**1. Ping Command**

The ping command is one of the most often used networking utilities for detecting devices on a network and for troubleshooting network problems.

When you ping a device you send that device a short message, which it then sends back **(the echo**).

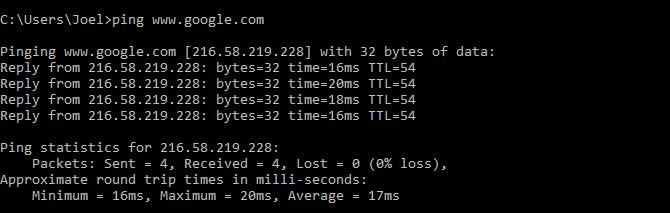
The general format is**ping hostname** or **ping IPaddress**.

Example

**ping www.google.com** or **ping 216.58.208.68**

This article covers the [ping command](http://www.steves-internet-guide.com/ping-command/) in more detail.

Sample usage and output:



The command works by sending out multiple data packets and seeing how many of them return. If some of them don’t return, it’ll tell you (“lost”). Packet loss leads to poor performance in games and streaming, and this is a nifty way to test.

**2. ipconfig Command**

Another indispensable and frequently used utility that is used for finding network information about your local machine like IP addresses, DNS addresses etc

**Basic Use: Finding Your IP Address and Default Gateway**

Type the command ipconfig at the prompt.

The following is displayed



**Ip config**has a number of switches the most common are**:**

**ipconfig /all** – displays more information about the network setup on your systems including the MAC address.

**ipconfig /release –**release the current IP address

**ipconfig /renew –**renew IP address

**ipconfig /?** -shows help

**ipconfig/flushdns** – flush the dns cache

## TRACERT

tracert stands for Trace Route. Like ping, it sends out a data packet as a way to troubleshoot any network issues you might have, but instead tracks the route of the packet as it hops from server to server.

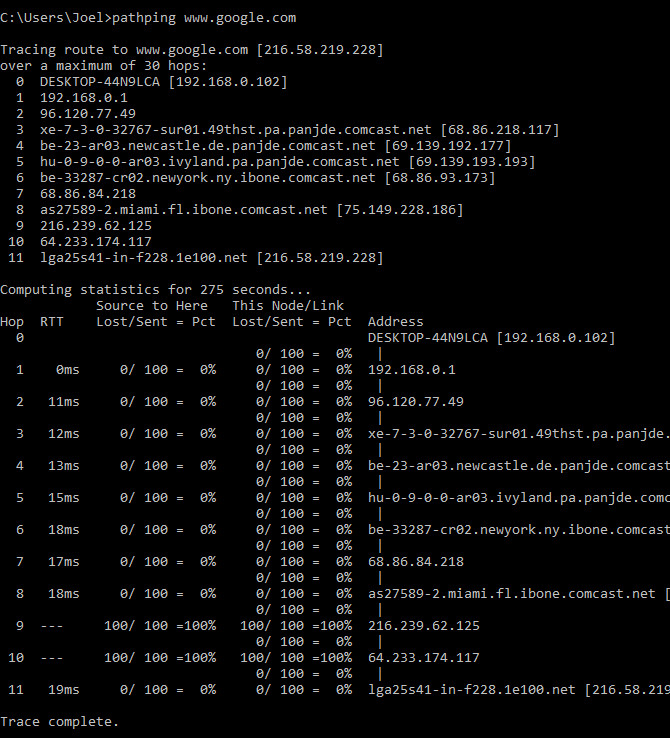
Sample usage:

The command outputs a line-by-line summary of each hop, including the latency between you and that particular hop and the IP address of that hop (plus domain name if available).

## 3. PATHPING

pathping is similar to tracert except more informative, which means it takes a lot longer to execute. After sending out packets from you to a given destination, it analyzes the route taken and computes packet loss on a per-hop basis.

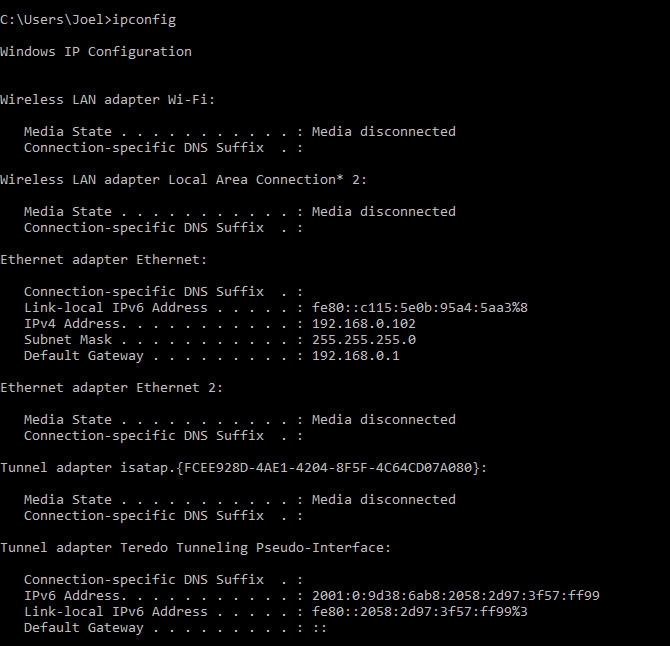
Sample usage and output:



## 4. IPCONFIG

ipconfig may just be the most-used networking command on Windows. Not only is it useful for the information it provides, but you can combine it with a couple switches to execute certain tasks.

Sample usage and output:



The default output shows every network adapter on your system and how they resolve. The **IPv4 Address** and **Default Gateway** details under the Wireless LAN Adapter and Ethernet Adapter sections are the most important to know.

Use this switch to flush your DNS cache:

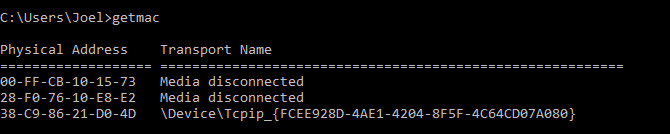
ipconfig /flushdns

Flushing the DNS cache can help when your internet is working, but a specific website or server is unreachable for some reason (e.g. a website times out and won’t load).

## 5. GETMAC

Every device that’s compliant with IEEE 802 standards has a unique MAC address (Media Access Control). MAC addresses are assigned by the manufacturer and are stored in the device’s hardware. Some people use MAC addresses to limit which devices can connect to the network.

Sample usage and output:

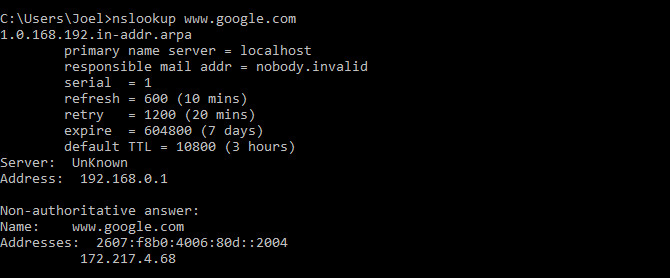


You may see more than one MAC address depending on how many network-related adapters are on your system. For example, Wi-Fi and Ethernet connections would have separate MAC addresses.

## 6. NSLOOKUP

nslookup stands for Name Server Lookup. It’s a nifty utility that’s packed with a lot of power, but most users don’t need all of that power. For regular folks like you and me, its main use is finding out the IP address behind a certain domain name.

Sample usage and output:



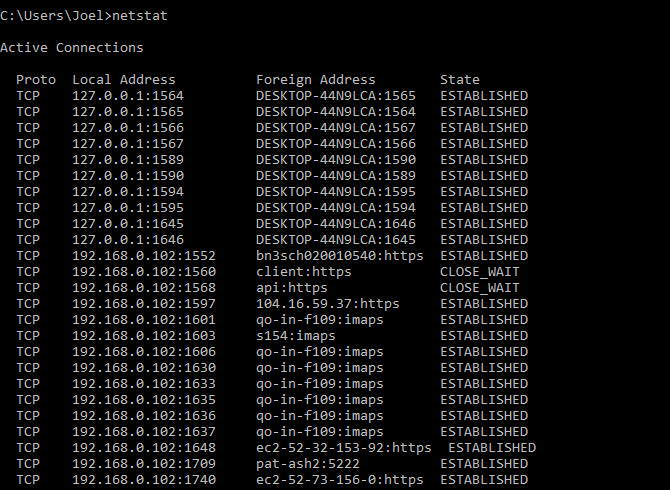
Note that certain domain names aren’t tied to a dedicated IP address, which means that you may get different IP addresses every time you run the command. This is normal for bigger websites because they spread their workload across many different machines.

If you want to convert an IP address into a domain name, just type it into your browser and see where it leads. Not all IP addresses lead to domain names though, and many IP addresses aren’t reachable over the web.

## 7. NETSTAT

netstat is a tool for network statistics, diagnostics, and analysis. It’s powerful and complex, but can be simple enough if you ignore the advanced aspects that you don’t need to know about (assuming you aren’t managing a massive business or campus network, for example).

Sample usage and output:



By default, the command shows all “active connections” on your system whether those connections are on LAN or across the internet. An active connection doesn’t mean data is being moved — it could just mean a port that’s open and ready to accept a connection.

Indeed, netstat is mostly useful to regular users for its ability to show port information, and that can come in handy when you need to forward ports.

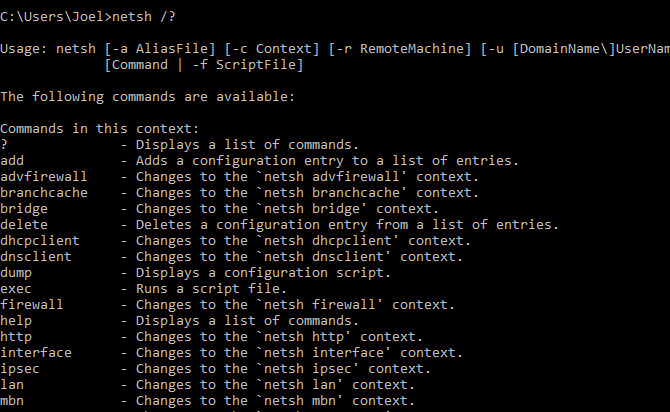
But the command also has about a dozen switches that change what kind of information is displayed, such as the -r switch which shows a routing table instead.

## 8. NETSH

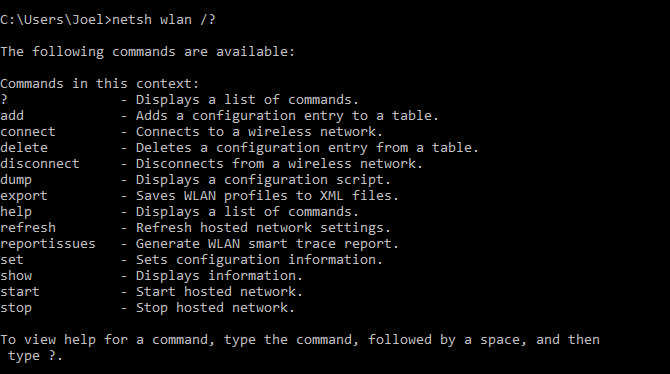
netsh stands for Network Shell. It’s a command that lets you view and configure pretty much every network adapter on your system, in more detail and granularity than any of the preceding commands.

Running the netsh command on its own will shift the Command Prompt into network shell mode. There are several different “contexts” within this shell, including one for routing-related commands, one for DHCP-related commands, and one for diagnostics, among others. But you can use it to run individual commands, too.

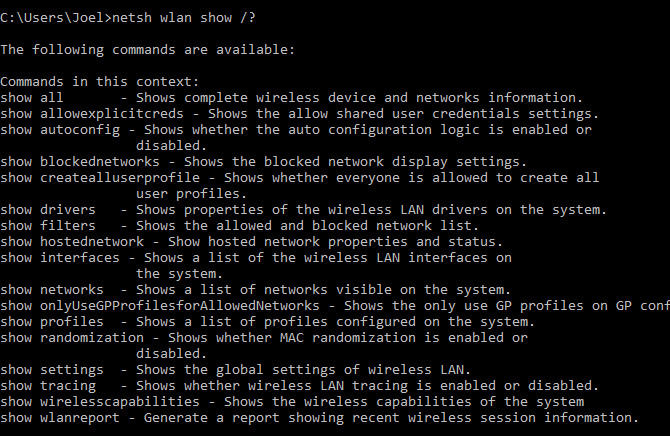
To see all network shell contexts:



And to see all commands within a context:



You can drill down one more layer to find all of the subcommands within those commands:



So for example, you can run this command to view all of the wireless network drivers on your system and their properties:

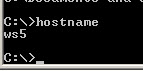
netsh wlan show drivers

It’s an advanced command that’s complex enough to deserve an entire article of its own. Just know that if you want to get real technical with your network configuration, you’ll probably need to use this command line utility.

Then again, everyone should have at least a little bit of Command Prompt experience. It can come in handy when you least expect it.

**3. Hostname Command**

A very simple command that displays the host name of your machine. This is much quicker than going to the control**panel>system** route.



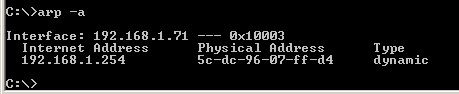
**4. getmac Command**

Another very simple command that shows the MAC address of your network interfaces



**5. arp Command**

This is used for showing the**address resolution cache**. This command must be used with a command line switch **arp -a** is the most common.



Type **arp** at the command line to see all available options.

See [using arp in the basic networking course](https://stevessmarthomeguide.com/basic-networking-course/#arp)

**6. NSlookup**

Used for checking DNS record entries. See [Using NSlookup](http://www.steves-internet-guide.com/using-nslookup/)for more details

**7. Nbtstat**

Diagnostic tool for troubleshooting netBIOS problems. See This [technet](https://technet.microsoft.com/en-us/library/cc940106.aspx" \t "_blank) article.

**8 Net Command**

Used for managing users,service,shares etc see [here](https://www.microsoft.com/resources/documentation)

**9. Netstat Command**

Used for displaying information about tcp and udp connections and ports. See [tcp and udp ports and sockets](http://www.steves-internet-guide.com/tcpip-ports-sockets/) and [how to use the netstat command](https://www.lifewire.com/netstat-command-2618098)

**10. TaskKill Command**

View a list of running tasks using the**tasklist** command and kill them by name or processor ID using the **taskKill** command- See this [tutorial](http://tweaks.com/windows/39559/kill-processes-from-command-prompt/).