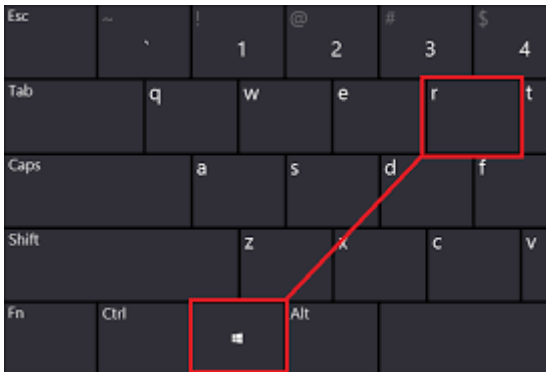


WINDOWS COMMAND LINE TOOLS

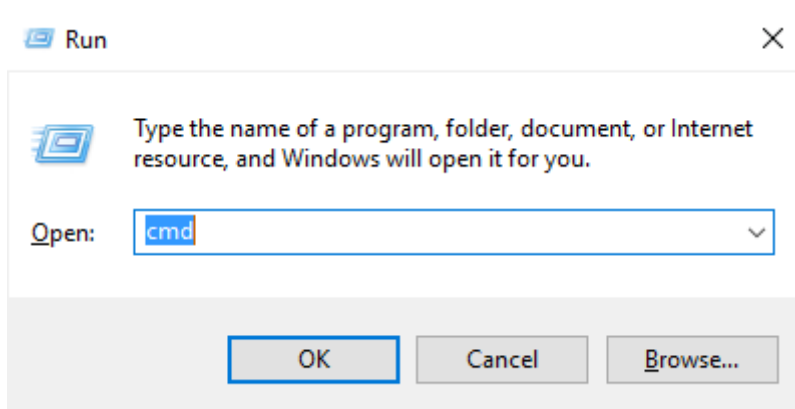
Command line tools are an excellent method of establishing the settings of a computer and obtaining valuable evidence or fixing connection problems.

Some of the information you can obtain from the command line is available elsewhere, some is not.

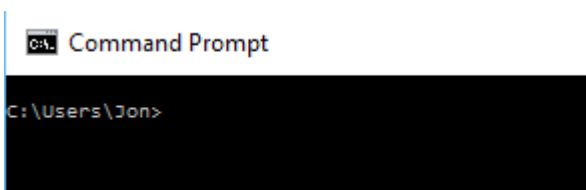
To open the command line on a Windows machine, hold the 'Windows Key' down and press the 'r' key



The 'Run' dialogue box will open. Type in the letters '**cmd**', which is short for command, and press 'OK'



This will open up the command line prompt. From here you can type the various commands discussed in this document.



ipconfig

This tool displays the current configuration of your computers IP connections, including your LOCAL IP address on your network and your DEFAULT GATEWAY (router). This is useful if you want to address the default gateway (router) directly and alter its settings.

Also displayed here is the SUBNET MASK which helps you establish how large a network may be or how it is configured.

There are sometime many connections displayed, the current active one is the one which has an IP address after DEFAULT GATEWAY. Non active connections will not have this field populated.

```
CA: Command Prompt
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\Jon>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix . . . : home
    Link-local IPv6 Address . . . . . : fe80::5c1ecb4:7552:c23e%8
    IPv4 Address. . . . . : 192.168.1.84
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.254

Ethernet adapter VirtualBox Host-Only Network:

    Connection-specific DNS Suffix . . . :
    Link-local IPv6 Address . . . . . : fe80::7146:d84b:dda3:3753%7
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Ethernet adapter Ethernet 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Connection-specific DNS Suffix . . . :
    IPv6 Address. . . . . : 2001:0:5ef5:79fd:0:2ded:ae79:d406
    Link-local IPv6 Address . . . . . : fe80::2ded:ae79:d406%4
    Default Gateway . . . . . : ::

Tunnel adapter isatap.home:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . : home

Tunnel adapter isatap.{CD9CC8A0-A74E-4A61-9FDD-4AA64590CEAE}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . :

C:\Users\Jon>
```

ipconfig /all

This tool is similar to ipconfig, but provides more information.

This most important pieces of extra information displayed are a description of the network, the PHYSICAL or MAC ADDRESS of the connection to the network, the address of the DNS servers being used if any and the address of the DHCP server, which deals with allocating IP addresses on a local network.

As with ipconfig, there are sometimes many connections displayed, the current active one is the one which has an IP address after DEFAULT GATEWAY. Non active connections will not have this field populated.

Command Prompt

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

Windows IP Configuration

Host Name . . . . . : jonserver
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : home

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : home
Description . . . . . : Intel(R) 82579LM Gigabit Network Connection
Physical Address. . . . . : 8C-DC-D4-43-D3-52
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::9a:ecb4:7552:c23e%8(Preferred)
IPv4 Address. . . . . : 192.168.1.84(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 04 April 2016 10:08:02
Lease Expires . . . . . : 06 April 2016 10:08:02
Default Gateway . . . . . : 192.168.1.254
DHCP Server . . . . . : 192.168.1.254
DHCPv6 IAD . . . . . : 59563220
DHCPv6 Client DUID. . . . . : 00-01-00-01-10-00-78-39-8C-DC-D4-43-D3-52
DNS Servers . . . . . : 192.168.1.254
NetBIOS over Tcpip. . . . . : Enabled
```

ipconfig /displaydns

This is a useful tool which displays internet activity on a computer, even if the history is deleted from the browser.

This is VOLATILE CACHE and is over written or deleted after a set period of time.

The entry Time To Live (TTL) specifies how long that record will remain in the cache, in seconds.

```
C:\> Command Prompt

C:\Users\Jon>ipconfig /displaydns

Windows IP Configuration

bbc.co.uk
-----
No records of type AAAA

bbc.co.uk
-----
Record Name . . . . . : bbc.co.uk
Record Type . . . . . : 1
Time To Live . . . . . : 86400
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 194.61.183.46

46.183.61.194.in-addr.arpa
-----
Record Name . . . . . : 46.183.61.194.in-addr.arpa.
Record Type . . . . . : 12
Time To Live . . . . . : 86400
Data Length . . . . . : 8
Section . . . . . : Answer
PTR Record . . . . . : bbc.co.uk

v10.vortex-win.data.microsoft.com
-----
Record Name . . . . . : v10.vortex-win.data.microsoft.com
Record Type . . . . . : 5
Time To Live . . . . . : 136
Data Length . . . . . : 8
Section . . . . . : Answer
CNAME Record . . . . . : v10-win.vortex.data.microsoft.com.akadns.net
```

nslookup

This tool is NAMESERVER LOOKUP.

It returns the IP address where a website is hosted and uses DNS to obtain this information. It also displays the name and IP address of the default gateway used to carry out the DNS enquiry.

```
nslookup bbc.co.uk
```

Command Prompt

```
C:\Users\Jon>nslookup bbc.co.uk
Server:   BTBusinessHub.home
Address:  192.168.1.254

Non-authoritative answer:
Name:     bbc.co.uk
Addresses: 212.58.246.78
           212.58.244.22
           212.58.244.23
           212.58.246.79

C:\Users\Jon>
```

ping

The ping tool establishes if a connection exists between a local machine and a local or external resource, such as a website or server. If a connection is available, the time taken and the efficiency of the connection is displayed.

If no connection is available, the request will time out.

To test your connection to your default gateway (router) you can ping it, having obtained its IP address using **ipconfig**

ping 192.168.1.254

```
C:\> Command Prompt

C:\Users\Jon>ping 192.168.1.254

Pinging 192.168.1.254 with 32 bytes of data:
Reply from 192.168.1.254: bytes=32 time=1ms TTL=64
Reply from 192.168.1.254: bytes=32 time=1ms TTL=64
Reply from 192.168.1.254: bytes=32 time=1ms TTL=64
Reply from 192.168.1.254: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\Jon>
```

Or you can ping a domain, which is a good way of testing your connection to the Internet

ping google.com

```
C:\> Command Prompt

C:\Users\Jon>ping google.co.uk

Pinging google.co.uk [216.58.198.227] with 32 bytes of data:
Reply from 216.58.198.227: bytes=32 time=171ms TTL=51
Reply from 216.58.198.227: bytes=32 time=14ms TTL=51
Reply from 216.58.198.227: bytes=32 time=14ms TTL=51
Reply from 216.58.198.227: bytes=32 time=14ms TTL=51

Ping statistics for 216.58.198.227:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 14ms, Maximum = 171ms, Average = 53ms

C:\Users\Jon>
```