS command shell session exists.

? Displays a list of available commands and a short description of their functions.

C Closes the status file.

c Deletes all jobs in a single printer's queue. Prompts for printer name, and deletes all jobs in the queue for that printer.

D Controls the display of debugging information. When used, the LPD server displays longer messages on the console screen for print jobs that it receives and prints.

d Displays kernel debugging information. For a full explanation of the output, see **the inet debug** command description.

F Writes the information that **lpd** displays on the console screen to a status file. The command prompts you for a filename. You can specify an existing filename, or a new filename. If you specify a new filename **lpd** creates the file.If you specify an existing filename,**lpd** overwrites the existing file.

k Displays kernel statistics.

L Prompts for a printer name, and lists statistics about that printer and the jobs in that printer's queue.

l Lists all the printers, their spooling and printing status, some statistics about the printer, and the following information about the jobs in the printer's queue:

- Job name
- User ID of originating user
- Originating host
- Job number

Use this command to view the contents of print spooler queues before you stop the LPD server.

n Displays kernel network statistics. For a full explanation of the output, see the **inet stats** command description.

o Lists statistics for all open TCP connections to the LPD server.Use this command to determine if a remote host has an open connection to the server before you stop the server.

p Lists all the printers the server recognizes, and the following information for each printer: the spooling directory, the configured printer device (for example, LPT1, COM2), the status of spooling (on or off), and the printing status (on or off).

q Exits from the LPD server, and returns to the DOS prompt. If a print job is already executing when you stop the lpd program, the LPD server may not be able to finish the currently executing print job. Any print jobs waiting in spooler queues are unaffected; when you restart the LPD server, these print jobs are processed in the order that they were received. (Determine the status of open connections, and of print spooler queues with the **o** and **l** commands before you stop the server.)

r Prompts for a printer name and a job number to remove, and then removes that job from the queue.

s Displays server statistics that show information about network connections to clients that have sent jobs or requested queue information from the server.

v Displays the current version number of the LPD server.

Examples

To load the LPD server in the default message mode, enter

```
C:\> lpd

No host table, no restrictions on users
List of printers in config file: lp

List of printers and printer status
#   name    directory      spooling printing      device
1   lp      C:\printers\lp on       on            lpt1

Type 'q' to abort; '?' for other commands.
```

To load the LPD server in verbose message mode, enter

```
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.
    Sending printer-init string to printer lp...

Type 'q' to abort; '?' for other commands.
```

See Also

inet, lpq, lpr, lprm

lpd

lpq

Usage

lpq [**-q**] [**-S** *server*] [**-P** *printer*] [*username...*] [*job#...*]
lpq [**-?** | **-version**]

Description

The **lpq** command reports the status of print jobs in a line printer daemon (LPD) job queue. The output includes the job number, username, hostname, and job name for each print job. The job number can be used with the **lprm** command to remove a job from the queue.

Command Line Options

job#	Specifies a job or jobs whose numbers were obtained in a previous iteration of this command. Separate multiple job numbers with spaces.
-P *printer*	Specifies the name of a printer controlled by an LPD server. This option overrides the value of the `printer=` entry in the `[pctcp lpr]` section of your PCTCP.INI file.
-q	Suppresses status messages. The LPD job queue will continue to display error messages.
-S *server*	Specifies the hostname or IP address of an LPD server. This option overrides the value of the `server=` entry in the `[pctcp lpr]` section of your PCTCP.INI file.
username	Requests status of the specified user's or users' jobs only. Separate multiple usernames with spaces.
-?	Displays and explains the usage line of the command.
-version	Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Example

To display the job queue for the hp2 printer controlled by the print server green, enter

```
C:\> lpq -S green -P hp2

Trying printer hp2 on server green ...open

printer hp2: spooling is on, printing is on

List of queue for printer hp2.
    Job #   user   host                jobname
    66      chris  bunny.xyz.com       test.prn
    67      pat    wander.xyz.com      test.txt
    68      robin  kite.xyz.com        manual.prn
```

See Also

lpd, lpr, lprm

lpq

lpr

Usage

lpr [**-S** *server*] [**-P** *printer*] [**-C** ***class***] [**-J** *jobname* [**-#** *number*] [**-qrhpltndgvcf**] [*filename...*]
lpr [**-?** | **-version**]

Description

The **lpr** command sends a text or graphics file to a system running a line printer daemon (LPD) server.

You can use wildcard characters in the filenames. If you do not specify a filename, **lpr** sends DOS command output or your keystrokes to the printer. (Press Ctrl+Z to signal the end of printing from keyboard input.)

Command Line Options

-# *number* — Specifies the number of copies to print.

Note: The **lpr** command transfers the file to the printer only once no matter how many copies you specify. The server software controls the printing of multiple copies.

-C *class* — Specifies a class name that prints on the job's header page (use of this option is site-dependent). This class name can be used as a project or group name. This option overrides the `class=` entry in the `[pctcp lpr]` section of your PCTCP.INI file.

-c — Specifies that the files to print contain data produced by cifplot.

-d — Specifies that the files to print contain data from tex (DVI format from Stanford University).

-f — Uses a filter that interprets the first character of each line as a standard FORTRAN carriage control character. The **lpr** command uses the **-f** option by default.

filename... — Specifies the file or files to be printed. You may use wildcard characters.

-g — Specifies that the files contain standard plot data produced by UNIX **plot** routines. See the UNIX **plot** manpage for the filters used by the printer spooler.

-h — Suppresses printing of the header page. By default, the **lpr** command prints a header page identifying your username, hostname, class name, and job name. The username and hostname are taken from the `[pctcp general]` section of your PCTCP.INI file. This option overrides the `banner=` entry under the `[pctcp lpr]` section of your PCTCP.INI file.

-J *jobname* — Specifies a job name to print on the header page. By default, the job name is the name of the file being printed.

-l — Specifies that you are printing a text file in which the print server should preserve

(not interpret) control characters. This is not the same as the **-v** option, because end-of-line (EOL) translation may still occur. For example, with this option, the LPD server might stop printing the file if it encounters a Ctrl+Z character, whereas with the **-v** option, printing would continue.

-n Specifies that the files to print contain data from ditroff (device-independent troff).

-P Specifies the name of a printer controlled by an LPD print server. This option overrides the `printer=` entry in the `[pctcp lpr]` section of your PCTCP.INI file.

Note: Type **`-P local`** to specify a printer attached directly to your PC. The **lpr** command uses the DOS **print** command to print your files.

-p Notifies the server to use the **pr** program to format the file. The program formats pages with a five-line margin at the top and bottom, and a heading consisting of the date, time, name of file, and page number on the third line of each page. Note that if the print server is on a DOS system, it may not have a **pr** filter.

-q Suppresses status messages. The LPD server continues to display error messages.

-r Deletes the file from your PC after printing successfully.

-S *server* Specifies the hostname or IP address of an LPD print server. This option overrides the `server=` entry in the `[pctcp lpr]` section of your PCTCP.INI file.

-t Specifies that the files to print contain data from troff.

-v Prints the data verbatim without any translation. This option is for use with files that contain raster images, or with devices like the Benson Varian. You can also use this option with files in binary, or printer-specific, formats (for example, IMAGEN ImPRESS format, PostScript format, or Hewlett-Packard Printer Control Language (PCL) format). The **-v** option may not work for binary files on some systems. If it does not work, try one of the other **lpr** options instead, such as the **-l** option.

-? Displays and explains the usage line of the command.

-version Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Examples

To send the file MANUAL.PS to the remote printer psprinter on the server post, enter

```
C:\> lpr -S post -P psprinter manual.ps

Trying printer psprinter on server post...entire document sent
```

To print a listing of files in the current directory using a DOS pipe (|) to the default printer, enter

```
C:\> dir | lpr

Reading from standard input...
```

```
Trying printer lp on server post...entire document [standard input] sent
```

See Also

lpd, lpq, lprm

lpr

lprm

Usage

lprm [**-q**] [**-S** *server*] [**-P** *printer*] (*username... | job#...*)
lprm [**-?** |**-version**]

Description

The **lprm** command removes print jobs from an LPD server's queue, and displays server response messages. Because the LPD spooling directory is protected from users, the **lprm** command is the only method by which users can remove a print job from the print queue. The LPD server may return the message `Permission denied` if you try to remove files other than your own.

Command Line Options

job#	Specifies the print job number. You can specify more than one job number, separated by spaces on the command line. Use the **lpq** command to get job numbers.
-P *printer*	Specifies a printer controlled by an LPD print server. This option overrides the `printer=` entry in the `[pctcp lpr]` section of your PCTCP.INI file.
-q	Suppresses status messages. The LPD job queue continues to display error messages.
-S *server*	Specifies the hostname or IP address of an LPD print server. This option overrides the `server=` entry in the `[pctcp lpr]` section of your PCTCP.INI file.
username	Removes all print jobs that the user sent. **Note:** You cannot specify someone else's username from your PC, or your username from someone else's PC.
-?	Displays and explains the usage line of the command.
-version	Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Examples

To remove job number 13 from the print queue for the hp2 printer controlled by server green, enter

```
C:\> lprm -S green -P hp2 13

Trying printer hp2 on server green...open
Removing job #13 from printer hp2's queue
```

To remove all jobs with the username chris from the queue on the configured print server, enter

```
C:\> lprm chris

Trying printer lp on server blue...open
Removing job #15 from printer lp's queue
```

```
Removing job #16 from printer lp's queue
```

Note that this removes only jobs that are sent from the same system from which the **lprm** command is issued.

See Also

lpd, lpq, lpr

lprm

lwpe

Usage

lwpe [**-u**]
lwpe [**-?** | **-version**]

Description

The **lwpe** command starts the LWPE.COM TSR program that lets users run Novell NetWare/IP over any PC/TCP TSR kernel. The LWPE.COM program emulates the Novell LAN WorkPlace TCP/IP application programming interface (API), which allows users to run such LAN WorkPlace applications as Novell NetWare/IP or TNVT220.

The LWPE program intercepts calls from a LAN WorkPlace application or NetWare/IP and redirects these calls to the TSR kernel.

To support NetWare/IP, LWPE.COM must be run over the ODIPKT driver. This is due to dependencies between NetWare/IP, the NetWare redirector (VLM), and the Link Support Layer (LSL).

Note: This TSR is not compatible with the OnNet VxD kernel.

Command Line Options

-u Unloads the LWPE.COM program.

-? Displays and explains the usage line of the command.

-version Displays the version and patch level of the command. Refer to this information if you call Technical Support.

lwpe

netbios

Usage

netbios [**-a**] [**-u**]
netbios [**-?** | **-version**]

Description

The **netbios** command starts and unloads the PC/TCP NetBIOS (NETBIOS.COM) TSR program. To load the corresponding OnNet VxD kernel, see the **vxdinit** command.

PC/TCP NetBIOS configuration option defaults are defined in the `[pctcp netbios]` section of your PCTCP.INI configuration file.

Command Line Options

-a Uses the alternate interrupt interface (interrupt 0x2A) to the transport layer. By default PC/TCP NetBIOS uses interrupt 0x5C (and does not use the alternate interrupt interface).

For network operating systems that support interrupt 0x2A (such as LAN Manager), this option lets you remove MINSES.EXE from the network services list (thus saving approximately 2K of conventional memory). To remove MINSES.EXE from your LAN Manager network services list, delete `minses` from the `netservices=` entry in your LANMAN.INI file.

-u Unloads PC/TCP TSR NetBIOS.

-? Displays and explains the usage line of the command.

-version Displays the version and patch level of the command. Refer to this information if you call Technical Support.

See Also

vxdinit

netbios

nicname

Usage

nicname [**-i**] [**-d**] [**-s** *address*] user
nicname [**-help** | **help**]
nicname [**-?** | **-version**]

Description

The **nicname** command sends a request to the InterNIC name resolution service, for information about the name of a host or a user.

This command is useful only if your PC has access to the Internet. The InterNIC hostname is RS.INTERNIC.NET, and the InterNIC IP address is 198.41.0.5. The InterNIC host normally responds with a few lines of text, which **nicname** then displays on your PC. If InterNIC does not respond within two minutes, **nicname** ends its request.

You can also specify an address in the `nicname-server=` entry in the `[pctcp addresses]` section of your PCTCP.INI file. All further requests would then be sent to the specified address unless you override this address with an appropriate command line option.

Command Line Options

-d Sends the request to the Department of Defense database at NIC.DDN.MIL (192.112.36.5), overriding the default NIC address and any address specified by the entry `nicname-server=` in the `[pctcp addresses]` section of the PCTCP.INI file.

-help Displays some hints on how to use the **nicname** command.

help If you specify **help** without a hyphen, your request is sent to the InterNIC, which responds with information about making more sophisticated inquiries.

-i Sends the request to the InterNIC address RS.INTERNIC.NET (198.41.0.5), overriding any address specified by the entry `nicname-server=` in the `[pctcp addresses]` section of the PCTCP.INI file.

-s *address* Sends the request to the specified address, overriding the default InterNIC address and any address specified by the entry `nicname-server=` in the `[pctcp addresses]` section of the PCTCP.INI file.

user Inquires about *user*, which may be a username, hostname, domain name or last name of a InterNIC-registered Internet user.

.user A period (.) prefix displays only matching hostnames and last names of users.

user. A period suffix displays an expanded list of every username, hostname, and last name that begins with the exact spelling of *user*.

!*user* An exclamation point (!) prefix inquires about a InterNIC-generated username called a handle, which serves as a shortcut for **nicname** queries. InterNIC displays directory information for the only handle with that exact spelling.

-version Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Example

To request information for every username, hostname, and last name that starts with the word george, enter

```
C:\>nicname george.

Connected to 198.41.0.5
Fuller, Georgeanne (GF6)                GEORGEANNE@PAXRV-NES.NAVY.MIL
(301) 555-8700
George Air Force Base (APDS-II-OS10)    APDS-II-OS107.AF.MIL 26.5.0.39
George Mason University (GMU-DOM)       GMU.EDU
George, Abra (AG158)                    1txlgsc@TACHOST.AF.MIL (DSN)
555-4673
George, Lisa E. (EHG3)                  EGeorge@DDN-WMS.DCA.MIL
(703) 555-9400
George, Maynard G. (RVG)                george@NOSC.MIL
(619) 555-4788
Georges, Harris K. (ILG2)               1995cs-kt@AFCC-OA1.AF.MIL (DSN)
317-555-2177
Georgetown University (GEORGETOWN-DOM)  GEORGETOWN.EDU
Jenning, George W., Jr. (GOJ)           george@NGP.UTEXAS.EDU
(512) 555-4353
Ramir, George E. (GLR16)                GEORGE@S5.INFO.WPAFB.AF.MIL (DSN)
555-6924
```

To single out one record, look it up with **!***xxx*, where *xxx* is the handle shown in parenthesis following the username. For example, to look up the handle for the user George, Harris K. in the preceding list, enter

```
C:>nicname !ILG2

net_connect: Connection reset
Connected to 198.41.0.5
Harris,George (ILG2)   georgeh@fictional.com
Fictional Tec Systems, Inc.
2 Nowhere Road
Beverly Hills, CA 90210
(508) 555-5555
Record last updated on 03-Mar-94
```

See Also

finger, whois

nicname

nntp

Usage

nntp [**-a**] [**-c** *client_section*] [**-d**] [**-e**] [**-k**] [**-q**] [**-s**]
nntp [**-?** | **-version**]

Description

The **nntp** command runs the Network News Transfer Protocol (NNTP) client program, based on RFCs 977 and 1036. The nntp program lets you have access to the network news groups and post (send) messages to them.

To use the nntp program, you must create a unique top-level directory on your PC in which to store your nntp directories and files, and your unread messages. In addition, you or your system administrator must install an NNTP server on a remote host in your network.

The first time you use **nntp**, the NNTP client connects to the server and retrieves the entire list of news groups residing on the server. After the client retrieves the list, run the vmail program to compose, forward, and reply to network news group messages.

After you exit from the vmail program, you must run the NNTP client to process the actions you have queued, such as obtaining a new copy of the list or posting a message. Note that the nntp program uses the Simple Mail Transfer Protocol (SMTP) only to send your replies to network news group messages.

Command Line Options

-a Processes only your actions file. Use this option to post messages without waiting for new messages to be retrieved from the server.

-c *client_section* Specifies a client section of the PCTCP.INI file for use by the nntp program. Use this option to specify a section other than the default section.

-d Turns on debugging. Shows network transactions in detail.

-e Expunges (removes) messages that have exceeded the expiration time limit. You can specify in the `expire-`*`newsgroup`*` =` entry of the `[pctcp nntp]` section of your PCTCP.INI file the amount of time, in days or weeks, that elapses before the messages expire on specific news groups or on all news groups to which you subscribe.

-k Deletes all directories and files in the top-level **nntp** directory. The command prompts you to verify this action.

-q Suppresses status messages unless the program encounters an error.

-s Retrieves only the new message descriptors (message summaries) from the server, rather than the messages themselves. This option is also known as the “short” option.

-? Displays and explains the usage line of the command.

-version Displays the version and patch level of the command. Refer to this information if

you call Technical Support.

Examples

To access the NNTP server, enter

```
C:\> nntp

Scanning mail directory... done
Updating local mbox list
Connecting to xyz.xyz.com, port 119... logged in. Posting is permitted
Processing actions
    Expunging mailbox misc.writing... Done
    Getting message alt.folklore.computers/13039... Done
    All actions have been processed
    Fetch new messages
    Checking misc.writing for messages... there are 2 new messages
           c:/pctcp/spool/nntp/mbox2/1991 not on-line; 57 lines, 2633 bytes
           c:/pctcp/spool/nntp/mbox2/1992 not on-line; 46 lines, 1945 bytes
    Checking alt.folklore.computers for messages... no new messages
    Checking to.xyz for messages... no new messages
    Checking comp.risks for messages... there are 3 new messages
           c:/pctcp/spool/nntp/mbox10/1961 not on-line; 19 lines, 954 bytes
           c:/pctcp/spool/nntp/mbox10/1962 not on-line; 42 lines, 2156 bytes
           c:/pctcp/spool/nntp/mbox10/1963 not on-line; 31 lines, 1615 bytes
    Checking to.pqr for messages... no new messages
    Logging out from xyz.xyz.com...
```

To run only the actions file, enter

```
C:\> nntp -a
```

To remove expired messages, enter

```
C:\> nntp -e
```

To retrieve only new descriptors from the NNTP server, enter

```
C:\> nntp -s
```

To use a different server than your default NNTP server, enter

```
C:\> nntp -c machine1
```

The nntp program uses the configuration section specified by `[pctcp machine1]` in the PCTCP.INI file.

See Also

vmail

RFCs 977 and 1036

nntp

onpredir

Usage

onpredir [**config**] [**prog** *path* [**spool** *path*] [**swap** *path*]
[**printer** (**LPT***n* | *n* | **PRN | off**)] [**hotkey** (**on** | **off**)] [**oneof** (**on** | **off**)]
[**onexit** (**on** | **off**)] [**timeout** (*seconds* | **off**)] [**unload**] [**report**]
onpredir [**help** | **-version**]

Description

The **onpredir** command displays the status of the print redirector.

Both **predir** and **onpredir** accept the same command line arguments. The difference between the commands is that **predir** loads the print redirector into memory, and **onpredir** requires the redirector to already be running. The **onpredir** command without any arguments displays a message indicating whether **predir** is loaded and, if so, what its current settings are.

By default, the **onpredir** command reads configuration parameters from the `[pctcp print]` section of your PCTCP.INI file. You can specify **onpredir** command line options to override these parameters.

The **onpredir** executable file (ONPREDIR.EXE *)* must reside in the same directory as the **predir** executable file (PREDIR.EXE *)*.

Command Line Options

See **predir** for an explanation of command line options. The **onpredir** options are identical.

Examples

To determine whether the print redirector is resident in memory, enter

```
C:\> onpredir
```

If **predir** is not loaded, you see the following message:

```
Print redirector not loaded
```

If **predir** is loaded, you see output like the following system response:

```
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 enabled
print-on-timeout = 300 secs.
print-on-eof is disabled
```

See Also

dopredir, predir

onpredir

Chapter 1
Overview of DOS Commands

OnNet™ and PC/TCP® include a variety of DOS commands that you can use to perform network tasks at your PC, such as transferring files or sending mail messages.

Because OnNet and 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 commands listed and described in this book, with the exception of the ypcat and ypmatch commands, which are only distributed with the CD-ROM version of OnNet.
- One version of OnNet is distributed on CD-ROM and includes all of the commands listed and described in this book.
- One version of OnNet is distributed on diskettes, and includes a subset of the DOS commands described in this book, 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	

This chapter briefly describes the tasks that the DOS commands can perform, as follows:

Networking Task	**DOS Commands**
Learning about hosts and users on the network	**finger, host, inet, nicname, ping, whois**
Transferring files	**ftp, ftpsrv, passwd, rcp, rloginvt, tftp, tn**
Logging in to a remote host, customizing terminal emulation, and remapping your keyboard	**keymap, rlogingl, rloginvt, rsh, setcolor, tn, tnglass**

Sharing network files	**dos2unix, idchmod, idconfig, idls, idmnt, idnet, idprint, idrive, idumnt, idutil, unix2dos**
Printing to a network printer	**dopredir, lpd, lpq, lpr, lprm, idprint, onpredir, predir**
Exchanging mail and network news	**nntp, pcmail, pop2, pop3, smtp, vmail**
Archiving and restoring files	**ddates, rmt, tar**
Connecting to remote hosts over a modem or a serial line	**comscrpt, inet**
Using Kerberos security	**kdestroy, kinit, klist, kpasswd, rcp, rloginvt, rmt, rsh, tar, tn**
Configuring and tuning	**bootp, dhcp, inet, kernel, lwpe, netbios, pctcpcfg, setclock, snmpd, vxdinit**
Troubleshooting	**ftpver, inet, ping**

In addition, both OnNet and PC/TCP provide Windows applications that let you transfer files, log in to remote systems, connect to remote file systems and printers, get information about your network, and send messages to other hosts. Refer to the *PC/TCP User's Guide* or OnNet for Windows *User's Guide* for information about these applications.

1.1 Learning About Hosts and Users on the Network

The following commands let you obtain information about the hosts and users on your network. You can use this information to debug the network when problems arise.

finger Lists users logged in to another system, or lists directory information about a registered user of another host.

host Searches for the IP address that corresponds to a character-string name, or the hostname that corresponds to an IP address.

inet Gets network statistics from the TSR kernel or unloads the kernel from memory.

nicname Obtains information about a specific username or hostname from the InterNIC name resolution service. The **nicname** command is useful only if you are on the Internet and can reach the InterNIC directly.

ping Sends an echo request to another host and reports on the success or failure of the response.

whois Lists users currently logged in to another system, or lists information about a registered user of another host. You can use this command with any system that has a whois server program running.

1.2 Transferring Files

The following commands let you copy files between machines:

ftp Transfers files between your PC and remote hosts running an FTP server. This command is the easiest to use for transferring files between hosts.

ftpsrv Lets users at a remote host transfer files to and from your PC. When you start the ftpsrv program on your machine, the user at the remote machine can run the ftp program from the remote machine, specifying your PC's hostname or Internet address. The remote machine can be any machine using an implementation of the FTP protocol over a TCP/IP network.

passwd Creates or changes passwords in your PC's local PASSWD file.

rcp Copies files or directories between a remote host and your PC using the 4.2 Berkeley UNIX RCP protocol.

rloginvt Emulates a DEC VT220 terminal on a 4BSD UNIX host using the UNIX security scheme. The rloginvt program provides a built-in FTP server.

tftp Transfers a single file between your PC and a remote host running a TFTP server. This command does not require a password.

tn Emulates a DEC VT, IBM 3270, or IBM PC terminal on a remote host running a Telnet server. The Telnet program provides a built-in FTP server.

1.3 Logging In to a Remote Host, Customizing Terminal Emulation, and Remapping Your Keyboard

You can use the following commands to log in to a remote host, customize terminal emulation, and remap your keyboard:

keymap Provides a character-based window interface you can use to customize key mappings for a terminal emulation session.

rlogingl Logs you in to a 4BSD UNIX host using the UNIX security scheme and a specified terminal emulation program.

rloginvt Emulates a DEC VT220 terminal on a 4BSD UNIX host using the UNIX security scheme.

rsh Connects you to a specified UNIX host to execute a command.

setcolor Previews and sets display colors for terminal emulation.

tn Emulates a DEC VT, IBM 3270, or IBM PC terminal on a remote host running a Telnet server. The Telnet program provides a built-in FTP server.

tnglass Logs you in to any remote host running a Telnet server.

1.4 Sharing Network Files

InterDrive® is a Network File System (NFS) client program that lets you connect to and use file systems and applications that reside on remote hosts running an NFS server. Use the following InterDrive commands to configure InterDrive, allocate memory, examine statistics and configured entries, and use InterDrive on your PC.

Files that reside on the NFS host are written in a different format than DOS files. Files that are copied between the two environments need to be translated to the appropriate format before they are used by applications software.

dos2unix Replaces the DOS carriage-return line-feed combination with the UNIX new-line character.

idchmod Sets and changes permission attributes for remote files and directories.

idconfig Sets a variety of configuration entries for InterDrive; adjusts memory requirements and speed of operation to suit the local environment.

idls Produces directory listings of remote file systems.

idmnt Displays currently mounted file systems and mounts new file systems.

idnet Sets a default username and password for InterDrive network connections. Starts a character-based window interface that you can use for managing file system connections and print connections.

idprint Prints files to and controls a remote printer.

idrive Loads InterDrive and sets configuration entries and memory use values.

idumnt Unmounts remote drives and may be used to unload InterDrive.

idutil Controls many functions of the program and displays statistics and information about InterDrive states and performance. May also be used to gracefully unmount any mounted drive and unload InterDrive.

unix2dos Replaces the UNIX new-line character with the DOS carriage-return line-feed combination.

1.5 Printing to a Network Printer

The following commands support printing on remote printers. Together, these commands let you redirect DOS application print jobs to a spool file and print this spool file on a remote printer using a network print program or DOS batch file.

dopredir	Initiates printing of a redirected print job that has not already been printed.
idprint	Sends a file directly to an IMAGEN laser printer on the network for printing.
lpd	Lets remote hosts send files to the system for printing on printers connected to the PC.
lpq	Examines the spooling area used by the LPD server, and reports the status of all jobs currently in the queue.
lpr	Sends files from a PC to a server running LPD. A printer attached to the LPD server prints the file.
lprm	Removes jobs from the print queue, either by job number or by user name.
onpredir	Displays the status of the print redirector.
predir	Loads the print redirector into your computer's main memory. You must use predir before using the related commands **dopredir** and **onpredir**.

1.6 Exchanging Mail and Network News

The following commands let you exchange electronic mail and network news on your PC.

nntp Transfers messages to and from network news groups on the network or the Internet, using the Network News Transfer Protocol (NNTP).

pcmail Works in conjunction with the Pcmail protocol to send and receive messages. The Pcmail server program acts as the repository. The **vmail** command uses the Pcmail client program to access the server repository of messages, and displays your mailboxes and messages on your PC.

pop2 Works in conjunction with the SMTP protocol to transmit messages. The POP2 server program acts as the repository. The **vmail** command uses the POP2 client program to access the server repository of messages, and displays your mailboxes and messages on your PC.

pop3 Performs the same actions as the POP2 client program, but uses a POP3 server program.

smtp Transmits messages from the PC using the Simple Mail Transfer Protocol (SMTP).

vmail Lets you use the editor you have on your PC to send, forward, and reply to electronic mail messages, create mailboxes and addresses, use bulletin boards, save messages to text files, copy messages to other mailboxes, and generally simplify the process of reading and saving your mail. The vmail program is a visual, screen-oriented mail reading program.

1.7 Archiving and Restoring Files

The following commands let you back up and restore your files.

ddates	Displays contents of the dump dates file created by the tar program.
rmt	Lets you control a remote tape drive.
tar	Creates a single tape archive file that you can read and modify. The tar program can also write directly to a magnetic tape.

1.8 Dialing a Remote Host

The TSR kernels use the following serial protocol commands.

comscrpt Dials a modem or dedicated line from within Windows or from DOS.

inet Unloads the SLIP or PPP kernel after the current modem session ends.

1.9 Using Kerberos Security

The Kerberos security commands let you use services that support Kerberos security on your Kerberos realm. The other commands that support Kerberos security let you perform a variety of network tasks in a secure environment.

kdestroy	Deletes a Kerberos ticket-granting ticket or service ticket.
kinit	Logs you in to the Kerberos authentication and authorization system.
klist	Displays information about currently held Kerberos tickets.
kpasswd	Changes a password on the Kerberos server.
rcp	Copies files or directories between a remote host and your PC using the 4.2 Berkeley UNIX protocol.
rloginvt	Emulates a DEC VT220 terminal on a 4BSD UNIX host using the UNIX security scheme.
rmt	Controls a remote tape drive.
rsh	Connects to a specified host to execute a command.
tar	Archives and restores files between local and remote files, disks, and tapes.
tn	Emulates a DEC VT, IBM 3270, or IBM PC terminal on a remote host that is running a Telnet server.

1.10 Configuring and Tuning Network Software

The following commands let you configure network information on your PC, and help you to tune your network performance. You must run the **kernel** command or the **vxdinit** command before using any other command.

Note: The boldface term **kernel** represents a particular TSR kernel command (such as **ethdrv**). Elsewhere, the term "kernel" refers to any of the kernels.

bootp	Configures network information on your PC from a Bootp server.
dhcp	Configures network information on your PC from a DHCP server.
inet	Gets network statistics from the TSR kernel or unloads the kernel from memory.
kernel	Loads the TSR kernel into memory.
lwpe	Lets users run Novell NetWare IP over the OnNet or PC/TCP protocol stack.
netbios	Starts and stops NetBIOS.
pctcpcfg	Lists current values or sets new values in your PCTCP.INI configuration file.
setclock	Synchronizes your PC (within a few seconds) with other machines on your network.
snmpd	Lets other hosts using the SNMP protocol examine a PC's statistics and configuration information.
vxdinit	Instructs Windows to load the OnNet VxD kernel and optionally the NetBIOS, InterDrive (NFS client), and NFS server VxD kernels into memory.

1.11 Troubleshooting

The following commands help to diagnose network problems.

ftpver Displays the name and version of any Windows executable file.

inet Gets network statistics from the TSR kernel or unloads the kernel from memory.

ping Sends an echo request to another host and reports on the success or failure of the response.

passwd

Usage

passwd [*username*]
passwd [**-?** | **-version**]

Description

The **passwd** command lets you create or change a password in a PC's local password file.

With a password file, you can permit only selected users to open an **ftp** session to your PC. You can also use a password file to restrict the directories a remote user can access with the ftp program. Users *not* entered in this password file *cannot* open an **ftp** session on your PC. To prompt users for a password, you must give them one with the **passwd** command.

Before using the **passwd** command, the `pfile=` entry in the `[pctcp general]` section of your PCTCP.INI file must specify the filename of your password file.

Caution: PCs are not designed to be secure machines, even with a password file. Any person who can physically access your PC 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.

Command Line Options

username	Specifies your username, or that of the person whose password you want to create or change. The **passwd** command then prompts you for a new password for the specified user. If you omit *username*, **passwd** prompts you for it.
-?	Displays and explains the usage line of the command.
-version	Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Example

To add a password to the configured password file for the username rtm, enter the following:

```
C:\> passwd rtm

User rtm 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]: robert t. madison
Enter home directory for new user [C;\]: C:\REPORTS
Enter drive restrictions for new user [none]: C,F
```

This release of PC/TCP 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. If that fails, it attempts to verify the password using the old method.

Note: When using a text editor to modify your password file, note that there are seven separate

fields associated with each user: username, password (encrypted), UID, GID, full name, a reserved field, and home directory. The reserved field is a placeholder that makes the password file appear the same as a UNIX passwd file.

See Also

ftpsrv, rloginvt, tn

passwd

pcmail

Usage

pcmail [**-a**] [**-c** *client_section*] [**-k**] [**-d**] [**-s**] [**-f** (*mailbox* | **all**)] [**-r** (*mailbox* | **all**)] [**-o**] [**-q**] [**-z**]
pcmail [**-?** | **-version**]

Description

The **pcmail** command runs the Pcmail client program on your PC, which implements the Pcmail protocol (as specified in RFC 1056). The pcmail program retrieves your messages from the Pcmail server and transfers your messages to the Pcmail server for transport around the network. (Note that the pcmail program can rely on the Simple Mail Transfer Protocol (SMTP) to transfer messages as a backup for its own protocol.) In addition to having access to mail, the pcmail program lets you send messages to and read messages on your local network's electronic bulletin boards.

The pcmail program is used in conjunction with the vmail program. Each time that you run the **pcmail** command, the pcmail program processes all of the actions that are queued in an actions file as a result of commands that you have issued while using the vmail program to read and handle your mail messages. After it finishes processing your actions file, the Pcmail client updates your local mail state to match the one that exists for you on the server.

Note: If you use a local host table with no domain name server defined for name resolution, the mail server requires hostnames in the form *hostname.domain*. If the table contains only the domain name or the hostname without the domain name, the pcmail program returns a message that it cannot find the mail server.

Command Line Options

-a Runs only the actions file on your PC. Use this option to mail messages quickly, without waiting for new messages to be retrieved from the repository. Note that you cannot use this option with other options.

-c *client_section* Specifies a mail client section of the PCTCP.INI file for use by the pcmail program. Use this option to specify a section other than the default. (See the entry on **vmail** for more information about using multiple servers.)

-d Turns on debugging. Shows network transactions in detail.

-f (*mailbox* | **all**) Deletes everything in the specified *mailbox*, then retrieves all messages (both old and new) and all descriptors from the repository. If you specify **all**, the Pcmail client performs these actions for every mailbox on your PC. This option lets you recover from a corrupted local mail state on your PC. Note that you have to delete your subscription to a bulletin board, then rejoin the board, to reset your subscription.

-k Deletes all directories and files used by the pcmail program in the top-level mail directory on your PC. Any file or directory that you create independently of the pcmail program, such as a text file, is ignored by the program and remains in the top-level directory.

Before the pcmail program deletes its files and directories on your machine, the command specifies the name of the top-level directory, and requests your confirmation to remove the contents of the directory. You must type the word **yes** in response to the prompt if you want pcmail to proceed. Any other response cancels the removal of the directories and files.

-o Scans for and retrieves from the server only the text of messages marked with the `U` message flag. (A `U` flag in the vmail program flags unseen messages.) This option increases the speed of message retrieval if you store numerous messages in your mailboxes.

Caution: If you have more than one Pcmail client (on different PCs), the **-o** option can put them out of synchronization with each other. If you run pcmail on one PC, and later run **pcmail -o** on another PC, messages viewed on the first client remain offline. To retrieve an offline message use the vmail program's **g** command.

-q Suppresses status messages unless the program encounters an error.

-r (*mailbox* | **all**) Resets your local descriptor file for the specified *mailbox* (or **all** for all of them) by deleting the current descriptor file(s), then getting a new copy of the file from the repository. Note that you have to delete your subscription to a bulletin board, then rejoin the board, to reset your subscription.

-s Retrieves only the changed descriptors (not messages) from the repository. Use this option to save space on your PC's hard disk. This option is also known as the "short" option.

-z Speeds up the processing of actions. Use this option when you are working with slow networks or slow servers.

-? Displays and explains the usage line of the command.

-version Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Examples

To process only the queued actions file for pcmail, enter

```
C:\> pcmail -a

Connecting to xyz.xyz.com, port 158...logged in
Scanning mail directory...done
    Processing actions
           Message chris/1740 marked as seen.
           Message chris/1741 marked as seen.
           Message staff/2267 marked as seen.
           Message staff/2270 marked as seen.
           Reset subscription tcp-ip to 3929
           Reset subscription pc-ip to 320
    All actions have been processed.
```

```
Skipping synchronization of mailboxes.
```

To retrieve only new descriptors, enter

```
C:\>pcmail -s
```

To delete the mail descriptor file for the mailbox `chris` and get a new copy from the server, enter

```
C:\> pcmail -r chris
```

To use a Pcmail server other than your default server, enter

```
C:\> pcmail -c machine1
```

The pcmail program uses the configuration section specified by `[pctcp machine1]` in the PCTCP.INI file, which specifies a server other than the default Pcmail server.

See Also

vmail

RFC 1056

pcmail

pctcpcfg

Usage

pctcpcfg [**-k** | **-K**] [**-b**] [**-i** *ini-file*] [**-p** *package*] *section* [**-s** *subsection*]
("" | *variable* ["" | *value ...*])
pctcpcfg [**-help]**
pctcpcfg [**-?** | **-version**]

Description

The **pctcpcfg** command lets you set new values in the PCTCP.INI configuration file. If you use the **-k** or **-K** options, you can set new values in the active kernel. You can set more than one value at a time. You can also use this command in DOS batch files.

Command Line Options

""	Displays all variables for the section or subsection.
-b	Specifies that a backup file not be created.
-help	Displays a list of kernel variables you can set using the **-k** or **-K** options.
-i *ini-file*	Specifies the pathname of an alternative configuration file.
-K	Sets a value in the kernel only.
-k	Sets a value in the kernel and the PCTCP.INI file.
-p *package*	Specifies the name of the product package you want to configure.
-s *subsection*	Specifies the configuration file subsection.
section	Specifies the configuration file section.
value	Specifies the new value, or values, for the variable.
variable	Displays the variable specified (for example, `sec-arg`).
variable ""	Clears the value for the specified variable.
variable value	Changes the value for the specified variable.
-?	Displays and explains the usage line of the command.
-version	Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Examples

To display the list of variables and their values for a specific section, enter

```
C:\> pctcpcfg tn ""

[pctcp tn] - cmdline = tunes
[pctcp tn] - ftpsrv = on
```

To display the list of variables and their values for a specific subsection, enter

```
C:\> pctcpcfg idrive -s vex ""

[pctcp idrive vex] - host = vex.xyz.com
[pctcp idrive vex] - path = /fw/usrs/dfg
[pctcp idrive vex] - drive = g:
[pctcp idrive vex] - sec-key = pcnfs
[pctcp idrive vex] - sec-arg = dfg
[pctcp idrive vex] - lock = Y
```

To clear (reset) the domain-name-server address(es) in the kernel, enter a pair of quotation marks instead of an address, as follows:

```
C:\> pctcpcfg -K addresses domain-name-server ""
```

To set two domain-name-server addresses in the `[pctcp addresses]` section of your PCTCP.INI file and the kernel, enter a command similar to the following. Note that this command removes previous addresses and replaces them with specified IP addresses.

```
C:\> pctcpcfg -k addresses domain-name-server 128.127.50.101 128.127.50.102
```

To display the value of the `subnet-mask=` in the `[pctcp ifcust 0]` configuration file section, enter

```
C:\> pctcpcfg ifcust -s 0 subnet-mask

[pctcp ifcust 0] - subnet-mask = 255.255.0.0
```

See Also

kernel

pctcpcfg

ping

Usage

ping [*-options*] *host*
ping [**-?** | **-version**]

Description

Use **ping** to determine if a host is active and to isolate host connection problems. The **ping** command sends an echo request to another host and waits for a response, using the Internet Control Message Protocol (ICMP).

The **ping** command reports success with a `Host responding` message followed by statistics for the host that initiated the connection. The command might also report failure with a `Ping failed` or `cannot resolve hostname` message followed by statistics about the host that initiated the connection.

Command Line Options

When typing the following options on the command line, leave a space between the option and any values or arguments that correspond to it.

Options **-j**, **-k**, **-o**, **-r**, **-s**, and **-x** add IP options to the packet header. Options may be combined, and space is allotted to a variable length option depending on what else is selected. Variable length options take up three bytes of header space in addition to whatever is used up by the data. If the selected combination totals more than 40 bytes, **ping** prints out an error message and fails.

-d [*bytes*] Displays header and debugging information about the incoming packet. Use the *bytes* value to specify the number of bytes to display in hexadecimal notation. If you specify the **-t** option with the **-d** option, the program repeatedly contacts the target host and displays the first input packet along with a changing display of the number of echoes.

-d# [*bytes*] Displays header and debugging information about the outgoing packet. Use the *bytes* value to specify the number of bytes to display in hexadecimal notation. If you specify the **-t** option with the **-d#** option, the program repeatedly contacts the target host and displays the first output packet along with a changing display of the number of echoes. If you specify both the **-d#** and **-d** options, **ping** displays information for the outgoing packet first.

-e Cancels any configured IP extended security levels or authority that **ping** would otherwise insert.

host Specifies the name or Internet address of the remote host.

-i *number* Sets the IP Time-to-Live (TTL) value on the outgoing packet and displays the TTL value for the incoming packet. The range for *number* is 1–255; the default is 64.

-j *dest1 ... destn* Turns on the IP Loose Source Routing option, which lets the packet pass through unlisted routers between destinations. Each destination is the IP address of a

router through which the packet must pass on the way to the final destination. The **-j** option cannot be used with the **-k** option.

-k *dest1 ... destn* Turns on the IP Strict Source Routing option, which does not let the packet pass through unlisted routers between destinations. Each destination is the IP address of a router through which the packet must pass on the way to the final destination. The **-k** option cannot be used with the **-j** option.

-l *length* Sets the length in bytes of the data in a packet. The default *length* is 256 bytes. You can use this option to send longer packets through the network if the transport to which your PC is connected supports a data length greater than 256 bytes.

-n *times* Sends a specific number of echo requests and then stops. By default, **ping** sends only one echo request. The **-t** option overrides this option.

-o Turns on the IP No-Op option, which has no effect on the transmission but is sometimes used for alignment purposes. It uses 1 byte of option space.

-p *precedence* Sets the IP Precedence level. The variable *precedence* is a number in the 0–7 range. This option overrides any Precedence options configured in PCTCP.INI.

The IP precedence levels and descriptions are as follows:

Level	Precedence	Level	Precedence
0	Routine	4	Flash override
1	Priority	5	CRITIC/ECP
2	Immediate	6	Internetwork control
3	Flash	7	Network control

-Q Turns on the Trace Route option, which performs like the **-q** option except that IP addresses are not translated to domain names.

-q Turns on the Trace Route option. The option increments the TTL to identify all of the routers encountered when trying to reach the target host, and denotes each router by its IP address and domain name. The option displays the number of hops required to reach the target host. If it does not reach a host after 96 hops, **ping** times out.

-r Turns on the IP Record Route option.

-s *level* [*authority*] Sets the IP Security level and, if specified, the type of authority. The variable *level* is a number in the 0–4 range, and the variable *authority* is a number in the 1–5 range. If you do not specify an authority value, **ping** inserts the basic security value from PCTCP.INI. The **ping** command also takes any value for *level* outside of the list range as the basic security level. The valid Security levels, functions, authority values, and names are as follows:

Level	Function	Authority	Name
0	Turns off basic security	1	GENSER
1	Unclassified	2	SIOP
2	Confidential	3	SCI
3	Secret	4	NSA
4	Top Secret	5	DOE

Caution: Running the **ping** command with some security levels might abruptly stop a remote host.

-t Continuously sends echo requests to the target host, each time waiting for a response before sending the next request. When in this request-response-request loop, **ping** reports all echo failures and an incremental summary of trials and successes. To exit from this command, type **q**. The **-t** option overrides the **-n** option, if specified.

-v *type* Requests an IP Type of Service option. The variable *type* is a number in the 0– 15 range. This option overrides any Type of Service options configured in PCTCP.INI. The service depends on the router and is not guaranteed; therefore, requesting this option may have no effect on the performance of **ping**.

The value and description for each valid *type* are as follows:

Type	Description		Type	Description	
0	Normal		8	Low delay	(LD)
1	Low cost	(LC)	9	= 8 + 1	(LC, LD)
2	High reliability	(HR)	10	= 8 + 2	(HR, LD)
3	= 2 + 1	(LC, HR)	11	= 8 + 2 + 1	(LC, HR, LD)
4	High throughput	(HT)	12	= 8 + 4	(HT, LD)
5	= 4 + 1	(LC, HT)	13	= 8 + 4 + 1	(LC, HT, LD)
6	= 4 + 2	(HR, HT)	14	= 8 + 4 + 2	(HR, HT, LD)
7	= 4 + 2 + 1	(LC, HR, HT)	15	= 8 + 4 + 2 + 1	(LC, HR, HT, LD)

-w *seconds* Specifies a number of seconds to wait for a response. The default value is 6. The range for *seconds* is 1 through 32767.

-x Turns on the IP Timestamp option. All routers that implement Timestamp will stamp the packet when encountered.

-x 1 Specifies that each time stamp is preceded by the IP address of the recording entity. Each recorded time stamp takes 8 bytes of option space.

-x 3 *dest1 ... destn* Specifies that time stamps will be filled in only by designated routers (including the final host on the route). Each recorded time stamp takes 8 bytes of option space.

-z Specifies quiet mode, which reports success or failure rather than full statistics.

-? Displays and explains the usage line of the command.

-version Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Examples

To send an echo request to the host lee.xyz.com and display network debugging information, enter

```
C:\> ping lee.xyz.com

host responding, time = 25 ms

Debugging information for interface ifcust Addr(6): 00 00 c0 ea 93 10
interrupts: 49 (0 receive, 0 transmit)
packets received: 42, transmitted: 7
receive errors: 0, unknown types: 14
           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: 0
ARP statistics:
arps received: 9 (7 requests, 2 replies)
           bad: opcodes: 0, hardware type: 0, protocol type: 0
arps transmitted: 2 (2 requests, 0 replies)
3 large buffers; 2 free now; minimum of 0 free
3 small buffers; 3 free now; minimum of 1 free
```

To trace the route an echo request takes to get to a target host, enter

```
C:\> ping -q 128.127.53.118

hop 1:     128.127.55.10                      router-55.xyz.com
hop 2:     128.127.52.7                       router-52.xyz.com
```

```
hop 3:     128.127.53.11                        router-53.xyz.com

Target (128.127.53.118) reached on hop 4, round-trip time 160 ms.
```

See Also

host, inet

ping

pop2, pop3

Usage

pop2 [**-c** *client_section*] [**-d**] [**-h** *hostname*] [**-k**] [**-n** *mbox_name*] [**-q**] [**-u** *username*] [**-s**]
pop2 [**-?** | **-version**]

pop3 [**-c** *client_section*] [**-d**] [**-h** *hostname*] [**-k**] [**-n** *mbox_name*] [**-q**] [**-u** *username*] [**-s**]
pop3 [**-?** | **-version**]

Description

The **pop2** and **pop3** commands run mail client programs on your PC that implement versions 2 and 3, respectively, of the Post Office Protocol (POP). The main differences between the pop2 and pop3 programs are that the pop2 program, but not the pop3 program, supports the use of multiple mailboxes, and the pop3 program, but not the pop2 program, supports access to bulletin boards.

Both client programs initiate connections with a corresponding POP server to receive messages. Each pop program prompts you for your system password to authorize retrieval of your messages, but some versions of the POP3 client use the .RHOSTS file for user authentication.

Both the POP2 and POP3 client programs require a unique top-level directory (the directory below which all of your mail system files and directories are kept) on your PC in which to store messages. After either POP client retrieves your messages successfully from the server, the POP server software deletes your messages on the server. This aspect of the pop programs can be configured by your system administrator.

Use the vmail program to read and compose messages. You can use the vmail program's commands to queue such actions as forwarding mail or replying to messages, but you must run your POP client after you exit from the vmail program to carry out those actions. To use the vmail program with either the POP2 or POP3 client, your system administrator must install either a POP2 or a POP3 server program on the remote host that acts as your mail server.

Refer to RFCs 1081 and 1082 for more information about the Post Office Protocol.

Command Line Options

-c *client_section* Specifies a mail client section of the PCTCP.INI file other than the default. (See the entry for **vmail** for more information about using multiple servers.)

-d Turns on debugging. Shows network transactions in detail.

-h *hostname* Specifies a *hostname* from which to receive mail. Use this option to specify a hostname other than the default hostname. This option is useful if you are receiving your mail from more than one server program.

-k Deletes all directories and files in the top-level mail directory. The program prompts for your confirmation before performing this action.

-n *mbox_name* Specifies a mailbox other than the default mailbox name.

-q Suppresses status messages unless the program encounters an error.

-s Processes the actions file, but does not retrieve new messages.

-u *username* Specifies the *username* of the user to receive mail from the repository. Use this option to specify a username other than the default for the PC. This option is useful if you are sharing your PC with another user.

-? Displays and explains the usage line of the command.

-version Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Examples

The following example illustrates typical system output for the **pop3** command. The **pop2** command presents the same kind of information.

```
C:\> pop3

Enter password for chris@xyz.xyz.com:
Scanning mail directory... done
    Updating local mbox list
    Connecting to xyz.xyz.com, port 110... Logged in
    Processing actions
    Transmitting message 1... trying local smtp... Done
    Creating mailbox new-staff...Done
    All actions have been processed
    Fetch new messages
    There are 3 new messages for mailbox chris
d:/pop3/mbox1/3459 not on-line; 49 lines, 2292 bytes... done
d:/pop3/mbox1/3460 not on-line; 24 lines, 751 bytes... done
    d:/pop3/mbox1/3461 not on-line; 19 lines, 703 bytes... done
    Skipping synchronization for work
    Skipping synchronization for personal
    Logging out from xyz.xyz.com...
```

To use a server other than your default POP2 server, type

```
C:\> pop2 -c machine1
```

The pop2 program uses the configuration section specified by `[pctcp machine1]` in the PCTCP.INI file.

See Also

smtp, vmail

RFCs 822, 1081, and 1082

pop2, pop3

predir

Usage

predir [**config**] [**prog** *path* [**spool** *path*] [**swap** *path*]
[**printer** (**LPT***n* | *n* | **PRN | off**)] [**hotkey** (**on** | **off**)] [**oneof** (**on** | **off**)]
[**onexit** (**on** | **off**)] [**timeout** (*seconds* | **off**)] [**unload**] [**report**]
predir [**help** | **-version**]

Description

The **predir** command loads, customizes, and unloads a DOS print redirector. The print redirector sends files to a remote printer, using a network printing program such as **lpr** or a DOS batch file that contains print commands.

You can use **predir** command line options to override parameters configured in the `[pctcp print]` section of your PCTCP.INI file.

Note: The **predir** command works only with the terminate-and-stay-resident (TSR) version of the PC/TCP kernel.

Command Line Options

config Loads print redirection configuration values from your PCTCP.INI file.

help Displays and explains the usage line of the command.

hotkey (**on** | **off**) Enables or disables the hotkey print condition. With this condition enabled, **predir** sends your file to the printer when you press the Ctrl+LeftShift+RightShift key combination.

oneof (**on** | **off**) Enables or disables the end-of-file print condition. With this condition enabled, **predir** sends your file to the printer when it detects the file being closed.

onexit (**on** | **off**) Enables or disables the print-on-exit print condition. With this condition enabled, **predir** sends your file to the printer when you exit from the application from which you choose to print the file.

Note that this option is automatically disabled when you are using **predir** from a DOS session within Windows. If print-on-exit were enabled, **predir** might print a job prematurely when it detected other applications stopping.

printer (**LPT***n* | *n* | **PRN | off**)

Sets the printer port from which **predir** redirects print jobs. You can specify the port as LPT1, LPT2, LPT3, LPT4, or PRN (PRN is equivalent to LPT1). You also can specify an absolute number, such as 0 for LPT1 and so on. Specify **`off`** to disable print redirection without unloading **predir** from memory.

prog *path* Specifies the pathname of a network printing program or batch file that sends the redirected print job to a printer. The pathname must be in the form *drive:\path\filename.*

report Reports the current configuration settings of the print redirector.

spool *path* Specifies a directory or file for storing spooled print jobs. If you specify a directory, the print redirector automatically names the spool file PREDIR.SPL. By default, the redirector automatically spools print jobs to the file and directory C:\PREDIR.SPL.

swap *path* Specifies a temporary directory or file for swapping out memory while print redirection occurs. The redirector needs 128K of memory; if that is not available, **predir** temporarily stores the memory it uses in a swap file. If you specify a directory, **predir** creates the swap file in that directory with the name PREDIR.SWP. By default, the redirector uses C:\PREDIR.SWP as its swap file.

If Windows is active, **predir** will not swap a print program into high memory.

timeout (*seconds* | **off**)

Sets the timeout print condition to the number of seconds specified. The print redirector waits the specified number of seconds after you choose to print a file, then sends the file to a remote printer. The timeout ensures that the application has enough time to format the file for printing. To disable the timeout print condition, specify `0` or `off`.

unload Unloads the print redirector.

Note: If you loaded another TSR (such as the DOS print program) into memory after loading **predir**, you must unload it before you can unload **predir**.

-version Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Technical Comments

- If the redirector is loaded, pressing the Print Screen key redirects the contents of the screen to a spool file for subsequent printing. Because PC BIOS only sends Print Screen data to LPT1, it is not possible to use the **predir** command to send Print Screen data to LPT2, LPT3, or LPT4.
- DOS 3.2 specific — If you have problems using **predir** to print to LPT1 or PRN (for example, it discards bytes on 512-byte boundaries), try using LPT2, LPT3, or LPT4.

Examples

To load the print redirector with a specified swap file, enter

```
C:\> predir swap e:\swap
```

To display the current settings for the print redirector, enter

```
C:\> predir report

Current loaded version: 3.0
lpt1/prn is redirected
prog =c:\pctcp\lpr.exe
spool = c:\predir.spl
swap = e:\swap
print-on-hotkey is enabled
```

```
print-on-exit is enabled
print-on-timeout = 300 secs.
print-on-eof is disabled
```

See Also

dopredir, onpredir

predir

rcp

Usage

rcp [**-r**] [**-a** | **-b**] [**-s** |**-z**] [**-k** *realm*] [**-m** *prot_mask*] [*user* @] *host:file file*
rcp [**-r**] [**-a** | **-b**] [**-s** |**-z**] [**-k** *realm*] [**-m** *prot_mask*] *file* [*user* @] *host:file*
rcp [**-?** | **-version**]

Description

The **rcp** command copies files or directories between a remote host and your PC using the 4.2 Berkeley UNIX remote login protocol. You can use wildcards to transfer multiple files.

The **rcp** command uses the Kerberos, RSH, or Rexec authentication protocols as needed. If you configured Kerberos, **rcp** first attempts Kerberos authentication. If Kerberos authentication fails, **rcp** attempts authentication using the RSH protocol. If RSH authentication fails, **rcp** attempts authentication using the Rexec protocol and prompts you for a password if necessary.

Use the **-z** or **-s** options when you know that only a specific authentication protocol will succeed, and you do not want to wait for the other protocols to time out (or for another to begin if one fails).

Command Line Options

-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.

Note: You cannot specify both **-a** and **-b** for a given transfer.

file Specifies the path and filename of the file to transfer. If the path you specify does not begin with a backslash (\), the remote host interprets it relative to your login directory.

host Specifies the name or Internet address of the remote host.

-k*realm* Obtains Kerberos authentication for the specified *realm*. Use this option when the remote host is not in your default realm, as defined in the configuration file KRB.CON, or when it is not included in the realm translation file, KRB.REA.

-m *prot_mask* Specifies the umask protection for the file on a remote host. Because your PC does not have protection bits, you can use this option to set the read, write, and execute bits.

Note: This option overrides the default owner permissions, so you must respecify owner permissions when using this option. This option also overrides the `umask=` entry in the `[pctcp host]` section of your PCTCP.INI configuration file.

-r Specifies a recursive copy. This option lets you copy all files in the current or specified directory and all files and directories below it in the directory hierarchy.

Note: The **-r** option requires that you specify a period (.) instead of a filename.

-s Initially uses the RSH protocol. If unsuccessful, it then uses the Rexec protocol that prompts you for a password.

user Specifies the username on the target host. The default username is the value of the `user=` entry in the `[pctcp general]` section of your PCTCP.INI file.

-? Displays and explains the usage line of the command.

-version Displays the version and patch level of the command. Refer to this information if you call Technical Support.

UNIX Configuration

To use this command with a UNIX host, be sure that

- The `user=` entry in the `[pctcp general]` section of your PCTCP.INI configuration file, or another username you supply on the command line, matches a username in the /etc/passwd file on the remote host.
- Your PC's hostname is in the /etc/hosts file on the remote system.

The 4BSD UNIX remote login and command execution protocol uses two files that let you log in to a remote system without supplying a password. The /etc/hosts.equiv file is normally administered by a system manager and includes the names of trustworthy hosts and accounts whose security levels are considered equivalent to that of the local system. Users also can create local .rhosts files in their home directories that list additional remote hosts and accounts permitted to log in without a password. A remote user listed in either of these files does not have to supply a password when logging in to the system where the file exists.

Caution: Never include PC names in the /etc/hosts.equiv or .rhosts files. Listing a PC name in these files can cause security problems, because it means anyone can initiate a remote login from an unattended PC and masquerade as a trustworthy network user.

Technical Comments

You cannot use **rcp** for direct third-party transfers (that is, you cannot transfer a file directly from one system running UNIX to another system running UNIX). You must first copy the file to your PC.

Protection bits for ordinary files copied from a PC to a UNIX system host are set to 600 by default (read and write permission for the owner and no access permissions for group or world). For executable files (*.BAT, *.COM, *.EXE, etc.), protection bits are set to 700 by default (read, write, and execute permissions for the owner and no permissions for others). Note that you cannot set execute bits for unexecutable files; such a setting will be ignored, and the permissions will remain at a unexecutable setting.

Examples

To copy the file /etc/hosts from the host green.xyz.com into a local file HOSTS.TXT on your PC, enter the following:

```
C:\> rcp green.xyz.com:/etc/hosts hosts.txt
```

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 (and do not forget the colon):

```
C:\> rcp -b *.exe green.xyz.com:
```

To copy all files from your current directory and its subdirectories to your login directory on the host green.xyz.com, enter the following (and do not forget the colon):

```
C:\> 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:

```
C:\> 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 (and do not forget the space before the final period):

```
C:\> rcp -r green.xyz.com:* .
```

See Also

ftp, tftp, kinit

rcp

rlogingl

Usage

rlogingl *host* [*user*] [**-tt** *ttype*] [**-c** *channel*] [**-i**] [**-e** *emulator command_list*]
rlogingl [**-?** | **-version**]

Description

The **rlogingl** command uses the 4BSD UNIX remote login protocol (Rlogin) to connect your PC to a remote UNIX host. Because **rlogingl** does not emulate characteristics of any specific terminal and does not interpret data, the resulting terminal type is what is known as a "glass" or dumb terminal. You can use **rlogingl** with terminal emulation. On the command line, specify a DEC VT terminal type, or any commercial terminal emulator that supports the IBM PC BIOS Interrupt 14 interface. The anonymous FTP server ftp.ftp.com has more information about glass terminal emulation and the IBM PC BIOS Interrupt 14 interface.

Command Line Options

-c *channel* Specifies an asynchronous communication channel on your PC to use for the connection. The value of *channel* identifies the communication port. The standard PC serial ports are COM1 and COM2. Enter a `0` to specify COM1 or a `1` to specify COM2. This option is useful if your PC has direct connections to one or more of its asynchronous communications ports.

-e *emulator command_list*
Enables external terminal emulation through the IBM PC BIOS Interrupt 14 interface. The *emulator* argument specifies the terminal emulator path and filename. The *command_list* argument includes any arguments required to run the emulator. The specified emulator runs after the connection opens.

host Specifies the name or Internet address of the remote host.

-i Specifies to (1) keep a Telnet session open until the external emulator is loaded and (2) send an Int 14 **init** command. This command line option does not work if the commercial terminal emulator you are using does not support the Int 14 **init** command (if you are unsure, ask your system administrator). You must specify this with the **-e** command line option.

-tt *ttype* Specifies a DEC VT terminal type to emulate. The value of *ttype* can be **vt220**, **vt100**, or **vt52**.

user Specifies the username on the target host. The default username is the value of the `user=` entry in the `[pctcp general]` section of your PCTCP.INI file.

-? Displays and explains the usage line of the command.

-version Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Escape Commands

You can use escape commands to change terminal characteristics, to manage the transfer of data

between your PC and the remote system, and to manage your session. Use the Ctrl+6 escape key to gain access to the commands. If you are using a commercial terminal emulator with **rlogingl**, you cannot use the escape key.

!	Invokes a nested DOS command interpreter.
?	Displays a help message listing the escape commands.
c	Closes the connection and exits from the program.
i	Sends the contents of a PC file as input to the remote host command line. You are prompted for the name of the file, whose contents are then sent to the remote host exactly as if you typed and entered them there. If the remote host is a UNIX system, you can enter the **cat** command on the remote host to redirect the input to a file. For example, entering the command **cat > test** followed by the **i** escape command transfers the contents of the file you specify to a file named TEST on the remote system. To terminate the input redirection on the remote system, press Ctrl+D.
o	Records your keystrokes and the resulting remote system output in a file on your PC. The remote login program prompts you for a filename in which to store the data. If the file already exists, the new data overwrites the existing contents of the file. You also can specify a device such as a printer as the output file. Press the **o** escape command again to close an open output file.
q	Ends the current remote login session by resetting the connection instead of closing it gracefully. Use this option only when you cannot exit from the session normally by logging out or by using the **c** escape command.

Example

To log in to the remote host vex.xyz.com, specifying COM1 as the communications port and \ TERM\EM4105 as the pathname of an emulator, use the following command:

```
C:\> rlogingl vex.xyz.com -c 0 -e \term\em4105
```

See Also

rcp, rloginvt, rsh, tn, tnglass

rlogingl

rloginvt

Usage

rloginvt *host* [**-s** | **-z**] [**-k** *realm*] [**-43** | **-50**] [*user*]
rloginvt [**-?** | **-version**]

Description

The **rloginvt** command uses the 4BSD UNIX Rlogin protocol to connect your PC to a remote UNIX system host. The appropriate server must be running on the remote system.

The rloginvt program includes an embedded FTP server that lets you transfer files between your PC and the remote system during the remote session. An escape key provides access to the FTP server, as well as to many functions for manipulating data and managing your session.

Note: If you configured Kerberos on your system, **rloginvt** first attempts Kerberos authentication. If that fails, **rloginvt** executes without Kerberos authentication.

Command Line Options

-43 or **-50** — Requests a 43- or 50-line screen instead of the default 24-line screen. The rloginvt program uses the last line to display the status line. Use 43-line mode with an EGA video card; use 50-line mode with a VGA video card.

host — Specifies the name or Internet address of the remote host.

-k*realm* — Obtains Kerberos authentication for the specified *realm*. Use this option when the remote host is not in your default realm, as defined in the configuration file KRB.CON, or when it is not included in the realm translation file, KRB.REA.

-s — Does not attempt Kerberos authentication. Uses only the Rlogin protocol.

user — Specifies the username on the target host. The default username is the value of the `user=` entry in the `[pctcp general]` section of your PCTCP.INI file.

-z — Uses only Kerberos for authentication.

-version — Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Escape Commands

You can use escape commands to change terminal characteristics, to manage the transfer of data between your PC and the remote system, and to manage your session.To gain access to the escape commands, use the F10 or Alt+F10 escape key.

! — Invokes a nested DOS command interpreter.

Note: The FTP server in rloginvt program is suspended during the escape to a DOS shell. For example, if someone is transferring a file to your PC over an FTP connection, that file transfer is suspended until you exit from the DOS shell. When you exit from the DOS shell, the FTP server reactivates and the file transfer continues.

? Displays a help message listing the escape commands.

0– 9 Creates a new connection, or switches to an existing connection identified by the number you supply. To see a list of existing connections, use the **Ctrl+s** escape command. To create a new connection, press the escape key and enter any number 0 through 9 that is not in use for an existing connection. The following prompt appears:

```
No connection. Host to connect to?
```

Enter the name of the host to which you want to connect, or press the Enter key to return to the current connection.

B Causes the Backspace (←)key to send the ASCII backspace character and the Ctrl+Backspace (Ctrl+←) keys to send the ASCII delete character. The **D** escape command reverses this behavior.

c Closes the connection and exits from the program.

D Causes the Backspace (←) key to send the ASCII delete character and the Ctrl+Backspace (Ctrl+←) keys to send the ASCII backspace character. This behavior is the default; the **B** escape command reverses it.

d Turns off line wrap. If a line is too long for the display, extra characters overwrite existing characters on the line. (This option is the default). To reverse this behavior, use the **w** escape command.

F Starts or stops an FTP server on your PC. Disabling the server prevents new connections, but does not terminate existing connections. To prevent existing connections from writing or deleting files, use the **W** command to enable write protection.

i Sends the contents of a PC file as input to the remote host command line. You are prompted for the name of the file, whose contents are then sent to the remote host exactly as if you typed and entered them there. If the remote host is a UNIX system, you can enter the **cat** command on the remote host to redirect the input to a file. For example, entering the command **cat > test** followed by the **i** escape command transfers the contents of the file you specify to a file named TEST on the remote system. To terminate the input redirection on the remote system, press Ctrl+D.

m Lets you change from one DEC VT terminal emulator mode to another. This command displays a message showing you the five modes available, and identifies each mode by a number 0 through 4. Specify the mode by typing the corresponding number.

Note: Mode 1 (vt220 mode, 8 bit controls) is binary mode. Not all hosts support emulation in binary mode.

o Records your keystrokes and the resulting remote system output in a file on your PC. The remote login program prompts you for a filename in which to store the data. If the file already exists, the new data overwrites the existing contents of the

file. You also can specify a device such as a printer as the output file. Press the **o** escape command again to close an open output file.

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 give the **o** escape command a second time.

p Specifies the DOS code page to use for remote login sessions. The code page in use can affect how PC/TCP displays special and multilingual characters on your screen. The PC/TCP terminal emulators support DOS code pages 437 (IBM PC English) and 850 (IBM PC multilingual).

After you enter this command, a prompt in the following form appears:

```
Select DOS codepage (press Enter to remain at nnn):
```

where *nnn* indicates the active code page. Enter a new code page number, or press Enter to keep the current code page number.

Note: You should normally change the code page using the DOS **chcp** command. Use the **p** escape command only for problem solving.

q Ends the current remote login session by resetting the connection instead of closing it gracefully. Use this option only when you cannot exit from the session normally by logging out or by using the **c** escape command.

U Turns on the display of the status line at the bottom of the terminal screen (this is the default). If you request extended screen height and your PC's card and monitor can display only 43 lines, the status line is automatically turned off. In addition to the time and hostname, the following other indicators may appear when the status line is on:

Indicator	Condition
`i`	An input file on your PC is open.
`o`	An output file on your PC is open.

u Turns off the display of the status line at the bottom of the terminal screen. Some escape commands display messages regardless of whether the status line is turned on or off.

W Enables or disables write protection for the FTP server (the default state 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 server has never been enabled, this command has no effect.

w Turns on line wrap. If a line is too long for the display, the extra characters appear on the next line. To reverse this behavior, use the **d** escape command.

Ctrl+d Displays kernel debugging information similar to the output of the **ping** command.

Ctrl+h	Displays a help message listing the control character escape commands.
Ctrl+l	Redraws the screen for the current connection.
Ctrl+n	Displays network status information, including kernel TCP, IP, UDP, and ICMP statistics. The output is similar to that of the **inet stats** command.
Ctrl+s	Lists current connections, and shows the status of the active connection and the FTP server.

Example

To log in to the host vex.xyz.com using the default DEC VT220 terminal emulator, enter

```
C:\> rloginvt vex.xyz.com
```

See Also

kinit, rcp, rlogingl, rsh

rloginvt

rmt

Usage

rmt [**-h** *host*] [**-f** *device*] [**-z** |**-s**] [**-k** *realm*] *command* [*count*]
rmt [**-?** | **-version**]

Description

The **rmt** command controls a remote tape drive.

You can use **rmt** in conjunction with the **tar** command to perform remote backups for your PC. The **rmt** command uses **rsh** to run the UNIX **mt** (magnetic tape) command on the remote host.

If you configured Kerberos, **rmt** first attempts Kerberos authentication. If Kerberos authentication fails, **rmt** tries to authenticate your username and password using the RSH protocol and the .rhosts file on the remote host. If that fails, **rmt** uses the Rexec protocol and prompts you for a password. You will see your password as you type it.

Note: Tape manipulation programs such as **mt** are best used with a device that does not rewind tapes automatically.

Command Line Options

command	Specifies a command that **mt** on the remote host will accept. See the "Interactive rmt Commands" section for a list of available commands.
count	For commands that require a count, the default value for *count* is 1.
-f *device*	Specifies a tape device to use instead of the configured tape device.
-h *host*	Specifies a remote host to use instead of the default host. The value of *host* is either a character-string name of the target host, or an IP address in standard form (for example, 128.126.50.160).
-k *realm*	Obtains Kerberos authentication for the specified *realm*. Use this option when the remote host is not in your default realm, as defined in the configuration file KRB.CON, or when it is not included in the realm translation file, KRB.REA.
-s	Initially uses the RSH protocol. If not successful, it then uses the Rexec protocol that prompts you for a password.
-z	Uses only Kerberos for authentication.
-?	Displays and explains the usage line of the command.
-version	Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Interactive rmt Commands

Note that some servers may not accept all of these commands.

bsf *count*	Moves backward on the tape over the number of files specified in *count*.

bsr *count*	Moves backward on the tape over the number of records specified in *count*.
fsf *count*	Moves forward on the tape over the number of files specified in *count*.
fsr *count*	Moves forward on the tape over the number of records specified in *count*.
offl	Takes the tape offline.
rew	Rewinds the tape.
stat	Displays the status of the tape.
weof *count*	Writes End-of-File markers at the current position on the tape. *Count* specifies the number of markers to write.

Example

To display the status of a tape located at device /dev/rst0 on remote host vex.xyz.com, enter

```
C:\> rmt -h vex.xyz.com -f /dev/rst0 stat
```

See Also

ddates, kinit, klist, rsh, tar

rmt

rsh

Usage

rsh *host* [**-s** | **-e** | **-z**] [**-k** *realm*] [**-b**] [**-d**] [**-l** *userid*] *commandline*
rsh [**-?** | **-version**]

Description

The **rsh** command executes 4BSD UNIX commands from your PC. It supports execution of a single command on a remote host. Enter all options on the command line; **rsh** does not support interactive commands.

Use the **-z**, **-s**, and **-e** options when you know that only a particular authentication protocol will succeed, and you do not want to wait for the other protocols to time out (or for another to begin if one fails).

Command Line Options

-b	Specifies that the output from the remote command is binary, and disables conversion between UNIX end-of-line notation and PC end-of-line notation.
commandline	Specifies any remote command (or series of commands for some hosts).
-d	Turns on debugging. Shows network transactions in detail.
-e	Uses only the Rexec protocol for authentication and prompts you for a password.
host	Specifies the name or Internet address of the remote host.
-k*realm*	Obtains Kerberos authentication for the specified *realm*. Use this option when the remote host is not in your default realm, as defined in the configuration file KRB.CON, or when it is not included in the realm translation file, KRB.REA.
-l *userid*	Passes the remote host the user ID you specify. This option overrides the `user=` parameter in the `[pctcp general]` section of your PCTCP.INI file. For Kerberos, **rsh -l** *userid* lets you specify a Kerberos principal different from the `user` parameter.
-s	Uses only the Rsh protocol for authentication.
-z	Uses only Kerberos for authentication.
-?	Displays and explains the usage line of the command.
-version	Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Example

To request the host vex.xyz.com to list the contents of the /etc/hosts file, enter the following:

```
C:\> rsh vex.xyz.com cat /etc/hosts
```

See Also

rloginvt, rlogingl, rcp, kinit

rsh

setclock

Usage

setclock [*time_server*]
setclock [**-?** | **-version**]

Description

The **setclock** command obtains a reading from a network time server and sets the PC date and time accordingly. You may add the **setclock** command to your AUTOEXEC.BAT file, as long as the **kernel** command goes before it. Using **setclock** in your AUTOEXEC.BAT file synchronizes your PC (within a few seconds) with other machines on your network. This synchronization is useful if you share files with other people.

To set the time zone and offset for your PC, set the DOS TZ global variable from the DOS command line. For Eastern Standard Time, type the command **`set TZ=EST5EDT`** to set Daylight Savings Time. For Japan, type the command **`set TZ=JST-9`**. For Switzerland (Central Europe), type the command **`set TZ=CET-1CDT`**.

You can also set the time zone and offset by setting two entries in the `[pctcp general]` section of the PCTCP.INI configuration file. Set the time zone with the `time-zone=` entry, and the time zone offset with the `time-zone-offset=` entry. The time zone offset starts with Universal Time Coordinated (UTC), then adjusts according to the number of minutes you are ahead or behind UTC. For example, for Eastern Standard Time, use `time-zone=EST` and `time-zone-offset=300`. For Japan, use `time-zone=JST` and `time-zone-offset=-540`. For Switzerland (Central Europe), use `time-zone=CET` and `time-zone-offset=-60`.

The setclock command accepts alternative dates for the change between Standard and Daylight Savings Time (DST). You specify these changes with the `dst-begins=` and `dst-ends=` entries in the `[pctcp time]` section of the PCTCP.INI configuration file. Indicate the starting and ending days for DST by the number of days from January 1; for example, `dst-begins=94` and `dst-ends=305`.

Command Line Options

time_server — Specifies either hostname or an IP address of a network host that provides User Datagram Protocol (UDP) time service.

If *time_server* is omitted, **setclock** sends requests to any time serversthat you configure in your PCTCP.INI file. There are no default time servers. You can specify a default time server by adding its IP address to the `time-server=` entry in the `[pctcp addresses]` section of your PCTCP.INI file. You can configure as many as five time servers.

-? — Displays and explains the usage line of the command.

-version — Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Examples

To request the time server green.xyz.com to return a reading that sets the date and time on your PC, enter

```
C:\> setclock green.xyz.com

setting date to Friday, 6/24/94
setting time to 18:59:22 EST
```

If the network is not operational, you see the following message instead:

```
Time service not responding. Clock not set.
```

See Also

idrive, idutil, idconfig, kinit

setclock

setcolor

Usage

setcolor [**-3**] [**-d**] [**-l**] [**-h**] [**-w**]
setcolor [**-?** | **-version**]

Description

The setcolor program lets you preview and set display colors for the tn, rloginvt, and vmail programs.To exit from the program, press the Esc key.

Command Line Options

-3 Configures colors for IBM 3270 and DEC VT terminal emulation. If you do not specify this option, colors are configured for VT terminal emulation only. To define these color values for IBM 3270 terminal emulation, set the `ftp-sfe-attr=` and `ftp-sfe-rv-attr=` entries in the `[pctcp 3270]` section of the PCTCP.INI file.

-d Displays debugging information.

-h Uses 43-line or 50-line high-resolution mode (if supported).

-l Uses low-resolution mode.

-w Uses wide mode (if supported).

-? Displays and explains the usage line of the command.

-version Displays the version and patch level of the command. Refer to this information if you call Technical Support.

setcolor

smtp

Usage

smtp *mail_file* **-f** *from* [**-n** *net_timeout*] [**-r** *relay*] [**-v**] (**-t** *to_list* | **-i** *to_file*)
smtp [**-?** | **-version**]

Description

The **smtp** command, a client implementation of the Simple Mail Transfer Protocol (SMTP), transfers mail from your PC to the network. The SMTP client generates dates in message headers that comply with RFC 822 format.

Typically, the mail program calls the smtp program when it is ready to send a message, but you can run the smtp program manually, using its command options to receive the debugging messages that are displayed when the mail program runs in verbose mode. The pop2, pop3, and nntp programs also use the smtp program to transfer mail to the mail server.

Command Line Options

-f *from* — Sends the message coming from the user named by *from*. (You must have a space before the username indicated by *from*.)

-i *to_file* — Identifies a file that contains a mailing list of multiple recipients (one address per line) to receive the message. Note that if an error exists in the file, the message is not sent to subsequent recipients. The **smtp** command requires either the **-i** *to_file* option or the **-t** *to_list* option, and the chosen option must be the last one supplied at the `c:\>` prompt.

mail_file — Identifies the name of the mail file being sent.

-n *net_timeout* — Breaks the connection with the mail server after waiting *net_timeout* minutes.

-r *relay* — Specifies a mail relay server, even if none is specified in your PCTCP.INI file. You can use this option to override the default mail relay server specified by `relay-server=` parameter in the `[pctcp addresses]` section of your PCTCP.INI file.

-t *to_list* — Lists the addresses, separated by spaces, to which a message is being sent. (Put a space before the first address.) The **smtp** command requires either the **-i** *to_file* option or the **-t** *to_list* option, and the chosen option must be the last one supplied at the `c:\>` prompt.

-v — Enables verbose mode for debugging.

-? — Displays and explains the usage line of the command.

-version — Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Example

To send the file C:\LETTER.TXT from the username `sam` to `chris@green.xyz.com`, enter

```
C:\> smtp -f sam c:\letter.txt -t chris@green.xyz.com
```

See Also

pop2, pop3

RFC 822

smtp

snmpd

Usage

snmpd
snmpd [**-?** | **-version**]

Description

The **snmpd** command lets other hosts and network management stations using SNMP (Simple Network Management Protocol) examine your PC's statistics and configuration information over the network. An SNMP management station obtains this information from your PC's Management Information Base (MIB), for use in troubleshooting and tuning network operations and for determining network performance.

The **snmpd** command starts a terminate and stay resident (TSR) program that provides an agent for SNMP requests that adhere to RFCs 1065 and 1067. This agent can send out two types of error conditions (traps): Cold Start and Authentication Failure, depending on how you configure the **snmpd** program.

Note the following requirements and parameters before you run the **snmpd** command.

- In order for another host to access your PC's SNMP agent, that host must have an SNMP management product (such as the PC/SNMP Tools available from FTP Software, or software from another vendor).
- You must load the PC/TCP TSR kernel before you invoke the **snmpd** command.
- The **snmpd** command does not support the SNMP SetRequest Protocol Data Unit (PDU). Because of this, you cannot modify **snmpd** command MIB variables over the network using an SNMP management product.
- The SNMP agent created by the snmpd program uses approximately 39K of DOS memory, independent of the size or configuration of the PC/TCP kernel. You can load the snmpd program into your PC's upper memory area.

Use the **inet unload** command to unload the PC/TCP TSR kernel and remove the snmpd program from memory.

Command Line Options

-?	Displays and explains the usage line of the command.
-version	Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Example

The following example shows the default startup of the snmpd program.

```
C:\> snmpd

communit.cnf not found; Using community "public", read-only
trapcomm.cnf not found: No Traps will be sent.
```

```
System Description = SNMPD v2.3 (9.3.1) IBM-PC MS-DOS FTP Software
    System Object Identifier = 1.3.6.1.4.1.121.1.1
    Communities: 1 authentication, 0 trap
    agent occupies 37680 bytes}
```

See Also

kernel, inet

RFCs 1065 and 1067

snmpd

tar

Usage

tar (**t** | **x** | **c**) [**vfuazpobm0**– **9Zsk**] [*filename*.**TAR**] [*blocks*] [*realm*] [*files...*] [\ | **.**]
tar [**-?** | **-version**]

Description

The **tar** command copies (backs up or restores) your files between local and remote files, disks, and tapes. It works in conjunction with the **rmt** and **ddates** commands. (To back up files to a tape, the machine with a tape device must have a functional 4BS UNIX-style rmt program.)

If you configured Kerberos authentication, **tar** first attempts Kerberos authentication. If Kerberos authentication fails, **tar** tries the RSH protocol using the remote host's .rhosts file. If that fails, **tar** uses the Rexec protocol and prompts you for a password.

Command Line Options

. (Period) — Backs up all files in your current directory (useful if the command line specifies another directory as well); restores all subdirectories in the specified directory.

**** (Slash **)** — Copies all directories regardless of your current directory. It is safer to go to the root directory and back up or restore your files with the period (**.**) option.

0– **9** — Specifies a number 0 through 9 that controls the "dump" (or copy) level.

For example, you can back up files with the dump level set to 1. For your next backup, set the dump level to 2. The **tar** command backs up only files that have changed since the backup date for level 1. After that, you can set the dump level to 2 again to back up only files that were stored at the same dump level (or at a lower level). Set the dump level to 0 to ignore all dump dates and levels and back up the entire file system. (Use the **ddates** command to see the time for each back up.)

a — Switches between UNIX format and ASCII format. (UNIX terminates each line in a file with a line-feed character; ASCII terminates with both carriage-return and line-feed characters.)

b — Lets you specify the outgoing block size with the *blocks* option. This option should only be used when backing up to a streaming device, such as a tape.

blocks — Specifies the blocking factor (the number of 512-byte blocks) for each **tar** output record. The default value is 20 (10240 bytes). Use this argument with the **b** option.

If you plan to restore files on a machine that has a block size other than 20, specify this remote block size before you back up your files.

c — Creates a new backup file.

f *filename*.**TAR** — Lets you specify the filename to which your data is backed up.

You must specify the filename after the options (including **f**), but before the *files*

argument. The filename is of the form [[*user@*] *host:*] */directories/filename*.TAR. If you do not specify a filename, tar takes it from the `[pctcp tar]` section of your PCTCP.INI file.

files Specifies files to back up or restore.

k Obtains tickets for the remote host specified by *realm*.

m Does not restore file dates during the restoration process. Otherwise, **tar** restores file dates.

o Prompts you for permission to overwrite an existing file with a restored file of the same name.

You must press the y key to overwrite a file. Pressing any other key except P prevents overwriting of the existing file. Pressing the P key automatically allows overwriting to take place. This feature is particularly useful because **tar** automatically translates the name of any restored file that does not conform to DOS filename conventions to a name that does conform. (Note that this translation can lead potentially to the creation of identical filenames for two different files.)

p Compares file creation dates to prevent restored versions of files from replacing more recent files on your PC.

realm Obtains Kerberos authentication for the specified *realm*. Use this option when the remote host is not in your default realm, as defined in the configuration file KRB.CON, or when it is not included in the realm translation file, KRB.REA. Use this option in conjunction with the **k** option.

s Does not attempt Kerberos authentication.

t Gives a directory listing of an existing backup file. If the *files* argument is given, the **t** option searches for those files only.

u Marks files to prevent subsequent backing up. Use the DOS **backup**, **restore**, and **xcopy** commands to modify the file that resides on your system to remove the archival bit associated with it.

v Displays a verbose listing of information during a **tar** process.

x Restores files from an existing backup file and copies them into your current directory. If the *files* argument is given, the **x** option scans only for those files.

Z Uses only Kerberos for authentication.

z Compresses files during backup; decompresses files during restoration.

Note: You cannot decompress a backup file that is not first compressed by a 12-bit compression scheme. Most UNIX system archival compression is 16 bits by default; refer to your UNIX man page for more information. If you attempt to decompress a file that is incompatible with this **tar** feature, **tar** displays an error message and exits to DOS without affecting the backup file.

-? Displays and explains the usage line of the command.

-version Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Technical Comments

Some entries in the `[pctcp tar]` section of PCTCP.INI contain default values for **tar**. You can specify a hostname and (for the backup file) a filename.

When the **tar** command uses the RSH protocol to gain access to the remote system, some security problems can result. See the **rmt** command for a discussion of how this access of a remote system works.

PC/TCP tar requires that the UNIX server has the /etc/rmt and the /bin/touch files. FTP does not support **tar** on a system that does not have an /etc/rmt file. This 4BSD UNIX program is generally not found on UNIX System V machines.

Examples

For the following examples, pat is the username, vex is the remote host, and /dev/1600 refers to the remote tape drive.

To copy and compress your PC's entire file system or disk to magnetic tape, first go to your root directory (DOS command **cd **), and then enter the following (remember the space before the final period):

```
C:\> tar czvf pat@vex:/dev/1600 .
```

To list a directory of files on the tape and confirm a successful execution of tar, enter

```
C:\> tar tvf pat@vex:/dev/1600
```

To do a full recovery of your compressed files from the tape, enter

```
C:\> tar xzvf pat@vex:/dev/1600
```

To recover one compressed file named stuff.txt from the tape, enter

```
C:\> tar xzvf pat@vex:/dev/1600 .\dir\stuff.txt
```

To recover two compressed files named april.txt and may.doc from the tape, enter

```
C:\> tar xzvf pat@vex:/dev/1600 .\dir\april.txt .\dir\may.doc
```

(If nothing happens when you enter these commands, there may be an error in your command line. If you specify the **z** option with any of these command lines and the file is not compressed, **tar** displays an error message.)

See Also

ddates, kinit, klist, rmt, rsh

tar

tftp

Usage

tftp (**get** | **overwrite** | **put**)*local_file host remote_file* [**image**]
tftp serve
tftp [**-?** | **-version**]

Description

The **tftp** command lets you transfer one file at a time between hosts on a network, without requiring you to enter a password. The tftp program uses the Trivial File Transfer Protocol (RFC 783) on PCs.

Since the command does not provide authentication of the user, you can usually transfer only publicly accessible files.

The tftp program can also act as a file transfer server that lets remote users transfer files to and from your PC. The TFTP server provides no access control whatever; that is, it lets a remote host initiate any **tftp** operation for any file on any accessible disk.

When you have the TFTP server running, DOS transfers files to and from the current working directory. The user on the remote machine, however, can specify a full pathname.

The TFTP server permits only one file transfer at any time. If any host requests a transfer while one is already in operation, the TFTP server refuses the second request.

Command Line Options

get	Transfers a file from a remote machine to your PC.
host	Specifies the name or Internet address of the remote host.
image	Transfers binary files literally byte-by-byte from one computer to the other. If this option is omitted, **tftp** processes the file as a text file and performs any necessary character set conversions to and from the network standard character set.
local_file	Specifies the name of the file on your PC file system.
overwrite	Overwrites an existing local file with the contents of a different remote file.
put	Transfers a file from your PC to a remote machine. You usually cannot transfer a file to overwrite an already existing file of the same name.
remote_file	Specifies the name of the file in the remote machine file system. **Note:** The remote machine may require that this filename be fully qualified; that is, the remote filename may need to include a full and exact directory name so the remote system can identify the wanted file. If the remote filename syntax requires the use of greater-than (>), less-than (<), or bar (|) characters, you must enclose the remote filename in quotation marks (“ ”).
serve	Starts up a TFTP server, letting other hosts transfer files to and from your PC.

While the TFTP server is running, you cannot use the PC. Type **q** to end the server program.

-? Displays and explains the usage line of the command.

-version Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Example

To transfer a file called MANUAL.TXT from the host vex.xyz.com to a file with the same name on your PC, enter

```
C:\> tftp get manual.txt vex.xyz.com manual.txt
```

See Also

ftp, ftpsrv, rcp

RFC 783

tftp

tn

Usage

tn [**-a**] [**-b**] [**-D**] [**-h**] [**-k** *realm*] [**-n**] [**-p** ***service-name***] [**-t** *ttype*|**-x** *ttype*] [**-w**] *host* [*port*]
tn [**-?** | **version**]

Description

The **tn** command lets you log in to a remote host using the TCP/IP Telnet protocol. A Telnet server must be running on the remote host.

The tn program negotiates with the remote host to determine the appropriate terminal to emulate (in accordance with the Telnet Terminal Type Negotiation protocol described in RFC 1091). If the remote host does not comply with RFC 1091, **tn** offers only the default DEC VT220 terminal type, unless you use the **-t** or **-x** command line options to request a specific terminal type or a range of types.

Once you connect to a remote host, you can use escape commands to change features of the connection, create connections to other hosts, display information about the connection, and transfer data between the remote host and your PC. See the "Escape Commands" section for more information.

To end a Telnet connection, log out of the remote host (for example, by pressing Ctrl+D or typing **`exit`**). If you cannot log out normally, use the **c** or **q** escape command (see the "Escape Commands" section for details).

Command Line Options

-a Causes **tn** to use the alternate screen size for the chosen terminal type. For use with certain 3270 applications that require the alternate screen size.

-b Specifies that binary mode not be negotiated during VT emulation.

-D Turns on Kerberos debugging. Messages include information such as whether Kerberos authentication is requested and whether the authentication succeeded.

-h Increases the number of screen lines displayed. The screen height varies depending on the type of terminal being emulated and the capabilities of your PC's video card and monitor:

DEC VT type terminals and IBM PC terminals	Screen height increases from the default 24 lines to 43 or 50 lines, depending on your PC's video card and monitor characteristics.
IBM 3278 terminals	Screen height increases from the default 24 lines to 32 or 43 lines, depending on your video card and monitor, and on the `model-3/4=` entry in the `[pctcp 3270]` section of the PCTCP.INI file.
IBM 3279 terminals	Screen height increases to 32 lines.

Your video card and monitor must support high-resolution display for the **-h** option to work correctly. Also, if you are logging in to a remote 4BSD UNIX host, the /etc/termcap file must include a terminal type definition that supports extended screen height.

host Specifies the name or Internet address of the remote host.

If you have specified a default host in the `cmdline=` entry in the `[pctcp tn]` section of the PCTCP.INI file, you can create a **tn** connection to that host by entering the **tn** command with no *host* argument.

-k*realm* Obtains Kerberos authentication for the specified *realm*. Use this option when the remote host is not in your default realm, as defined in the configuration file KRB.CON, or when it is not included in the realm translation file, KRB.REA.

-n Requests that **tn** negotiate only for terminal types without extended attributes. Using a terminal type without extended attributes eliminates the exchange of control information, known as "data stream orders," related to the use of those attributes. This additional data can slow down interactions with some remote hosts. If you know that you are logging in to an IBM host and you know that you do not want to use a terminal with extended attributes, you can improve the response time of your **tn** connection by using the **-n** option.

-p *service-name* Specifies a Kerberos service name other than rcmd. The tn program requests the RFC 1411-compliant name rcmd; hosts using various Telnet server implementations may use a different name.

The following lists the service name and associated provider of Telnet server implementations:

telnet Sandia National Laboratories

port Specifies the number of a port on the remote host machine, letting you connect to a remote host through a port other than the default port (port 23). This option can be useful for solving problems with connecting to remote servers.

-t *ttype* Requests that **tn** offer a range of terminal types, beginning with the specified type, during negotiation with the remote host. The tn program sends a name from an ordered list in response to each request from the remote host, cycling 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

IBM 3278 Model 2

You can change this default list by specifying the **-t** option. Use one of these *ttype* keywords to indicate the beginning point in the list:

vt vt220 vt100 vt52 ibmpc 3277 3277 3278 3279

Keywords are case sensitive; you must enter them exactly as shown.

Note: The **-t** and **-x** options are mutually exclusive.

-w Enables a wide screen display, if **tn** negotiates 3270 emulation and if your video card and monitor support wide screen display. This option is available only with the 3278 terminal type (the default IBM terminal type). For most display adapters this option causes the screen to have 132 columns and 43 lines. Some video display adapters support other screen heights.

You do not need to use **-w** to enable 132-column mode for the VT220. The DEC VT220 emulator enters 132-column mode if an application on the remote system requests it and if your video card and monitor are capable of it.

-x *ttype* Requests negotiation of a specific terminal type. Use one of the following keywords:

vt vt220 vt100 vt52 ibmpc 3277 3278 3279

If the terminal you request is a specific type, **tn** negotiates for that terminal type only.

If you use the keyword **vt**, **tn** offers the three DEC VT types from the list of terminal types in the following order: VT220, VT100, and VT52. This is synonymous with **-t vt**.

Note: The **-t** and **-x** options are mutually exclusive.

-? Displays and explains the usage line of the command.

-version Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Escape Commands

To invoke an escape command in a **tn** session, press the escape key; then enter the escape command at the `Command:` prompt. The escape key is Alt+F10. Escape commands are case sensitive.

? Displays a help message listing the escape commands.

! Invokes a nested DOS command interpreter, but does not close the Telnet connection. To return to the remote host, type **`exit`** at the DOS prompt.

Note: If the tn program's built-in FTP server is running when you enter this escape command, the server suspends activity during the escape to a DOS shell. For example, if someone is transferring a file to your PC over an FTP connection,

that file transfer is suspended while you are using the DOS shell. When you exit from the DOS shell, the FTP server restarts and the file transfer continues.

0– 9 Creates a new connection, or switches to an existing connection identified by the number you supply. To see a list of existing connections, use the **Ctrl+s** escape command. To create a new connection, press the escape key and enter any number 0 through 9 that is not in use for an existing connection (use the **Ctrl+s** escape command to see a list of existing connections).

The following prompt appears:

```
No connection. Host to connect to?
```

Enter the name of the host to which you want to connect, or press the Enter key to return to the current connection.

Options that you specify on the **tn** command line to create the first connection do not carry over to subsequent connections. To specify an option on a subsequent connection, type the option before the hostname at the `Host to connect to?` prompt.

Note: If the `cmdline=` entry in the `[pctcp tn]` section of the PCTCP.INI file names a host, you can simply press the Enter key to create a new connection to that host. If you decide you do not want a new connection, but your `cmdline=` entry names a host, type **`-?`** or **`-version`**; then press the Enter key to return to current connection.

a Sends a Telnet protocol IAC Are-You-There command to the remote host to determine if the Telnet connection is active. Most hosts respond `yes`.

b Sends a Telnet protocol IAC Interrupt Process command to the remote host. For some remote hosts, this stops a process running on the remote host but does not terminate the Telnet connection.

c Closes the current Telnet connection gracefully.

Enter key Switches from the current connection to the next open connection in the list. As many as 10 connections can be open at a time. When **tn** reaches the end of the list, it returns to the first connection. If you have only one **tn** connection open, pressing the Enter key at the escape command prompt returns you to that connection.

F Starts or stops an FTP server on your PC, so you can transfer files between your local system and the remote host. Disabling the server prevents new connections, but does not terminate existing connections. To prevent existing connections from writing or deleting files, use the **W** command to enable write protection.

By default, the FTP server is off when you begin a Telnet session. You can change the default to `on` or `never` with the `ftpsrv=` entry in the `[pctcp tn]` section of your PCTCP.INI file. If the default is `never`, the **F** escape command does not enable the FTP server.

I Displays the local host's IP address on the status line.

i Sends the contents of a PC file as input to the remote host command line. You are prompted for the name of the file, whose contents are then sent to the remote host exactly as if you typed and entered them there. If the remote host is a UNIX system, you can enter the **cat** command on the remote host to redirect the input to a file. For example, entering the command **cat > test** followed by the **i** escape command transfers the contents of the file you specify to a file named TEST on the remote system. To terminate the input redirection on the remote system, press Ctrl+D.

Note: The IBM 3270 terminal emulator does not accept this command.

l Enables local echo mode. The remote host receives your keystrokes, but does not send them back to your PC. DOS displays the keystrokes on your PC screen.

Note: IBM mainframes do not accept the **l** escape command, nor do some other hosts.

o Records your keystrokes and the resulting remote system output in a file on your PC. The remote login program prompts you for a filename in which to store the data. If the file already exists, the new data overwrites the existing contents of the file. You also can specify a device such as a printer as the output file. Press the **o** escape command again to close an open output file.

p Specifies the DOS code page to use for remote login sessions. The code page in use can affect how PC/TCP or OnNet displays special and multilingual characters on your screen. The PC/TCP and OnNet terminal emulators support DOS code pages 437 (IBM PC English) and 850 (IBM PC multilingual).

After you enter this command, a prompt in the following format appears:

```
Select DOS codepage (press Enter to remain at nnn):
```

where *nnn* indicates the active code page. Enter a new code page number, or press Enter to keep the current code page number.

Note: To change the code page, use the DOS **chcp** command. Use the **p** escape command only for problem solving.

Q Ends all existing connections by resetting them instead of closing them gracefully.Use this option only when you cannot exit from the session normally by logging out or by using the **c** escape command.

q Ends the current remote login session by resetting the connection instead of closing it gracefully. Use this option only when you cannot exit from the session normally by logging out or by using the **c** escape command.

r Enables remote echo mode. The remote host echoes keystrokes back to the local host over the Telnet connection. This is the default mode. Use the **Ctrl+t** escape command to see whether local or remote echo mode is enabled.

S Enables or disables the passing of all keystrokes to DOS in addition to their

normal transmission to the remote host. Use this command to prevent inappropriate activation of a DOS screen-saver program in a remote session.

s Indicates that you want the terminal emulator to pass your next keystroke to DOS only (normally, the terminal emulator sends all keystrokes to the remote host). This command lets you enable a pop-up program during a remote login session. If the keystroke you type after giving the **s** command is not recognized as a hotkey, the command has no effect.

Note: Use this command (and not **S)** with the DOS 5.0 Task Swapper. Press **F10+s Ctrl+Esc** to get back into the Task Swapper from the Telnet session.

t Sends a Telnet break signal to the remote host.

U Turns on the display of the status line at the bottom of the terminal screen (this is the default). If you request extended screen height and your PC's card and monitor can display only 43 lines, the status line is automatically turned off. If your terminal type is IBM PC, this escape command is disabled.

In addition to the time and hostname, these other indicators may appear when the status line is on:

Indicator	Condition
`F`	An FTP server on your PC is enabled and accepting connections.
`i`	An input file on your PC is open.
`o`	An output file on your PC is open.
`^`	The insert key is on. (Applies to IBM 3270 terminal types only.)
`Xsys`	The keyboard is locked while the remote host processes an attention identifier key. (Applies to IBM 3270 terminal types only.)

u Turns off the display of the status line at the bottom of the terminal screen. Some escape commands display messages regardless of whether the status line is turned on or off. You also can turn the status line on or off with the `status=` entry in the `[pctcp tn]` section of your PCTCP.INI file.

W Enables or disables write protection for the FTP server (the default state 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 server has never been enabled, this command has no effect.
If the FTP server was previously running and is now disabled, enabling write

protection affects the remaining connected users.

z Sends a Telnet protocol IAC Abort Output command to the remote host. This command lets the current process finish, but does not send you its output.

Ctrl+b Turns binary (8-bit) mode on or off for a DEC VT terminal emulator. The default setting for binary mode is off. Use the **Ctrl+t** escape command to determine if the remote and local hosts are sending data in binary (8-bit) mode. You also can enable binary mode by changing terminal types with the **m** escape command.

Note: Not all hosts support or work correctly in binary mode.

Ctrl+d Displays kernel debugging information similar to the output of the **ping** command.

Ctrl+e Turns encryption off and on during a **tn** session. Use the **Ctrl+t** escape command to determine if encryption is enabled or disabled.

Ctrl+h Displays a help message listing the control character escape commands.

Ctrl+k Displays the settings of some of the variables in the PCTCP.INI file. The command output also indicates configuration file entries that are not found, are in error, or are being used.

Ctrl+l Redraws the screen for the current connection.

Ctrl+n Displays network status information, including kernel TCP, IP, UDP, and ICMP statistics. The output is similar to that of the **inet stats** command.

Ctrl+s Lists current connections, and shows the status of the active connection and the FTP server.

Ctrl+t Displays information about the **tn** session and the current connection, and shows the status of the FTP server. This command also indicates whether the emulator is passing keystrokes to DOS, and if input or output file processing is active.

DEC VT and IBM PC Escape Commands

These escape commands can be used for **tn** connections using DEC VT or IBM PC terminal emulators.The escape key is Alt+F10 or F10. (You can set line wrap and backspace key behavior (controlled by the **B**, **D**, **d**, and **w** escape commands) in the PCTCP.INI file.

B Causes the Backspace (←) key to send the ASCII backspace character and the Ctrl+Backspace (Ctrl+←) key to send the ASCII delete character. The **D** escape command reverses this behavior.

D Causes the Backspace (←) key to send the ASCII delete character and the Ctrl+Backspace (Ctrl+←) key to send the ASCII backspace character. This behavior is the default; the **B** escape command reverses it.

d Turns off line wrap. If a line is too long for the display, extra characters overwrite existing characters on the line. (This option is the default.) To reverse this behavior, use the **w** escape command.

E Sends a line of characters to the remote host when you press the Enter key. In this mode, you can erase a character or line in a local buffer before sending the line to the remote host. When **tn** is unable to negotiate a 3270 terminal type with a remote IBM mainframe and enters line mode, this escape command lets you more closely emulate IBM terminal behavior. This **E** command functions only in local echo mode, and resets to send each character if you change back to remote echo mode with the **r** escape command.

e Sends each character to the remote host as you type it. This is the default.

m Lets you change from one DEC VT terminal emulator mode to another. This command displays a message showing you the five modes available, and identifies each mode by a number 0 through 4. Specify the mode by typing the corresponding number. This option is not valid with the IBM PC terminal emulator.

Note: Mode 1 (vt220 mode, 8-bit controls) is binary mode. Not all hosts support emulation in binary mode.

N Causes the Enter key to send the Telnet protocol CR LF sequence. This sends a return and a line-feed (new-line) character. This is the default.

R Causes the Enter key to send the Telnet protocol CR NUL sequence. This sends a return character without sending a line-feed (new-line) character.

w Turns on line wrap. If a line is too long for the display, the extra characters appear on the next line. To reverse this behavior, use the **d** escape command.

IBM 3270 Escape Commands

These escape commands are for **tn** connections using IBM 3270 terminal emulation.

M Enables or disables emulation of your mouse cursor or light pen as a 3270 selector pen on the remote host. When the mouse cursor is enabled and you select a selector pen field, **tn** emulates a selector pen click on the remote host. You must install a mouse driver on your PC before you can use the **M** escape command.

Y Turns on Yale null processing. The terminal emulator replaces the null characters in a modified 3270 field with blanks. This is the default setting. If a `yale=` entry exists in the `[pctcp 3270]` section of the PCTCP.INI file, this command overrides it.

y Turns off Yale null processing. The terminal emulator preserves null characters as null characters in a 3270 field. If a `yale=` entry exists in the `[pctcp 3270]` section of the PCTCP.INI file, this command overrides it.

3270 Emulator Compatibility

These IBM and compatible mainframe host implementations have been tested with FTP's 3270 terminal emulators:

- IBM VM Interface Program for TCP/IP, 5798-FAL
- University of Wisconsin WISCNET (for VM)

- Fibronics (Spartacus) KNET TCP/VM and KNET TCP/MVS
- Network Solutions UCLA ACP (for MVS)

3270 Emulator Partition Support

When a user turns on a real IBM 3270 terminal, the device creates a single logical area, called a "partition," for displaying characters on your screen. This default partition is known as the *"*implicit partition." An application can divide the screen into additional partitions by sending a CREATE or ACTIVATE PARTITION request.

However, the 3270 emulator supports use of the implicit partition only. If an application you are running on the remote IBM host tries to create and use additional partitions, you may receive error messages. A request for any of the following functions results in an error message on the status line:

- Create, activate, or destroy new partitions.
- Modify the presentation space or characteristics of the implicit partition (or any others).
- Load Programmed Symbols using a Write Structured Field command.

In addition, if the 3270 emulator receives a READ PARTITION QUERY request, its reply includes information about the following attributes only: HIGHLIGHT, COLOR, USABLE AREA, IMPLICIT PARTITION, SUMMARY, and REPLY MODE. Absence of information about certain attributes, such as PARTITIONS, FIELD VALIDATION, and CHARACTER SETS, indicates that the emulator does not support those attributes.

Unsupported VT Features

The VT emulator does not support enabling of the following VT terminal features:

Double-height characters	Double-width characters
Programmable LEDs	Soft Scroll (DECSCLM)
Character attributes (DECSCA)	Screen mode (DECSCM)
Hardware control function keys F1, F3–F5	

Examples

To open a Telnet connection to the host xyz.com and allow **tn** to negotiate the terminal type, enter

```
C:\> tn xyz.com
```

To request emulation of a DEC VT100 terminal with a 43- or 50-line screen on the host xyz.com, enter

```
C:\> tn -h -x vt100 xyz.com
```

To request negotiation of an IBM 3278-5-E terminal emulator with wide screen display capabilities on the host mainframe.com, and to use port 158 for the connection, enter

```
C:\> tn -w -t 3278 mainframe.com 158
```

If the IBM 3278-5-E terminal type is unavailable, **tn** offers the 3278-5 without extended attributes.

To request negotiation of an IBM PC terminal emulator, enter

```
C:\> tn -x ibmpc xyz.com
```

If the IBM PC terminal type is unavailable, **tn** offers IBM 3270 Model 2-E and IBM 3270 Model 2.

See Also

rloginvt, tnglass

RFC 1091

tn

tnglass

Usage

tnglass *host* [*port*] [**-b**] [**-c** *channel*] [**-l**] [**-i**] [**-e** *emulator command_list*]
tnglass [**-?** | **-version**]

Description

The **tnglass** command lets you log in to a remote host using the TCP/IP Telnet protocol. It implements the Telnet standard Network Virtual Terminal, a set of basic common terminal characteristics, as the interface to the remote system. Because **tnglass** does not emulate characteristics of any specific terminal and does no interpretation of data, the resulting terminal type is what is known as a "glass," or dumb terminal. You can use an alternative terminal emulator with **tnglass** by supplying its name on the command line.

To end a **tnglass** session, log out of the remote host (for example, by pressing Ctrl+D or typing `exit)`. If you cannot log out normally, use the **c** or **q** escape command (see the "Escape Commands" section for details). The anonymous FTP server ftp.ftp.com has information about glass terminal emulation and the IBM PC BIOS Interrupt 14 interface.

Command Line Options

-b Causes the Enter key to send the Telnet protocol CR (carriage return) sequence only.

-c *channel* Specifies an asynchronous communication channel (COM port) on your PC to use for the **tnglass** connection. The variable *channel* identifies the communication port. The standard PC serial ports are COM1 and COM2. Enter a `0` to specify COM1 or a `1` to specify COM2. This option is useful if your PC has direct connections to one or more of its asynchronous communications ports.

-e *emulator command_list*
Enables terminal emulation through any external emulator that supports the IBM PC BIOS Interrupt 14 interface. The *emulator* variable specifies the terminal emulator path and filename. The *command_list* variable includes any arguments required to run the emulator.

host Specifies the name or Internet address of the remote host.

port Specifies the number of a port on the remote host machine. This option can be useful for solving problems with connecting to remote servers.

-i Specifies to (1) keep a Telnet session open until the external emulator is loaded and (2) send an Int 14 **init** command. This command line option does not work if the commercial terminal emulator you are using does not support the Int 14 **init** command (if you are unsure, ask your system administrator). You must specify this with the **-e** command line option.

-l Causes the Enter key to send the Telnet protocol CR NUL sequence. This sends a return character without sending a line-feed (new-line) character.

-? Displays and explains the usage line of the command.

-version Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Escape Commands

To invoke an escape command in a **tnglass** session, press the escape key (Ctrl+6); then enter the escape command at the `Command:` prompt. If you are using a commercial terminal emulator with **tnglass**, you cannot use the escape key.

? Displays a help message listing the escape commands.

! Invokes a nested DOS command interpreter, but does not close the Telnet connection. To return to the remote host, type **`exit`** at the DOS prompt.

a Sends a Telnet protocol IAC Are-You-There command to the remote host to determine if the Telnet connection is active. Most hosts respond `Yes`.

b Sends a Telnet protocol IAC Interrupt Process command to the remote host. For some remote hosts, this stops a process running on the remote host but does not terminate the Telnet connection.

c Closes the current Telnet connection gracefully.

i Sends the contents of a PC file as input to the remote host command line. You are prompted for the name of the file, whose contents are then sent to the remote host exactly as if you typed and entered them there. If the remote host is a UNIX system, you can enter the **cat** command on the remote host to redirect the input to a file. For example, entering the command **cat > test** followed by the **i** escape command transfers the contents of the file you specify to a file named TEST on the remote system. To terminate the input redirection on the remote system, press Ctrl+D.

l Enables local echo mode. The remote host does not echo keystrokes back to the local host over the Telnet connection. DOS is responsible for displaying the keystrokes on your screen.

o Records your keystrokes and the resulting remote system output in a file on your PC. The remote login program prompts you for a filename in which to store the data. If the file already exists, the new data overwrites the existing contents of the file. You also can specify a device such as a printer as the output file. Press the **o** escape command again to close an open output file.

q Ends the current remote login session by resetting the connection instead of closing it gracefully. Use this option only when you cannot exit from the session normally by logging out or by using the **c** escape command.

r Enables remote echo mode. The remote host echoes keystrokes back to the local host over the Telnet connection. This is the default.

t Sends a Telnet break signal to the remote host.

Example

To connect to host secondvax.xyz.com using an EM4105 terminal emulator from the \TERM directory, enter

```
C:\> tnglass secondvax.xyz.com -e \term\em4105
```

See Also

tn, rlogingl

tnglass

unix2dos

Usage

unix2dos [*source* [*destination*]]
unix2dos [**-?** | **-version**]

Description

The **unix2dos** command converts ASCII text files created on a UNIX system to a format that displays properly on an MS-DOS system. UNIX files contain end-of-line characters that are not interpreted as such on an MS-DOS system. The **unix2dos** command replaces UNIX new-line characters in the specified *source* file with MS-DOS end of line characters and stores the result in the specified *destination* file. The *source* and *destination* filenames must be different. Names mapped by the InterDrive client are valid *source* names.

Command Line Options

destination	Specifies a DOS filename. If you do not specify a destination, the command displays the formatted output on your screen.
source	Specifies a UNIX filename. If you do not specify a source, the command takes input from your keyboard.
-?	Displays and explains the usage line of the command.
-version	Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Example

To convert the UNIX file march.uni to the DOS file MARCH.DOS, enter

```
C:\> unix2dos march.uni march.dos
```

See Also

dos2unix, idrive

unix2dos

vmail

Usage

vmail [**-2**] [**-h**] [**-c***client_section*] [**-o**]
vmail [**-?** |**-version**]

Description

The **vmail** command runs a mail reading program that lets you read messages retrieved by the Pcmail, POP2, POP3, or NNTP client programs. The vmail program displays the mailboxes, bulletin boards, descriptors, and messages from only one of these programs at a time; it automatically displays them for your default mail client.

The vmail program can display as many as four screen layers: the Mailbox, Descriptor, Message, and Bulletin Board screens. The vmail program prompt appears at the bottom of each screen.

Command Line Options

-2 Specifies 25-line (high resolution) mode in screen output (see also **-h**).

-c *client_section* Specifies which client section of the PCTCP.INI file that the vmail program should use.

-h Specifies high resolution (25-line) mode. The number of lines displayed on the screen is set automatically, to provide the best possible resolution (see also **-2**).

-o Directs the vmail program to omit scanning the repository for off-line messages. If the vmail program does not scan for each off-line message, its message access rate significantly improves.

-? Displays and explains the usage line of the command.

-version Displays the version and patch level of the command. Refer to this information if you call Technical Support.

vmail Commands

The vmail program commands operate differently, depending on which mail client you use. Almost all of the commands listed in this section work for the Pcmail client, but some commands may not work with the POP2, POP3, or NNTP clients. When this is the case, the command you enter at the vmail program prompt generates a tone (beep) on your machine, indicating that the command is invalid. Any of the vmail program's commands that performs a change on a mailbox or message, such as sending a message, copying a message to a different mailbox, or deleting a mailbox, will not take effect until you exit from the vmail program and reissue the **pcmail**, **pop2**, **pop3**, or **nntp** command at the DOS prompt.

You can type the following commands at the vmail program prompt.

Note: Commands in the following list that are followed by an asterisk (*) can be used with numeric prefixes. The prefixes let you handle your mail messages faster.

+ |**–**, **0**… **9** Increase the number of times that a command in this list marked by an asterisk (*) performs its function. To handle your mail messages faster, at the vmail

program prompt you type a prefix, then a number, then the command you want to use. For example, if you type a plus sign (+) before the number 14, then press **d**, the command deletes the 14 messages that follow the current message. If you type a hyphen (–) before the 14, it deletes 14 messages that precede the current message.

←, < Goes to the previous message, descriptor, or mailbox when you press the left arrow key or the left angle bracket key.

→, > Goes to the next message, descriptor, or mailbox when you press the right arrow key or the right angle bracket key.

A Adds a new mailbox or address. When you press **A**, the vmail program displays the name of the current (highlighted) mailbox. (To add only an address to that mailbox, press Enter and the vmail program prompts you for the address). To create a new mailbox, type the new mailbox name and press Enter; the vmail program then prompts you for an address. At this point, you can press **?** or press **F1**, and the vmail program displays a list of existing addresses for that mailbox. Type the address and press Enter. (If you are using the POP or NNTP protocols, the vmail program does not prompt you for an address.)

a Displays a list of your aliases or adds an alias to the list. When you add an alias, it is appended to the aliases file specified in the `[pctcp vmail]` section of your PCTCP.INI file. (Edit the aliases file to delete or change aliases that you have added to the file.) To display a list of aliases, press **F1** or press **?**.

B Queues a request that your mail client retrieve the local list of bulletin boards (or network news groups) from the server. This command gets a new list of available bulletin boards or network news groups to which you can subscribe. The **B** command works at the Mailbox and Bulletin Board screens. (Pcmail and NNTP only)

b Updates the network news groups list. (NNTP only)

backspace key* Pages up through the contents of a message or a list of bulletin boards, depending on which screen is displayed.

c Copies a message. The vmail program prompts you for the name of the mailbox to which you want the message copied. Type the mailbox name and press Enter.

D Deletes the address of the current mailbox after prompting you for the address and corresponding mailbox name. To display the address of the current mailbox, press **?** or **F1** at the prompt.

del, **d*** Marks the current message or mailbox for deletion, depending on which screen is displayed. When you delete a message, it is not removed from the system until you issue the **e** (expunge) command and rerun the client; you can still undelete a deletion, using the **u** command. When you delete a mailbox, you also delete the corresponding address and all messages contained in the mailbox. However, the vmail program prompts for confirmation before deleting the information.

E Expunges (removes) the deleted messages from all mailboxes. See the **e** command for a description of expunging.

e Expunges (removes) the deleted messages from the mailbox. This command permanently removes deleted messages from the selected mailbox after you issue the **pcmail**, **pop2**, or **pop3** command. If you are using the NNTP client, note that the deleted messages are expunged automatically. If you use the pcmail program, deleted messages cannot be undeleted after you use the **e** command. If you use the pop2 or pop3 programs, you can still undelete deleted messages after you have expunged them, provided that you have not yet run your client.

End key Moves the cursor to the end of the message, the last descriptor, the last mailbox, or the last bulletin board, depending on which screen is displayed.

Enter key Displays the current message; or at the Mailbox screen, displays the message descriptors.

Esc key Backs up or goes to the previous vmail program screen level; halts further action of a command; and stops retrieving messages from a mailbox.

f Forwards a message. Select the message you want to forward (by selecting the message descriptor or by going into the message itself), then press **f**. The vmail program prepares a blank header field at the top of the screen with the message below it, and invokes the text editor specified for the `editor=` parameter in the `[pctcp vmail]` section of your PCTCP.INI file. Fill in the `To:` field with the address of the person to whom you are forwarding the mail. A signature file is not appended to the message.

F1 key, **?** key Displays the help screen at any screen. The **F1** and **?** commands also display existing addresses of mailboxes.

F2 key Synonymous with **Ctrl+L**.

G Removes old messages from the program's memory. If you receive an error message such as `Not enough memory`, this command may free the memory you need.

g Gets off-line messages. When there is not enough disk space on your PC, the pcmail program retrieves the header of the message, not the text. The message is flagged with an `O`, for off-line. The **g** command is used to bring the message back online.

h When used at the Message screen, **h** displays the Descriptor screen. The Descriptor screen displays the number of messages, the message status or flags, the sender, the message subject, and size of the message in bytes.

When executed at the Descriptor screen, **h** displays selected descriptors. The selected descriptors contain specified text in the `To:`, `From:`, and `Subject:` fields.

Home key, **.** (dot) Moves the cursor to the top of the message, the first descriptor, the first mailbox, or the first bulletin board, depending on which screen is displayed.

j	Joins or subscribes to a bulletin board or network news group. The vmail program prompts you for the name of a bulletin board or network news group to join. This command works at the Mailbox and Bulletin Board screens.
k	Cancels (kills) your subscription to a bulletin board or network news group. The vmail program prompts you for the name of the bulletin board or network news group. This command works at the Mailbox and Bulletin Board screens.
L	Removes the local copy of the current message from your PC. This command removes the message from your PC (without deleting it) by placing the message off-line. The **L** command is useful for preserving disk space for new messages. To put the message back on your PC, use the **g** command, which can be issued only if you are using the pcmail or nntp programs.
l	Lists all available bulletin boards or network news groups. Bulletin boards or network news groups that you previously joined appear highlighted. Use the **B** command to get a new list, and **b** (for NNTP client program only) to update the list.
M*	Marks the current message as read without your actually having read it.
m	Invokes the text editor specified in your PCTCP.INI file, and displays a blank header field. You must leave a blank line between the header that the vmail program provides and the text you type. After you fill in the fields and type the message, use the editor commands you normally use to save and exit from the file. When the vmail program prompts you, verify that you want to send the message. A signature file, if present, is appended to the message.
N	Used to post a new message to a network news group. This command is specific to nntp and is similar to the **m** command. The difference is that the `To:` field in the header is replaced by the `Newsgroups:` field.
P	Sends the current message to the printer after you run your client. For the pcmail program, the name of the printer is set with the `printer=` entry in the `[pctcp vmail]` section of your PCTCP.INI file. The pop2, pop3, and nntp programs use the lpr program to print files.
p,	Depending on which screen is displayed, goes to the previous undeleted message or previous mailbox containing new messages.
n, ↓	Depending on which screen is displayed, proceeds to the next undeleted message or next mailbox containing new messages in the Descriptor and Message screens.
PgDn key	Moves one screen down through the message, descriptor, mailbox, or bulletin board list, depending on which screen is displayed.
PgUp key	Moves one screen up through the message, descriptor, mailbox, or bulletin board list, depending on which screen is displayed.
Q	Exits from a bulletin board without updating the status of the last message you read.

q	Exits from the current screen. When issued at the Mailbox screen, **q** causes the vmail program to exit to the operating system.
R	Sends a reply only to the person who sent the original message. Issuing this command invokes the text editor specified in your PCTCP.INI file. The program appends a signature file, if present, to the message.
r	Sends a reply to everyone who received the original message, not just to the individual who wrote the original message.
S	Sets the password only for the pcmail program on the next synchronization between the Pcmail client and server. The client program prompts for a new password the next time you run the program, and requires that you type the new password again for verification. If you have specified a password as the setting for the `password=` parameter of the `[pctcp pcmail]` section of your PCTCP.INI file, you must change the parameter's setting after you have changed your password.
s	Saves the current message to a text file that you specify and stores it in your current directory, unless you specify the full pathname of another directory. The vmail program prompts you for the name of the file. If you have already specified a filename the last time you used the **s** command, the vmail program appends the message to that file.
spacebar key	Pages down through the message on the Message screen; shows the selected message on the Descriptor screen; shows the message descriptors of the mailbox selected at the Mailbox screen; and pages down through the bulletin board list at the Bulletin Board screen.
t	Displays either a short or a long version of the header at the Message screen. If you forward or reply to a message, the header appears according to the last operation of the **t** command. Press **t** again to change the header length.
u*	Restores a deleted message. Use this command if you have deleted a message but want to change the message's delete status. When using the pcmail program, you cannot undelete a message once you have expunged a mailbox. When using the nntp, pop2, and pop3 programs, you can undelete a message after you have expunged a mailbox, provided you have not yet run the client.
Ctrl+D	Scrolls down one-half screen at the Message screen.
Ctrl+L	Redisplays the screen. Synonymous with **F2**.
Ctrl+N*	Moves to the next line at the Message screen.
Ctrl+P*	Moves to the previous line at the Message screen.
Ctrl+r	Searches backward through the descriptor list for specified text in the `Subject:`, `To:`, or `From:` fields. At the Bulletin Board screen, **Ctrl+r** searches for the name of a bulletin board in the list. Enter the text that you want to locate at the prompt. To search for the next occurrence of the specified text, press Ctrl+r again. You can use the **Ctrl+r** command at the Message, Descriptor, and Bulletin Board

screens.

Ctrl+s Searches forward through the descriptor list for specified text in the `Subject:`, `To:`, or `From:` fields. At the Bulletin Board screen, **Ctrl+s** searches for the name of a bulletin board. Enter the text that you want to locate at the prompt. To search for the next occurrence of the specified text, press Ctrl+s again. You can use the **Ctrl+s** command at the Message, Descriptor, and Bulletin Board screens.

Ctrl+U Scrolls up one-half screen at the Message screen.

Message Flags

At the vmail program Descriptor screen, flags identify the status of a message. For example, the letter `U` next to a message is a flag that means that the user has not yet read the message. The flags appear in two separate columns to the left of the messages. If you issue more than one flag that occupies the same column, you may not see the flag for the action that you just issued. For example, if a message has been replied to, then saved to a file, only the `R` flag appears. Note that you can select a message's descriptor, and look at the status line for the message at the Message screen to see what flag is in effect. Eight flags are used.

The flags of the first column appear next to each message in the following order.

First Column Message Flag	Meaning
`D`	Deleted. The `D` flag leaves the state of the message unchanged. When you run the pcmail program, issuing the **e** command permanently removes a deleted message. When you use the pop2 or pop3 programs, the message is permanently removed.
`G`	Queued for retrieval. The next time you run the client, the client retrieves the off-line message from the server.
`O`	Off-line. The body of the message cannot be displayed because there was not enough disk space when you last ran the mail or news client. Use the **g** command to retrieve this message, or wait for the message to appear online the next time you run the client.

The flags of the second column appear next to messages in the following order.

Second Column Message Flag	Meaning
`R`	A reply was sent to this message.

F	This message has been forwarded.
S	This message has been saved to a file.
C	This message has been copied to another mailbox.
U	This message is unread.

There can be more than one flag next to a given message. For example, the flag OU means that the message is both off-line and unread. A blank beside the message header means that you have read the message and have issued no other commands (such as **r**, **c**, **d**, **s** and so on). When issued, each flag is defined for you on the bottom right-hand corner of the screen.

Examples

To access your mailboxes, enter

```
C:\> vmail

Parsing Configuration file
Loading mboxes
Loading aliases
```

After the vmail program loads the mailboxes and the aliases, it displays the Mailbox screen.

To use a client program that is not your default client, enter

```
C:\> vmail -c pop3
```

The vmail program uses the [pctcp pop3] section of the PCTCP.INI file.

If another user whose user ID is chris shares your PC, you can enter

```
C:\> vmail -c chris
```

to specify that the vmail program use the configuration specified in the [pctcp chris] section of the PCTCP.INI file.

See Also

nntp, pcmail, pop2, pop3

vmail

vxdinit

Usage

vxdinit [-u] [(+ | -)**i**] [(+ | -)**n**] [(+ | -)**t**]
vxdinit [**-?** | **-version**]

Description

The **vxdinit** command instructs Windows to load the VxD kernel and optionally other VxDs (such as, NetBIOS and the InterDrive NFS client). The command line options override settings in the `[pctcp vxdinit]` configuration file section.

Note: The VXDINIT.EXE TSR loads into upper memory by default. To load it into conventional memory you can set `loadhigh= no` in the `[pctcp vxdinit]` section of the PCTCP.INI file.

You can use **vxdinit -u** to unload the VxD initialization TSR. (Use **inet unload** to unload the kernel.)

Note: If you use the VxD kernel, you must also use the VxD versions of other OnNet applications (such as NetBIOS and InterDrive).

You can use the Statistics application to determine which type of kernel is running.

The OnNet VxD applications use the same PCTCP.INI file sections and options as the corresponding TSR versions. This table lists the configuration file sections for each VxD.

This VxD	Uses this section first	Then this section
kernel	`[pctcp kernel-vxd]`	`[pctcp kernel]`
NFS client (InterDrive)	`[pctcp idrive-vxd]`	`[pctcp idrive]`
NetBIOS	`[pctcp netbios-vxd]`	`[pctcp netbios]`

Note: If you are in an environment where you alternate between VxD and TSR kernels, OnNet looks in a special application configuration file section for defaults that apply only to the VxD. (These configuration file sections have a `-vxd` suffix.)

Command Line Options

+i Instructs Windows to load the InterDrive NFS Client VxD. This option overrides the `vidrive=` setting in the `[pctcp vxdinit]` PCTCP.INI configuration file section.

-i Instructs Windows *not* to load the InterDrive VxD. This option overrides the `vidrive=` setting in the `[pctcp vxdinit]` PCTCP.INI configuration file section. This is the default.

+n Instructs Windows to load the NetBIOS VxD. This option overrides the `vnebp=` setting in the `[pctcp vxdinit]` PCTCP.INI configuration file section.

-n	Instructs Windows *not* to load the NetBIOS VxD. This option overrides the `vnebp=` setting in the `[pctcp vxdinit]` PCTCP.INI configuration file section. This is the default.
+t	Displays error messages while configuring.
-t	Suppresses the display of error messages while configuring. This is the default.
-u	Unloads the VxD loader TSR (approximately 2.5K). You can also use the **inet unload** command.
-?	Displays and explains the usage line of the command.
-version	Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Example

This example loads the kernel and InterDrive NFS client VxDs. It does *not* load the NetBIOS VxD. This command overrides `vidrive=` and `vnbep=` configuration parameter settings (respectively) in the `[pctcp vxdinit]` section of the PCTCP.INI file.

```
C:\>vxdinit +i -n
```

See Also

inet, kernel

vxdinit

whois

Usage

whois [*user*] *@host*
whois [**-?** | **-version**]

Description

The **whois** command either lists who is currently logged in to another host or obtains directory information about a registered user of another network host.

The **whois** command sends an inquiry and displays the response, if any. The remote host determines the form and contents of the response. If the remote host does not respond within approximately 20 seconds, **whois** will stop its inquiry. Note that some hosts do not respond to **whois** requests. The host may ignore the request (and display the message `. . . host not responding`) or reject the request (and display the message `Closed: foreign reset`).

The TCP/IP **whois** protocol is an option of the Finger protocol that requests additional information. The 4.2 BSD Finger server does not send its responses in NETASCII; thus, its response may be poorly formatted. PC/TCP and OnNet accept server output in both formats.

Command Line Options

host	Specifies the hostname or IP address of the remote host. You must prefix the hostname with the @ character.
user	Specifies the username on the target host. The username is optional.
-?	Displays and explains the usage line of the command.
-version	Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Example

```
C:\> whois frg@vex

[vex.xyz.com] Login name: FRG            In real life: Fred Garvin
Directory: /u/FRG                        Shell: /bin/csh
On since May 31 13:07:53 on ttyp0 from Blue.xyz.com
1 hour 9 minutes Idle Time
Project: To document accounting software.
Plan: Document all accounting tasks the user can perform with the software.
```

See Also

finger, nicname

whois

ypcat

Usage

ypcat [**-d** ***domain***] [**-ktx**] *mname*

ypcat [**-?** | **-version**]

Description

The **ypcat** command prints out values in a Network Information Service (NIS) map specified by *mname*, which may be either a map name or a map nickname. Because the command uses NIS, you do not need to specify an NIS server.

Command Line Options

-d*domain*	Specifies a domain other than the default domain.
-k	Displays the keys for those maps in which the values are null or the key is not part of the value.
-t	Prevents translation of *mname* to map name. The exact and complete map name must be used.
-x	Displays the map nickname and indicates the correct map name associated with each nickname that the command knows about.
-?	Displays and explains the usage line of the command.
-version	Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Note: This command is only available with the CD-ROM version of OnNet for Windows.

See Also

ypmatch

ypcat

ypmatch

Usage

ypmatch [**-d** ***domain***| **-ktx**] *key...mname*
ypmatch [**-?** | **-version**]

Description

The **ypmatch** command prints out the values associated with one or more keys from the Network Information Service (NIS) map specified by *mname*, which may be either a map name or a map nickname. Multiple keys may be specified; the same map is searched for all specified keys.

Command Line Options

-d*domain*	Specifies a domain other than the default domain.
-k	Before printing the value of a key, the commands prints the key, followed by a colon (:). This is useful if you are specifying multiple keys and the output could be confusing.
t	Prevents translation of nickname to map name (*mname*). The exact and complete map name must be used.
-x	Displays the map nickname table and indicates the correct map name associated with each nickname that the command knows about.
key . . . mname	Assigns a map name (*mname*) to the specified key.
-version	Displays the version and patch level of the command. Refer to this information if you call Technical Support.

Note: This command is only available with the CD-ROM version of OnNet for Windows.

See Also

ypcat

ypmatch