

Windows Commands and Residential Networking

1st edition, version 1.0

Seema Gupta

Table of Contents

<u>Chapter 1: Introduction</u>	1
<u>1.1 Basic Tools</u>	3
<u>Chapter 2: Command Line Interface</u>	7
<u>2.1 File and folder management</u>	10
<u>2.2 Networking</u>	18
<u>2.3 System management</u>	30
<u>2.3.1 Disk Management</u>	42
<u>2.3.2 User, groups and shares</u>	46
<u>Chapter 3: Administration of PC</u>	49
<u>3.1 Defending Yourself</u>	50
<u>Chapter 4: Residential Networking</u>	52
<u>4.1 Residential Connection Technologies</u>	55
<u>4.2 OSI Layers</u>	57
<u>4.3 Transport Protocols</u>	58
<u>4.4 Metrics</u>	59
<u>4.5 Application Layer Protocols</u>	59
<u>Chapter 5: Basic Network Devices</u>	62
<u>5.1 Bridge</u>	62
<u>5.2 Switch</u>	63
<u>5.4 Access Point</u>	65
<u>5.3 VPNs and Firewalls</u>	66
<u>Appendix</u>	
A. <u>MMC snap-ins</u>	68
B. <u>Powershell Basics</u>	69
C. <u>Windows Troubleshooting</u>	73
<u>References</u>	78

Chapter 1 Introduction

The first part of this booklet focuses on Windows Command Line. The second part of this booklet focuses on home networking and related basic networking at a very high level. The audiences for this booklet include beginners and anyone who wants to learn the basics of Windows commands and home networking to utilize this knowledge in maintaining their Windows PC. This booklet is best read in front of a PC by trying out commands as you read about them.

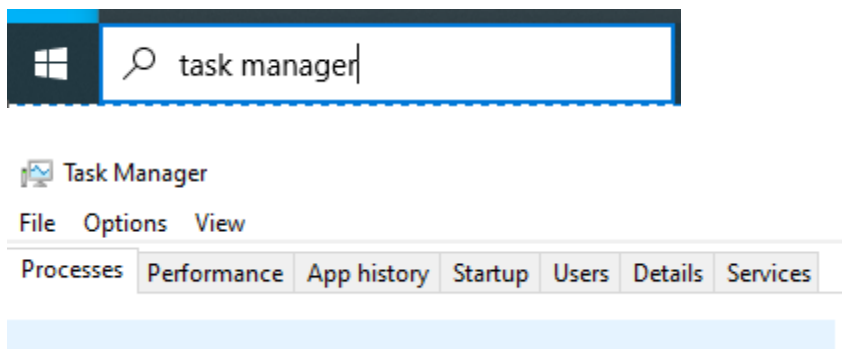
Chapter 1 focuses on tools to help you understand what's going on inside your Windows personal computer. These include Task Manager, Event Viewer and System Information. Chapter 2 focuses on the Command Line Interface (CLI) for file and folder management, networking and system administration. Chapter 3 focuses on home administration and best practices to defend you. Chapter 4 focuses on home networking and connectivity technologies. Chapter 5 briefly describes basic networking devices, VPNs and Firewalls. Appendices have information on system management.

1.1 Basic Tools

Following is a partial list of tools in Windows. Some of these may require administrative privileges.

Task Manager

Task Manager can be used to get information on processes, performance, app history, startup services and users. To launch the Task Manager, type task manager in the search box and press enter, or select the Task Manager App and click it.



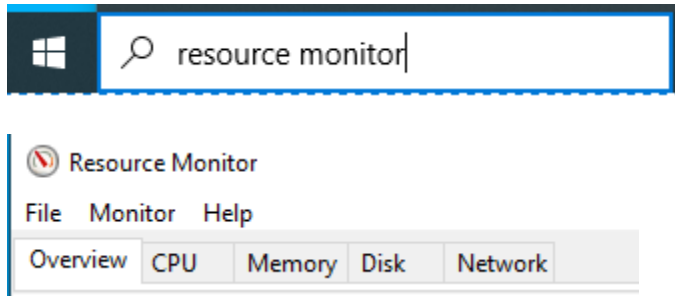
On the processes tab, you'll see Central Processing Unit (CPU), memory, disk and network activity for apps and services. You could see the network traffic and if anything is using up too much resources.

The performance tab displays the current CPU, memory, disk and network activity as a live graph. At the bottom of the performance tab is a link to Resource Monitor.

Additionally, the App history tab will show how much CPU time and network data apps have been using over a period of time. The Startup tab shows the apps that are enabled during startup. Details tab shows the executables that are running. Finally, the Services tab shows the services that are running.

Resource Monitor

The Resource Monitor takes the reporting of Task Manager and scales it up. To launch the Resource Monitor, type resource monitor in the search box and press enter, or select the Resource Monitor App and click it. Launching this may require administrative privilege.

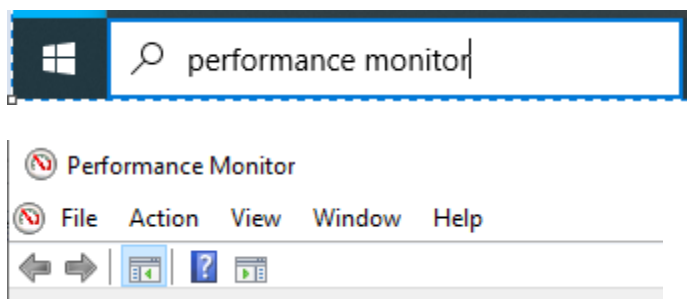


The overview tab contains panels displaying the apps, drivers and services currently using the device's CPU, disk, networking, and memory. Network tab has collapsible panels including Processes with Network Activity, Transmission Control Protocol (TCP) connections and port numbers. Each of the processes using the network has a check box to the left of its name. By checking the box for a process, the rest of the panels will change to show only the network information relevant to that particular process.

Additionally, the Network Activity and TCP connections panels will provide information on the Internet Protocol (IP) address or hostname of the resource being accessed and reveal information about the processes that are communicating with the outside world over the network.

Performance Monitor

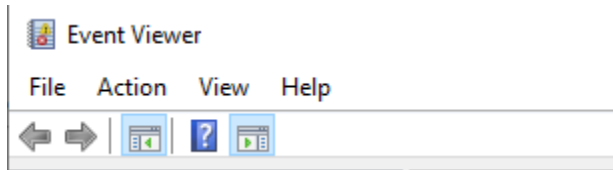
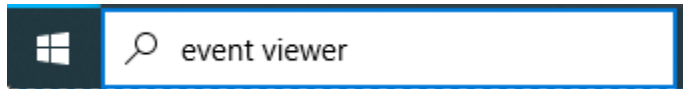
Performance Monitor is similar to Resource Monitor in some ways, in that it provides live data about what's happening on the PC. However, the Performance Monitor displays data according to Operating System (OS) function instead of based on process activity. To launch the Performance Monitor, type performance monitor in the search box and press enter, or select the Performance Monitor App and click it.



It displays data according to OS function like available memory, network interface cards data transfer rate, and processor & disk information. After selecting "Performance Monitor" on the left, you can use the green plus (+) icon to add a counter or counters to the graph. If you need to keep an eye on specific OS functions, then Performance Monitor is a good tool for this purpose.

Event Viewer

Almost nothing happens on a PC without it being recorded in the Windows Event Viewer. To launch the Event Viewer, type event viewer in the search box and press enter, or select the Event Viewer App and click it.



Event Viewer's summary of events classifies events into Information, Warnings, Errors, and Critical categories. Each event is clickable and comes with a text description of what happened, along with the time and date of the event and any error codes (in hex format) that can be searched online for more information.

Windows event log helps analyze problems. Local logging may need to be enabled on systems and networking devices. Events are placed into categories, each of which is related to a log that Windows keeps:

Application event log records events related to Windows components.

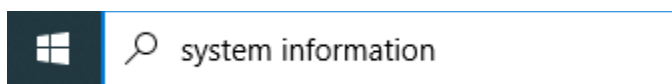
Security event log records events related to security such as logon attempts and resources accessed.

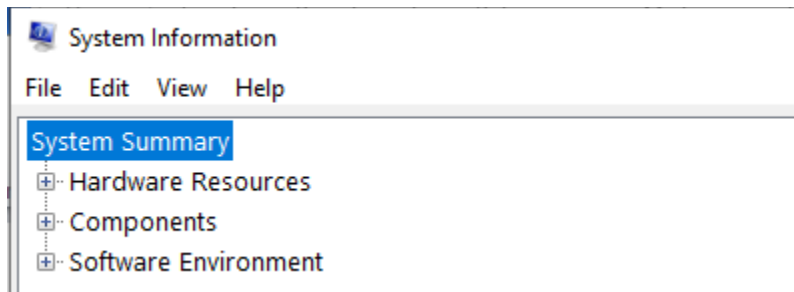
System event log records events about programs installed.

Custom views can be created in the right-side panel. This provides data on specific operating system function for tracking errors and events over time. Also in the right panel is a Filter Current View option to filter any custom view to narrow down the data contained in it.

System Information

To launch the System Information, type system information in the search box and press enter, or select the System Information App and click it.



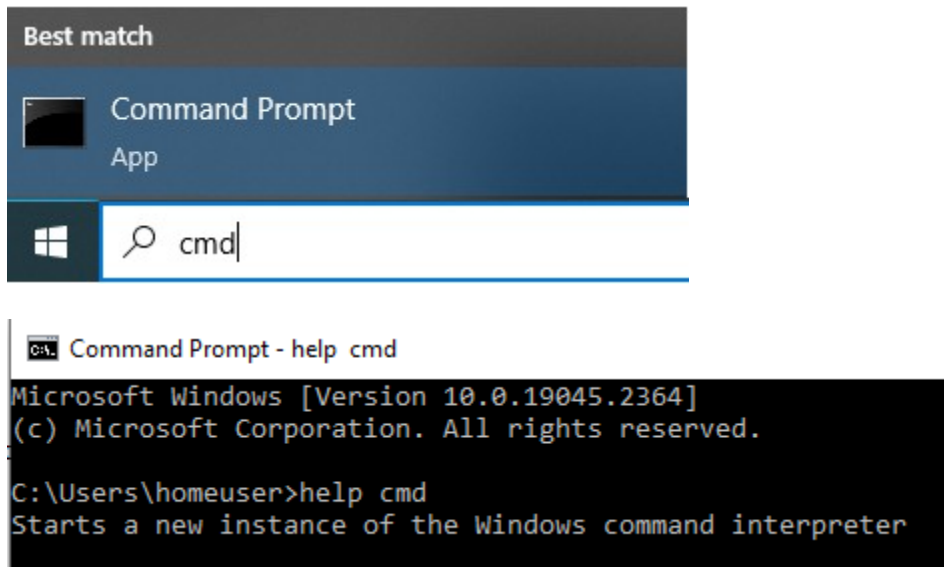


System information provides detailed information about the system and everything installed on it, including information on manufacturer, OS, processor, memory, network adapters and disks.

Sec 1.1 adapted from Windows Networking Troubleshooting, Halsey, Ballew

Chapter 2 Command Line Interface

Command Prompt is the Windows Command Interpreter. To launch the Command prompt, type cmd in the task bar and press enter, or select the Command Prompt App and click it.



To get information about the underlying computer system, systeminfo command can be used. System information can be retrieved by invoking systeminfo command at the Command Prompt. A partial list of output is as follows. This includes information about the Operating System (OS), processor, memory, network card and disk. For brevity, output of several commands has been snipped in this chapter.

```
C:\Users\homeuser>systeminfo
```

```
Host Name:          <name of host>
OS Name:            Microsoft Windows 10 Home
OS Version:         <version>
OS Manufacturer:    Microsoft Corporation
OS Configuration:   Standalone Workstation
Original Install Date: <date>
<snip>
```

32-bit vs 64-bit

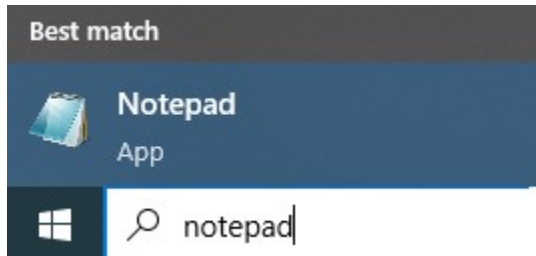
32-bit operating systems can only use up to 2^{32} (about 4 Giga Byte minus overhead) of memory even if you have more installed. This can be slow if say you're editing videos. 64-bit versions of applications like Office take advantage of the full 64-bit CPU capability and additional memory making them faster.

Day-to-day use: files and common commands

On the computer, information is stored in files, which are like generic office files. Each file has a name, content, place to keep it and additional information such as who owns it and how big it is. A file might

contain a letter, or a list of tasks, or the source code statements of a program, or data to be used by a program, or even programs in executable form or other non-textual information like a photograph.

Files can be created using an *editor*. An *editor* like notepad can be used to create files containing text. An editor is a program for storing and updating information in a file. To launch notepad, type notepad in the taskbar and press enter or select the Notepad App and click it.



To list the files in the current folder or directory, *dir* command can be used. It displays the directory listing for the current folder or the specified folder. Helpful information can be retrieved for a command by invoking *help command-name* at the prompt. Command names aren't always italicized in this chapter.

```
C:\Users\homeuser>help dir
```

Displays a list of files and subdirectories in a directory.

```
C:\Users\homeuser>dir
```

Volume in drive C is Windows

Volume Serial Number is <snip>

Adding the */p* option to the *dir* command will cause the output to pause after each screenful of information. This is helpful when listings span multiple pages.

```
C:\Users\homeuser>dir /p
```

The computer distinguishes one user's file from other users' files by grouping files into directories. Generally each user has a personal or home directory, also known as the login directory which contains only files that belong to the user. When the user logs in, he or she is in his or her home directory. *whoami* command tells you who you are logged in as.

Help for a command can be retrieved by typing the command name followed by */?* (forward slash and question mark).

```
C:\Users\homeuser>whoami /?
```

```
C:\Users\homeuser>whoami
```

You could change the directory you are working in by using the *cd* (for change directory) command.

```
C:\Users\homeuser>cd /?
```

Displays the name of or changes the current directory.


```
C:\Users\homeuser>cd Documents
C:\Users\homeuser\Documents>
```

A directory can contain other directories as well as files. To move back one level up, use `cd ..` (cd space dot dot) command.

```
C:\Users\homeuser\Documents>cd ..
C:\Users\homeuser>
```

Mkdir command can be used to create a new directory or folder.

```
C:\Users\homeuser>mkdir /?
Creates a directory.
```

```
C:\Users\homeuser>mkdir Example
```

Similarly, *copy*, *move*, *ren* and *del* commands can be used to copy, move, rename and delete files or folders respectively.

```
C:\Users\homeuser>cd Example
```

Use the *echo* command to display a message. Then redirect the output into a file to create a file named hello.

```
C:\Users\homeuser\Example>echo hi > hello
```

Use the *copy* command to copy the contents of file named hello into a new file names hello_again.

```
C:\Users\homeuser\Example>copy hello hello_again
1 file(s) copied.
```

Use the *ren* command to rename the file hello_again to hello2.

```
C:\Users\homeuser\Example>ren hello_again hello2
```

Use the *dir* command to list the contents of the current directory. Dot refers to the current directory and dot dot refers to the parent directory.

```
C:\Users\homeuser\Example>dir
Volume in drive C is Windows
Volume Serial Number is <snip>
Directory of C:\Users\homeuser\Example
01/12/2022 10:13 AM <DIR>      .
01/12/2022 10:13 AM <DIR>      ..
01/12/2022 10:10 AM           5 hello
01/12/2022 10:10 AM           5 hello2
                2 File(s)      10 bytes
```

Use *more* command to display the contents of a text file.

```
C:\Users\homeuser\Example>more /?
Displays output one screen at a time.
```

```
C:\Users\homeuser\Example>more hello
```

Use the *move* command to move a file from one directory to another. To move the file hello to the parent directory specify ../ (dot dot forward slash) as the destination.

```
C:\Users\homeuser>move /?
```

Moves files and renames files and directories.

```
C:\Users\homeuser\Example>move hello ../
```

Use the *del* command to delete a file.

```
C:\Users\homeuser\Example>del hello2
```

Finally, to clear the screen use the *cls* command.

```
C:\Users\homeuser>cls
```

Command Line Interface (CLI)

Windows Command Line Interface has commands for File and Folder management, Disk Management, System Management, Users, Groups and Shares management and Networking. In the subsequent chapters Windows and Windows 10 are referred to interchangeably. The specifics of the CLI commands that follow may have changed since the writing of this booklet but the general concepts remain the same. These commands are case insensitive. In other words, they can be specified using uppercase or lowercase letters. Information in Sections 2.1 and 2.3 has been adapted from Windows 10 in depth, by Knittel and McFedries.

2.1 File and folder Management

Windows command line file and folder management tools are listed in the following table.

Command	Description
Attrib	Applies or removes attributes for the specified file or folder
Cd	Change to the specified folder
Comp	Compares the contents of two specified files, byte by byte
Compact	Displays or modifies the compression settings for the specified file (located on the NTFS partition)
Copy	Creates a copy of the specified file or folder in another location
Del	Deletes the specified file or folder
Dir	Displays the directory listing for the current folder or the specified file or folder
Fc	Compares the contents of two specified files
Find	Searches for and displays all instances of a specified string in a file

Findstr	Uses a regular expression to search for and display all instances of a specified string in a file
Mkdir	Creates the specified folder
Move	Moves the specified file or folder to another location
Path	Displays or sets a search path for executable files
Ren	Rename the specified file or folder
Replace	Replaces files in the destination folder with files in the source folder that have the same name
Rmdir	Deletes the specified folder
Sort	Sorts the specified file and then displays the results
Sfc	Runs the file system checker, which scans and verifies files
Takeown	Enables an administrator to take ownership of the specified file
Tree	Displays a graphical tree diagram showing the subfolder hierarchy of the current folder or the specified folder
Where	Searches for and displays all files that match a specified pattern in the current folder and in the PATH folders
Xcopy	Creates a copy of the specified file or folder in another location. This offers many more options than copy command.

Attrib: modifying file and folder attributes

C:\Users\homeuser>attrib /?
Displays or changes file attributes.

ATTRIB [+R | -R] [+A | -A] [+S | -S] [+H | -H] [+O | -O] [+I | -I] [+X | -X] [+P | -P] [+U | -U]
[drive:][path][filename] [/S [/D]] [/L]

- + Sets an attribute.
- Clears an attribute.
- R Read-only file attribute.
- A Archive file attribute.
- S System file attribute.
- H Hidden file attribute.
- O Offline attribute.
- I Not content indexed file attribute.
- X No scrub file attribute.
- V Integrity attribute.
- P Pinned attribute.
- U Unpinned attribute.

B SMR Blob attribute.

[drive:][path][filename]

Specifies a file or files for attrib to process.

/S Processes matching files in the current folder
and all subfolders.

/D Processes folders as well.

/L Work on the attributes of the Symbolic Link versus
the target of the Symbolic Link

```
C:\Users\homeuser>attrib testfile.txt
```

```
A          C:\Users\homeuser\testfile.txt
```

A files attributes are special codes that indicate the status of the file. There are 7 attributes:

1. Archive: when turned on it means, the file has been modified since it was last backed up.
2. Hidden: when turned on it means the file does not show up in a dir listing and isn't included when you run most command-line tools. For example if you run `del *.*` in a folder, it'll delete all files in the current folder except the hidden ones.
3. Integrity: when set it means the volume is configured with integrity, where data is stored in such a way that it is protected from certain types of file errors. This only works with Win 10 server volumes formatted with Resilient File system.
4. No scrub: This only works with Win 10 server volumes formatted with Resilient File system.
5. Not content indexed: when set the file contents will not be indexed for searching.
6. Read-only: when set the file cannot be modified or erased.
7. System: when set it means the file is an operating system file (that was installed with windows).

Following command will make the testfile.txt read-only, preventing any modification to it.

```
C:\Users\homeuser>attrib +r testfile.txt
```

```
C:\Users\homeuser>attrib testfile.txt
```

```
A R          C:\Users\homeuser\testfile.txt
```

Find: locating a text string in a file

```
C:\Users\homeuser>find /?
```

Searches for a text string in a file or files.

```
FIND [/V] [/C] [/N] [/I] [/OFF[LINE]] "string" [[drive:][path]filename[ ...]]
```

/V Displays all lines NOT containing the specified string.

/C Displays only the count of lines containing the string.

/N Displays line numbers with the displayed lines.

/I Ignores the case of characters when searching for the string.

/OFF[LINE] Do not skip files with offline attribute set.

"string" Specifies the text string to find.

[drive:][path]filename

Specifies a file or files to search.

If a path is not specified, find searches the text typed at the prompt or piped from another command.

```
C:\Users\homeuser\Example>notepad examplefile
```

After editing examplefile, search for the string test in the contents of examplefile. The search string needs to be enclosed in double quotes.

```
C:\Users\homeuser\Example>find "test" examplefile
```

As an example of piping a command output into another command, the last line of *dir* listing tells you the number of bytes free on the current drive. You can pipe the output of another command through find. Find searches the *dir* listing piped to it and looks for the word free.

```
C:\Users\homeuser\Example>dir | find "free"
```

Ren: renaming a file or folder

```
C:\Users\homeuser>ren /?
```

Renames a file or files.

RENAME [drive:][path]filename1 filename2.

REN [drive:][path]filename1 filename2.

```
C:\Users\homeuser>ren testfile.txt samplefile.txt
```

```
C:\Users\homeuser>dir samplefile.txt
```

To rename all filenames with 2015 to 2016,
ren *2015* *2016*

If the filename has space, put it in double quotes,
ren "from file" "to file"

Replace: smarter file copy

Replace can do three useful things:

- It copies files, but only if their names match those in the target directory
- It copies files but only if their names do not exist in the target directory
- It copies files, but only if their names match those in the target directory and the matching files in the target directory are older than the files being copied

```
C:\Users\homeuser>replace /?
```

Replaces files.

REPLACE [drive1:][path1]filename [drive2:][path2] [/A] [/P] [/R] [/W]

REPLACE [drive1:][path1]filename [drive2:][path2] [/P] [/R] [/S] [/W] [/U]

[drive1:][path1]filename Specifies the source file or files.

[drive2:][path2] Specifies the directory where files are to be replaced.

/A Adds new files to destination directory. Cannot use with /S or /U switches.

/P Prompts for confirmation before replacing a file or adding a source file.

/R Replaces read-only files as well as unprotected files.

/S Replaces files in all subdirectories of the destination directory. Cannot use with the /A switch.

/W Waits for you to insert a disk before beginning.

/U Replaces (updates) only files that are older than source files. Cannot use with the /A switch.

If you don't specify switches, replace copies a file from the source folder to the target folder if and only if it finds a file with a matching name in the target.

```
C:\Users\homeuser\Example>replace testfile.txt G:\
```

Use the following steps to backup all files in a folder by specifying the /A flag first time only and /U during subsequent backups.

```
C:\Users\homeuser\Example>replace *.* G:\Example\ /A
```

```
C:\Users\homeuser\Example>replace *.* G:\Example\ /U
```

/U update switch is also useful for example, when copying files to a disk or memory card so that you can use them on another machine. When you need to copy the files back to the first machine, the following replace command can be used to replace if the file on the USB drive is newer. Dot refers to the current working directory.

```
C:\Users\homeuser\Example>replace G:\testfile.txt . /U
```

Sort: sorting the contents of a file

```
C:\Users\homeuser>sort /?
```

```
SORT [/R] [/+n] [/M kilobytes] [/L locale] [/REC recordbytes]
```

```
[[drive1:][path1]filename1] [/T [drive2:][path2]]
```

```
[/O [drive3:][path3]filename3]
```

/+n Specifies the character number, n, to begin each comparison. /+3 indicates that each comparison should begin at the 3rd character in each line. Lines with fewer than n characters collate before other lines. By default comparisons start at the first character in each line.

/L[OCAL] locale Overrides the system default locale with the specified one. The ""C"" locale yields the fastest collating sequence and is

currently the only alternative. The sort is always case insensitive.

/M[EMORY] kilobytes Specifies amount of main memory to use for the sort, in kilobytes. The memory size is always constrained to be a minimum of 160 kilobytes. If the memory size is specified the exact amount will be used for the sort, regardless of how much main memory is available.

The best performance is usually achieved by not specifying a memory size. By default the sort will be done with one pass (no temporary file) if it fits in the default maximum memory size, otherwise the sort will be done in two passes (with the partially sorted data being stored in a temporary file) such that the amounts of memory used for both the sort and merge passes are equal. The default maximum memory size is 90% of available main memory if both the input and output are files, and 45% of main memory otherwise.

/REC[ORD_MAXIMUM] characters Specifies the maximum number of characters in a record (default 4096, maximum 65535).

/R[EVERSE] Reverses the sort order; that is, sorts Z to A, then 9 to 0.

[drive1:][path1]filename1 Specifies the file to be sorted. If not specified, the standard input is sorted. Specifying the input file is faster than redirecting the same file as standard input.

/T[EMPORARY]

[drive2:][path2] Specifies the path of the directory to hold the sort's working storage, in case the data does not fit in main memory. The default is to use the system temporary directory.

/O[UTPUT]

[drive3:][path3]filename3 Specifies the file where the sorted input is to be stored. If not specified, the data is written to the standard output. Specifying the output file is faster than redirecting standard output to the same file.

First create the text file num.txt.

C:\Users\homeuser>notepad num.txt

<Enter numbers in unsorted order>

C:\Users\homeuser>sort num.txt

1

2
3
4
6

Use the following command to redirect the output of sorting to a new file called numsorted.txt.

```
C:\Users\homeuser>sort num.txt > numsorted.txt
C:\Users\homeuser>more numsorted.txt
```

Xcopy: advanced file copy

```
C:\Users\homeuser>xcopy /?
Copies files and directory trees.
```

```
XCOPY source [destination] [/A | /M] [/D[:date]] [/P] [/S [/E]] [/V] [/W]
        [/C] [/I] [/Q] [/F] [/L] [/G] [/H] [/R] [/T] [/U]
        [/K] [/N] [/O] [/X] [/Y] [/Y] [/Z] [/B] [/J]
        [/EXCLUDE:file1[+file2][+file3]...] [/COMPRESS]
```

source Specifies the file(s) to copy.

destination Specifies the location and/or name of new files.

/A Copies only files with the archive attribute set, doesn't change the attribute.

/M Copies only files with the archive attribute set, turns off the archive attribute.

/D:m-d-y 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.

/EXCLUDE:file1[+file2][+file3]... Specifies a list of files containing strings. Each string should be in a separate line in the files. When any of the strings match any part of the absolute path of the file to be copied, that file will be excluded from being copied. For example, specifying a string like \obj\ or .obj will exclude all files underneath the directory obj or all files with the .obj extension respectively.

/P Prompts you before creating each destination file.

/S Copies directories and subdirectories except empty ones.

/E Copies directories and subdirectories, including empty ones. Same as /S /E. May be used to modify /T.

/V Verifies the size of each new file.

/W Prompts you to press a key before copying.

/C Continues copying even if errors occur.

/I If destination does not exist and copying more than one file, assumes that destination must be a directory.

/Q Does not display file names while copying.

/F Displays full source and destination file names while copying.

/L Displays files that would be copied.

- /G Allows the copying of encrypted files to destination that does not support encryption.
- /H Copies hidden and system files also.
- /R Overwrites read-only files.
- /T Creates directory structure, but does not copy files. Does not include empty directories or subdirectories. /T /E includes empty directories and subdirectories.
- /U Copies only files that already exist in destination.
- /K Copies attributes. Normal Xcopy will reset read-only attributes.
- /N Copies using the generated short names.
- /O Copies file ownership and ACL information.
- /X Copies file audit settings (implies /O).
- /Y Suppresses prompting to confirm you want to overwrite an existing destination file.
- /-Y Causes prompting to confirm you want to overwrite an existing destination file.
- /Z Copies networked files in restartable mode.
- /B Copies the Symbolic Link itself versus the target of the link.
- /J Copies using unbuffered I/O. Recommended for very large files.
- /COMPRESS Request network compression during file transfer where applicable.

In its most basic form, xcopy works just like copy. For example, to copy all .doc files in the current folder to a folder called Documents in G:, use the command,

```
Xcopy *.doc g:\documents
```

The X in the xcopy means its an extended copy command. For example, suppose you want to copy all the .doc files in the current folder and all the .doc files in any attached subfolders to G:\Documents. With copy, you first have to create the appropriate folders on the destination and then perform separate copy commands for each folder, which is not very efficient. With xcopy, all you do is add a single switch /s:

```
Xcopy *.doc g:\documents /s
```

The /s switch tells xcopy to copy the current folder and all nonempty subfolders, and to create the appropriate subfolders in the destination, as needed. If you want xcopy to copy empty subfolders, include the /E switch as well.

Another useful feature of xcopy is the ability to copy files by date. This is handy for performing incremental backups of files that you modified on or after a specific date. For example, suppose you want to make backup copies in your windows user share of all your *.doc files that have changed since Nov 10, 2013, you could do,

```
Xcopy *.doc g:\documents /d:11-10-2013
```

2.2 Windows Networking

Following is a list of networking or network troubleshooting utilities in windows. This section has also been adapted from Windows Networking Troubleshooting, by Halsey and Ballew.

Command	Description
Arp	Displays IP-to-Ethernet address translation information
Netstat	Displays protocol stats information
Ping	Checks a network connection to a remote computer
Tracert	Checks the route taken to a remote host
Ipconfig	Displays the current TCP/IP network configuration
nslookup	Used to find the IP address of a host
route	Used to get routing table information
net	Used to view or update network information
netsh	Used to review or update information about the networks that are accessible

Address Resolution Protocol (ARP)

ARP displays Internet Protocol (IP) to Physical address translation tables used by Address Resolution Protocol. Physical address is the Media Access Control (MAC) address of the Network Interface Card (NIC) which could be using Ethernet for wireline or 802.11 protocols for wireless access.

```
C:\Users\homeuser>arp -?
```

Displays and modifies the IP-to-Physical address translation tables used by address resolution protocol (ARP).

```
ARP -s inet_addr eth_addr [if_addr]
```

```
ARP -d inet_addr [if_addr]
```

```
ARP -a [inet_addr] [-N if_addr] [-v]
```

-a Displays current ARP entries by interrogating the current protocol data. If inet_addr is specified, the IP and Physical addresses for only the specified computer are displayed. If more than one network interface uses ARP, entries for each ARP table are displayed.

-g Same as -a.

-v Displays current ARP entries in verbose mode. All invalid entries and entries on the loop-back interface will be shown.

inet_addr Specifies an internet address.

-N if_addr Displays the ARP entries for the network interface specified by if_addr.

-d Deletes the host specified by inet_addr. inet_addr may be wildcarded with * to delete all hosts.

-s Adds the host and associates the Internet address inet_addr with the Physical address eth_addr. The Physical address is

given as 6 hexadecimal bytes separated by hyphens. The entry is permanent.

eth_addr Specifies a physical address.

if_addr If present, this specifies the Internet address of the interface whose address translation table should be modified. If not present, the first applicable interface will be used.

For example to display the ARP table, use the following.

```
> arp -a
```

Network Statistics (Netstat)

Netstat displays protocol statistics and current Transmission Control Protocol / Internet Protocol (TCP/IP) connections. Netstat is a network utility tool that displays incoming and outgoing networking connections, routing tables and other details such as protocol statistics. It can help discover which ports are open for incoming connections, which ports are currently in use and what is the current state of the connections that already exist. The output displays the current state of all connections. Using the Netstat command with the options -a for all and -n for addresses and ports, enables listing all active network connections on the machine. The 0.0.0.0 in the output refers to no particular address. The number after the colon is the port number. Port number specifies the application layer protocol like 25 is the port number for Simple Mail Transfer Protocol (SMTP). Ports can be TCP or UDP User Datagram Protocol ports. Internet Assigned Numbers Authority (IANA) maintains the official assignment of well-known port numbers which are in the range 0-1023. Note that even if the output shows that the host is listening at a specific port, the firewall may not always be allowing traffic to get to the machine on that port.

-? or /? switch can be used to invoke help.

```
C:\Users\homeuser>netstat -?
```

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [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 can be time-consuming and will fail unless you have sufficient permissions.
- e Displays Ethernet statistics. This may be combined with the -s option.
- f Displays Fully Qualified Domain Names (FQDN) for foreign addresses.
- 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.
- q Displays all connections, listening ports, and bound nonlistening TCP ports. Bound nonlistening ports may or may not be associated with an active connection.
- 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.
- t Displays the current connection offload state.
- x Displays NetworkDirect connections, listeners, and shared endpoints.
- y Displays the TCP connection template for all connections. Cannot be combined with the other options.
- 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.

Use the following commands to list stats for Internet Protocol (IP), User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) respectively.

```
netstat -sp IP
netstat -sp UDP
netstat -sp TCP
```

Use the following command to list all connections and listening ports for the TCP protocol.

```
netstat -an -p TCP
```

Use the following command to output the protocol, local & remote address, state, and the process identifier (PID) associated with the connections.

```
netstat -nao
```

Ping

Ping checks a network connection to a remote host. Based on the output of the ping command, you can tell if the remote host is reachable or not. Following is an example of ping to www.example.com. The output shows that the IP address of the host is 93.184.216.34, four requests were sent and all four responses were received from the host, and the average round trip time was 13 milli-seconds. Time-To-Live (TTL) of 55 means that the request assumes that the host is not more than 55 hops away. Getting successful replies without losses confirms that the host was indeed less than 55 hops away.

```
C:\Users\homeuser >ping www.example.com
```

```
Pinging www.example.com [93.184.216.34] with 32 bytes of data:
```

```
Reply from 93.184.216.34: bytes=32 time=12ms TTL=55
```

```
Reply from 93.184.216.34: bytes=32 time=13ms TTL=55
```

Reply from 93.184.216.34: bytes=32 time=14ms TTL=55
Reply from 93.184.216.34: bytes=32 time=13ms TTL=55

Ping statistics for 93.184.216.34:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 12ms, Maximum = 14ms, Average = 13ms

To invoke help,

C:\Users\homeuser>ping /?

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
[-r count] [-s count] [[-j host-list] | [-k host-list]]
[-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
[-4] [-6] target_name

Options:

- t Ping the specified host until stopped.
To see statistics and continue - type Control-Break;
To stop - type Control-C.
- 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 (IPv4-only).
- i TTL Time To Live.
- v TOS Type Of Service (IPv4-only. This setting has been deprecated and has no effect on the type of service field in the IP Header).
- r count Record route for count hops (IPv4-only).
- s count Timestamp for count hops (IPv4-only).
- j host-list Loose source route along host-list (IPv4-only).
- k host-list Strict source route along host-list (IPv4-only).
- w timeout Timeout in milliseconds to wait for each reply.
- R Use routing header to test reverse route also (IPv6-only).
Per RFC 5095 the use of this routing header has been deprecated. Some systems may drop echo requests if this header is used.
- S srcaddr Source address to use.
- c compartment Routing compartment identifier.
- p Ping a Hyper-V Network Virtualization provider address.
- 4 Force using IPv4.
- 6 Force using IPv6.

Following are examples of ping command.

C:\Users\homeuser>ping www.example.com

C:\Users\homeuser>ping 8.8.8.8

Simplified version of ping syntax is:

Ping [-t] [-n count] target_name

-t	Ping the target until you interrupt
-n count	Send these many number of request packets
Target_name	IP address or hostname of the remote host you want to ping

Ping is a networking utility used to test whether a host is alive. Ping sends an ICMP (Internet Control Message Protocol) echo request to the target and waits for a reply. It reports any problems, trip time and packet loss information if the host is alive and can be reached. If the host is not alive or cannot be reached, it returns an ICMP error. It has many optional arguments including size of the packet, number of requests to send and time to live (TTL). TTL is decremented at each hop where the request is processed. So, it should be as big as the number of gateways the request has to hop to reach the destination. After a connection has been made, ping returns information on latency between the hosts. To ping yourself, you could use the loopback address 127.0.0.1. If pinging the loopback interface causes error, then it indicates there is a problem with your system's IP configuration.

If you can't connect to any remote host, you could try the following.

- First check if you can ping the loopback address:
>Ping 127.0.0.1
This may fail if your computer doesn't have TCP/IP installed correctly.
- If the previous step works, then try ping-ing your computer's IP address. If you're using Dynamic Host Control Protocol (DHCP), run the ipconfig utility to get your current IP address. If you don't get a successful reply, there may be a problem with your Network Interface Card (NIC) configuration.
- If the previous step works, try ping-ing your default gateway (router). If you can't successfully ping the router's internal IP address, you won't be able to access remote internet sites. In this case, check the IP address you entered for the gateway, check the cable connections, and make sure the router is turned on. You may need to power cycle the router.
- If you get this far, try ping-ing the remote hostname or IP address you're trying to contact.

Tracert

Tracert on Windows or traceroute on Unix based systems is a simple network diagnostics tool for identifying the routing path of a packet and the latency for each intermediate hop in the network. Tracert checks the route taken to a remote host. To identify the individual hops, tracert sends a sequence of ICMP echo packets toward the destination with an increasing "hop limit" of 1, 2, 3 and so on. When the hop limit is reached, the intermediary returns an ICMP Time Exceeded message back to the source, allowing the tool to measure the latency for each network hop on the way. ICMP is one of Internet's protocols used by network devices to send operational information or error messages. It is used to report errors in the processing of packets. Each router along the path subtracts the packet's "hop limit" or Time To Live (TTL) value by 1 and forwards the packet to the destination. It is a useful tool to find out how far a packet may have reached or gotten dropped along the way.

```
C:\Users\homeuser>tracert /?
```

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
[-R] [-S srcaddr] [-4] [-6] target_name

Options:

- 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 (IPv4-only).
- w timeout Wait timeout milliseconds for each reply.
- R Trace round-trip path (IPv6-only).
- S srcaddr Source address to use (IPv6-only).
- 4 Force using IPv4.
- 6 Force using IPv6.

Use the following command to trace the route to www.example.com.

```
C:\Users\homeuser>tracert www.example.com
```

If you can't ping a remote host, your echo packets might be getting held up along the way. To find out more, you can use the tracert command.

Tracert operates by sending ICMP echo packets with varying Time To Live (TTL) values. TTL places a limit on the number of hops that a packet can take. Each host along the packet's route decrements the TTL value by one. In tracert, the ICMP packets specify that whichever host decrements the TTL to 0 should send back a response. So, the first packet has a TTL value of 1, second has a TTL value of 2, and so on. Tracert keeps sending packets with incrementally higher TTL values until either a response is received from the remote host or a packet receives no response.

In the output, the first column is the hop number (that is, the TTL value set in the packet). The next three columns contain round-trip times for an attempt to reach the destination with that TTL value. Asterisks indicate that the intermediary did not reveal its name, IP address and other information. The last column contains the host name or the IP address of the responding system.

Ipconfig

Ipconfig on Windows and ifconfig on Unix based systems displays the current TCP/IP network configuration. Ipconfig /all returns more detailed information about current system network configuration information including physical address, IP address & subnet mask for each NIC, and default gateway among other information.

```
C:\Users\homeuser>ipconfig /?
```

USAGE:

```
ipconfig [/allcompartments] [/? | /all |  
/renew [adapter] | /release [adapter] |  
/renew6 [adapter] | /release6 [adapter] |  
/flushdns | /displaydns | /registerdns |  
/showclassid adapter |  
/setclassid adapter [classid] |
```

```
/showclassid6 adapter |  
/setclassid6 adapter [classid] ]
```

where

adapter Connection name
 (wildcard characters * and ? allowed, see examples)

Options:

```
/?            Display this help message  
/all          Display full configuration information.  
/release      Release the IPv4 address for the specified adapter.  
/release6     Release the IPv6 address for the specified adapter.  
/renew        Renew the IPv4 address for the specified adapter.  
/renew6       Renew the IPv6 address for the specified adapter.  
/flushdns     Purges the DNS Resolver cache.  
/registerdns   Refreshes all DHCP leases and re-registers DNS names  
/displaydns   Display the contents of the DNS Resolver Cache.  
/showclassid   Displays all the dhcp class IDs allowed for adapter.  
/setclassid    Modifies the dhcp class id.  
/showclassid6 Displays all the IPv6 DHCP class IDs allowed for adapter.  
/setclassid6   Modifies the IPv6 DHCP class id.
```

Examples:

```
> ipconfig                    ... Show information  
> ipconfig /all               ... Show detailed information
```

```
C:\Users\homeuser>ipconfig
```

Windows IP Configuration

Ethernet adapter Ethernet 2:

```
Media State . . . . . : Media disconnected  
Connection-specific DNS Suffix . :  
<snip>
```

```
C:\Users\homeuser>ipconfig /all
```

Windows IP Configuration

```
Host Name . . . . . : hostname  
<snip>
```

If ping to www.example.com times out, check the default gateway for the active interface in the output of ipconfig. If the default gateway is listed as 0.0.0.0 then your machine is not configured to reach your router which is causing the ping to fail.

Dynamic Host Control Protocol (DHCP) is a network protocol whose server dynamically assigns an IP address to a host on a network so it can communicate with other hosts. The router often is configured to run a DHCP server. DHCP decides which machine gets what IP address and for how long. The output of `ipconfig /all` shows how long the IP address lease is for. Following are DHCP related `ipconfig` switches.

- a. Release the current DHCP lease by running the following command.

`Ipconfig /release`

- b. Renew the DHCP lease by running the following command.

`Ipconfig /renew`

A DHCP lease is a guarantee that the Dynamic Host Control Protocol (DHCP) client computer will have the IP address supplied by the DHCP server for a specified period of time. In most cases, to avoid lease expiration, client usually sends a DHCP request for lease renewal to the server after 50% of the lease time has expired, and if 87.5% of its lease time has expired, the client sends a lease renewal request to all DHCP servers.

- c. Flush the arp cache. ARP handles the conversion of IP address to physical or Media Access Control (MAC) address of the network adapter. To improve performance, OS stores resolved addresses in the ARP cache for a short time. The cache is normally flushed regularly, but to force a flush, run,

`Arp -d`

To see the contents of arp cache, run,

`Arp -a`

Domain Name System (DNS) is a naming system for all hosts. A DNS server provides the IP address corresponding to a hostname like www.example.com.

`Ipconfig /displaydns` provides a record of domain names and IP addresses you've visited on a host.

`Ipconfig /flushdns` flushes the DNS cache. DNS responses are stored in a cache to speed up subsequent requests for the same host. `Flushdns` switch will force the host to query nameservers for the latest information. This can be used when there's a problem with the cache and you start getting a lot of HTTP 404 file not found error codes.

- d. Flush the DNS cache. DNS handles the conversion of domain names to IP addresses. To improve performance, Windows stores resolved domain names in the DNS cache. To solve problems caused by DNS cache entries that are obsolete or bad, clear the cache by running the command,

`Ipconfig /flushdns`

- e. Reregister the computer with the DNS server. This capability is useful if you're having trouble solving domain names or if you're having trouble with a dynamic DNS server.

Ipconfig /registerdns

Nslookup

Nslookup is used to help with any DNS problems. It can be used to find the IP address of a host, or domain name of an IP address.

```
C:\Users\homeuser>nslookup
```

```
Default Server: UnKnown
```

```
Address: fec0:0:0:ffff::1
```

```
> ?
```

```
Commands: (identifiers are shown in uppercase, [] means optional)
```

```
NAME          - print info about the host/domain NAME using default server
```

```
NAME1 NAME2   - as above, but use NAME2 as server
```

```
help or ?     - print info on common commands
```

```
set OPTION    - set an option
```

```
all           - print options, current server and host
```

```
[no]debug     - print debugging information
```

```
[no]d2        - print exhaustive debugging information
```

```
[no]defname   - append domain name to each query
```

```
[no]recurse   - ask for recursive answer to query
```

```
[no]search    - use domain search list
```

```
[no]vc        - always use a virtual circuit
```

```
domain=NAME   - set default domain name to NAME
```

```
srchlist=N1[/N2/.../N6] - set domain to N1 and search list to N1,N2, etc.
```

```
root=NAME     - set root server to NAME
```

```
retry=X       - set number of retries to X
```

```
timeout=X     - set initial time-out interval to X seconds
```

```
type=X        - set query type (ex. A,AAAA,A+AAAA,ANY,CNAME,MX,NS,PTR,SOA,SRV)
```

```
querytype=X   - same as type
```

```
class=X       - set query class (ex. IN (Internet), ANY)
```

```
[no]mxfr      - use MS fast zone transfer
```

```
ixfrver=X     - current version to use in IXFR transfer request
```

```
server NAME   - set default server to NAME, using current default server
```

```
lserver NAME  - set default server to NAME, using initial server
```

```
root          - set current default server to the root
```

```
ls [opt] DOMAIN [> FILE] - list addresses in DOMAIN (optional: output to FILE)
```

```
-a            - list canonical names and aliases
```

```
-d            - list all records
```

```
-t TYPE       - list records of the given RFC record type (ex. A,CNAME,MX,NS,PTR etc.)
```

```
view FILE     - sort an 'ls' output file and view it with pg
```

```
exit         - exit the program
```

```
> exit
```

```
C:\Users\homeuser>nslookup www.example.com  
Server: UnKnown  
Address: 192.168.0.1
```

```
Non-authoritative answer:  
Name: www.example.com  
Addresses: 2606:2800:220:1:248:1893:25c8:1946  
          93.184.216.34
```

Route

Route enables viewing or manipulating the network routing table (LMHOSTS).

```
C:\Users\homeuser>route -?
```

Manipulates network routing tables.

ROUTE [-f] [-p] [-4|-6] command [destination]
[MASK netmask] [gateway] [METRIC metric] [IF interface]

- f Clears the routing tables of all gateway entries. If this is used in conjunction with one of the commands, the tables are cleared prior to running the command.
- p When used with the ADD command, makes a route persistent across boots of the system. By default, routes are not preserved when the system is restarted. Ignored for all other commands, which always affect the appropriate persistent routes.
- 4 Force using IPv4.
- 6 Force using IPv6.

command One of these:

- PRINT Prints a route
- ADD Adds a route
- DELETE Deletes a route
- CHANGE Modifies an existing route

destination Specifies the host.

MASK Specifies that the next parameter is the 'netmask' value.

netmask Specifies a subnet mask value for this route entry.
If not specified, it defaults to 255.255.255.255.

gateway Specifies gateway.

interface the interface number for the specified route.

METRIC specifies the metric, ie. cost for the destination.

All symbolic names used for destination are looked up in the network database file NETWORKS. The symbolic names for gateway are looked up in the host name database file HOSTS.

If the command is PRINT or DELETE, destination or gateway can be a wildcard, (wildcard is specified as a star *), or the gateway argument may be omitted.

If Dest contains a * or ?, it is treated as a shell pattern, and only matching destination routes are printed. The '*' matches any string, and '?' matches any one char. Examples are: 157.*.1, 157.*, 127.*. Pattern match is only allowed in PRINT command.

Following are examples.

```
> route PRINT
> route PRINT -4
> route PRINT -6
> route PRINT 157*      .... Only prints those matching 157*
```

Net

Net enables you to view or update network information.

```
C:\Users\homeuser>net help
The syntax of this command is:
```

```
NET HELP
command
-or-
NET command /HELP
```

Commands available are:

NET ACCOUNTS	NET HELPMSG	NET STATISTICS
NET COMPUTER	NET LOCALGROUP	NET STOP
NET CONFIG	NET PAUSE	NET TIME
NET CONTINUE	NET SESSION	NET USE
NET FILE	NET SHARE	NET USER
NET GROUP	NET START	NET VIEW
NET HELP		

NET HELP NAMES explains different types of names in NET HELP syntax lines.
NET HELP SERVICES lists some of the services you can start.
NET HELP SYNTAX explains how to read NET HELP syntax lines.
NET HELP command | MORE displays Help one screen at a time.

```
C:\Users\homeuser>net help statistics
The syntax of this command is:
```

```
NET STATISTICS
[WORKSTATION]
```

NET STATISTICS displays the statistics log for the local Workstation service. Used without parameters, NET STATISTICS displays the services for which statistics are available.

WORKSTATION Displays the Workstation service statistics.

NET HELP command | MORE displays Help one screen at a time.

```
C:\Users\homeuser>net statistics
Statistics are available for the following running services:
<snip>
```

Netsh

Netsh enables you to review or update information about the networks you can access. Examples are,

```
C:\Users\homeuser>netsh help
C:\Users\homeuser>netsh show
```

Use the following commands to see Wi-Fi network information.

Netsh wlan show profiles displays a list of all Wi-Fi networks for which connections are stored on the PC.

Netsh wlan show profiles name="SSID" will display full details about a specific network.

Netsh wlan show settings displays the current global settings for all of the PCs Wi-Fi network connections.

```
C:\Users\homeuser>netsh wlan show profiles
```

Profiles on interface Wi-Fi:

Group policy profiles (read only)

```
-----
<None>
```

User profiles

```
-----
All User Profile    : WonderfulWiFi
```

Following are examples of netsh commands.

```
C:\Users\homeuser> netsh wlan ?
```

The following commands are available:

```
<snip>
```

```
C:\Users\homeuser> netsh wlan show ?
```

```
C:\Users\homeuser>netsh wlan show interfaces
```

```
C:\Users\homeuser>netsh wlan show networks
```

```
C:\Users\homeuser>netsh wlan show profiles name=WonderfulWiFi
```

```
C:\Users\homeuser>netsh wlan show settings
```

```
C:\Users\homeuser>netsh wlan show drivers
```

Additionally, netsh commands include options and information in the context of several technologies including IPsec, Remote access, Windows Firewall, DHCP, DNS, and wired & wireless networks.

```
C:\Users\homeuser>netsh  
netsh>?
```

The following commands are available:

Commands in this context:

```
..      - Goes up one context level.  
?       - Displays a list of commands.  
abort   - Discards changes made while in offline mode.  
add     - Adds a configuration entry to a list of entries.  
<snip>
```

2.3 System Management

System management tools enable you to monitor system performance, shutdown, restart, change system date and time and modify the windows system management instrumentation (WMI) interface. Some of these commands may need administrative privileges. In addition to the following commands, Appendix A has a list of Management Console snap-ins. Appendix B has a brief introduction to Powershell including information on retrieving logs. Finally, Appendix C has information on troubleshooting problems on Windows.

Command line system management tools include the following.

Command	Description
Bcdedit	Displays or modifies the boot manager startup parameters
Chcp	Displays or changes the number of active console code pages
Date	Displays or sets the system date
Eventcreate	Creates a custom event in the event log
Reg	Adds, modifies, displays and deletes registry keys and settings
Regvr32	Register dynamically linked libraries (DLL) files as command components in the registry
Shutdown	Shuts down or restarts computer
Systeminfo	Displays detailed configuration info

Time	Display or set the system time
Typeperf	Monitors a performance counter
Whoami	Displays information about the current user
Wmic	Operates windows system management instrumentation (WMI) interface
Powercfg	Configure power options

Following are examples of these commands.

```
C:\Users\homeuser>date
The current date is: Mon 09/13/2021
Enter the new date: (mm-dd-yy)
```

```
C:\Users\homeuser>time
The current time is: 12:58:22.29
Enter the new time:
```

```
C:\Users\homeuser>date /?
Displays or sets the date.
```

DATE [/T | date]

Type DATE without parameters to display the current date setting and a prompt for a new one. Press ENTER to keep the same date.

If Command Extensions are enabled the DATE command supports the /T switch which tells the command to just output the current date, without prompting for a new date.

```
C:\Users\homeuser>time /?
Displays or sets the system time.
```

TIME [/T | time]

Type TIME with no parameters to display the current time setting and a prompt for a new one. Press ENTER to keep the same time.

If Command Extensions are enabled the TIME command supports the /T switch which tells the command to just output the current time, without prompting for a new time.

Systeminfo: returning system configuration data

```
C:\Users\homeuser>systeminfo /?
```

SYSTEMINFO [/S system [/U username [/P [password]]]] [/FO format] [/NH]

Description:

This tool displays operating system configuration information for a local or remote machine, including service pack levels.

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.

/FO format Specifies the format in which the output is to be displayed.
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 message.

Examples:

```
SYSTEMINFO
SYSTEMINFO /?
SYSTEMINFO /S system
SYSTEMINFO /U user
SYSTEMINFO /FO LIST
```

```
C:\Users\homeuser>systeminfo
```

```
Host Name:          <snip>
OS Name:            Microsoft Windows 10 Home
OS Version:         <snip>
OS Manufacturer:   Microsoft Corporation
OS Configuration:  Standalone Workstation
<snip>
```

```
C:\Users\homeuser>systeminfo > sysinfo.txt
C:\Users\homeuser>more sysinfo.txt
C:\Users\homeuser>systeminfo | more
```

Whoami: getting information about the current user

```
C:\Users\homeuser>whoami
hostname\homeuser
```


C:\Users\homeuser>whoami /?

WhoAml has three ways of working:

Syntax 1:

WHOAMI [/UPN | /FQDN | /LOGONID]

Syntax 2:

WHOAMI { [/USER] [/GROUPS] [/CLAIMS] [/PRIV] } [/FO format] [/NH]

Syntax 3:

WHOAMI /ALL [/FO format] [/NH]

Description:

This utility can be used to get user name and group information along with the respective security identifiers (SID), claims, privileges, logon identifier (logon ID) for the current user on the local system. I.e. who is the current logged on user? If no switch is specified, tool displays the user name in NTLM format (domain\username).

Parameter List:

/UPN Displays the user name in User Principal Name (UPN) format.

/FQDN Displays the user name in Fully Qualified Distinguished Name (FQDN) format.

/USER Displays information on the current user along with the security identifier (SID).

/GROUPS Displays group membership for current user, type of account, security identifiers (SID) and attributes.

/CLAIMS Displays claims for current user, including claim name, flags, type and values.

/PRIV Displays security privileges of the current user.

/LOGONID Displays the logon ID of the current user.

/ALL Displays the current user name, groups belonged to along with the security identifiers (SID), claims and privileges for the current user access token.

`/FO` `format` Specifies the output format to be displayed.
Valid values are TABLE, LIST, CSV.
Column headings are not displayed with CSV
format. Default format is TABLE.

`/NH` Specifies that the column header should not
be displayed in the output. This is
valid only for TABLE and CSV formats.

`/?` Displays this help message.

Examples:

WHOAMI
WHOAMI /UPN
WHOAMI /FQDN
WHOAMI /LOGONID
WHOAMI /USER
WHOAMI /USER /FO LIST
WHOAMI /GROUPS
WHOAMI /GROUPS /FO CSV /NH
WHOAMI /CLAIMS
WHOAMI /CLAIMS /FO LIST
WHOAMI /PRIV
WHOAMI /PRIV /FO TABLE
WHOAMI /USER /GROUPS
WHOAMI /USER /GROUPS /CLAIMS /PRIV
WHOAMI /ALL
WHOAMI /ALL /FO LIST
WHOAMI /ALL /FO CSV /NH
WHOAMI /?

C:\Users\homeuser>whoami /all

C:\Users\homeuser>whoami /all /fo list > whoami.txt

C:\Users\homeuser>more whoami.txt

Reg: working with registry keys and settings

Windows registry is a database in which Windows and application programs store hardware and software configuration settings, setup information, last viewed files and other information. It holds information about installed program components and subcomponents like Dynamically Linked Libraries (DLLs). It stores information about file types and applications that create and use them (like launch Word when a doc file is clicked). Registry information is set and read by applications, services, device drivers and other sub-systems.

C:\Users\homeuser>reg /?

REG Operation [Parameter List]

Operation [QUERY | ADD | DELETE | COPY | SAVE | LOAD | UNLOAD | RESTORE |
COMPARE | EXPORT | IMPORT | FLAGS]

Return Code: (Except for REG COMPARE)

0 - Successful
1 - Failed

For help on a specific operation type:

REG Operation /?

Examples:

REG QUERY /?
REG ADD /?
REG DELETE /?
REG COPY /?
REG SAVE /?
REG RESTORE /?
REG LOAD /?
REG UNLOAD /?
REG COMPARE /?
REG EXPORT /?
REG IMPORT /?
REG FLAGS /?

C:\Users\homeuser>reg query /?

REG QUERY KeyName [/v [ValueName] | /ve] [/s]
[/f Data [/k] [/d] [/c] [/e]] [/t Type] [/z] [/se Separator]
[/reg:32 | /reg:64]

KeyName [\[\\Machine\\]FullKey](#)

Machine - Name of remote machine, omitting defaults to the
current machine. Only HKLM and HKU are available on
remote machines

FullKey - in the form of ROOTKEY\SubKey name

ROOTKEY - [HKLM | HKCU | HKCR | HKU | HKCC]

SubKey - The full name of a registry key under the
selected ROOTKEY

/v Queries for a specific registry key values.
If omitted, all values for the key are queried.

Argument to this switch can be optional only when specified
along with /f switch. This specifies to search in valuenames only.

- `/ve` Queries for the default value or empty value name (Default).
- `/s` Queries all subkeys and values recursively (like `dir /s`).
- `/se` Specifies the separator (length of 1 character only) in data string for `REG_MULTI_SZ`. Defaults to `"\0"` as the separator.
- `/f` Specifies the data or pattern to search for.
Use double quotes if a string contains spaces. Default is `"*"`.
- `/k` Specifies to search in key names only.
- `/d` Specifies the search in data only.
- `/c` Specifies that the search is case sensitive.
The default search is case insensitive.
- `/e` Specifies to return only exact matches.
By default all the matches are returned.
- `/t` Specifies registry value data type.
Valid types are:
REG_SZ, REG_MULTI_SZ, REG_EXPAND_SZ,
REG_DWORD, REG_QWORD, REG_BINARY, REG_NONE
Defaults to all types.
- `/z` Verbose: Shows the numeric equivalent for the type of the valuenam.
- `/reg:32` Specifies the key should be accessed using the 32-bit registry view.
- `/reg:64` Specifies the key should be accessed using the 64-bit registry view.

Examples:

```
REG QUERY HKLM\Software\Microsoft\ResKit /v Version
Displays the value of the registry value Version
```

Shutdown: shutdown or restart the system

You could use the shutdown command to restart or shutdown your computer.

```
C:\Users\homeuser>shutdown /?
Usage: shutdown [/i | /l | /s | /sg | /r | /g | /a | /p | /h | /e | /o] [/hybrid] [/soft] [/fw] [/f]
[/m \computer\\[/t xxx\][/d [p|u:]xx:yy [/c "comment"]]
```

No args Display help. This is the same as typing `/?`.

/? Display help. This is the same as not typing any options.

/i Display the graphical user interface (GUI).
This must be the first option.

/l Log off. This cannot be used with /m or /d options.

/s Shutdown the computer.

/sg Shutdown the computer. On the next boot, if Automatic Restart Sign-On is enabled, automatically sign in and lock last interactive user.
After sign in, restart any registered applications.

/r Full shutdown and restart the computer.

/g Full shutdown and restart the computer. After the system is rebooted, if Automatic Restart Sign-On is enabled, automatically sign in and lock last interactive user.
After sign in, restart any registered applications.

/a Abort a system shutdown.
This can only be used during the time-out period.
Combine with /fw to clear any pending boots to firmware.

/p Turn off the local computer with no time-out or warning.
Can be used with /d and /f options.

/h Hibernate the local computer.
Can be used with the /f option.

/hybrid Performs a shutdown of the computer and prepares it for fast startup.
Must be used with /s option.

/fw Combine with a shutdown option to cause the next boot to go to the firmware user interface.

/e Document the reason for an unexpected shutdown of a computer.

/o Go to the advanced boot options menu and restart the computer.
Must be used with /r option.

/m [\\computer Specify the target computer.](#)

/t xxx Set the time-out period before shutdown to xxx seconds.
The valid range is 0-315360000 (10 years), with a default of 30.
If the timeout period is greater than 0, the /f parameter is implied.

/c "comment" Comment on the reason for the restart or shutdown.
Maximum of 512 characters allowed.

/f Force running applications to close without forewarning users.
The /f parameter is implied when a value greater than 0 is specified for the /t parameter.

/d [p|u:]xx:yy Provide the reason for the restart or shutdown.
p indicates that the restart or shutdown is planned.
u indicates that the reason is user defined.
If neither p nor u is specified the restart or shutdown is unplanned.
xx is the major reason number (positive integer less than 256).
yy is the minor reason number (positive integer less than 65536).

Reasons on this computer:

(E = Expected U = Unexpected P = planned, C = customer defined)

Type Major Minor Title

```

U   0   0   Other (Unplanned)
E P   0   0   Other (Planned)
U   0   5   Other Failure: System Unresponsive
E   1   1   Hardware: Maintenance (Unplanned)
U   5   15  System Failure: Stop error
U   6   11  Power Failure: Cord Unplugged
U   6   12  Power Failure: Environment
P   7   0   Legacy API shutdown
<snip>

```

For example to restart the computer immediately, (/r restarts the computer; /t specifies the number of seconds after which the computer is shut down).

Shutdown /r /t 0

If you've launched a restart or shutdown using some nonzero value for /T and you need to cancel the pending shutdown, run shutdown with the /A switch before the timeout interval is over.

Shutdown /a

Typeperf: monitor performance

Typeperf writes performance data to the command window or to a log file. To stop Typeperf, press CTRL+C.

```
C:\Users\homeuser>typeperf /?
```

Usage:

```
typeperf { <counter [counter ...]> | -cf <filename> | -q [object] | -qx [object] } [options]
```

Parameters:

```
<counter [counter ...]>    Performance counters to monitor.
```

Options:

```

-?                Displays context sensitive help.
-f <CSV|TSV|BIN|SQL>  Output file format. Default is CSV.
-cf <filename>      File containing performance counters to monitor, one per line.
-si <[[hh:]mm:]ss>   Time between samples. Default is 1 second.
-o <filename>        Path of output file or SQL database. Default is STDOUT.
-q [object]          List installed counters (no instances). To list counters for one object,
                     include the object name, such as Processor.
-qx [object]          List installed counters with instances. To list counters for one object,
                     include the object name, such as Processor.
-sc <samples>         Number of samples to collect. Default is to sample until CTRL+C.
-config <filename>    Settings file containing command options.
-s <computer_name>    Server to monitor if no server is specified in the counter path.
-y                  Answer yes to all questions without prompting.

```

Note:

Counter is the full name of a performance counter in "[\\<Computer>\<Object>\(<Instance>\)\<Counter>](#)" format, such as "[\\Server1\Processor\(0\)\% User Time](#)".

Examples:

```
typeperf "\Processor(_Total)\% Processor Time"  
typeperf -qx PhysicalDisk -o counters.txt
```

```
C:\Users\homeuser> typeperf "\Processor(_Total)\% Processor Time"
```

Most counter paths use one of the following two formats:

```
\Object\Counter  
\Object(Instance)\Counter
```

For example, here's a typeperf command that displays 5 samples of the available memory counter .

```
C:\Users\homeuser>typeperf "\Memory\Available Mbytes" -sc 5
```

As another example, here's a typeperf command that displays 5 samples of the first processor instance counter every 3 seconds and saves the results to a file named processor.txt

```
C:\Users\homeuser>typeperf "\Processor(0)\% Processor Time" -sc 5 -si 3 -o processor.txt
```

The command completed successfully.

```
C:\Users\homeuser>more processor.txt
```

Wmic

Wmic operates windows system management instrumentation (WMI) interface.

Use the following commands to get help.

```
Wmic /?
```

```
Wmic process /?
```

```
Wmic process list /?
```

Use the following command to list a summary of processes.

```
C:\Users\homeuser>wmic process list brief
```

```
HandleCount Name Priority ProcessId ThreadCount WorkingSetSize  
<snip>
```

Powercfg

Powercfg enables users to control power settings on a system.

```
C:\Users\homeuser>powercfg /?
```

```
POWERCFG /COMMAND [ARGUMENTS]
```

Description:

Enables users to control power settings on a local system.

For detailed command and option information, run "POWERCFG /? <COMMAND>"

Command List:

/LIST, /L Lists all power schemes.

/QUERY, /Q Displays the contents of a power scheme.

/CHANGE, /X Modifies a setting value in the current power scheme.

/CHANGENAME Modifies the name and description of a power scheme.

/DUPLICATEScheme Duplicates a power scheme.

/DELETE, /D Deletes a power scheme.

/DELETESetting Deletes a power setting.

/SETACTIVE, /S Makes a power scheme active on the system.

/GETACTIVEScheme Retrieves the currently active power scheme.

/SETACVALUEINDEX Sets the value associated with a power setting while the system is powered by AC power.

/SETDCVALUEINDEX Sets the value associated with a power setting while the system is powered by DC power.

/IMPORT Imports all power settings from a file.

/EXPORT Exports a power scheme to a file.

/ALIASES Displays all aliases and their corresponding GUIDs.

/GETSECURITYDESCRIPTOR
Gets a security descriptor associated with a specified power setting, power scheme, or action.

/SETSECURITYDESCRIPTOR
Sets a security descriptor associated with a power setting, power scheme, or action.

/HIBERNATE, /H Enables and disables the hibernate feature.

/AVAILABLESLEEPSTATES, /A

Reports the sleep states available on the system.

`/DEVICEQUERY` Returns a list of devices that meet specified criteria.

`/DEVICEENABLEWAKE` Enables a device to wake the system from a sleep state.

`/DEVICEDISABLEWAKE` Disables a device from waking the system from a sleep state.

`/LASTWAKE` Reports information about what woke the system from the last sleep transition.

`/WAKETIMERS` Enumerates active wake timers.

`/REQUESTS` Enumerates application and driver Power Requests.

`/REQUESTSOVERRIDE` Sets a Power Request override for a particular Process, Service, or Driver.

`/ENERGY` Analyzes the system for common energy-efficiency and battery life problems.

`/BATTERYREPORT` Generates a report of battery usage.

`/SLEEPSTUDY` Generates a diagnostic system power transition report.

`/SRUMUTIL` Dumps Energy Estimation data from System Resource Usage Monitor (SRUM).

`/SYSTEMSLEEPDIAGNOSTICS`
Generates a diagnostic report of system sleep transitions.

`/SYSTEMPOWERREPORT` Generates a diagnostic system power transition report.

`/POWERTHROTTLING` Control power throttling for an application.

```
C:\Users\homeuser>powercfg /batteryreport
Battery life report saved to file path C:\Users\homeuser\battery-report.html.
```

```
C:\Users\homeuser>powercfg /batteryreport /?
POWERCFG /BATTERYREPORT [/OUTPUT <FILENAME>] [/XML] [/TRANSFORMXML <FILENAME.XML>]
```

Description:

Generates a report of battery usage characteristics over the lifetime of the system. The `BATTERYREPORT` command will generate an HTML report file in the current path.

Parameter List:

/OUTPUT <FILENAME> Specify the path and filename to store the battery report HTML or XML file.

/XML Format the report file as XML.

/DURATION <DAYS> Specify the number of days to analyze for the report.

/TRANSFORMXML <FILENAME.XML> Reformat an XML report file as HTML.

Examples:

```
POWERCFG /BATTERYREPORT
```

```
POWERCFG /BATTERYREPORT /OUTPUT "batteryreport.html"
```

```
POWERCFG /BATTERYREPORT /OUTPUT "batteryreport.xml" /XML
```

```
POWERCFG /BATTERYREPORT /TRANSFORMXML "batteryreport.xml"
```

```
POWERCFG /BATTERYREPORT /TRANSFORMXML "batteryreport.xml" /OUTPUT "batteryreport.html"
```

Tasklist

Tasklist displays a list of currently running processes on a machine.

```
C:\Users\homeuser>tasklist /?
```

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

Description:

This tool displays a list of currently running processes on either a local or remote machine.

```
C:\Users\homeuser>tasklist
```

```
Image Name          PID Session Name    Session#  Mem Usage  
=====
```

<snip>

2.3.1 Disk Management

Windows CLI Disk Management Tools include the following commands.

Command	Description
Chkdsk	Checks a specified volume for errors
Chkntfs	Configures automatic disk checking
Convert	Converts a specific volume to a different file system
Defrag	Defragments a specified volume

Diskpart	Enables you to list, create, select, delete and extend disk partitions
Expand	Extracts one or more files from a compressed file such as, a .cab file found on some installation discs
Format	Formats the specified volume
Fsutil	Performs a number of file system tasks
Label	Changes or deletes the name of a specified volume
Mountvol	Creates, displays or deletes a mount point
Vol	Displays the name and serial number of a specified volume

Chkdsk

Checks a disk and displays a status report.

```
C:\Users\homeuser>chkdsk /?
Chkdsk [volume [filename]] [/F] [/V] [/R] [/B] [/X] [/I] [/C] [/L:[Size]] [/scan]
[/forceofflinefix] [/perf] [/spotfix] [/freeorphanedchains] [/markclean] [/offlinescanandfix]
<snip>
```

Example: chkdsk C:

```
C:\WINDOWS\system32>chkdsk
The type of the file system is NTFS.
Volume label is Windows.
```

```
WARNING! /F parameter not specified.
Running CHKDSK in read-only mode.
<snip>
```

Diskpart

Enables you to list, create, select, delete and extend disk partitions

```
C:\WINDOWS\system32>diskpart /?
```

```
Microsoft DiskPart version X
```

```
Copyright (C) Microsoft Corporation.
On computer: <snip>
```

```
Microsoft DiskPart syntax:
    diskpart [/s <script>] [/?]
```

/s <script> - Use a DiskPart script.

/? - Show this help screen.

C:\WINDOWS\system32>diskpart

Microsoft DiskPart version X

Copyright (C) Microsoft Corporation.
On computer: <snip>

DISKPART> help

Microsoft DiskPart version X

ACTIVE - Mark the selected partition as active.
ADD - Add a mirror to a simple volume.
ASSIGN - Assign a drive letter or mount point to the selected volume.
ATTRIBUTES - Manipulate volume or disk attributes.
ATTACH - Attaches a virtual disk file.
AUTOMOUNT - Enable and disable automatic mounting of basic volumes.
BREAK - Break a mirror set.
CLEAN - Clear the configuration information, or all information, off the disk.
COMPACT - Attempts to reduce the physical size of the file.
CONVERT - Convert between different disk formats.
CREATE - Create a volume, partition or virtual disk.
DELETE - Delete an object.
DETAIL - Provide details about an object.
DETACH - Detaches a virtual disk file.
EXIT - Exit DiskPart.
EXTEND - Extend a volume.
EXPAND - Expands the maximum size available on a virtual disk.
FILESYSTEMS - Display current and supported file systems on the volume.
FORMAT - Format the volume or partition.
GPT - Assign attributes to the selected GPT partition.
HELP - Display a list of commands.
IMPORT - Import a disk group.
INACTIVE - Mark the selected partition as inactive.
LIST - Display a list of objects.
MERGE - Merges a child disk with its parents.
ONLINE - Online an object that is currently marked as offline.
OFFLINE - Offline an object that is currently marked as online.
RECOVER - Refreshes the state of all disks in the selected pack.
Attempts recovery on disks in the invalid pack, and resynchronizes mirrored volumes and RAID5 volumes that have stale plex or parity data.
REM - Does nothing. This is used to comment scripts.
REMOVE - Remove a drive letter or mount point assignment.
REPAIR - Repair a RAID-5 volume with a failed member.

RESCAN - Rescan the computer looking for disks and volumes.
 RETAIN - Place a retained partition under a simple volume.
 SAN - Display or set the SAN policy for the currently booted OS.
 SELECT - Shift the focus to an object.
 SETID - Change the partition type.
 SHRINK - Reduce the size of the selected volume.
 UNIQUEID - Displays or sets the GUID partition table (GPT) identifier or master boot record (MBR) signature of a disk.

DISKPART> list

Microsoft DiskPart version X

DISK - Display a list of disks. For example, LIST DISK.
 PARTITION - Display a list of partitions on the selected disk.
 For example, LIST PARTITION.
 VOLUME - Display a list of volumes. For example, LIST VOLUME.
 VDISK - Displays a list of virtual disks.

DISKPART> list disk

DISKPART> list volume

Volume ###	Ltr	Label	Fs	Type	Size	Status	Info

<snip>							

DISKPART> list vdisk

There are no virtual disks to show.

DISKPART>

C:\WINDOWS\system32>fsutil

---- Commands Supported ----

8dot3name	8dot3name management
behavior	Control file system behavior
dax	Dax volume management
dirty	Manage volume dirty bit
file	File specific commands
fsInfo	File system information
hardlink	Hardlink management
objectID	Object ID management
quota	Quota management
repair	Self healing management
reparsePoint	Reparse point management
storageReserve	Storage Reserve management
resource	Transactional Resource Manager management

sparse	Sparse file control
tiering	Storage tiering property management
transaction	Transaction management
usn	USN management
volume	Volume management
wim	Transparent wim hosting management

```
C:\WINDOWS\system32>fsutil fsinfo
---- FSINFO Commands Supported ----
```

drives	List all drives
driveType	Query drive type for a drive
ntfsInfo	Query NTFS specific volume information
refInfo	Query REFS specific volume information
sectorInfo	Query sector information
statistics	Query file system statistics
volumeInfo	Query volume information

```
C:\WINDOWS\system32>fsutil fsinfo drives
```

```
Drives: C:\ D:\ E:\
```

```
C:\WINDOWS\system32>fsutil fsinfo drivetype C:
C: - Fixed Drive
```

Several of the following commands require administrative privileges or you'll get an error message saying access is denied.

```
C:\WINDOWS\system32>fsutil fsinfo ntfsinfo C:
```

```
C:\WINDOWS\system32>fsutil fsinfo sectorinfo C:
```

```
C:\WINDOWS\system32>fsutil fsinfo statistics C:
```

```
C:\WINDOWS\system32>fsutil fsinfo volumeinfo C:
```

Additional tools include Chkntfs for scheduling automatic disk checks, and defrag for defragmenting the system drive.

2.3.2 Users, Groups, and Shares

You can script your user and group tasks using the net user and net localgroup commands. These commands enable you to add users, change passwords, modify accounts, add users to groups and remove users from groups. You must run these commands as administrator.

Net user: working with users

You could use net user command to add users, set account passwords, disable accounts, set account options (such as times of the day the user is allowed to log on) or remove accounts of local users.

```
C:\Users\homeuser>net user /?
```

The syntax of this command is:

NET USER

```
[username [password | *] [options]] [/DOMAIN]
    username {password | *} /ADD [options] [/DOMAIN]
    username [/DELETE] [/DOMAIN]
    username [/TIMES:{times | ALL}]
    username [/ACTIVE: {YES | NO}]
```

/Times:{times | ALL} specifies the times that the user is allowed to log on to the system. Use single days or day ranges. For times use 24-hour notation or 12 hour notation with am or pm. Separate the day and time with comma, and separate day/time combinations with semicolons. Here are some examples:

M-F,9am-5pm

M,W,F,08:00-13:00

Sa,12pm-6pm;Su,1pm-5pm

If you execute net user without any parameters, it displays a list of local user accounts:

```
C:\Users\homeuser>net user
```

Net localgroup: working with groups

You could use net localgroup command to add users to or remove users from a specific security group.

```
C:\Users\homeuser>net localgroup /?
```

The syntax of this command is:

NET LOCALGROUP

```
[groupname [/COMMENT:"text"]] [/DOMAIN]
    groupname {/ADD [/COMMENT:"text"] | /DELETE} [/DOMAIN]
    groupname name [...] {/ADD | /DELETE} [/DOMAIN]
```

To list groups use the following command.

```
C:\Users\homeuser>net localgroup
```

Aliases for [\\machinename](#)

```
-----
*Administrators
*Distributed COM Users
*Event Log Readers
*Guests
*Hyper-V Administrators
*IIS_IUSRS
*Performance Log Users
```

- *Performance Monitor Users
- *Remote Management Users
- *System Managed Accounts Group
- *Users

The command completed successfully.

To list users, use the following command.
C:\Users\homeuser>net localgroup users

To list administrators, use the following command.
C:\Users\homeuser>net localgroup administrators

Net use: mapping folders

You could map a network folder to a local drive by using the net use command.

C:\Users\homeuser>net use
New connections will be remembered.

There are no entries in the list.

C:\Users\homeuser>net use /?
The syntax of this command is:

NET USE

[devicename | *] [[\\computername\sharename\volume](#)] [password | *]
[/USER:[domainname\]username]
[/USER:[dotted domain name\]username]
[/USER:[username@dotted domain name]
[/SMARTCARD]
[/SAVECRED]
[/REQUIREINTEGRITY]
[/REQUIREPRIVACY]
[/WRITETHROUGH]
[[/DELETE] | [/PERSISTENT:{YES | NO}]]

NET USE {devicename | *} [password | *] /HOME

NET USE [/PERSISTENT:{YES | NO}]

For example the following command maps the shared folder [\\Test\Example](#) to Z: drive. /persistent switch enables you to reconnect the mapped network drive the next time you log on when you add yes.
Net use z: [\\Test\Example](#) /persistent:yes

Chapter 3 Administration of PC

Best practices for PC administration include protecting your computer with a password, backing up data regularly, and enabling automatic system updates or manually keeping the system up-to-date.

Windows 10 comes with four security features enabled by default and it is a good practice to make sure that these are effective and turned on:

1. Windows defender protects your computer against spyware in real-time by scanning files regularly. It should be on.
2. Windows firewall blocks unauthorized attempts to send data to your computer. It should be on.
3. User Account Control is first line of defense against unwanted system changes. It is on by default and the default setting is to notify when changes are being made to the PC.
4. Admin account may be disabled. It is highly recommended that you use a standard user account as opposed to the admin account for day-to-day work like email and browsing.

Anti-malware features

Windows SmartScreen

SmartScreen is an online service that checks incoming e-mails and downloads against white- and black-lists of known phishing sites and malware payloads, and if it finds something that's known to be malicious, it blocks it.

Windows Defender

Defender is the free included antivirus package for Windows. As a basic package, it's promoted as being effective and lightweight with almost no negative effect on performance or boot time.

Firewall

Firewall examines network traffic that is attempting to make its way across a network interface and onto the computer. A firewall blocks unwanted traffic. Depending on the settings configured, the firewall software can block or allow any traffic. An incorrectly configured firewall or a computer without a personal firewall is vulnerable to remote connections to the local system services. Only allowed traffic should gain access to internal resources.

Windows comes with two different firewall interfaces: the default windows firewall and windows firewall with advanced security. Users with admin privileges can configure advanced settings by typing "wf.msc" into the taskbar search box or by running it from the command line using the "wf" command. Inbound rules, outbound rules, connection security rules, and monitoring can be configured. Windows firewall with advanced security allows low-level packet filtering and refining of network traffic, such as the ability to filter by source or destination IP addresses, port numbers and protocol types, such as TCP or UDP (for Transmission Control Protocol and User Datagram Protocol respectively).

User Account control (UAC)

UAC is a security subsystem that acts as the first line of defense against any malicious software installations or unwanted OS system changes. It is accessed through the Security Center or by searching

for "UAC" in the taskbar search box. Any user wanting to change UAC settings will first have to have admin permissions.

UAC displays an alert dialog in the secure Windows environment that's used to display the sign-in dialog. In this special environment, nothing can be done with the OS except interact with the single dialog that's displayed, and only the user can do that as all background processes are suspended.

There are four separate settings for UAC that begin at Never notify which will turn UAC off completely through to Always notify, which can be annoying. The default setting is to notify when changes are being made to the PC that will affect all or other users on the machine, which include disabling features, installing an app, and accessing the core system folder, but not changes that would affect your own account such as setting the correct time.

Even as an admin, Windows will still use the UAC prompt to make you aware that your intended action will perform a task that will have system-wide impact. Although as an admin, you'll not have to provide your credentials, you do have to provide consent. There are two types of elevation prompts:

Consent: only shown to admins for approval

Credential: shown to standard users when they attempt to perform an administrative task

Examples of cases when a standard user would be prompted by UAC for the elevation of admin privileges include installing new software.

3.1 Defending yourself

Choose passwords thoughtfully so no one can guess them or use a tool to manage them. A phrase of several words that includes upper and lower case letters, numbers and special characters is a decent compromise between safety and ease of use. Never use the same password for critical sites like paying bills as you do for throwaways like online news. Never use the same password at work as you do for personal accounts. Don't use single site like Google for signing into other sites as it can be a single point of failure if something goes wrong and you'll be giving away information about yourself. Password managers like LastPass make password management easy. They generate and store safe random passwords for all your sites, and you only have to remember one master password. Use two-factor authentication if it's available. Two-factor authentication requires both a password and an additional mechanism like a one-time-code received over phone for authentication. Always use passwords to lock your devices and change the default password of all devices.

Use anti-virus software and keep software like browsers and operating system up-to-date. Don't click on popups that you did not initiate. Backup your information to a safe local drive regularly.

Don't open attachments from strangers and unexpected attachments in email from anyone. Never automatically accept, click or install anything when prompted. Be wary about downloading and installing software unless it comes from a trusted source. This is true for your phone as well as for your computer. Do not share sensitive information like credit card details over email unless encryption or password protection is used. Keep your personal and work emails separate.

Don't do anything important at places that offer open Wi-Fi, like, don't do online payments at Starbucks. Make sure that connections use HTTPS, but don't forget that HTTPS only encrypts the contents. Someone listening can still find out information about the site you are visiting and other meta-data.

A partial list of settings for better privacy include using a local account as opposed to an online account, using local storage as opposed to cloud storage, and using standard apps as opposed to modern apps as modern apps perform additional recording and tracking; turning off the laptop's Wi-Fi when Internet

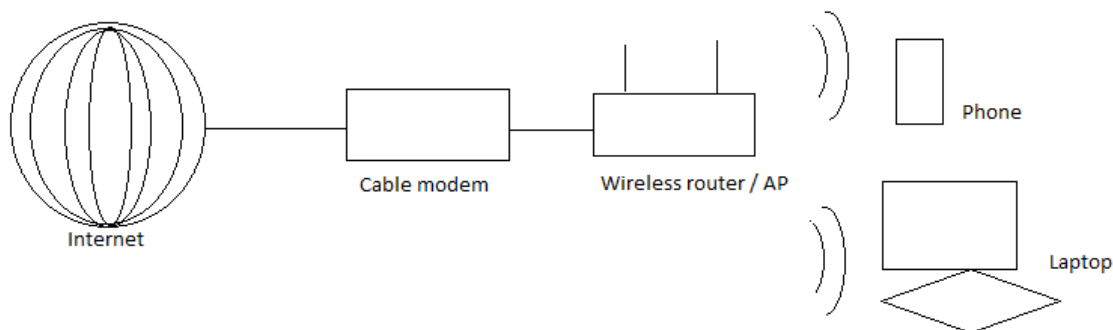
connectivity is not needed, and destroying data before disposing off old devices. An example of a search engine that does not maintain search logs is duckduckgo.com. Additionally, third party cookies should be turned off in browsers.

Finally, a partial list of general best practices include never giving credit card information over email, making sure HTTPS is being used when providing account information, exercising caution before installing programs or downloading files sent as attachments in email, not clicking links from unknown sources, not entering personal information in unsolicited popup windows, not posting sensitive information on social media sites and being careful about who you connect with on social media.

Sec 3.1 adapted from Windows 10 in depth, Knittel, McFedries; Understanding the digital world, Kernighan

Chapter 4 Residential Networking

The Internet Service Provider (ISP) typically provides one external facing (Internet Protocol) IP address to residential customers. In the example illustrated here, connection is delivered to the home over coaxial cable that goes into a cable modem. A cable modem is a type of network bridge (described in Chapter 5) that provides bi-directional data communication over coaxial cable. It is primarily used to deliver broadband internet access in the form of cable internet which uses the same infrastructure as a cable television. This infrastructure provides network edge connectivity or last mile access from the internet service provider to the home.



The Ethernet connection from the cable modem is often connected to a wireless Access Point (AP) and wireless router combination device which provides a bridge between the ISP's wired network and the home's internal wireless Local Area Network (LAN). A physical cable (typically Cat6) ties the AP to the wired network provided by the ISP. There are devices that combine the modem, router and AP functionalities into one device.

The wireless router typically runs the Dynamic Host Control Protocol (DHCP) server to allocate private IP addresses to devices on the internal wireless LAN. Additionally the router employs Network Address Translation (NAT) so multiple internal devices could share the single external facing IP address provided by the ISP to communicate on the Internet. NAT does this by maintaining a table of private IP address and port number mapping to public IP address and port number for all connections. NAT translates an internal IP address and port number to a public IP address and port number before a packet leaves the local network to determine where to send back the responses from outside. The router running NAT mediates all connections between devices on the internal LAN and the Internet.

Your home laptop would typically have at least two Network Interface Cards (NICs), one for wireless LAN connectivity and the second for wireline LAN connection. Each NIC comes with its unique MAC address. Cable modem is a layer 2 bridge and has a MAC address of its own. Cable modem adheres to the Data over Cable Service Interface Specification (DOCSIS). It carries signals over a broadband cable that also carries cable TV signal. Contrary to broadband, baseband refers to a cabling technology that can carry only one type of signal.

The ISP usually provides the DNS server information which can be overridden. The router's default password should be changed. The firewall on the router should be turned on. Many routers have a built-

in Stateful Packet Inspection (SPI) firewall that does dynamic packet filtering. The firewall on the laptop should also be turned on in addition to the firewall on the router.

Wi-Fi network is configured on the AP and is identified by a Service Set Identifier (SSID). The devices that connect to the Wi-Fi use 802.11 wireless LAN connectivity protocol. These devices use the SSID to identify what wireless data traffic is allowed to connect to the network. SSID is the wireless Service Set Identifier which enables the client to join the wireless network. The AP uses the SSID to determine whether the client is to become a member of the wireless network which is confirmed after providing the Wi-Fi password for a protected Wi-Fi connection. The term association is used to describe a wireless connection that is made. The wrong SSID prevents an association keeping the client from being able to become a member of the wireless LAN network.

The AP/wireless router device has a MAC address of its own and it often serves as the default gateway. The AP uses an association to build a table of clients on the wireless network. This association table lists the MAC addresses of each networking device connected to the wireless network. The wireless client adapter can also notify the user whether the client has lost an association with the AP.

With wireless LANs, there is the notion of maximum distance the signal can be transmitted to. Many obstacles can reflect and attenuate wireless signals causing reception to suffer. Signal level for mobile users is hampered by increased distance from the AP. It is important to determine an appropriate location for placing the AP for providing maximum radio frequency coverage for wireless clients. The farther the signal travels, the weaker it gets. Signal travels better in air than through solid materials. Wireless signal interference can be caused by the following.

- 1) Building construction materials absorb or reflect radio waves. For example, if metals, concrete or ceramics are used in construction, they can degrade signal.
- 2) Electronic devices like microwaves have their own radio waves frequency and if that happens to be on the same frequency as your wireless network, it can cause interference. It is best to keep them away from each other.
- 3) External factors like powerlines, broadcast TV, or cameras can also cause interference.

Home router setup

To access your home router, type <http://192.168.0.1> in the browser. Use the following steps to setup the router.

- Locate the firewall settings and make sure the firewall is turned on.
- Always change the router's default password. Default passwords are published at www.routerpasswords.com
- Change the router's SSID name.
- You can hide the Wi-Fi SSID in the router settings. Then you'll have to type the SSID manually into each device.
- Enable Wi-Fi encryption (WPA2 or better) and enter a strong passphrase to protect the Wi-Fi.
- Keep the router firmware up-to-date.

Speed check

www.speedtest.net tests and provides network speed results while your computer is sitting idle and not downloading or streaming content.

Cable Modem

Data over Cable Service Interface Specification (DOCSIS) is an international standard that enables high speed data transfer over the cable TV system. Cable modems use the high-bandwidth network to deliver high speed two-way data. Neighboring residential subscribers share the same upstream system which may lead to collisions. A technique called ranging is used to minimize the collision rate. Ranging determines the time it takes for data to travel to the cable headend.

In network topology, a cable modem is a network bridge that provides Ethernet networking. The cable modem bridges Ethernet frames between a customer LAN and the coax network. Technically, it is a modem because it must modulate data to transmit it over the cable network, and it must demodulate data from the cable network to receive it.

With respect to the OSI model (described in sec 4.2) of network design, a cable modem is both physical layer (layer 1) device and a data link layer (layer 2) forwarder. As an IP addressable network node, cable modems support functionality at other layers. The Network Layer (Layer 3) may be implemented as an IP host in that it has its own IP address used by the network operator to maintain the device. In the transport layer (layer 4) the cable modem may support UDP. In the Application Layer (Layer 7), the cable modem may support certain protocols that are used for management and maintenance. The next section includes more information on cable modem.

Cable modem information in the above paragraph is adapted from <https://en.wikipedia.org/wiki/Cable_modem>

Dynamic Host Control Protocol (DHCP)

An IP address is one of the most basic pieces of information needed for a computer to communicate on a network. An IP address can be configured manually or assigned dynamically. DHCP automates and simplifies the steps for IP address assignment. DHCP's function is to assign a pool of IP addresses to requesting clients. The DHCP client on the computer requests an IP address from the DHCP server. The DHCP server retrieves an available IP address from a pool dedicated to the subnet of the requesting client. The IP address is passed to the client, and the server specifies the length of the time that the client can hold the address. This is called the lease time. This helps an unused computer from unnecessarily tying up an IP address.

When a computer is configured to obtain an IP address automatically, the process of requesting an IP address involves the following steps:

- The client boots up and sends out a DHCP Discover message broadcast to all computers on the LAN.
- A DHCP server listening on the LAN takes the DHCP Discover message, retrieves an available IP address from the configured address pool, and sends the address to the DHCP client via a DHCP Offer message. The server sends the IP address, lease time, subnet mask, default gateway and domain name server information.
- The client receives the DHCP Offer message from the server and agrees to use the lease. It replies back to the server with a DHCP Request to formally request and confirm the offered IP address with the server.
- The server receives the DHCP Request message and sends back a DHCP ACK message, which is a unicast packet acknowledging the request of IP address information.
- The client applies the IP address and its network settings to the computer and it is ready to make network connections.

In Windows, the command `ipconfig /release` can be used to release the current IP address, and the command `ipconfig /renew` can be used to initiate the DHCP process.

4.1 Residential Connection Technologies

Cable modem is one of the several technologies used for providing Internet connectivity to residences. Following is a list of technologies that can be used for providing Internet connectivity to homes.

Analog modem

At the residential level, the traditional wired phone system carries analog voice signal, not data. So to send digital data, it is necessary to have a device that converts bits to sound and back again. The process of imposing an information carrying pattern on a signal is called modulation. At the other end, converting the pattern back to its original form is called demodulation. The device that does modulation and demodulation is called a modem. An analog modem enables using the telephone line for data connections. Using the telephone for data connections has major drawbacks. It requires a dedicated phone line. So if there's only one phone line in the house, the user has to choose between connecting to the Internet, or leaving the phone available for voice calls. The network speed is also low, about 56Kbps. This is an old technology and it may be the only option available in some areas that require only a standard telephone line and an analog modem.

Digital Subscriber Loop (DSL)

DSL service sends a high speed digital data signal over regular telephone wires. ADSL for asymmetric DSL is named so because download speeds are higher than upload speeds. DSL sends data on the telephone wire with a technique that doesn't interfere with the voice signal, so you can talk on the phone while surfing and neither affects the other. This works well but only up to a certain distance of about 5Kms from the local telephone company's switching office.

DSL's availability and speed are restricted by the home's distance from Telephone Company's equipment to the neighborhood. DSL modems can be external or could plug into the computer. A nice thing about DSL is that it is not a shared medium. It uses dedicated wire between the home and local phone company, so homes do not need to share the capacity with neighbors. A special box at the home, another modem with a matching one at the telephone company's building converts signals into the right form to be sent along wires.

Cable modem

The cable that carries cable TV to homes can carry hundreds of video channels simultaneously. It has enough excess capacity that it can be used to carry data to and from homes as well. The device that converts signals from the cable into bits for a computer and back again is a cable modem, since it does modulation and demodulation like a telephone modem, though it runs quite a bit faster than a telephone modem. Cable Internet access requires cable modems that support Ethernet.

The same TV signal goes to every house regardless of whether it is being watched or not. The local TV cable company sends data signals through the same distribution system it uses to carry TV signals. Data bandwidth has to be shared among data users of the cable i.e. neighbors. Cable networks offer two-way communication, to enable pay-per-view, which makes them usable as a communication system for computer data. At the cable head end, Cable Modem Termination System (CMTS) turns analog signal

sent from cable modems in many downstream homes back into digital format. There are two channels: downstream and upstream. They are shared broadcast medium. Every packet sent by the head end travels downstream on every link to every home and every packet sent by a home travels on the upstream channel to the head end. If several users are simultaneously downloading high bandwidth information at the same time, the actual rate at which a user receives its data may be lower than the aggregate cable downstream rate. Because the upstream channel is also shared, a distributed multiple access protocol is needed to co-ordinate transmission and avoid collisions. Data download speeds are higher than upload speeds. Cable modem service does not have the distance limitations of DSL.

Cellular service

Mobile phone service providers sell data service as a standalone service or as part of bundled package that include voice and text for phones with built-in cellular data modems. The hardware is built into the phone or tablet. Cellular modems for laptops may be purchased to give them Internet connectivity but the coverage may be patchy in certain regions. Cellular service uses 5G, 4G or 4G LTE cellular data technologies. Long Term Evolution LTE is a standard for wireless broadband communication for mobile devices and data terminals. Compared to 4G, it increases capacity and speed using different radio interfaces and other network improvements.

Hotspot

Small hotspot devices are available which contain both cellular data modem and Wi-Fi networking adapter. Cell phones and tablets with built-in cellular data capability can share their Internet data service by serving as a mobile hotspot for nearby computers.

Satellite service

Satellite Internet service uses microwave signals and small antennas to connect to an orbiting communication satellite. Whereas Satellite TV works in a single direction, Satellite Internet service is bi-directional (dish has both a transmitter and a receiver). Its advantage is that it is available where DSL or Cable hasn't reached yet. The disadvantage is that the equipment and service are expensive. Signal may be lost when it is raining or snowing. Users would need dish antenna, a transmitter & receiver, satellite modem and professional installation.

Fiber to the home (FTTH)

FTTH is up and coming newer technology. It provides an optical fiber path from the provider's Central Office (CO) to the home. There are several competing technologies for optical distribution from CO to homes. The simplest optical-distribution network is called direct fiber, with one fiber leaving the CO for each home. However, each fiber leaving the CO is shared by many homes, and it is not until the fiber gets relatively close to homes that it is split into individual customer-specific fibers. There are two competing optical distribution architectures that perform the splitting: 1) active optical network, 2) passive optical network. FTTH can provide very high speeds (but the effective rate may still be limited by the home's wireless router's limit when using in conjunction with it).

--- Sec 4.1 adapted from Windows 10 in depth, Knittle, McFries; Computer Networking, Kurose, Ross; Understanding the digital world, Kernighan

4.2 Open System Interconnect (OSI) Layers

Open System Interconnect defines seven layers. Going from the bottom up, the bottom most layer is the physical layer.

The **physical layer** details the protocols required to transmit data across physical mediums. This layer represents all the hardware that forms a network. All other layers work via software. There are wired and wireless network interface adapters, radio signals, Ethernet cables for transmission, cable/broadband lines, switches, hubs etc. Each of these resources has a manufacturer as well as a unique physical hardware. To see information on this look at **Device Manager -> Network adapters**. Within this architecture, the physical layer transmits logical communication requests to and from the data link layer, which is the layer above it.

Data-link layer is the second layer from the bottom. Data is transmitted across networks separated into small, transmittable packets. For this reason networks are called packet switching networks. Each packet must include information on what it contains, where it is from and where it is going amongst other things. During the progression, each packet goes through data encapsulation, where a frame is added to it. The frame contains a header and a footer, and includes the hardware address (Media Access Control MAC address) of the devices and the protocol used. Examples of protocols at this layer are IEEE 802.11 and Ethernet which are LAN protocols.

Network layer is the next layer up the protocol stack. This layer is responsible for IP addressing, routing and subnet masking. To move data packets across dissimilar networks or beyond the LAN, data packets must pass through a router. IP is used to do this. IP is an end-to-end protocol. Like the previous layer, this layer adds information as well. The IP header includes packet's source and destination IP addresses and protocol information amongst other things. The data is then passed to the transport layer. To see the Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) protocols installed, go to, **Control Panel\Network and Internet\Network Connections** then right click the Wi-Fi and Properties.

IPv4 versus IPv6

IPv4 addresses are 32 bits long. They are created with both a network identifier and a host identifier. The network part defines the destination network and the host part defines the specific host on that network. 192.168.10.1 is an example of IPv4 address. With only 32 bits, we've run out of IPv4 addresses. IPv6 was created to address this shortage of addresses.

IPv6 addresses are 16 bytes long represented as eight 2-byte values. An example of IPv6 address is 2021:0:0:0:8a2e:5c7d:0000:8a2e.

Following are approaches to IPv4 to IPv6 transition:

- Native IPv6 network will rely solely on IPv6 (this might not work just yet).
- Dual stack: both IPv4 and IPv6 stacks are supported and the network uses IPv6 when it can, otherwise it falls back to IPv4.
- Tunneling: This is a network that wants to use IPv6 as much as possible but encapsulates IPv6 into IPv4 packets when required (for example using 6-4 tunneling technique).

Transport layer is either connection-oriented (TCP) or connection-less (UDP) to describe how the device will connect to the other device. The protocol must be agreed by both the sender and the receiver before data can be transmitted. In a connection-oriented session, message is delivered reliably. There's acknowledgement and lost packets are retransmitted. In a connectionless protocol, it is ok for data bits to be lost like in the case of video streaming. As with previous layers, this layer adds its header, which includes information about the ports on each side of the connection. The receiving computer needs the port information to determine the application the data is meant for. When you combine the port with IP address, you get a socket. So, the packet with destination port number of 80 implies the destination computer will need to use something like a browser that can handle HTTP protocol. Additionally, data encapsulation at this layer includes TCP or UDP information.

Upper layers (Session, Presentation, Application) are often grouped together as they are related to what happens once the data has been sent across the network and appears at the destination computer. Data packets must be "un-encapsulated" through the same layers backwards to extract the information required to complete the delivery of data. Once the data is ready, the appropriate programs installed (like email or browser) take control from there, offering the data to the user.

4.3 Transport Protocols

TCP and UDP are the most common transport protocols.

Transmission Control Protocol (TCP)

TCP provides reliable communication where all bytes sent are identical to the bytes received and they're delivered in the same order. TCP ensures retransmission of data, in-order delivery, congestion control and avoidance, data integrity and more. In practice all HTTP traffic is delivered via TCP. Each TCP connection begins with a 3-way handshake (SYN, SYN-ACK and ACK) after which the sender can transmit data to the receiver.

TCP is a byte-stream oriented protocol capable of transmitting application messages spread across multiple packets without any explicit message boundaries within the packet themselves. To achieve this, connection state is allocated on both ends of the connection and each packet is sequenced, retransmitted when lost, and delivered in order.

User Datagram Protocol (UDP)

User Datagram Protocol is an unreliable service with no delivery guarantees or failure notifications. UDP often referred to as "unreliable datagram protocol" adds only four fields in the header: source port, destination port, length and checksum. Checksum may be optional when error detection and recovery are delegated to the application layer. At its core, UDP simply provides "application multiplexing" on top of IP by embedding the source and target application ports of the communicating hosts. Each UDP datagram is carried in a single IP packet and each application read yields the full message. Datagrams cannot be fragmented. UDP is a simple and stateless protocol.

4.4 Metrics

Latency and bandwidth

Latency is the time from source sending a packet to the destination receiving it. Latency involves propagation delay, transmission delay, processing delay and queueing delay. Bandwidth is the maximum throughput of a logical or physical communication path. Ironically it is often the last few miles where significant latency is introduced. The ultimate goal is to deliver higher bandwidth and lower latencies.

Sec 4.2-4.4 adapted from Windows networking troubleshooting, Halsey, Ballew; Computer Networking, Kurose, Ross

4.5 Application Layer

Application layer or layer-7 is the topmost layer. DNS, HTTP and HTTPS are examples of application layer protocols.

DNS

Domain Name System (DNS) translates a human-readable name like www.example.com to an IP address. DNS runs on UDP and TCP port 53.

The DNS hierarchy is a tree hierarchy. It starts with the root, then the top-level domains (.com in this case), and then subdomains. Root DNS servers have well-known IP addresses that have been programmed into DNS servers. When DNS is installed on a server, the root DNS server's IP addresses are automatically configured.

Say a computer wants to know the IP address of server that hosts en.wikipedia.org. It would ask its local DNS server for the IP address of en.wikipedia.org. Local DNS would ask the root server, do you know the IP address of en.wikipedia.org? The root server would respond with the IP address of .org registry. Then the local DNS would ask the .org registry for the IP address of en.wikipedia.org. The .org registry would respond with the IP address of the server that hosts wikipedia.org. Then the local DNS server would ask the server at wikipedia.org for en.wikipedia.org's IP address. Finally the server at wikipedia.org would respond with the IP address for en.wikipedia.org.

A DNS server keeps a cache of recent queries so it does not have to repeat the whole process again unnecessarily.

An authoritative name server is a name server that is authorized and configured to answer DNS queries for a particular domain or zone. Information about the domain and its hosts and services is defined by resource records (RR). Each zone contains resource records that define or describe its domain, its subdomains and its hosts' information. These resource records can be found by using the dig command on Unix based systems and nslookup on Windows.

HTTP

The Hypertext transfer protocol (HTTP) is the protocol for exchanging or transferring of hypertext (more than text), structured text. HTTP is used every time a user connects to a website. HTTP is the foundation of data communication over the World Wide Web (www).

HTTP is a request response protocol relying on client-server model. When the user visits a website or uploads data using a web browser, the client submits an HTTP request message to the server. The server which provides resources such as HTML files, images, video and other content, returns a response message to the client. The response contains information regarding the request, such as the completion status and the requested content.

HTTP works at the application layer of the OSI (Open Systems Interconnection) model. It is the protocol that makes a web browser and a web server understand each other. Underneath it at the transport layer, HTTP uses TCP to transport data. Following shows the TCP/IP stack on the client and the server.

Sender	Receiver
Web browser	Web server
HTTP request	HTTP response
TCP	TCP
IP	IP

The server responds by sending back HTTP data over the same TCP connection that was used for the request. The HTTP response contains the requested data which could be HTML page, image, video or a file. The response also contains the HTTP headers that describe the data including status code that reports on the completion of the request and content type. HTTP stores information about requests and responses in HTTP headers, which the browser and the web server read.

HTTP request	HTTP response
Header: requested resource, browser type Body: form data or empty	Header: status code, content type Body: requested resource as content

Following are some of the commonly seen HTTP status codes.

200: ok (request completed)

301: moved permanently (redirection)

404: not found

500: internal server error

Following is an example of establishing an HTTP session using the Ubuntu app on Windows.

```
LaptopPrompt>$telnet www.google.com 80
```

```
Trying 142.250.191.68...
```

Connected to www.google.com.
Escape character is '^]'.
get /index.html HTTP/1.1
<snip>

HTTPS

HTTPS uses TLS/SSL (Transport Layer Security/Secured Socket Layer) to encrypt HTTP requests and responses. TLS uses public key encryption wherein there are two keys, a public key and a private key, and the public key is shared with client devices via the server's SSL certificate. When a client opens an HTTPS connection with a server, the two devices use the public and private key to agree on new keys, called session keys, to encrypt further communications between them.

All HTTP requests and responses are then encrypted with these session keys, so that anyone who intercepts this communication would see a random string of characters, not the plaintext. HTTPS authenticates web server's identity. When a client opens a channel with an origin server (e.g. when a user navigates to a website), possession of the private key that matches with the public key in a website's SSL certificate proves that the server is actually the legitimate host of the website.

By using HTTPS client notifies the server that it desires a TLS connection instead of the standard insecure connection, so it sends along a message describing which TLS protocol version and encryption techniques it'd like to use. As long as the server supports the requested TLS protocol version and other options, it will respond with a confirmation, plus a digital certificate that contains its public key. If the client can verify the certificate, it continues on to the next step of shared key generation.

The client then knows the public key of the server, so it can use public key encryption to encrypt data that the server can decrypt with its corresponding private key. However, public key encryption takes much more time than symmetric encryption. So, when possible, computers prefer to use symmetric encryption to save time. The client and server first use public key encryption to privately generate a shared secret key, and then they use symmetric encryption with that key in future messages.

Eventually, the client and server are able to securely communicate information using symmetric encryption and the shared key.

Sec 4.5 adapted from Networking Essentials, Beasley, Nilkaew

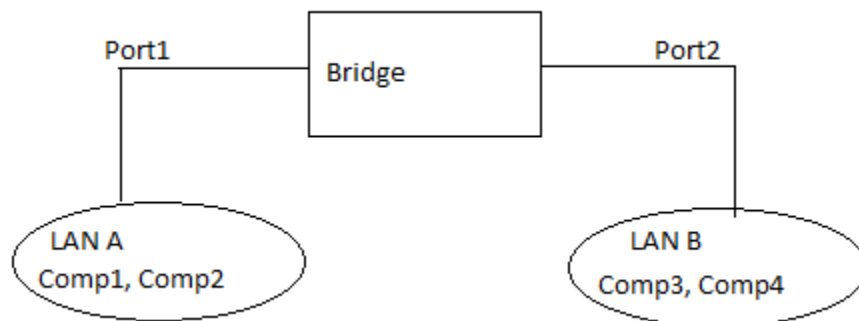
Chapter 5 Basic Network Devices

Some of the basic network devices include Hub, Bridge, Switch, and Router. These are described very briefly here.

Understanding the basics of a Bridge helps in understanding the workings of a cable modem at a high level. Additionally, home networks may employ Switch, Router or Hub.

5.1 Bridge

A Bridge can be used to interconnect two Local Area Networks (LANs) or separate network segments. A Bridge is a Layer 2 device that uses Media Access Control (MAC) address to make decisions regarding forwarding packets. Only the data that needs to be sent across the bridge to the adjacent network segment is forwarded. LAN refers to Local Area Network.



In this figure, LAN A is connected to the port 1 of the bridge and LAN B is connected to port 2 of the Bridge. Bridges use MAC addresses to build a table of MAC addresses and port locations for hosts connected to the Bridge ports. The source MAC address is stored in the table as soon as the host transmits a frame on the LAN. LAN A has devices Comp1 and Comp2 in it. Lan B has devices Comp3 and Comp4 in it. If Comp1 sends a frame to Comp3, then the Bridge will store the MAC addresses of both computers and record the port number they are connected to. The MAC addresses for Comp2 and Comp4 won't be added to the table until each transmits a frame. The Bridge monitors the data on its port to check for an association between the destination MAC address of the Ethernet frame and any of the hosts connected to its ports. An association indicates that the destination MAC address for a host is connected to one of the ports on the Bridge. If an association is found, the data is forwarded on that port.

The capability of a Bridge to forward data packets only when there is an association is used to isolate data traffic in each network segment. A potential problem with Bridges is related to the way broadcasts are handled. With a broadcast, a message is sent to all computers on the network. For example, the broadcast associated with ARP (Address Resolution Protocol) will appear on all hosts. An ARP request broadcasting the message "who has this IP address?" is sent to all hosts in the LAN. Excessive number of broadcasts being forwarded by the Bridge can lead to a broadcast storm, resulting in degraded network performance or network slowdown.

The MAC address entries stored in a Bridge table are temporary. Each MAC address entry in a Bridge table remains active as long as there is periodic data traffic from that host on its port. An entry into the

table is deleted if the port becomes inactive. An expiration timer commences once the MAC address is entered into the Bridge table. The lifetime for the entry is renewed with new data traffic and the MAC address is reentered.

In a similar manner, networking devices contain an ARP cache, which provides temporary storage for MAC addresses recently contacted. The ARP cache holds the MAC address of a host and enables the message to be sent directly to the destination MAC address without the computer having to issue an ARP request again for the MAC address.

Now-a-days, the use of a Bridge is not as common as it used to be except with wireless networking.

5.2 Switch

A Switch is a Layer 2 device that uses MAC (Media Access Control) addresses to differentiate traffic. MAC address is a unique hardware identification number assigned by the manufacturer of the device. It is 48 bits long containing six octets. Each node on the subnet has a NIC (Network Interface Card) with a unique MAC address.

At the hardware level, a switch contains a processor, RAM and ASICs so it can process network data. It understands MAC addresses and frames. The processor runs the Switch's OS and manages memory. A switch can process signals as frames. A switch has its own MAC address. Switches allow us to connect different devices on a network.

A Switch inspects the destination MAC address in the Ethernet frame and the frame is sent only to the intended destination. A switch can perform error checking and discard any packets with detected errors. A Switch utilizes the full potential throughput capacity by preventing collisions. An Ethernet frame is a logical data unit at the data link layer consisting of payload from network layer with the addition of Ethernet header and footer.

A Switch provides a direct data connection from the source to the destination host. Neither the bridge nor the hub provides a direct data connection for the hosts. A switch has multiple ports and can establish a data connection from any port to any port. In a star topology, each host has a direct connection to the switch. Therefore, when a link is established between any two hosts, the link is isolated from any other data traffic. However, there is an exception to this when broadcast or multicast traffic is sent in a LAN. The broadcast message is sent to all devices connected to the LAN. A multicast message is sent to a specific group of hosts on the network.

A Switch employs four major procedures: **learn, forward, drop and flood**.

The learn procedure involves the collection of MAC addresses from the source location in a frame. The Switch adds the source MAC address into a mapping table, along with the hardware port number that received the frame. Forwarding occurs once a frame's destination MAC address appears in the mapping table. If the destination MAC address is not in the mapping table, the switch reverts to flooding by transmitting the frame out to every port to identify the port with the destination MAC address. Finally, a switch does not need to transmit the frame back into the network segment from which it originated, instead it drops the frame.

To monitor traffic going through a switch, connect your computer running Wireshark to the switch. On the switch use the port monitor command to specify port numbers to monitor. Wireshark will show all the traffic that the computer is seeing from the switch it is connected to.

As an experiment, connect three computers A, B and C to three ports of a switch. When computer A is talking to computer C, packet capture on computer B will only reveal the broadcast messages between A and C. Whereas if these same computers were connected to three ports of a hub, and when computer A is talking to computer C, packet capture on computer B will reveal all communication between computers A and C.

The interfaces on a switch are labeled as: interface type slot#/interface #. An example is Gigabitethernet0/2. Gigabit Ethernet indicates that the interface supports 1000Mbps, 100Mbps, 10Mbps data rate connections. Slot number is 0 and interface number is 2.

A Switch has aging time associated with the length of time a MAC address remains assigned to a port. If there is no activity within this time, the assignment of the MAC address is removed. If the computer with the assigned MAC address initiates new data activity, the aging time counter is restarted, and the MAC address remains assigned to the port.

Say a Switch port number 1 is connected to a Hub which is connected to four computers. Then the Switch's MAC address table will have four MAC addresses associated with its port number 1.

Summary of Hub-Switch-Router comparison

A Hub connects devices on an Ethernet twisted-pair network. A Hub does not perform any tasks besides signal regeneration. It simply forwards data to all nodes connected to it.

A Switch connects devices on a twisted-pair network. A Switch forwards data to its destination by using MAC address embedded in each packet. It only forwards data to nodes that need to receive it.

A Router connects networks. Router forwards packets based on their destination IP address.

Hub	Switch	Router
Repeats signal on all ports	Connects different machines on a network	Connects networks
Does not have a processor or Operating System	Has a processor and an operating system	Has a processor and an operating system
Does not have a MAC address	Has a MAC address of its own	Has a MAC address of its own
No knowledge of MAC address	Has knowledge of MAC address but does not change the MAC address of packets	Changes the MAC address of packets

Mostly Layer 1 device	Layer 2 device	Layer 3 device
Works with signals	Works with frames	Works with packets
	Has lots of network ports (for example, 48 or more)	Has less network ports as they connect to other routers or switches
	Likely connects Ethernet cables	Likely connects T1s
	LAN centric	WAN centric

5.3 Access Point

An Access Point (AP) or a Wireless Access Point (WAP) is a device designed to interconnect wireless network nodes with wired networks. The access point functionality is incorporated into many Small Office Home Office (SOHO) wireless routers. In home networks a Basic Service Set (BSS) network can be created with a single access point and multiple clients. For larger areas the Wi-Fi network can be extended by adding one or more access points to create an Extended Service Set (ESS). AP offers a wireless LAN using the 802.11 standard. Following table summarizes the different 802.11 standards.

Wi-Fi	Standard	Frequency	Bandwidth
Wi-Fi 1	802.11b	2.4GHz	11Mbps
Wi-Fi 4	802.11n	2.4GHz & 5GHz	200Mbps
Wi-Fi 5	802.11ac	5GHz	500Mbps-1.3Gbps
Wi-Fi 6	802.11ax	2.4GHz & 5GHz	200Mbps

Most Wi-Fi networks are protected using Wi-Fi Protected Access (WPA/WPA2). A common way to setup WPA or WPA2 encryption is to use a WPA/WPA2 Pre-shared key (PSK). With these PSK versions, you create a secret key that must be added to any device that is going to be on that Service Set Identifier (SSID). There is no authentication with WPA-PSK or WPA2-PSK. An important thing to do to prevent the passphrase from being cracked is to use long passphrases (16 or more characters), thus making it hard to crack.

In home networks, cable modem, AP, and router functionalities could be clubbed into one device or each could be a separate device.

Sec 5.1-5.3 adapted from Networking Essentials, Beasley, Nilkaew; Head First Networking, Anderson, Benedetti

5.4 VPNs and Firewalls

Virtual Private Network (VPN) or Firewall may be implemented as a specialized software program on the host PC or each of them could be part of a specialized appliance. A Firewall provides controlled data access between networks. A Virtual Private Network extends a LAN by establishing a remote connection, a connection tunnel, using a public network such as the Internet.

Virtual Private Network (VPN)

A VPN allows a remotely located client to gain secure access to an internal network. VPNs create a secure tunnel through a public network. First connectivity comes, and then a VPN can be established. The communication between the VPN client and gateway is often encrypted. The client puts the encrypted packets into the data section of a TCP packet and sends that packet across the public network to the VPN gateway. The VPN gateway removes the encrypted packet, decodes it and sends it to the internal network.

Following are different types of VPN.

1. Layer 2 VPN: The data link layer protocol transfers data from one VPN endpoint to the other. Layer 2 Tunneling Protocol (L2TP) is an example of this. L2TP does not provide encryption.
2. Layer 3 VPN: IPSec is a VPN protocol that communicates at layer 3. IPSec supports two modes: a) Transport mode where the data packet payload is encapsulated while the packet header is left intact. b) Tunnel mode where the IP packet is entirely encapsulated and given a new header. OpenVPN is an open source software that implements layer 3 VPN.
3. Layer 7 VPN: Secured Socket Layer (SSL) VPN is often provided as an additional browser feature that can be turned on. For example, Opera browser has a SSL/TLS based VPN.
4. Secured Shell (SSH): Putty is an application providing terminal emulation and it can leverage SSH to provide secure connection to a host.

Firewalls

A Firewall is a filtering device that enforces network security policy and protects the network against external attacks. As a filtering device a Firewall watches for traffic that fails to comply with the rules defined by the admin. In general Firewalls philosophy is to deny by default and allow by exception. IOW the final rule is, "anything that did not match one or more exceptions is denied by default". If a Firewall is offline, locked or frozen, it should stop all traffic.

Firewalls manage and control traffic, allowing only authorized communications. Firewalls can filter based on source and/or destination IP addresses, ports, or protocols. Firewalls can filter based on content. Content filtering can focus on domain names, URL, filename or keywords in the content.

Types of filtering

1. Static packet filtering uses a static or fixed set of rules to filter network traffic. The rules can focus on source or destination IP address, source or destination port number, IP header protocol field values or ICMP types. Static packet filtering focuses on header contents and does not examine the

payload of packets or segments. Static packet filtering is fast but can be problematic if the rule set is large.

2. Stateful Inspection and Dynamic Packet Filtering determines whether or not a packet is part of an existing session and allows incoming response from outside if the packet is part of an existing session. If the packet is not part of an existing session, and is used for initiating a new authorized session it may allow outgoing packets, otherwise the packet will likely be dropped.
3. Application Proxy or Application Firewall is an application specific packet filter. It can inspect packet payload as well. It usually sits between a client and a server. Since Application Firewall can filter based on the content of the packet (or the application payload), it is also known as Deep Packet Inspection.
4. Content Filtering filters based on the content. It can filter based on domain name, URL, filename, file extension or keywords in a packet.

Sec 5.4 adapted from Network Security, Firewalls & VPNs, Stewart, Kinsey

Appendix

A. MMC Snap-ins

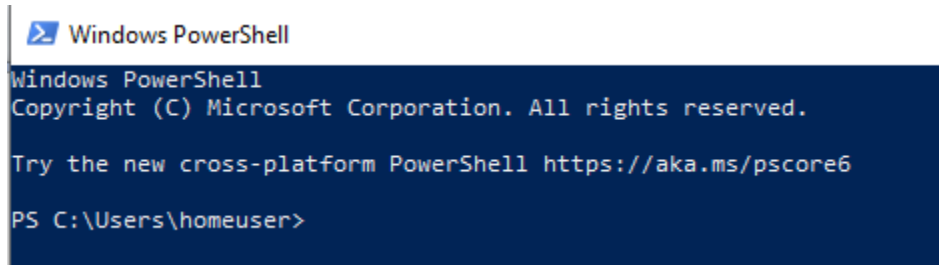
Microsoft Management Console (MMC) is a system administration program. When you work with MMC, you're working with a .msc file. These are called snap-ins. To launch an MMC snap-in, type the name in the taskbar search box and press enter. Following is a partial list of MMC snap-ins in Windows.

Snap-in	File (.msc)	Description
Auth Manager	Azman	To set permissions on applications
Component services	Comexp	View and work with COM component object model
Certificates	Certmgr	Browse certificates on your system
Computer management	Compmgmt	Folders, hard disk, device manager etc.
Device manager	Devmgmt	Add or manage system hardware
Disk management	Diskmgmt	View or manage disk drives
Event viewer	Eventvwr	View event logs
Perfmon	Perfmon	Monitor performance counters
Services	Services	Start, stop or pause services
Shared folders	Fsmgmt	Monitor activity on shared folders
Task scheduler	Taskschd	Schedule programs or scripts
TPM management	Tpm	Trusted platform module management
Firewall	Wf	Firewall
WMI control	Wmimgmt	Configure properties for Windows Management instrumentation

Adapted from Windows 10 in depth, Knittel, McFedries

B. Powershell

This section has a very brief introduction to the basics of Powershell. Powershell is a command prompt and a scripting language. To launch Powershell, type Powershell in the taskbar search box and press enter, or select the app and click it from the search results.

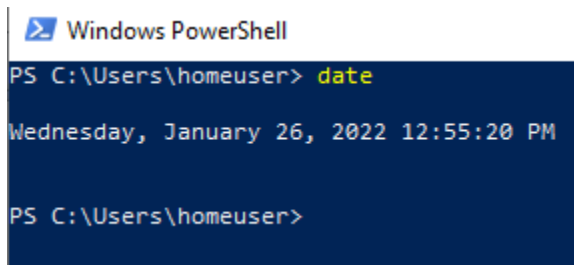


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\homeuser>
```

Windows Powershell is a proprietary command-line shell designed for administrators. To get date information, use the date command.

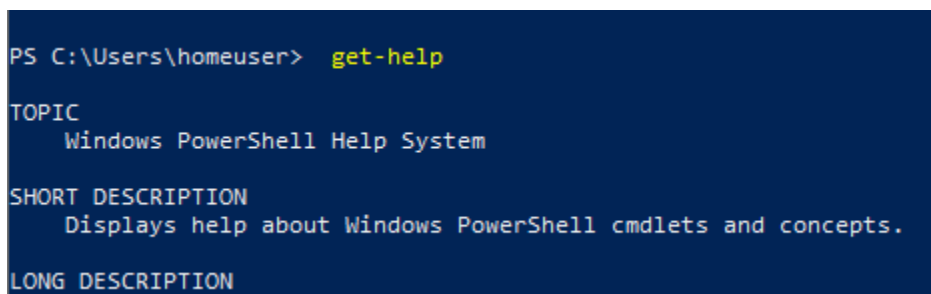


```
PS C:\Users\homeuser> date
Wednesday, January 26, 2022 12:55:20 PM

PS C:\Users\homeuser>
```

Powershell offers command line completion when you type a few characters of the command and press the tab key a couple times until the item you want appears. It also saves sequences of commands you used in the past which can be seen by using the up arrow to cycle through previous commands.

Powershell introduced the cmdlet. It is a simple one-function command specifying the action to perform. There are many cmdlets written as a verb-noun pair. For example, type 'get-help' which will output the description of the get-help cmdlet.



```
PS C:\Users\homeuser> get-help
TOPIC
    Windows PowerShell Help System

SHORT DESCRIPTION
    Displays help about Windows PowerShell cmdlets and concepts.

LONG DESCRIPTION
```

Powershell comes with built-in cmdlets. You can use cmdlets (short for command-lets) built into the Powershell. Cmdlets can be created by anyone. Powershell comes with core cmdlets. Cmdlets follow a verb-noun pattern, such as get-help, get-eventlog or get-process. The cmdlets using the get verb display information about the item on the right side of the dash. The cmdlets that use the set verb modify or set

information about the item on the right side of the dash. Examples of cmdlets are get-process and set-service. The cmdlet names are not case-sensitive.

Following are common parameters to cmdlets. Not all parameters may be available with all cmdlets.

Parameter	meaning
-whatif	Tell the cmdlet to not execute but tell you what would happen if executed. This applies to cmdlets with the set verb
-confirm	Tells the cmdlet to prompt before executing the command
-verbose	Provide a higher level of detail
-debug	Provide debugging information
-erroraction	Perform a certain action when the error occurs

To invoke the get-process cmdlet,
PS C:\Users\homeuser> get-process

```
Handles NPM(K) PM(K) WS(K) CPU(s) Id SI ProcessName
-----
136 13 6884 12016 3744 0 AdskLicensingService
<snip>
```

To get help for get-process cmdlet,
PS C:\Users\homeuser> get-help get-process

NAME
Get-Process

SYNTAX
Get-Process [[-Name] <string[]>] [-ComputerName <string[]>] [-Module]
[-FileVersionInfo] [<CommonParameters>]
<snip>

To get help for get-help cmdlet,
PS C:\Users\homeuser> get-help get-help

NAME
Get-Help

SYNTAX
<snip>

Following are additional examples.

```
PS C:\Users\homeuser> get-help get*
PS C:\Users\homeuser> get-help get-p*
```

Powershell prompt is being omitted for the following examples.

Following are examples of filtering get-process results.

```
get-process | get-member
get-process | sort-object cpu
get-process | sort-object cpu -descending
get-process | sort-object cpu -descending | out-gridview
```

To get a list of cmdlets that begin with g,
Get-command g*

Some cmdlets have shortened aliases. To see aliases for cmdlets which begin with g, use the following.
The output shows that Gcm is an alias for Get-command.
Get-alias g*

To list the cmdlets those use the set verb,
Gcm -verb set*

To list cmdlets whose noun begins with o,
Gcm -noun o*

To list cmdlets whose noun contains the keyword event,
Get-command -noun *event*

To get the syntax of get-command,
Gcm -syntax get-command

To list unique groups for the get-verb,
get-verb | select group -unique

To list the verb distribution of cmdlets,
get-command -commandtype cmdlet | group verb | sort count -descending

To get a list of all modules installed in Powershell,
Get-module -listavailable

Following are additional examples.

```
Get-item -path .
Get-variable *
Get-help get-eventlog
Get-help get-service
Get-help get-event
Get-host
Get-location
Get-help show-command
```

Get-help show-eventlog
Get-help test-connection
Get-help test-path
Get-eventlog application | get-member

To get-help for get-eventlog,

```
PS C:\Users\homeuser> Get-Help Get-EventLog_
NAME
    Get-EventLog

SYNTAX
    Get-EventLog [-LogName] <string> [[-InstanceId] <long[]>] [-ComputerName
```

To list log of events,

```
PS C:\Users\homeuser\logs> get-eventlog -list
```

To get the newest 50 system logs,

```
PS C:\Users\homeuser\logs> get-eventlog -logname system -newest 50
```

```
PS C:\Users\homeuser\logs> get-eventlog -logname system -newest 50 > system_50
```

To get System logs whose source is win32k,

```
PS C:\Users\homeuser\logs> get-eventlog -logname system -source win32k -newest 50 >
system_win32k_50
```

```
PS C:\Users\homeuser\logs> get-eventlog -logname "Windows PowerShell" -newest 10
```

Windows enables most log files by default, although you might need to define what level of logging you need. Turning on verbose mode may take up a lot of disk space. Great logging is about pulling out necessary critical events and alerts from large amounts of data.

Use the following command to get logs of a remote machine,

```
Get-eventlog -computername <remote_computer_name> -logname system
```

Adapted from Windows Powershell 3.0, Ed Wilson; and Cybersecurity blue team toolkit, Nadeen Tanner

C. Windows Troubleshooting

Windows network troubleshooting

The hosts file is in C:\Windows\System32\drivers\etc> folder.
C:\Windows\System32\drivers\etc>more hosts

Hosts file is used to map hostnames to specific Internet Protocol (IP) addresses. It can be used to point websites such as example.com to IP address 0.0.0.0 so as to make it inaccessible to the user because that address doesn't point to anything. Today the hosts file is not commonly used on modern PCs and Domain Name System (DNS) takes care of name resolution.

Connectivity options can be obtained from, Control Panel\Network and Internet\Network and Sharing Center and View Active Networks.

VPN settings can be obtained from Settings -> Network & Internet -> VPN.

Network profiles can be accessed from, Right clicking windows icon -> Network Connections -> Network & Sharing Center. Then clicking change advanced sharing settings in the left panel. You'll likely see your Wi-Fi SSID is the current profiles under Public profile with network discover turned off and file & print sharing also turned off. There are three profiles: private, public and domain. Private is designed for trusted network. Domain profile is applied when the user logs on to a domain wherein the user is assigned to a specific group and is given perms based on the group.

Network profiles can be changed from, Settings -> Network & Internet -> Status -> change connection properties.

Installed protocols like IPv4, IPv6 can be seen from,
Control Panel\Network and Internet\Network Connections then right clicking the Wi-Fi and Properties;
From here you could select protocols to install or uninstall.

Dynamic Host Control Protocol (DHCP)

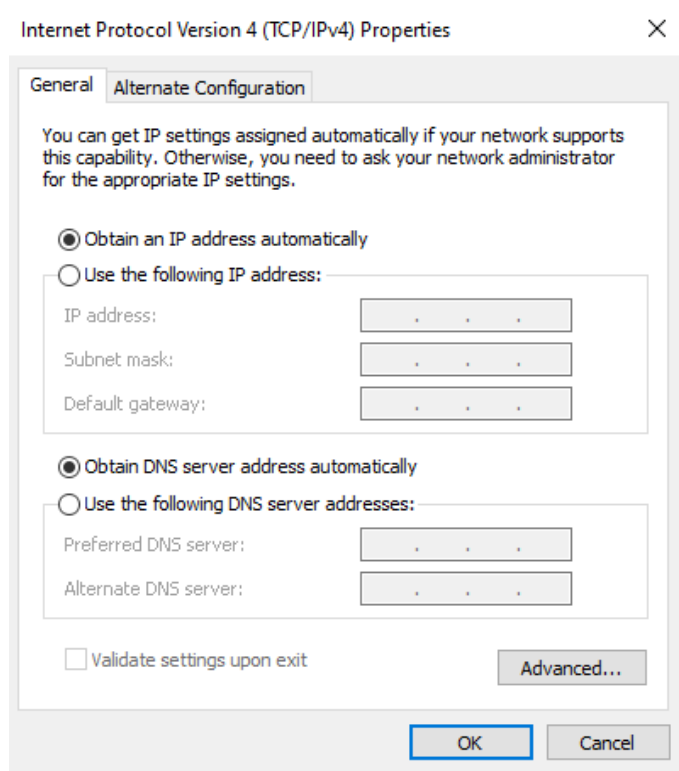
DHCP is a means to assign IP addresses to nodes on a network. DHCP is a protocol that enables nodes on a network to obtain their IP addresses automatically. Addresses are obtained and released as clients need them. DHCP settings can be accessed from, Control Panel\Network and Internet\Network and Sharing Center.

When you change settings, you can specify "to obtain IP address automatically" or manually assign it.

Domain Name System (DNS)

Domain Name System is a name resolution service that allows you to input a website name and get its IP address.

With administrative permissions you can change the default DNS server address manually.
You could view or update this from,
Control Panel\Network and Internet\Network and Sharing Center
Right click the active network adapter and click properties
Click IPv4, then, click Properties



Commands for troubleshooting connections include ping, ipconfig, tracert and netsh.

Ping can be used to check whether one computer can reach another. It uses echo requests to perform this task and transmits those requests using Internet Control Message Protocol (ICMP). The syntax is "ping www.example.com" on the command prompt.

To see whether your own computer's TCP/IP stack is configured properly, combine the ping command with the loopback address of 127.0.0.1. "ping 127.0.0.1" command sends packets to the local host for testing. If this is successful, the local computer's TCP/IP stack is configured properly.

```
C:\Users\homeuser>ping 127.0.0.1
```

```
Pinging 127.0.0.1 with 32 bytes of data:
```

```
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
```

```
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
```

```
Ping statistics for 127.0.0.1:
```

```
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

If this command shows a failure, something's wrong with the local host's TCP/IP configuration or with the computer itself. Perhaps the TCP/IP protocol isn't installed. Note that a successful ping to the local

host does not mean the network card is working. To see whether the network card is working, ping something outside the computer. If the request times out then there was no answer from the destination computer in the allotted time designated by TTL (Time To Live) value, or that no route back to the local host exists at this time.

The TTL types of failure can be caused by many reasons, but the most common is that the remote computer is not turned on. Here are a few others:

- Default gateway cannot be reached
- Firewall is misconfigured
- There are insufficient network resources
- There are hardware errors
- There are router problems
- The destination host can't receive ping requests
- Remote network is unreachable
- TTL limit expired for any reason

If packets are lost along the way from the host to destination computer, you can figure out where they are lost by using **tracert** command. In doing so, it's possible to see where packets get held up or fail in their transmission.

Say computers are connected as follows.

Computer A --- Router B --- Router C ----- Computer D

A tracert (traceroute on Unix variants) from Computer A to IP address that belongs to D involves the following steps.

1. Tracert or traceroute from A sends a block of three ICMP packets with value of 1 in its TTL field to D
2. Router B responds with ICMP packet back to A because the packets have a TTL of 1
3. Tracert or traceroute from A then sends a second block of three packets with a value of 2 in their TTL field to D. Router B changes the packets TTL to 1 and sends them to router C.
4. Router C responds with ICMP packet back to A because the packets have a TTL of 1
5. Tracert or traceroute from A then sends a 3rd block of three packets with a TTL value of 3 this time to D. Router B changes the packet's TTL to 2 and sends them to router C which changes the packet's TTL to 1 and sends them to D. D sends ICMP response back to A.

A star in the tracert or traceroute response means the intermediary did not reveal its name or IP address.

Pathping is ping and tracert put together. A single command pings each node. The output includes details of the path between the two hosts and time stats for each node. The behavior of the nodes is studied over 25 secs each. This is in comparison to the default ping sample or default tracert single-route trace. Pathping first does a tracert to the destination. Then it uses ICMP to ping each hop 100 times. This is used to verify latency between the source host and the destination. Sometimes on public hosts you cannot completely rely on ICMP which could result in failures. The output shows the number of hops needed to reach the destination. Pathping also computes the statistics of RTT round-trip time as well as percentage of how many packets were dropped between the two hosts. Loss rates indicate that these routes may be overloaded. Pathping is a better diagnostic tool to use if latency in your network is

a concern. As an aside, a tool that ISPs use to prevent overwhelming floods of ICMP is called Control Plane Policing (CoPP). This type of flood prevention can also alter Pathping results.

For example, try pathping 8.8.8.8

C:\Users\homeuser>pathping /?

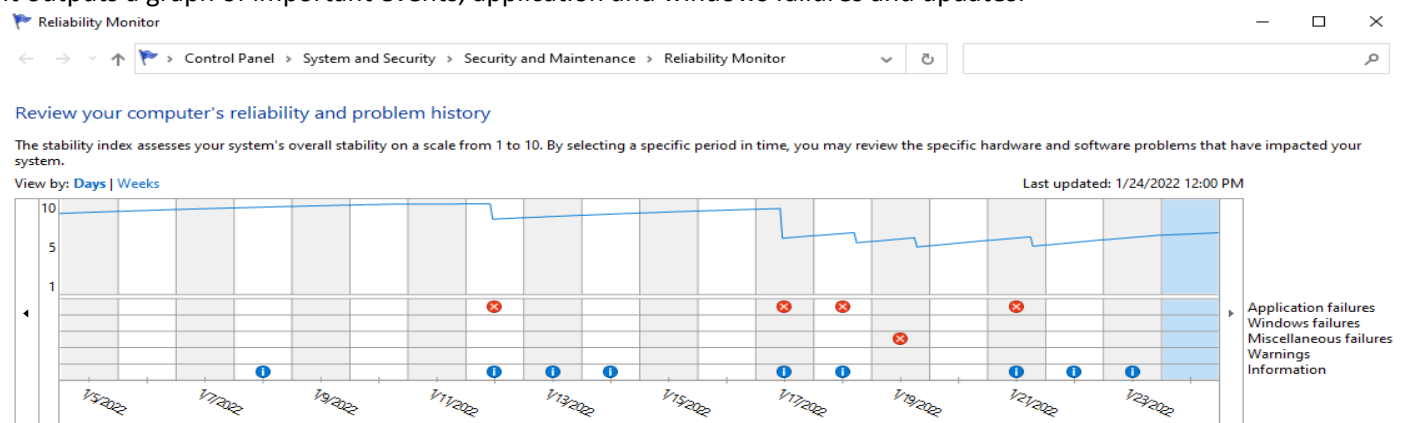
Usage: pathping [-g host-list] [-h maximum_hops] [-i address] [-n]
[-p period] [-q num_queries] [-w timeout]
[-4] [-6] target_name

Options:

- g host-list Loose source route along host-list.
- h maximum_hops Maximum number of hops to search for target.
- i address Use the specified source address.
- n Do not resolve addresses to hostnames.
- p period Wait period milliseconds between pings.
- q num_queries Number of queries per hop.
- w timeout Wait timeout milliseconds for each reply.
- 4 Force using IPv4.
- 6 Force using IPv6.

Additional tools for Troubleshooting include the following.

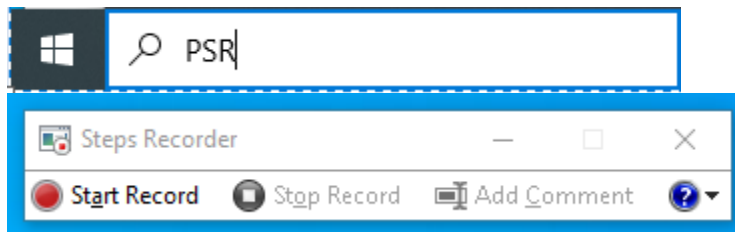
Reliability monitor shows the stability information for the machine in a timeline to see reliability history. It outputs a graph of important events, application and windows failures and updates.



It is showing critical events marked by red circles and informational events in blue circles. Failures reported can include when a program stopped working or when Windows did not shut down properly. This would also show the Blue/Black screen of Death (BSOD) marked with a red circle with a white x inside. Clicking on the red circle will give an indication of what caused the problem. BSOD may be caused by bad drivers, overheating or installing software that is incompatible with the hardware or OS.

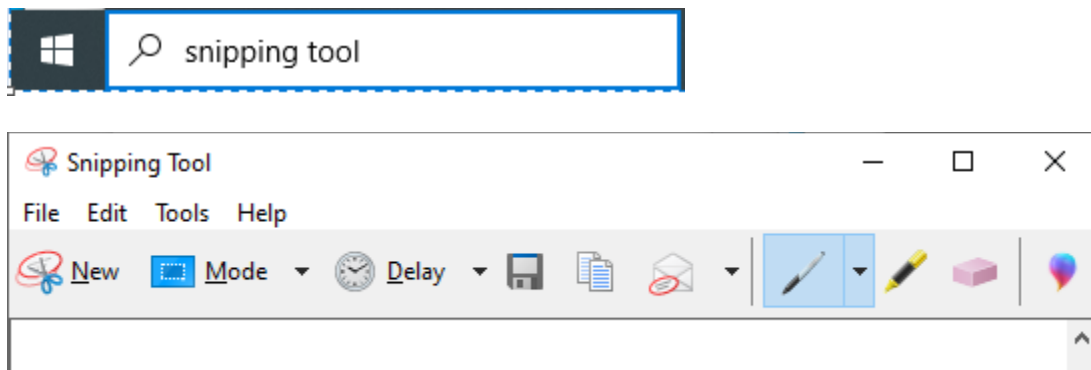
The lower left corner of the screen has a link to save Reliability history as an XML file. This file can be exported and analyzed. Next to this is the View all problem reports link.

Problem Steps Recorder (PSR) is a troubleshooting assistance, screen capture and annotation tool. It can be used to document steps with annotated screen shots. To open it type PSR in the taskbar search box and press enter or select the app and click it.



To record steps click "start Record". To stop, click "stop record" to review and save your recording of steps. When you save it, it is saved in a .zip file by default. This MHTML file can be opened and edited with Word. It includes the steps performed. PSR by default limits to 25 screenshots which can be adjusted from the settings in the Help menu. It won't capture streaming video or passwords or full screen games. The tool delivers a flat file.

Snipping tool can be used to collect screenshots or parts of screenshot. Snipping tool can be launch by typing snipping tool in the taskbar search box and pressing enter or by selecting the app and clicking it.



Snipped information could be saved as a picture.

Adapted from Windows network troubleshooting by Halsey, Ballew; Blue team toolkit, Nadeen Tanner

References

- [1] Windows 10 in depth, Knittel, McFedries
- [2] Windows Networking Troubleshooting, Halsey, Ballew
- [3] Head First Networking, Anderson, Benedetti
- [4] Cybersecurity blue team toolkit, Nadeen Tanner
- [5] Computer Networking, Kurose, Ross
- [6] en.wikipedia.org
- [7] Network Security, Firewalls & VPNs, Stewart, Kinsey
- [8] Understanding the digital world, Kernighan
- [9] Windows Powershell 3.0, Ed Wilson