

**Contents**

Sometimes DOS is the Best Tool.....	1	<i>Examples</i> .....	6
Using DOS Commands.....	1	DIR, to List Files.....	7
<i>Command Line Statements</i> .....	1	<i>Syntax</i> .....	7
<i>Batch (BAT) Files</i> .....	2	<i>Examples</i> .....	8
<i>Switches</i> .....	2	TREE, to Display Folder Structure .....	8
DOS Console Window Operation .....	3	DEL, to Delete File(s).....	9
<i>Console System Menu</i> .....	3	REN, to Rename File or Directory .....	9
<i>Console Window Keys</i> .....	3	PING, to Verify Network Connection.....	10
Helpful DOS Commands.....	3	TRACERT, to Trace Packet Route	
DOS File Commands.....	3	Over Network.....	11
CD, to Change Current Directory .....	4	MEM, to View Memory Amount.....	11
<i>Syntax</i> .....	4	FORMAT, to Clear Hard Drive or	
<i>Examples</i> .....	4	Data Storage Device .....	12
MD, to Create a Directory .....	5	NETSTAT, to Monitor Use of Ports.....	12
<i>Syntax</i> .....	5	<i>Example 1</i> .....	13
<i>Examples</i> .....	5	<i>Example 2</i> .....	15
RM or RMDIR, to Delete Directories .....	5	TASKLIST, to List Running Programs.....	16
<i>Syntax</i> .....	5	Port Usage Advice from Google.....	17
XCOPY, to Copy Files and Directories .....	5		
<i>Syntax</i> .....	5		

**Sometimes DOS is the Best Tool**

Sometimes DOS commands are the best, and often only, way to do something. Consider using them for file backups and when Windows Explorer has indigestion.

**Using DOS Commands**

DOS commands may be run as command line statements or as batch files.

DOS commands are case-insensitive.

DOS commands are documented on various websites and in the Windows help file (see “Command Reference Main Page”).

**Command Line Statements**

To run DOS commands:

1. Open the DOS command console window (aka command prompt):
  - (a) Use menu Start, Run, enter “cmd.exe”
  - (b) Use menu Start, Programs, Command Prompt
2. Type in the command.
3. Press [Enter].

## DOS Tools

The console window is where the DOS command interpreter can be run on demand. The command interpreter is CMD.EXE (for Windows NT, 2000, and XP) and COMMAND.COM (for older versions and backwards compatibility). CMD.EXE is in c:\windows\system32.

The console window opens at the default directory. For Windows XP this is c:\Documents and Settings\Owner. The current directory is always displayed immediately to the left of the ">" character. You type commands to the right of the ">" character. A new prompt appears when the current command is completed.

### Batch (BAT) Files

Batch files, named x.BAT, are collections of DOS commands and special batch file commands. The batch file approach makes it easy to rerun the command(s) and also documents it for future use.

A batch file is run by "opening" it in Windows Explorer, i.e., double-clicking its name. What happens is that when you "open" a BAT file, the DOS command console window opens, the BAT file commands are run, and the window is closed, all of which happens in the blink of an eye.

Batch files are described in detail at [www.computerhope.com/batch.htm](http://www.computerhope.com/batch.htm)  
[homepages.cambrianc.on.ca/isp1251/lab/BATCH1.html](http://homepages.cambrianc.on.ca/isp1251/lab/BATCH1.html)

I've been having trouble running BAT files by double-clicking their names. I created a File Type for them with edit and open actions, the former using PFE and the latter using CMD.EXE. Then I was able to open the CMD window but nothing happened, so I typed the name of the BAT file and it ran! Well, apparently, because I cannot find the results. And the BAT file disappeared! It may be that you have to create the directory into which you place your backup files.

### Switches

Most commands have switches which acts as arguments or parameters.

-?	Displays a complete list of available command line options—for some DOS commands.
/?	Displays a complete list of available command line options—for some DOS commands.
/P	Pause
MORE	Displays command output one screen at a time. You will be prompted to type any key to display the next screen of text.
> filename	Redirects output to named file.
>> filename	Appends output to named file
> lpt1	Redirects output to a device, LPT1 in this case.

## DOS Console Window Operation

### Console System Menu

The system menu is accessed with the icon in the upper left corner. You can change the window size, font, and colors. You can also use it for editing (it has actions for find, copy, paste, and select all).

The System menu can be opened in three ways: (1) left-click the icon, (2) right-click anywhere in the title bar, or (3) with shortcut keys [Alt+Spacebar].

### Console Window Keys

[↑] retrieves previous command, which you can then edit before using

[F7] opens popup window with command history

## Helpful DOS Commands

HELP <command>	Display help of named command. Example: help dir
TITLE	Set title of command console window. Helpful with using more than one window at a time.
EXIT	Ends Command Prompt session and closes the console window.

## DOS File Commands

There is a command-line reference A-Z in the Windows Help file.

ATTRIB	Display and change file attributes
CD, CHDIR	Change current directory
CHKNTFS	Check the hard disk drive running NTFS for errors
COPY	Copy one or more files to a second location
DEL, DELETE, ERASE	Delete one or more files
DELTREE	Delete one or more files and/or directories; not for Windows XP
DIR	List the contents of one or more directory
DISKCOPY	Copy the contents of one disk and place them on another disk
MD, MKDIR	Create a new directory
MOVE	Move one or more files from one directory to another directory
RD, RMDIR	Remove one or more directories
REN, RENAME	Rename a file or directory
TREE	View a visual tree of the hard disk drive
UNDELETE	Undelete a file that has been deleted
XCOPY	Copy multiple files, directories, and/or drives from one location to another. Useful for backups.

## CD, to Change Current Directory

CD displays the name of or changes the current directory. If the specified drive or path does not exist, there is no change.

### Syntax

```
CHDIR [/D] [drive:][path]
CHDIR [...]
CD [/D] [drive:][path]
CD [...]
CD\
drive:
```

Switches:

/D	Change current drive in addition to changing current directory for a drive.
drive:	Display the current directory in the specified drive.
..	Change to the parent directory.
path	Change to path. Depending on the other switches, this can be a path in the current directory, the current drive, or a new drive.
none	display the current drive and directory.

If Command Extensions are enabled, CD changes as follows:

The current directory string is converted to use the same case as the on disk names. So CD C:\TEMP would actually set the current directory to C:\Temp if that is the case on disk.

CD command does not treat spaces as delimiters, so it is possible to CD into a subdirectory name that contains a space without surrounding the name with quotes. For example:

```
cd \winnt\profiles\username\programs\start menu
```

is the same as:

```
cd "\winnt\profiles\username\programs\start menu"
```

which is what you would have to type if extensions were disabled.

### Examples

cd\	Moves to the highest level, the root of the drive.
cd ..	Moves back one directory. For example, if you are within the C:\WINDOWS\COMMAND directory, this moves to C:\WINDOWS.
cd windows	Moves to the windows subdirectory of current directory.
cd\windows	First moves back to the root of the drive and then into the windows directory.

## DOS Tools

<code>cd windows\system32</code>	Moves to the windows\system32 subdirectory of the current directory.
<code>d:</code>	Changes to the d drive.

### MD, to Create a Directory

#### Syntax

```
MKDIR [drive:]path  
MD [drive:]path
```

#### Examples

```
md test
```

The above example creates the "test" directory in the directory you are currently in.

```
md f:\data
```

Create the "data" directory on the f: drive.

### RM or RMDIR, to Delete Directories

#### Syntax

Switches only apply to Windows XP and 2000. When the switches are not used, acts only on empty directories.

```
RMDIR [/S] [/Q] [drive:]path  
RD [/S] [/Q] [drive:]path
```

<code>/S</code>	Removes all directories and files in the specified directory in addition to the directory itself. Used to remove a directory tree.
<code>/Q</code>	Quiet mode, do not ask if ok to remove a directory tree with /S.

### XCOPY, to Copy Files and Directories

Copies files and directory trees. Can be used to create backup media,

#### Syntax

```
XCOPY source [destination] [/A | /M] [/D[:date]] [/P] [/S [/E]] [/W] [/C] [/I]  
[/Q] [/F] [/L] [/H] [/R] [/T] [/U] [/K] [/N]
```

In the following table the most useful switches are highlighted.

<code>source</code>	Specifies the file(s) to copy. If file or directory name has embedded spaces, enclose in double quotes.
<code>destination</code>	Specifies the location and/or name of new files. If file or directory name has embedded spaces, enclose in double quotes.
<code>/A</code>	Copies files with the archive attribute set, doesn't change the attribute.

## DOS Tools

/C	Continues copying even if errors occur.
/D:date	Copies files changed on or after the specified date. If no date is given, copies only those files whose source time is newer than the destination time. Date is in MM-DD-YY format.
/E	Copies directories and sub directories, including empty ones. Same as /S /E. May be used to modify /T.
/EXCLUDE: filename	Excludes directories and files matching the strings (one or more). The argument is the name of a text file which contains the names of directories and filenames to be excluded. See example below.
/F	Displays full source and destination file names while copying.
/H	Copies hidden and system files also.
/I	If destination does not exist and copying more than one file, assumes that destination must be a directory.
/K	Copies attributes. Normal xcopy will reset read-only attributes.
/L	Displays files that would be copied.
/M	Copies files with the archive attribute set, turns off the archive attribute.
/N	Copy using the generated short names.
/P	Prompts you before creating each destination file.
/Q	Does not display file names while copying.
/R	Overwrites read-only files.
/S	Copies directories and sub directories except empty ones.
/T	Creates directory structure, but does not copy files. Does not include empty directories or sub directories. /T /E includes empty directories and sub directories.
/U	Updates the files that already exist in destination.
/V	Verifies each new file.
/W	Prompts you to press a key before copying.
/Y	Overwrites existing files without prompting.
/-Y	Prompts you before overwriting existing files.

If the destination does not exist, XCOPY will create it.

### Examples

```
xcopy h:\*.* /s /k /v
```

The above command will copy everything located on the H drive to the drive you are currently on. Only non-empty directories are copied. File attributes are copied intact. Each file is verified.

```
xcopy "c:\Data" "c:\Backup" /c /i /k /q /s
```

I use this configuration. Copying continues even if errors occur. Assumes the destination is a directory so you will not be prompted to so indicate. File attributes are copied intact. Filenames are not displayed as they are copied. Only non-empty directories are copied.

## DOS Tools

```
xcopy "c:\data" "f:\data" /d:10-01-01 /s /c /q /k
```

The above command will copy all files and directories, even empty ones, new or changed since 10-01-01 located in the c:\data directory to the f drive, continue copying when there are errors, will not display filenames, and will copy file attributes. Do not use /e with /d.

The exclusion feature can be particularly helpful.

```
xcopy "c:\Data\Ideas" "c:\Backup" /c /i /k /q /s /exclude:backup-excludes.txt  
xcopy "c:\Data" "c:\Backup" /exclude:d:\mine\backup-excludes.txt
```

File **backup-excludes.txt** contains:

```
\solstice\  
.$$$
```

The first entry, “\solstice\”, causes that directory and all files contained within it to be excluded. The second entry, “.\$\$\$”, causes all files named \*.\$\$\$ to be excluded. You can have one or more entries in the text file. The excluded file can be located anywhere, if not in the same directory as the BAT file being run, be sure to include its complete path.

## DIR, to List Files

You can use the DIR command to create a list of files in a named directory and, optionally, its subdirectories; the list can be saved as a text file for printing and later use. The capture in a text file allows you to permanently and easily document files in a directory structure.

### Syntax

```
DIR [drive:][path][filename] [/P] [/W] [/D] [/A[:attributes]]  
  [/O[:sort-order]] [/T[:time-field]] [/S] [/B] [/L] [/N] [/X] [/C]
```

Switches may be preset in the DIRCMD environment variable. Override preset switches by prefixing any switch with - (hyphen)--for example, /-W.

Some switches apply to Windows NT but not Windows 98: D T N X C

Some switches apply to Windows 98 but not Windows NT: V 4

[drive:][path][filename]	Specifies drive, directory, and/or files to list. Enclose in double quotes when names have embedded spaces.
/4	Years as 4 digits (ignored if /V also used).
/A	Displays files with specified attributes. Attribute values: D Directories                    R Read-only files H Hidden files                    A Files ready for archiving S System files                    - Prefix meaning not
/B	Uses bare format (no heading information or summary).
/C	Displays the thousand separator in file sizes. This is the default. Use /-C to disable display of separator.
/D	Lists in wide format but files are list sorted by column.
/L	Uses lowercase, i.e., changes all names to lowercase.

## DOS Tools

/N	New long list format where filenames are on the far right.
/O	Lists by files in sorted order: sort-order values: N By name (alphabetic) S By size (smallest first) E By extension (alphabetic) D By date & time (earliest first) G Group directories first - Prefix to reverse order
/P	Pauses after each screenful of information.
/S	Displays files in specified directory and all subdirectories.
/T	Controls which time field is displayed or used for sorting: time-field values: C Creation A Last Access W Last Written
/V	Verbose mode.
/W	Uses wide list format.
/X	This displays the short names generated for non-8dot3 file names. The format is that of /N with the short name inserted before the long name. If no short name is present, blanks are displayed in its place.

### Examples

Capture contents of directory on hard drive, then print it:

```
dir /s /b c:\data\lad > c:\temp\dir.txt  
copy c:\temp\dir.txt lpt1
```

Capture contents of directory on file server:

```
dir "v:\knowledge management" > "c:\data\directory lists\KMI Library Dir.txt"
```

Capture contents of a directory and all subdirectories, use full filenames, group subdirectories at the beginning of the list, and sort files by name.

```
dir /B /S /O:G /O:N /T:W "c:\data\pge 2001\manual" > "c:\data\pge  
2001\manual\dir.txt"
```

Capture contents of directory on website:

```
dir "\\iknow-sps.schwab.com\sites\is_at_fms\The Back Room" /o:n > "h:\web back  
directory list 120506.txt"
```

[In this example, the directory is a document library on a SharePoint site.]

### TREE, to Display Folder Structure

Graphically displays the folder structure of a drive or path.

```
TREE [drive:][path] [/F] [/A]
```

## DOS Tools

/F	Display the names of the files in each folder.
/A	Use ASCII instead of extended characters.

### DEL, to Delete File(s)

Deletes one or more files in current directory.

```
DEL [/P] [/F] [/S] [/Q] [/A[[:]attributes]] names  
ERASE [/P] [/F] [/S] [/Q] [/A[[:]attributes]] names
```

names Specifies a list of one or more files or directories.

Wildcards may be used to delete multiple files, e.g.,

DEL c:\data\\*. \* will delete all the files within the named directory

DEL c:\data\\*.wpd will delete all the files with the suffix “wpd” within the named directory

If a directory is specified, all files within the directory will be deleted, e.g., DEL c:\data

/P	prompts for confirmation before deleting each file.
/F	force deleting of read-only files.
/S	delete specified files from all subdirectories.
/Q	Quiet mode, do not ask if ok to delete on global wildcard
/A	selects files to delete based on attributes: R Read-only files      S System files H Hidden files        A Files ready for archiving - Prefix meaning not

If Command Extensions are enabled DEL and ERASE change as follows: The display semantics of the /S switch are reversed in that it shows you only the files that are deleted, not the ones it could not find.

### REN, to Rename File or Directory

Sometimes Windows Explorer will not let you rename a directory. It has its excuses. Make sure the directory is not in use, then use this DOS command. It renames files or directory in their current location.

```
RENAME [drive:][path][directoryname1 | filename1] [directoryname2 | filename2]  
REN [drive:][path][directoryname1 | filename1] [directoryname2 | filename2]
```

Note that you cannot specify a new drive or path for your destination—that would be moving the file/directory.

Examples:

rename c:\data mine	Rename the directory “data” to “mine”
rename *.txt *.bak	Rename all text files to files with .bak extension

## PING, to Verify Network Connection

Verifies connection to one or more remote computers. Available only if TCP/IP is installed.

PING destination (as URI or IP address)

Example:

```
PING en.wikipedia.org
PING 208.80.152.10
```

PING sends a small packet through the network to a particular address. The receiving address returns a packet with the IP address of the receiver. If there is no return packet, the destination address is either non-existent or has no network connection. If there is a return packet, PING determines the number of hops along the path and the elapsed time.

There are optional switches:

```
PING [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS] [-r count] [-s count] [[-j host-list] | [-k host-list]] [-w timeout] destination-list
```

-t	Ping the specified host until interrupted.
-a	Resolve addresses to hostnames.
-n count	Number of echo requests to send.
-l size	Send buffer size.
-f	Set Don't Fragment flag in packet.
-i TTL	Time To Live.
-v TOS	Type Of Service.
-r count	Record route for count hops.
-s count	Timestamp for count hops.
-j host-list	Loose source route along host-list.
-k host-list	Strict source route along host-list.
-w timeout	Timeout in milliseconds to wait for each reply.

In Windows 2000 you can press [Ctrl-Break] when running the -t option for a list of statistics. Press [Ctrl+C] to actually stop the ping.

Example of return messages:

```
C:\Documents and Settings\Owner>ping www.susandoreydesigns.com

Pinging susandoreydesigns.com [66.226.64.26] with 32 bytes of data:

Reply from 66.226.64.26: bytes=32 time=23ms TTL=55
Reply from 66.226.64.26: bytes=32 time=23ms TTL=55
Reply from 66.226.64.26: bytes=32 time=22ms TTL=55
Reply from 66.226.64.26: bytes=32 time=22ms TTL=55

Ping statistics for 66.226.64.26:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 22ms, Maximum = 23ms, Average = 22ms
```

## TRACERT, to Trace Packet Route Over Network

Aka TRACEROUTE, this TCP/IP utility allows you to determine the route packets take through a network to reach a particular host that you specify. If used properly, TRACERT can help you find points in your network that are either routed incorrectly or are not existent at all.

Syntax:

```
TRACERT [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name
```

Switches:

d	Do not resolve addresses to hostnames.
h maximum_hops	Maximum number of hops to search for target.
j host-list	Loose source route along host-list.
w timeout	Wait timeout milliseconds for each reply.

Example of results:

```
C:\Documents and Settings\Owner>tracert 66.226.64.26

Tracing route to pro25.abac.com [66.226.64.26]
over a maximum of 30 hops:

  1  <1 ms  <1 ms  <1 ms  192.168.1.1
  2   8 ms   9 ms   8 ms  ads1-70-137-159-254.dsl.snfc21.sbcglobal.net
[70
.137.159.254]
  3   9 ms   9 ms   8 ms  dist1-vlan52.snfccca.sbcglobal.net [206.13.3.65]
  4   9 ms   8 ms   8 ms  bb1-10g2-0.snfccca.sbcglobal.net
[216.102.176.224
]
  5  10 ms   9 ms   9 ms  151.164.95.198
  6  10 ms   9 ms  10 ms  asn2828-XO.pxpaca.sbcglobal.net
[151.164.249.102
]
  7  10 ms  10 ms  10 ms  te-3-2-0.rar3.sanjose-ca.us.xo.net
[207.88.14.97
]
  8  19 ms  18 ms  24 ms  207.88.14.98.ptr.us.xo.net [207.88.14.98]
  9  22 ms  22 ms  22 ms  207.88.186.54.ptr.us.xo.net [207.88.186.54]
 10  25 ms  24 ms  25 ms  gil-2.cr1.sandiego.abac.net [66.226.66.5]
 11  23 ms  22 ms  23 ms  pro25.abac.com [66.226.64.26]

Trace complete.
```

## MEM, to View Memory Amount

Displays the amount of used and free memory in your computer.

Example of result:

```
C:\DOCUME~1\Owner>mem
```

## DOS Tools

```
655360 bytes total conventional memory
655360 bytes available to MS-DOS
633168 largest executable program size

1048576 bytes total contiguous extended memory
  0 bytes available contiguous extended memory
941056 bytes available XMS memory
  MS-DOS resident in High Memory Area
```

### FORMAT, to Clear Hard Drive or Data Storage Device

FORMAT is used to erase all of the information off of a computer diskette or fixed drive thereby preparing it for new or fresh use. CDs can be purchased pre-formatted.

```
FORMAT drive: [/FS:file-system] [/V:label] [/Q] [size] [/C]
```

/FS:file-system	The file system: (FAT or NTFS). The NTFS file system does not function on floppy disks.
/V:label	The volume label.
/Q	Quick format.
/C	Compression - files added to the new disk will be compressed.
size	May be defined either with /F:size or /A:size . Default settings (via /F) are strongly recommended for general use. NTFS supports 512, 1024, 2048, 4096, 8192, 16K, 32K, 64K. FAT supports 8192, 16K, 32K, 64K, 128K, 256K. NTFS compression is not supported for allocation units above 4096.
/A:size	Allocation unit size.
/F:size	size is the size of the floppy disk (720, 1.2, 1.44, 2.88, or 20.8).

Looking for techniques to monitor use of ports.

### NETSTAT, to Monitor Use of Ports

```
C:\Documents and Settings\sdokey>netstat /? >c:\data\netstate.txt
```

Displays protocol statistics and current TCP/IP network connections.

```
NETSTAT [-a] [-b] [-e] [-n] [-o] [-p proto] [-r] [-s] [-v] [interval]
```

- a Displays all connections and listening ports.
- b Displays the executable involved in creating each connection or listening port. In some cases well-known executables host multiple independent components, and in these cases the sequence of components involved in creating the connection or listening port is displayed. In this case the executable name is in [] at the bottom, on top is the component it called, and so forth until TCP/IP was reached. Note that this option

## DOS Tools

- can be time-consuming and will fail unless you have sufficient permissions.
- e Displays Ethernet statistics. This may be combined with the -s option.
  - n Displays addresses and port numbers in numerical form.
  - o Displays the owning process ID associated with each connection.
  - p proto Shows connections for the protocol specified by proto; proto may be any of: TCP, UDP, TCPv6, or UDPv6. If used with the -s option to display per-protocol statistics, proto may be any of: IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
  - r Displays the routing table.
  - s Displays per-protocol statistics. By default, statistics are shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6; the -p option may be used to specify a subset of the default.
  - v When used in conjunction with -b, will display sequence of components involved in creating the connection or listening port for all executables.
- interval Redisplays selected statistics, pausing interval seconds between each display. Press CTRL+C to stop redisplaying statistics. If omitted, netstat will print the current configuration information once.

To view TCP/UDP ports which are in use by a given process we recommend the freeware utility Active Ports from SmartLine Inc.. This utility provides a real-time GUI view of which ports are in use by which processes which can be handy for troubleshooting issues like port conflicts between network-enabled applications. See <http://www.devicelock.com/freeware.html>.

[http://en.wikipedia.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers) is a good reference of the domain of port numbers.

### Example 1

If you are only interested in seeing which ports are currently open, running **netstat -a** from the command line will list the status of all ports in use. It will not, however, tell you which process is accessing those ports.

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
```

```
C:\Documents and Settings\sdokey>netstat -a
```

#### Active Connections

Proto	Local Address	Foreign Address	State
TCP	1USL14928:epmap	1USL14928.NOE.Nokia.com:0	LISTENING
TCP	1USL14928:microsoft-ds	1USL14928.NOE.Nokia.com:0	LISTENING
TCP	1USL14928:2967	1USL14928.NOE.Nokia.com:0	LISTENING
TCP	1USL14928:9495	1USL14928.NOE.Nokia.com:0	LISTENING
TCP	1USL14928:netbios-ssn	1USL14928.NOE.Nokia.com:0	LISTENING
TCP	1USL14928:1025	localhost:1026	ESTABLISHED
TCP	1USL14928:1026	localhost:1025	ESTABLISHED
TCP	1USL14928:1027	localhost:1028	ESTABLISHED
TCP	1USL14928:1028	localhost:1027	ESTABLISHED

## DOS Tools

```

TCP 1USL14928:1032 localhost:1033 ESTABLISHED
TCP 1USL14928:1033 localhost:1032 ESTABLISHED
TCP 1USL14928:1034 localhost:1035 ESTABLISHED
TCP 1USL14928:1035 localhost:1034 ESTABLISHED
TCP 1USL14928:1248 localhost:5550 ESTABLISHED
TCP 1USL14928:1249 localhost:1250 ESTABLISHED
TCP 1USL14928:1250 localhost:1249 ESTABLISHED
TCP 1USL14928:1251 localhost:1252 ESTABLISHED
TCP 1USL14928:1252 localhost:1251 ESTABLISHED
TCP 1USL14928:5550 1USL14928.NOE.Nokia.com:0 LISTENING
TCP 1USL14928:5550 localhost:1248 ESTABLISHED
TCP 1USL14928:9000 1USL14928.NOE.Nokia.com:0 LISTENING
TCP 1USL14928:11165 1USL14928.NOE.Nokia.com:0 LISTENING
TCP 1USL14928:49100 1USL14928.NOE.Nokia.com:0 LISTENING
TCP 1USL14928:netbios-ssn 1USL14928.NOE.Nokia.com:0 LISTENING
TCP 1USL14928:1313 dawdc102.americas.nokia.com:microsoft-ds
ESTABLISHED
TCP 1USL14928:1463 65.54.30.138:1025 ESTABLISHED
TCP 1USL14928:1470 65.54.30.11:1330 ESTABLISHED
TCP 1USL14928:1778 65.54.30.67:4021 ESTABLISHED
TCP 1USL14928:2718 dawdc101.americas.nokia.com:microsoft-ds
TIME_WAIT
AIT
TCP 1USL14928:2736 dawdc101.americas.nokia.com:microsoft-ds
TIME_WAIT
AIT
TCP 1USL14928:2753 dawdc101.americas.nokia.com:microsoft-ds
TIME_WAIT
AIT
TCP 1USL14928:2771 dawdc101.americas.nokia.com:microsoft-ds
TIME_WAIT
AIT
TCP 1USL14928:2790 dawdc101.americas.nokia.com:microsoft-ds
ESTABLISHED
UDP 1USL14928:259 *:*
UDP 1USL14928:microsoft-ds *:*
UDP 1USL14928:isakmp *:*
UDP 1USL14928:1029 *:*
UDP 1USL14928:1030 *:*
UDP 1USL14928:1031 *:*
UDP 1USL14928:1464 *:*
UDP 1USL14928:2786 *:*
UDP 1USL14928:4500 *:*
UDP 1USL14928:18234 *:*
UDP 1USL14928:ntp *:*
UDP 1USL14928:netbios-ns *:*
UDP 1USL14928:netbios-dgm *:*
UDP 1USL14928:1900 *:*
UDP 1USL14928:ntp *:*
UDP 1USL14928:1043 *:*
UDP 1USL14928:1079 *:*
UDP 1USL14928:1086 *:*
UDP 1USL14928:1097 *:*
UDP 1USL14928:1580 *:*
UDP 1USL14928:1900 *:*
UDP 1USL14928:2523 *:*
UDP 1USL14928:ntp *:*
UDP 1USL14928:netbios-ns *:*
UDP 1USL14928:netbios-dgm *:*
UDP 1USL14928:1900 *:*

```

C:\Documents and Settings\sdoirey>

## DOS Tools

### Example 2

```
C:\Documents and Settings\sdoirey>netstat -an
```

#### Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:2967	0.0.0.0:0	LISTENING
TCP	0.0.0.0:9495	0.0.0.0:0	LISTENING
TCP	10.186.150.13:139	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1025	127.0.0.1:1026	ESTABLISHED
TCP	127.0.0.1:1026	127.0.0.1:1025	ESTABLISHED
TCP	127.0.0.1:1027	127.0.0.1:1028	ESTABLISHED
TCP	127.0.0.1:1028	127.0.0.1:1027	ESTABLISHED
TCP	127.0.0.1:1032	127.0.0.1:1033	ESTABLISHED
TCP	127.0.0.1:1033	127.0.0.1:1032	ESTABLISHED
TCP	127.0.0.1:1034	127.0.0.1:1035	ESTABLISHED
TCP	127.0.0.1:1035	127.0.0.1:1034	ESTABLISHED
TCP	127.0.0.1:1248	127.0.0.1:5550	ESTABLISHED
TCP	127.0.0.1:1249	127.0.0.1:1250	ESTABLISHED
TCP	127.0.0.1:1250	127.0.0.1:1249	ESTABLISHED
TCP	127.0.0.1:1251	127.0.0.1:1252	ESTABLISHED
TCP	127.0.0.1:1252	127.0.0.1:1251	ESTABLISHED
TCP	127.0.0.1:5550	0.0.0.0:0	LISTENING
TCP	127.0.0.1:5550	127.0.0.1:1248	ESTABLISHED
TCP	127.0.0.1:9000	0.0.0.0:0	LISTENING
TCP	127.0.0.1:11165	0.0.0.0:0	LISTENING
TCP	127.0.0.1:49100	0.0.0.0:0	LISTENING
TCP	172.18.87.163:139	0.0.0.0:0	LISTENING
TCP	172.18.87.163:1463	65.54.30.138:1025	ESTABLISHED
TCP	172.18.87.163:1470	65.54.30.11:1330	ESTABLISHED
TCP	172.18.87.163:1778	65.54.30.67:4021	ESTABLISHED
TCP	172.18.87.163:2822	10.241.36.15:445	ESTABLISHED
TCP	172.18.87.163:3247	10.241.36.20:445	TIME_WAIT
TCP	172.18.87.163:3266	10.241.36.20:445	TIME_WAIT
TCP	172.18.87.163:3285	10.241.36.20:445	TIME_WAIT
TCP	172.18.87.163:3302	10.241.32.28:8080	ESTABLISHED
TCP	172.18.87.163:3308	10.241.36.20:445	TIME_WAIT
TCP	172.18.87.163:3326	10.241.32.28:8080	ESTABLISHED
UDP	0.0.0.0:259	*:*	
UDP	0.0.0.0:445	*:*	
UDP	0.0.0.0:500	*:*	
UDP	0.0.0.0:1029	*:*	
UDP	0.0.0.0:1030	*:*	
UDP	0.0.0.0:1031	*:*	
UDP	0.0.0.0:1464	*:*	
UDP	0.0.0.0:3328	*:*	
UDP	0.0.0.0:4500	*:*	
UDP	0.0.0.0:18234	*:*	

## DOS Tools

UDP	10.186.150.13:123	*:*
UDP	10.186.150.13:137	*:*
UDP	10.186.150.13:138	*:*
UDP	10.186.150.13:1900	*:*
UDP	127.0.0.1:123	*:*
UDP	127.0.0.1:1043	*:*
UDP	127.0.0.1:1079	*:*
UDP	127.0.0.1:1086	*:*
UDP	127.0.0.1:1097	*:*
UDP	127.0.0.1:1580	*:*
UDP	127.0.0.1:1900	*:*
UDP	127.0.0.1:2523	*:*
UDP	172.18.87.163:123	*:*
UDP	172.18.87.163:137	*:*
UDP	172.18.87.163:138	*:*
UDP	172.18.87.163:1900	*:*

C:\Documents and Settings\sdokey>

### TASKLIST, to List Running Programs

```
TASKLIST [/S system [/U username [/P [password]]]]  
          [/M [module] | /SVC | /V] [/FI filter] [/FO format] [/NH]
```

Description: This command line tool displays a list of application(s) and associated task(s)/process(es) currently running on either a local or remote system.

#### Parameter List:

- `/S system` Specifies the remote system to connect to.
- `/U [domain\]user` Specifies the user context under which the command should execute.
- `/P [password]` Specifies the password for the given user context. Prompts for input if omitted.
- `/M [module]` Lists all tasks that have DLL modules loaded in them that match the given pattern name. If the module name is not specified, displays all modules loaded by each task.
- `/SVC` Displays services in each process.
- `/V` Specifies that the verbose information is to be displayed.
- `/FI filter` Displays a set of tasks that match a given criteria specified by the filter.

## DOS Tools

- `/FO format` Specifies the output format.  
Valid values: "TABLE", "LIST", "CSV".
- `/NH` Specifies that the "Column Header" should not be displayed in the output.  
Valid only for "TABLE" and "CSV" formats.
- `/?` Displays this help/usage.

### Filters:

Filter Name	Valid Operators	Valid Value(s)
STATUS	eq, ne	RUNNING   NOT RESPONDING
IMAGENAME	eq, ne	Image name
PID	eq, ne, gt, lt, ge, le	PID value
SESSION	eq, ne, gt, lt, ge, le	Session number
SESSIONNAME	eq, ne	Session name
CPUTIME	eq, ne, gt, lt, ge, le	CPU time in the format of hh:mm:ss. hh - hours, mm - minutes, ss - seconds
MEMUSAGE	eq, ne, gt, lt, ge, le	Memory usage in KB
USERNAME	eq, ne	User name in [domain\]user format
SERVICES	eq, ne	Service name
WINDOWTITLE	eq, ne	Window title
MODULES	eq, ne	DLL name

### Examples:

```
TASKLIST
TASKLIST /M
TASKLIST /V
TASKLIST /SVC
TASKLIST /M wbem*
TASKLIST /S system /FO LIST
TASKLIST /S system /U domain\username /FO CSV /NH
TASKLIST /S system /U username /P password /FO TABLE /NH
TASKLIST /FI "USERNAME ne NT AUTHORITY\SYSTEM" /FI "STATUS eq running"
```

```
C:\Documents and Settings\sdoirey>
```

## Port Usage Advice from Google

Here is a quick and easy way to dig into what ports are being used, and what apps are using them.

## DOS Tools

**Step 1:** Find out what ports are being used:

```
C:\>NetStat -o
```

Which will return the following (your list will probably be much longer):

Proto	Local Address	Foreign Address	State	PID
TCP	EC968728:1108	somesite.corp.com:https	ESTABLISHED	4072

**Step 2:** See which app (& more) is using that port:

```
C:\>TaskList /FI "PID eq 4072" /FO LIST /V
```

Which will return the following

```
Image Name:   OUTLOOK.EXE
PID:          4072
Session Name: Console
Session#:     0
Mem Usage:    105,320 K
Status:       Running
User Name:    ****DomainName****\bgroth
CPU Time:     0:01:44
Window Title: Inbox - Microsoft Outlook
```