

15 Useful Windows Networking Commands You Should Know

by Chris Colwill

Affiliate Disclosure: As an Amazon Associate I earn from qualifying purchases.

Windows comes with some incredibly useful networking commands that are powerful, yet very easy to use and access from the command prompt, also referred to as cmd.

Here are 15 of the most useful networking commands available in Windows you should know about to make gathering information, identifying issues and fixing problems much easier and quicker.

Contents [[hide](#)]

How to Access Command Prompt in Windows

1. PING

Used for: Troubleshooting network connection issues

2. IPCONFIG

Used for: Quickly finding your IP address

3. GETMAC

Used for: Quickly finding your MAC address

4. ARP

Used for: Troubleshooting network connection issues

5. HOSTNAME

Used for: Quickly finding your hostname

6. NSLOOKUP

Used for: Troubleshooting network connection issues

7. NBTSTAT

Used for: Troubleshooting NetBIOS issues

8. NET

Used for: Displaying available Net switches

9. NETSTAT

Used for: Displaying network statistics

10. NETSH

Used for: Displaying and configuring network adapters

11. TASKKILL

Used for: Ending processes

12. TRACERT

Used for: Troubleshooting network connection issues

13. PATHPING

Used for: Troubleshooting network connection issues

14. SYSTEMINFO

Used for: Displaying system information

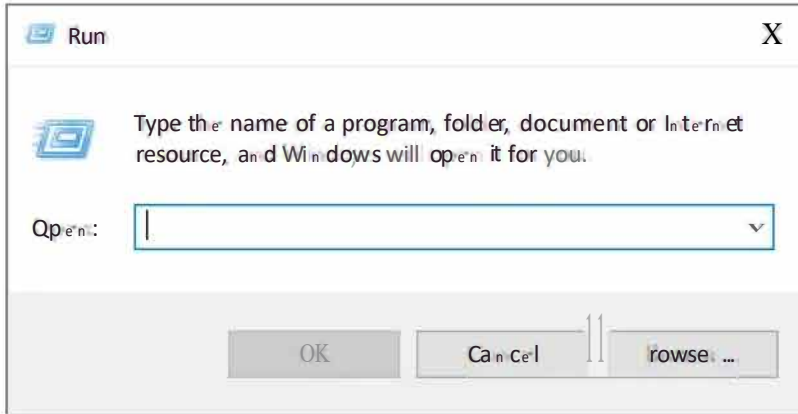
15. NET VIEW

Used for: Viewing devices connected to a network

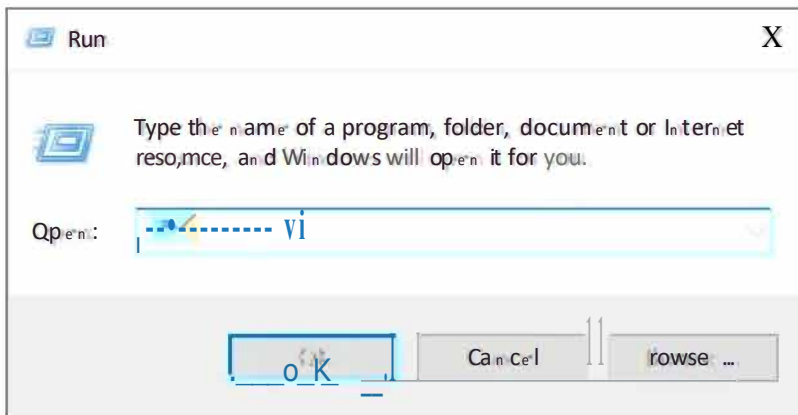
How to Access Command Prompt in

Windows

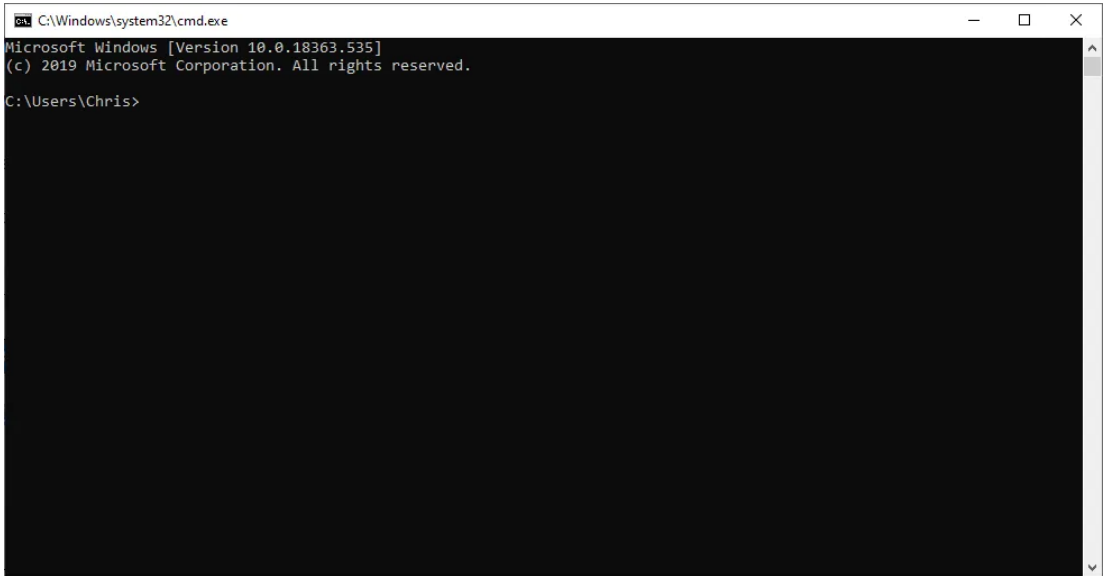
1. Right-click on the Start button and select Run to open the Run window



2. Type cmd into the field and click on OK



3. The Command Prompt window will open

A screenshot of a Windows Command Prompt window. The title bar at the top reads "C:\Windows\system32\cmd.exe". The window content shows the following text: "Microsoft Windows [Version 10.0.18363.535]" on the first line, "(c) 2019 Microsoft Corporation. All rights reserved." on the second line, and "C:\Users\Chris>" on the third line. The rest of the window is black with no visible text or cursor.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.18363.535]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\Users\Chris>
```

1. PING

Used for: Troubleshooting network connection issues

Command to enter: *ping*

The ping command is one you are likely to be familiar with as it is one of the most widely used utilities, but it is still essential nonetheless.

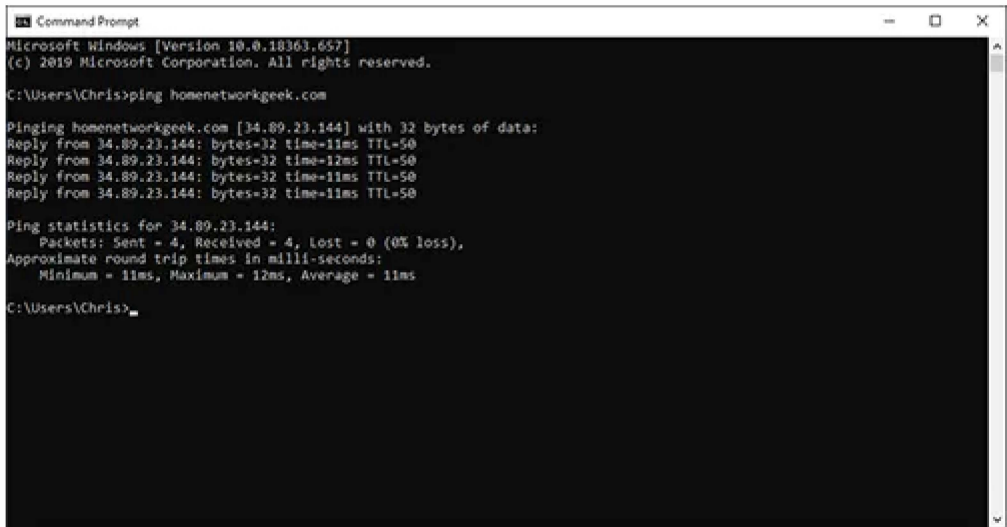
Ping is used to test whether one network host is able to communicate with another.

Assuming there is nothing in place to stop the ping reaching its destination, like a firewall or a network problem, the

device will respond to the ping with four data packets.

If you receive these packets back, the ping confirms that a working network path exists between you and the destination host.

I have a dedicated article on [how to use the ping command](#) that goes into this essential command in greater detail.



```
Command Prompt
Microsoft Windows [Version 10.0.18363.657]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Chris>ping homenetworkgeek.com

Pinging homenetworkgeek.com [34.89.23.144] with 32 bytes of data:
Reply from 34.89.23.144: bytes=32 time=11ms TTL=50
Reply from 34.89.23.144: bytes=32 time=12ms TTL=50
Reply from 34.89.23.144: bytes=32 time=11ms TTL=50
Reply from 34.89.23.144: bytes=32 time=11ms TTL=50

Ping statistics for 34.89.23.144:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 12ms, Average = 11ms

C:\Users\Chris>
```

2. IPCONFIG

Used for: Quickly finding your IP address

Command to enter: *ipconfig*

IPConfig is one command I find myself using a great deal as it can provide you with a lot of useful information from just the one command.

Simply, the IPConfig command displays basic IP address configuration information for the Windows device you are working on.

IPConfig has a few switches associated with it to provide additional information as well as perform certain actions:

- IPConfig /all- Displays additional information for all network adapters
- IPConfig /release - Releases the IP address you are currently using
- IPConfig /renew - Renews an IP address on your device
- IPConfig /flushdns - Flushes the DNS cache
- IPConfig /? - Displays help for IPConfig and its switches

```

Select Command Prompt
Microsoft Windows [Version 10.0.18363.657]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Chris>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

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

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 2:

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

Wireless LAN adapter Local Area Connection* 11:

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

Wireless LAN adapter WiFi:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : 
    IPv4 Address. . . . . : 
    Subnet Mask . . . . . : 
    Default Gateway . . . . . : 

Ethernet adapter Bluetooth Network Connection 2:

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

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2001:0:2851:7ae4:4dd:1aa:ccf6:ad40
    Link-local IPv6 Address . . . . . : fe80::4dd:1aa:ccf6:ad40%14
    Default Gateway . . . . . : ::

C:\Users\Chris>

```

3. GETMAC

Used for: Quickly finding your MAC address

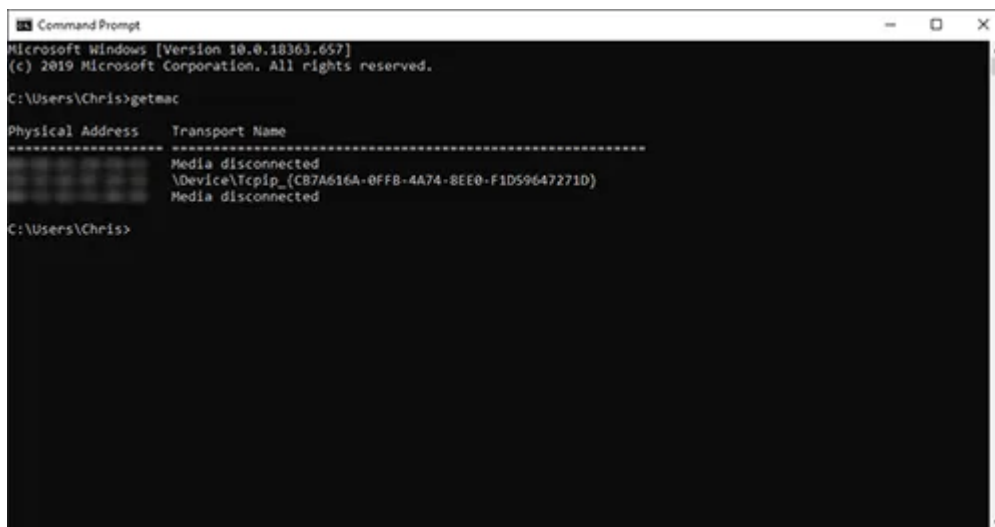
Command to enter: getmac

In order to be compliant with the IEEE 802 standards, each device must have a unique MAC (Media Access Control) address.

The manufacturer of your device will assign it a MAC address and store it within the hardware.

The `getmac` command provides an easy way to find the MAC address of your device. If you see more than one MAC address for your device, it will have multiple network adapters. As an example, a laptop with both Ethernet and Wi-Fi will have two separate MAC addresses.

Some administrators will use the unique MAC addresses of devices to limit what can and cannot connect to a network.



```
Command Prompt
Microsoft Windows [Version 10.0.18363.657]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Chris>getmac

Physical Address    Transport Name
-----
Media disconnected
\Device\NPF{CB7A616A-0FFB-4A74-BEE0-F1D59647271D}
Media disconnected

C:\Users\Chris>
```

4. ARP

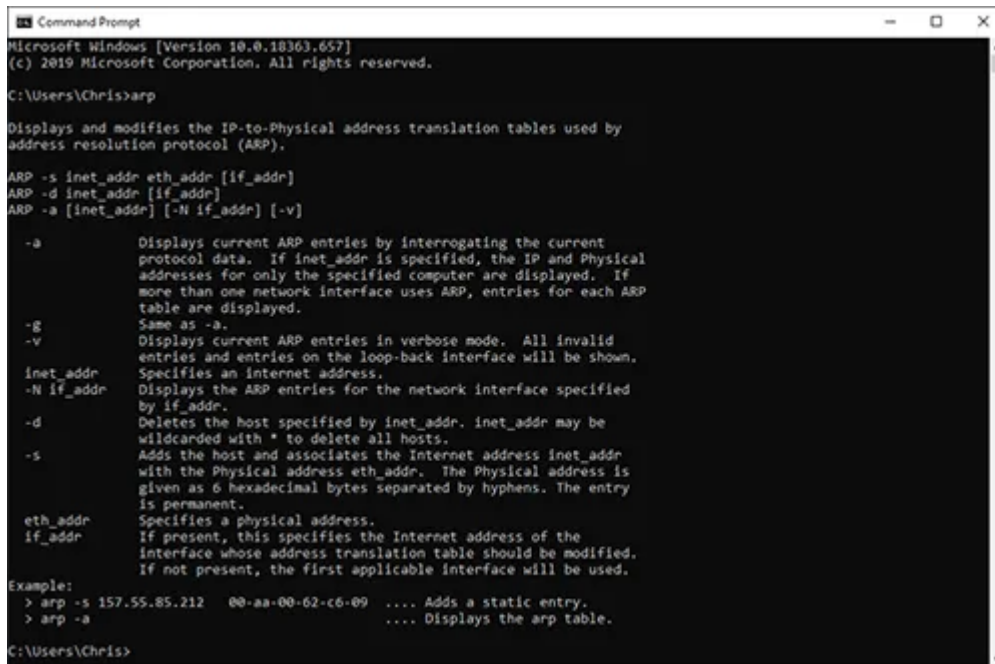
Used for: Troubleshooting network connection issues

Command to enter: *arp*

ARP stands for Address Resolution Protocol and the command is used to map an IP address to a MAC address.

It is easy to assume that communication over a network takes place using just IP addresses, but this is not the case. The delivery of packets is ultimately dependent on the MAC address of the device's network adapter, not the IP address.

By using the arp command, you can display and modify the Address Resolution Protocol cache; useful for resolving address resolution problems.



```
Microsoft Windows [Version 10.0.18363.657]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Chris>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.

Example:
> arp -s 157.55.85.212 00-AA-00-62-C6-09 .... Adds a static entry.
> arp -a              .... Displays the arp table.

C:\Users\Chris>
```

5. HOSTNAME

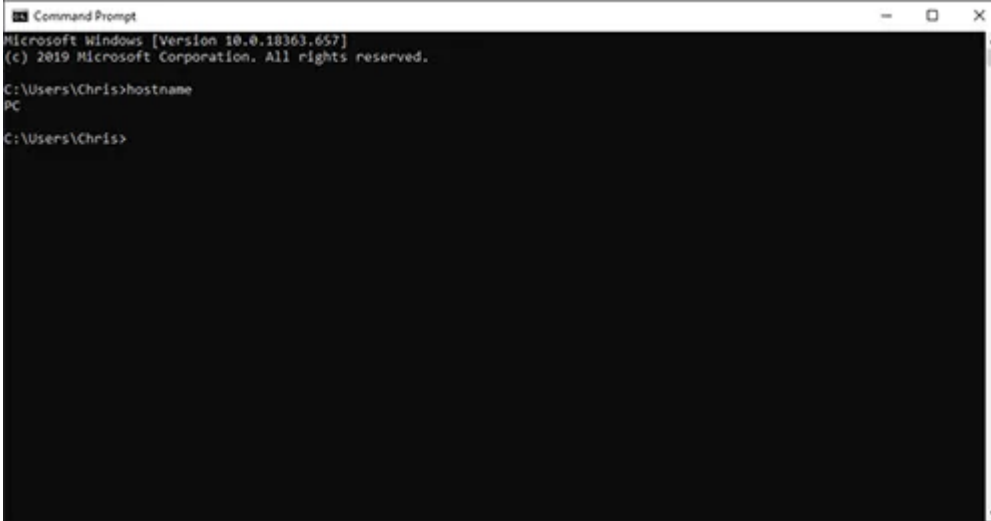
Used for: Quickening finding your hostname

Command to enter: *hostname*

The hostname command provides you with an easy way of identifying the hostname that has been assigned to your Windows device.

There are ways of being able to find this through Windows, but using the command line is much quicker.

Simply type hostname into the command prompt and it will present you with the local computer name of your device.

A screenshot of a Windows Command Prompt window. The title bar reads 'Command Prompt'. The window content shows the following text: 'Microsoft Windows [Version 10.0.18363.657]' followed by '(c) 2019 Microsoft Corporation. All rights reserved.' The prompt is 'C:\Users\Chris>hostname'. The output is 'PC'. The prompt is now 'C:\Users\Chris>'.

6. NSLOOKUP

Used for: Troubleshooting network connection issues

Command to enter: *nslookup*

NSLookup is useful for diagnosing DNS name resolution problems.

By typing nslookup into the command prompt, you will be presented with the name and IP address of your device's DNS server.

For you at home, this will more than likely be your router, but in enterprise environments, this will probably be a dedicated DNS server.

NSLookup can be used to find the IP address of a device, find the domain name of an IP address and find mail servers for a domain.

```
Command Prompt - nbtstat
Microsoft Windows [Version 10.0.18363.657]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Chris>nbtstat
Default Server: 192.168.1.100
Address: 192.168.1.100
>
```

7. NBTSTAT

Used for: Troubleshooting NetBIOS issues

Command to enter: *nbtstat*

As you now know from using the hostname command, each device running Windows will be assigned a computer name.

Often, there will be either a domain or workgroup that is also assigned and that the device is a member of. For you at home, your device is likely to be within its own workgroup.

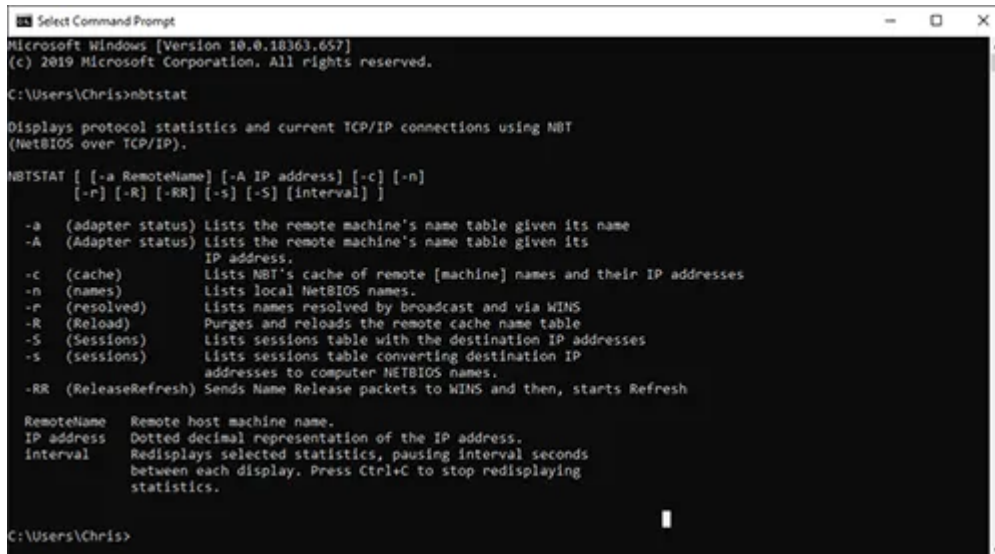
The technical term for the computer name is the NetBIOS name, which is where the nbtstat command comes into play.

Windows uses different methods to associate NetBIOS names with IP addresses; these include broadcast and LMHost lookup.

There are times in which this mapping breaks down, so the nbtstat command is used to help you diagnose and resolve these problems.

Nbtstat -n will show the NetBIOS names that are in use by a device, whereas the nbtstat -r command shows how many

NetBIOS names a device has recently been able to resolve.



```
Select Command Prompt
Microsoft Windows [Version 10.0.18363.657]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Chris>nbtstat

Displays protocol statistics and current TCP/IP connections using NBT
(NetBIOS over TCP/IP).

NBTSTAT [ [-a RemoteName] [-A IP address] [-c] [-n]
          [-r] [-R] [-RR] [-s] [-S] [interval] ]

-a (adapter status) Lists the remote machine's name table given its name
-A (Adapter status) Lists the remote machine's name table given its
                      IP address.
-c (cache)           Lists NBT's cache of remote [machine] names and their IP addresses
-n (names)           Lists local NetBIOS names.
-r (resolved)        Lists names resolved by broadcast and via WINS
-R (Reload)          Purges and reloads the remote cache name table
-S (Sessions)        Lists sessions table with the destination IP addresses
-s (sessions)        Lists sessions table converting destination IP
                      addresses to computer NETBIOS names.
-RR (ReleaseRefresh) Sends Name Release packets to WINS and then, starts Refresh

RemoteName  Remote host machine name.
IP address   Dotted decimal representation of the IP address.
interval     Redisplays selected statistics, pausing interval seconds
              between each display. Press Ctrl+C to stop redisplaying
              statistics.

C:\Users\Chris>
```

8. NET

Used for: Displaying available Net switches

Command to enter: *net*

The net command is definitely a versatile one, allowing you to manage many different aspects of a network and its settings such as network shares, users and print jobs, as just a few examples.

Running just net won't do much, but it will present you with a list of all the switches that are available.

These include accounts to set password and logon requirements, file to show a list of open files and sessions to list, or even disconnect, sessions on the network.

If you are ever in doubt as to what task each switch performs, run net help and I'm sure you'll find the answer.

```
Microsoft Windows [Version 10.0.18363.657]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Chris>net
The syntax of this command is:

NET
 [ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
  HELPMMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
  STATISTICS | STOP | TIME | USE | USER | VIEW ]

C:\Users\Chris>
```

9. NETSTAT

Used for: Displaying network statistics

Command to enter: *netstat*

Viewing network statistics is a great way to troubleshoot any problems you are experiencing on your network and may well point you in the direction of the root cause.

The netstat command does just that; present you with a useful network summary for your device.

Run netstat and you'll see a list of active connections, with more being added every few seconds. It will describe the protocol being used, the local address, the foreign address, and the connections state.

To see some interface statistics including bytes sent and received, errors sent and received, and unknown protocols use the netstat -e switch.

```
Command Prompt - netstat
Microsoft Windows [Version 10.0.18363.657]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Chris>netstat

Active Connections

Proto Local Address           Foreign Address         State
TCP    0.0.0.0:80                0.0.0.0:0               ESTABLISHED
TCP    0.0.0.0:443               0.0.0.0:0               ESTABLISHED
TCP    0.0.0.0:8080              0.0.0.0:0               ESTABLISHED
TCP    0.0.0.0:8080              0.0.0.0:0               ESTABLISHED
TCP    0.0.0.0:8080              0.0.0.0:0               CLOSE_WAIT
TCP    0.0.0.0:8080              0.0.0.0:0               ESTABLISHED
TCP    0.0.0.0:8080              0.0.0.0:0               ESTABLISHED
```

10. NETSH

Used for: Displaying and configuring network adapters

Command to enter: *netsh*

Netsh is another very powerful command, allowing you to view and configure almost all of the network adapters in your device in much greater detail compared with some other commands.

When you run the netsh command on its own, the command prompt will be shifted into network shell mode. Within this mode, there are several different “contexts”, such as one for DHCP-related commands, one for diagnostics and one for routing.

It is possible to still run individual commands from netsh, though.

In order to see all of the available netsh contexts, run netsh /?

To see all of the commands available within a context, run netsh contextname /?

Subcommands are available within certain commands. To view these, run `netsh contextname show /?`

As an example, you can run the `netsh wlan show drivers` command to view all of the wireless network drivers on your device and their properties.

11. TASKKILL

Used for: Ending processes

Command to enter: *taskkill*

I'm sure you are familiar with being able to end a process using the Task Manager, but did you know it is also possible from the command line?

Well, you certainly can, and you have the option to kill a task or process using either the process ID or by the file name.

If you aren't sure of which processes are running and therefore don't know what needs to be killed, first use the tasklist command to see the process name (listed as the image name) in addition to how much memory that process is using.

Once you know the process name, you can use taskkill /IM processname.exe to end it.

In some cases, using just the taskkill command is not enough and we need to forcibly stop a process. An example being if we try and kill Internet Explorer when we have multiple tabs open. In this case, you can use the taskkill /f /IM iexplore.exe to forcibly kill the process.

There are many different switches available for the taskkill command. To view them all, run taskkill /?.

12. TRACERT

Used for: Troubleshooting network connection issues

Command to enter: tracert

By using the tracert command you can trace the route a packet takes before reaching its destination, and see information on each "hop" along the route.

A hop refers to the number of routers that a packet passes through along its route. Sometimes a hop is counted when the packet passes through other pieces of networking

hardware, such as repeaters, switches, and access points, but this isn't always the case as it depends on how these devices are configured and the role they play on the network.

After running the `tracert` command, you will be presented with a line by line summary of each hop which includes the latency between your device and that particular hop and the IP address of the hop.

Let's say you run the `ping` command to test the reachability of a website. In this example, you do not receive a reply so the site cannot be contacted.

You can then use the `tracert` command to show you exactly where the problem is occurring. It could be a fault at your end, or the website itself may be unavailable.

13. PATHPING

Used for: Troubleshooting network connection issues

Command to enter: *pathping*

We have already described the `ping` and `tracert` commands and the similarities between the two.

As you have probably already guessed by the name of the command, pathping combines that best of both ping and tracert into a single utility.

Enter pathping followed by a hostname into the command prompt and it will initiate what looks like a regular old tracert command.

Let the process finish, however, and you will be provided with more detail than either ping or tracert can provide, such as latency reports and statistics on packet loss.

Be patient when using the pathping command as it will take five minutes in order to gather all of the statistics for you.

14. SYSTEMINFO

Used for: Displaying system information

Command to enter: *systeminfo*

If you need to know anything about the device you are using, be it details of the processor used, the version of Windows you are operating on, or what the boot device is configured as, you can find it all through the Windows GUI.

But why would you want to spend time doing that when you can run this simple command to see it all in one place?

This command will poll your device and display the most important information in a clean, easy to read format.

15. NET VIEW

Used for: Viewing devices connected to a network

Command to enter: *net view*

There may be a time where you want to see what devices are connected to your network. This is where the net view

command comes in.

Simply run the net view command and after a short while you will be presented with a list of devices that are connected to the same network as you.

The caveat with this command is that it may not show all of the devices connected to your network.

It works well enough for private networks but will fail to identify devices such as smartphones and printers, and it can have trouble identifying devices running a different operating system to Windows.

This simple command may work perfectly for you and your home network, but if not, you can always use the arp command we discussed earlier instead.

Affiliate Disclosure

Home Network Geek is a participant in the Amazon Services LLC Associates Program, an affiliate advertising program designed to provide a means for sites to earn advertising fees by advertising and linking to Amazon.com