NETWORK LAB ASSIGNMENT 6

SILJA C K

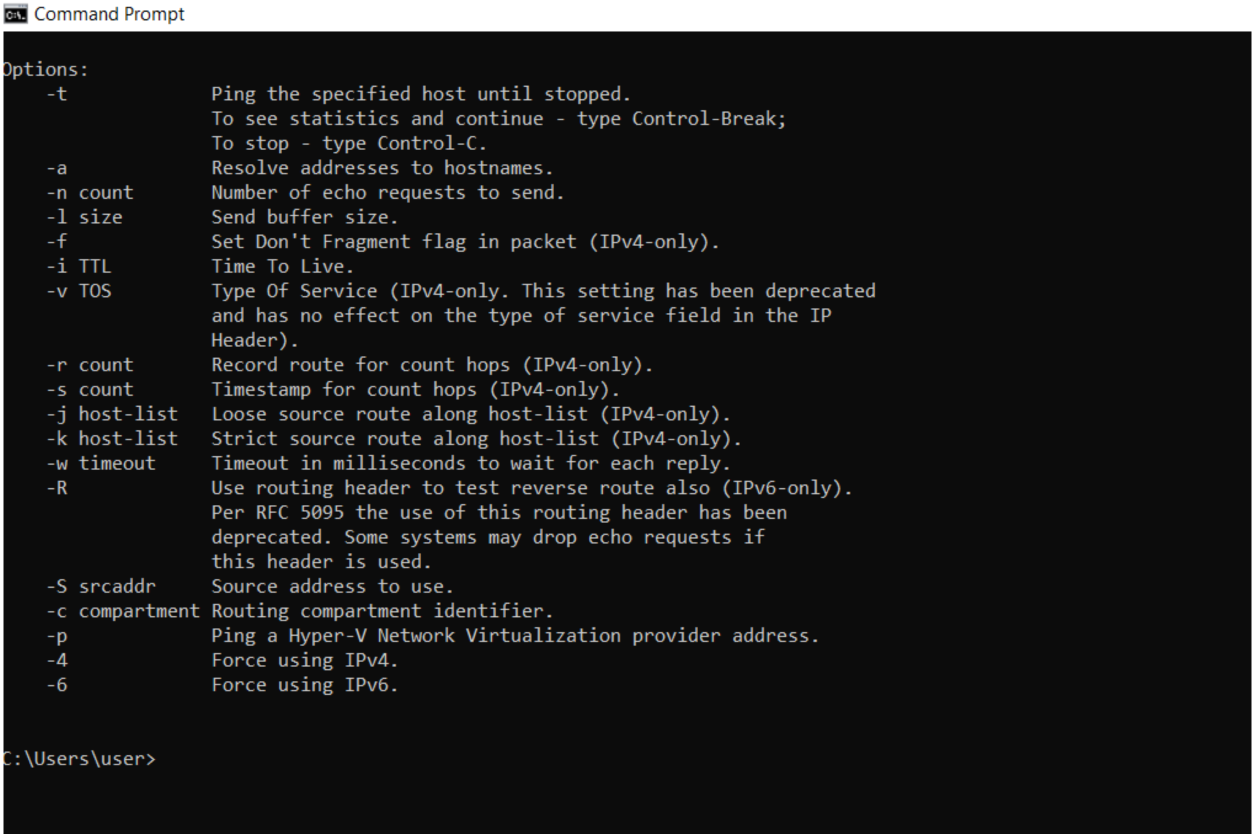
RMCA B

ROLL NO:20

Try out these network commands in Window as well as in Linux and perform at least 4 options with each command:ping, route traceroute, nslookup,IpConfig, NetStat .

- ping

Ping is an old Unix tool that has been around for a long time but many PC users are unfamiliar with the Windows version. Ping sends out a packet to a designated internet host or network computer and measures its response time.

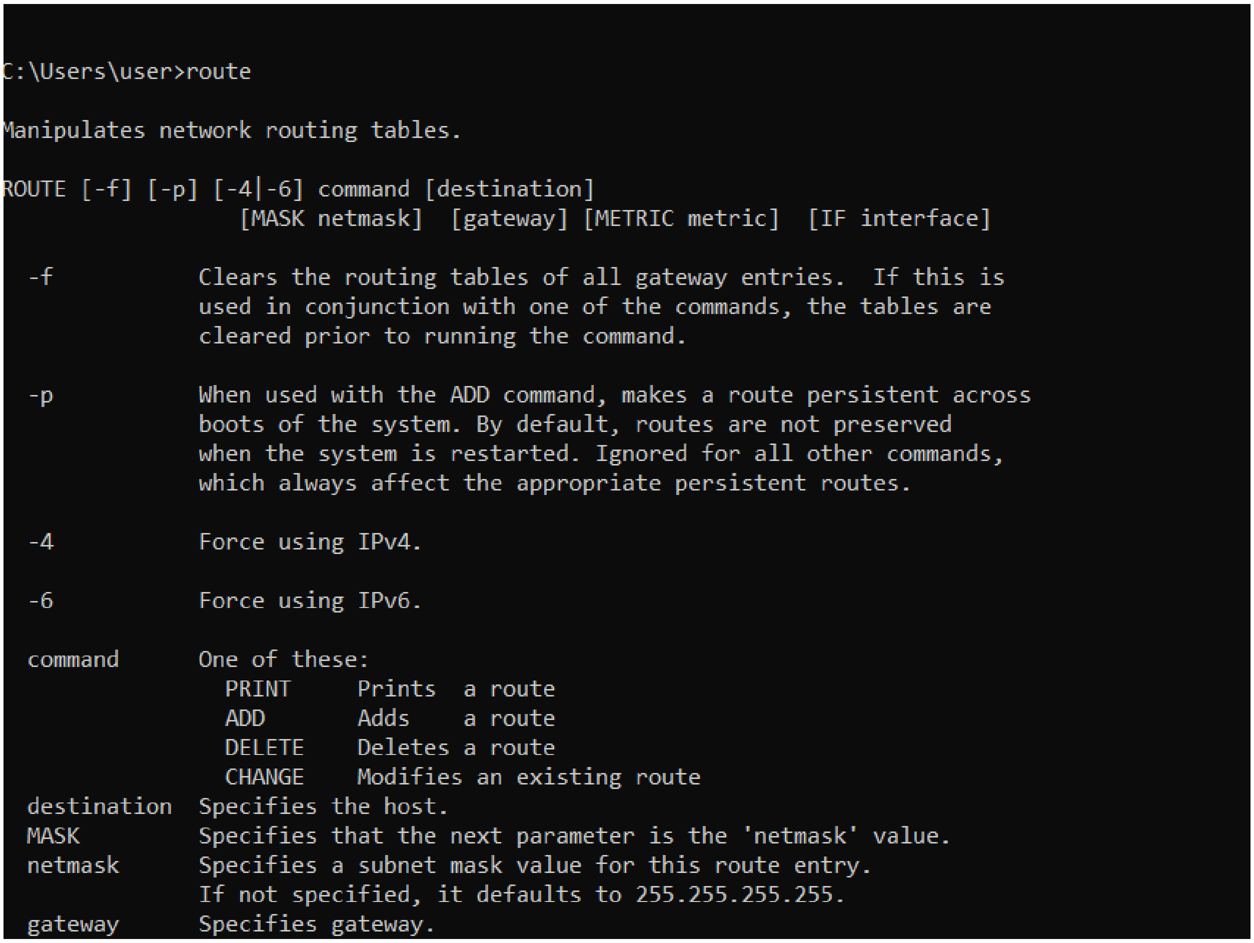


Command Prompt

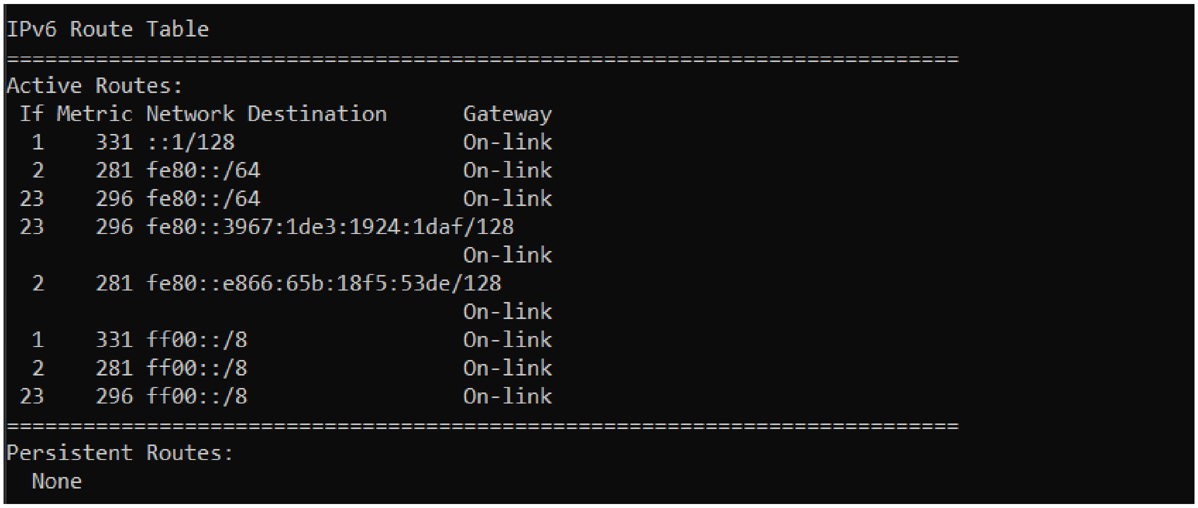
```
Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        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.


C:\Users\user>
```

- Route

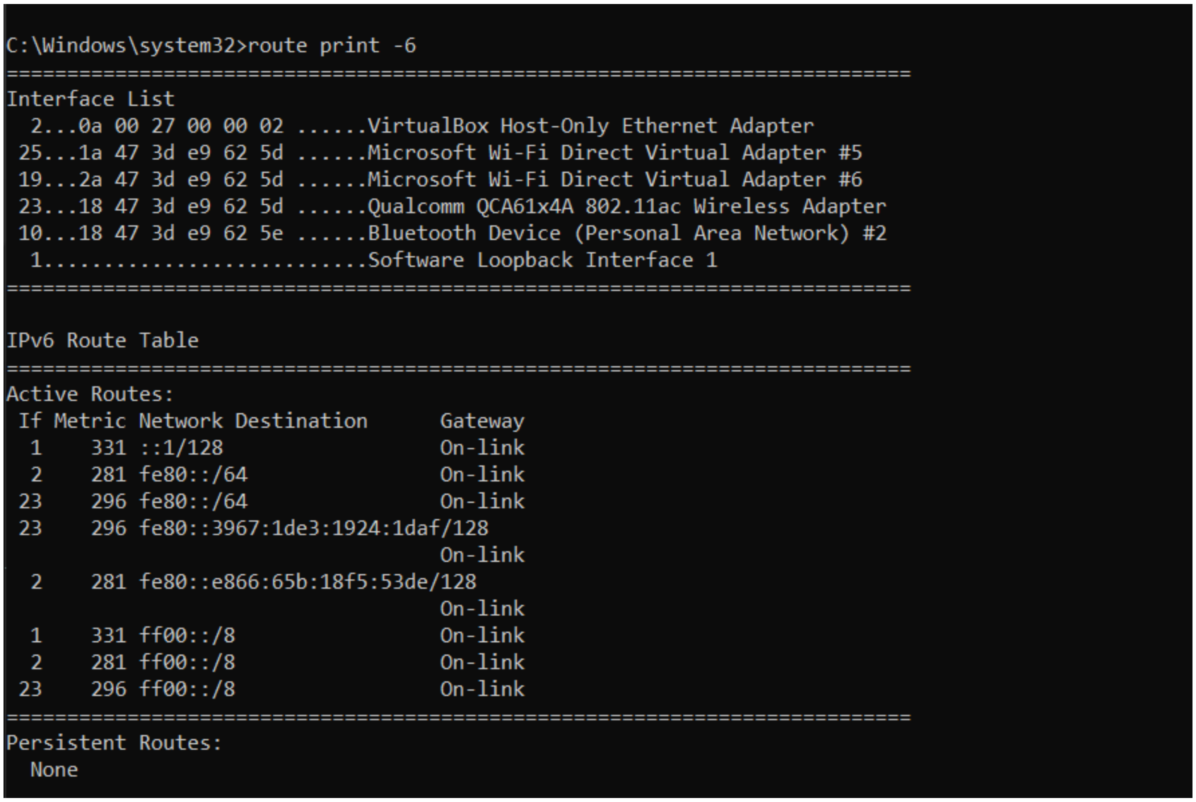
In computing, route is a command used to view and manipulate the IP routing table in Unix-like and Microsoft Windows[1] operating systems and also in IBM OS/2 and ReactOS.[2] Manual manipulation of the routing table is characteristic of static routing.



```
C:\Users\user>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.
```



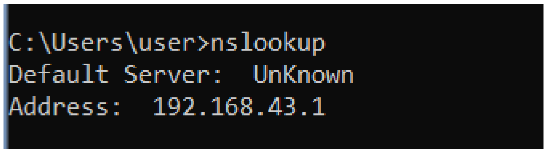
```
IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    331 ::1/128                  On-link
  2    281 fe80::/64                On-link
 23    296 fe80::/64                On-link
 23    296 fe80::3967:1de3:1924:1daf/128
                                    On-link
  2    281 fe80::e866:65b:18f5:53de/128
                                    On-link
  1    331 ff00::/8                 On-link
  2    281 ff00::/8                 On-link
 23    296 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```



```
C:\Windows\system32>route print -6
===========================================================================
Interface List
  2...0a 00 27 00 00 02 ......VirtualBox Host-Only Ethernet Adapter
 25...1a 47 3d e9 62 5d ......Microsoft Wi-Fi Direct Virtual Adapter #5
 19...2a 47 3d e9 62 5d ......Microsoft Wi-Fi Direct Virtual Adapter #6
 23...18 47 3d e9 62 5d ......Qualcomm QCA61x4A 802.11ac Wireless Adapter
 10...18 47 3d e9 62 5e ......Bluetooth Device (Personal Area Network) #2
  1...........................Software Loopback Interface 1
===========================================================================

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    331 ::1/128                  On-link
  2    281 fe80::/64                On-link
 23    296 fe80::/64                On-link
 23    296 fe80::3967:1de3:1924:1daf/128
                                    On-link
  2    281 fe80::e866:65b:18f5:53de/128
                                    On-link
  1    331 ff00::/8                 On-link
  2    281 ff00::/8                 On-link
 23    296 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

- Nslookup

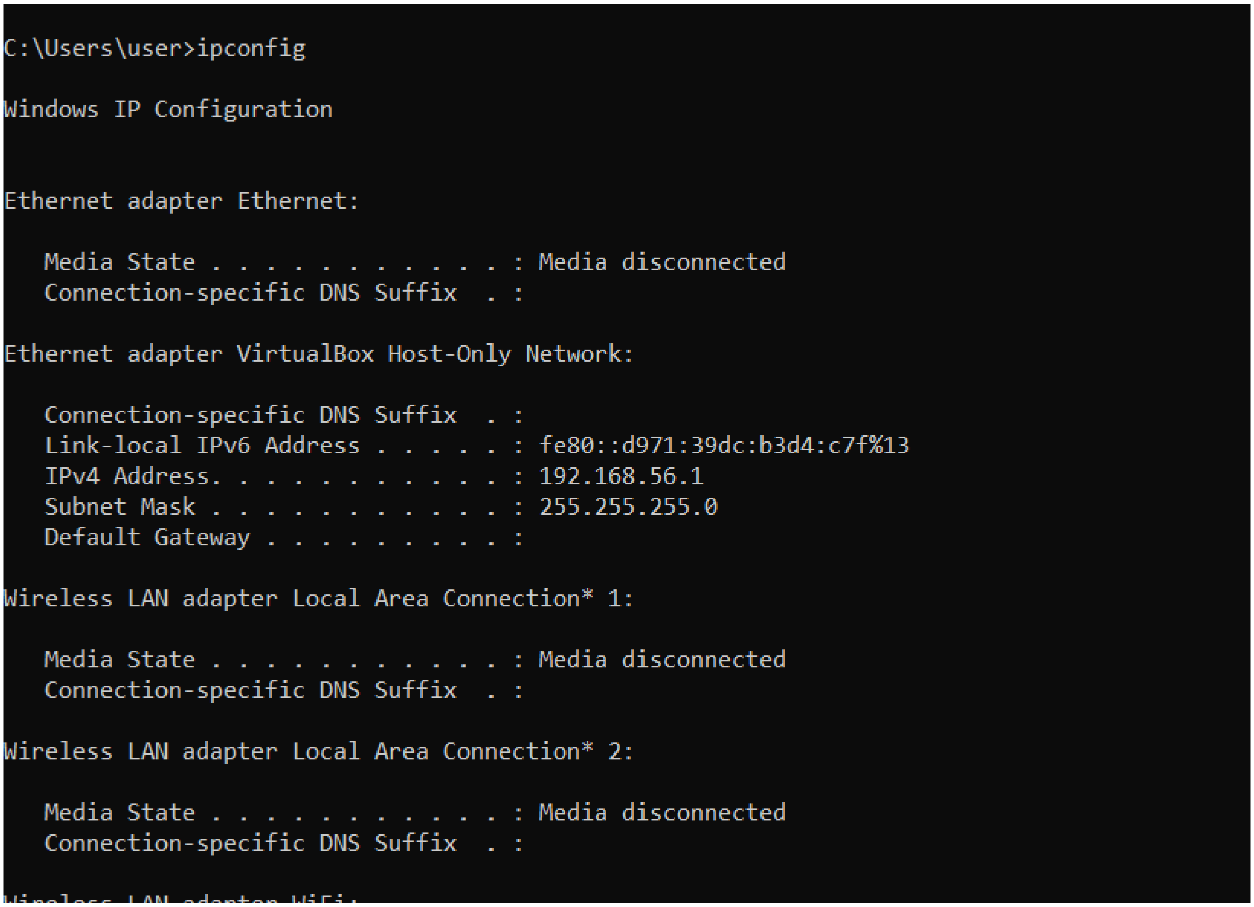
This command helps diagnose the Domain Name System (DNS) infrastructure and comes with a number of sub-commands. These are mainly for systems administrators. The primary interest for average PC users is its use to find the computer name corresponding to a numeric IP. For example, if you want to know who is "216.109.112.135" , enter "nslookup 216.109.112.135" and you will find that it is (or was anyway) a Yahoo computer. My firewall keeps a log of the IPs involved in the attempts to probe my computer and I sometimes look a few up to see who they are. (There are also Whois search sites available on the Web as mentioned in the Ipconfig section.)



```
C:\Users\user>nslookup
Default Server:  UnKnown
Address:  192.168.43.1
```

- ipconfig

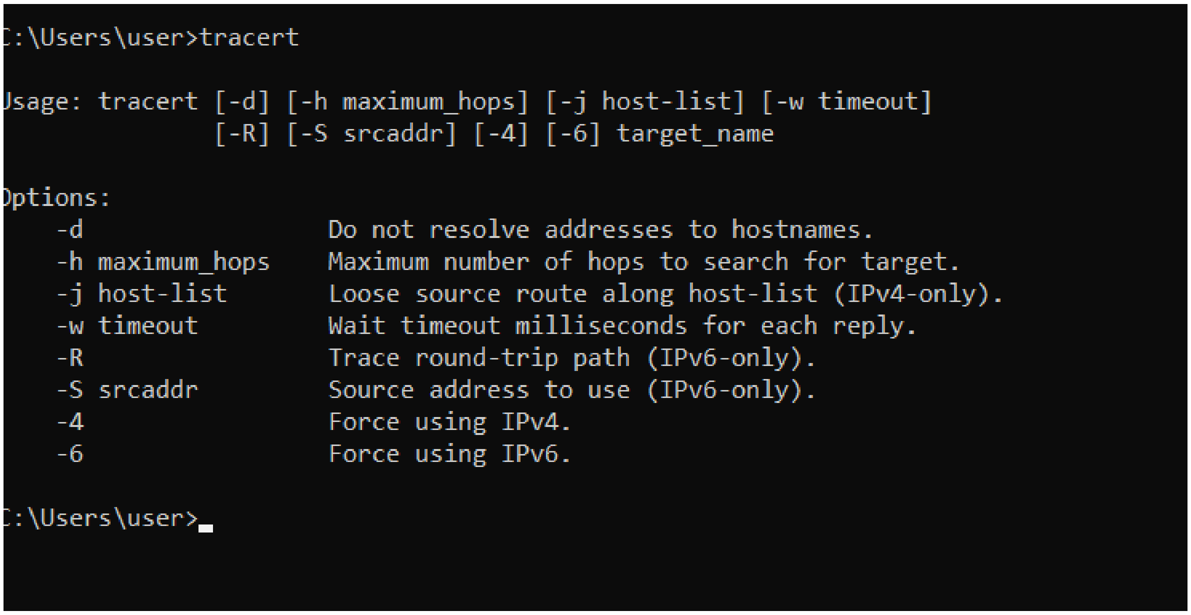
The Windows IP Configuration tool (ipconfig) is the command-line equivalent of the accessory "Winipcfg" that was present in Windows 9X/Me. It is used to display the TCP/IP network configuration values. To open it, enter "ipconfig" in the command prompt. If you are connected directly to the Internet, you will obtain your IP address.



```
C:\Users\user>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

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

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::d971:39dc:b3d4:c7f%13
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

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 WiFi:
```

- Traceroute

Tracert (traceroute) is another old tool borrowed from Unix. The actual path between two computers on the Internet is not a straight line but consists of numerous segments or "hops" from one intermediate computer to another. Tracert shows each step of the path taken. It can be interesting to see just how convoluted it is. The times for each hop and the IP addresses for each intermediate computer are displayed. Tracert shows up to 30 hops. It is convenient for finding if there is one particular segment that is causing a slow or bad connection. A typical command might be "tracert dell.com".

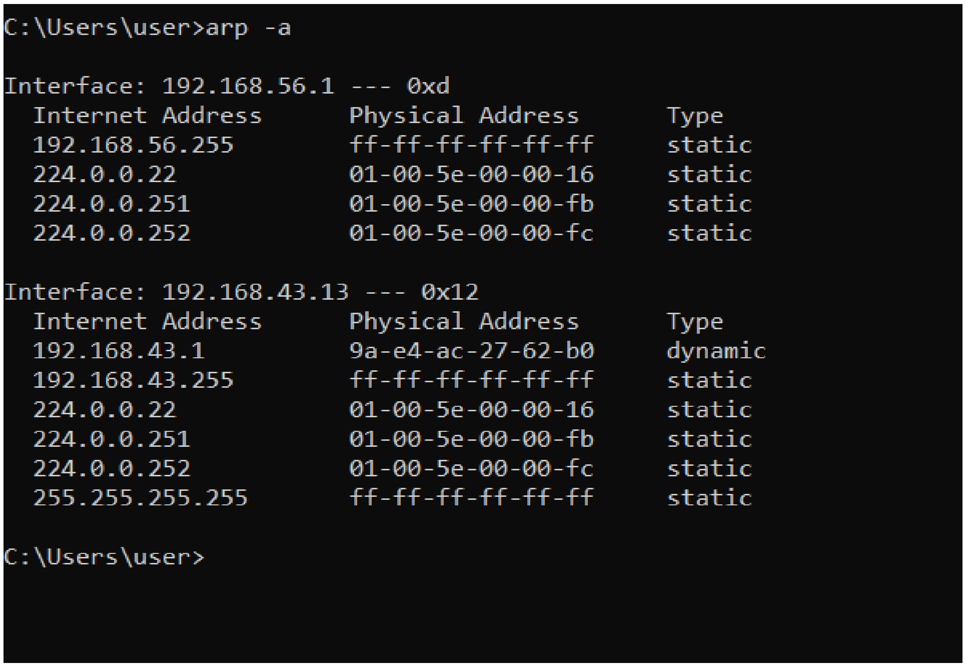


```
:\Users\user>tracert

Jsage: 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.

:\Users\user>_
```

2. Identify and perform 5 more network commands and it's working.

a). ARP

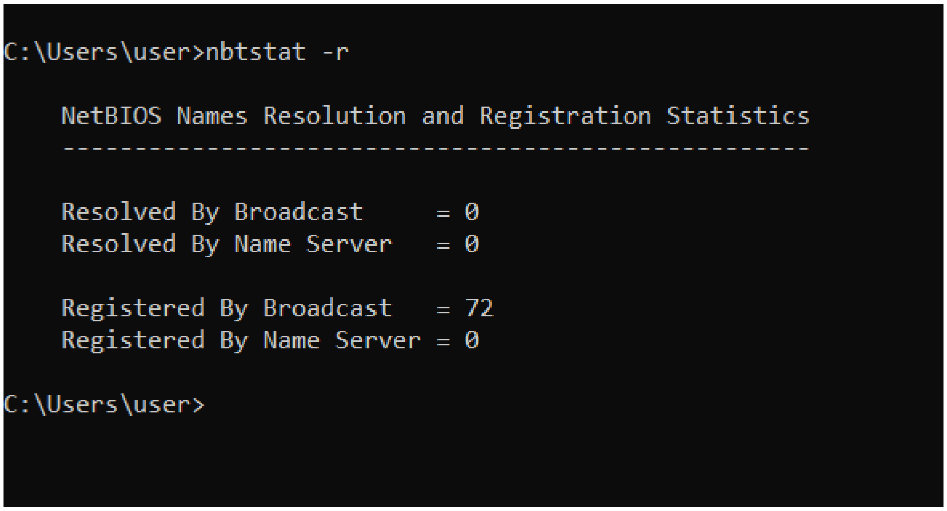
The ARP command corresponds to the Address Resolution Protocol. Although it is easy to think of network communications in terms of IP addressing, packet delivery is ultimately dependent on the Media Access Control (MAC) address of the device’s network adapter. This is where the Address Resolution Protocol comes into play. Its job is to map IP addresses to MAC addresses. Windows devices maintain an ARP cache, which contains the results of recent ARP queries. You can see the contents of this cache by using the ARP -A command. If you are having problems communicating with one specific host, you can append the remote host’s IP address to the ARP -A command.



```
C:\Users\user>arp -a

Interface: 192.168.56.1 --- 0xd
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static

Interface: 192.168.43.13 --- 0x12
  Internet Address      Physical Address      Type
  192.168.43.1          9a-e4-ac-27-62-b0     dynamic
  192.168.43.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\user>
```

b)NbtStat

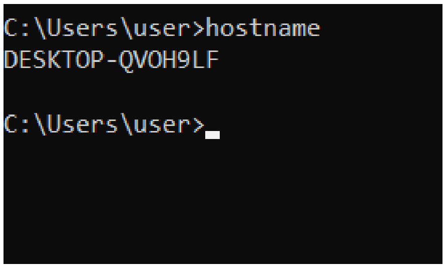
As I am sure you probably know, computers that are running a Windows operating system are assigned a computer name. Oftentimes, there is a domain name or a workgroup name that is also assigned to the computer. The computer name is sometimes referred to as the NetBIOS name. Windows uses several different methods to map NetBIOS names to IP addresses, such as broadcast, LMHost lookup, or even using the nearly extinct method of querying a WINS server. Of course, NetBIOS over TCP/IP can occasionally break down. The NbtStat command can help you to diagnose and correct such problems. The NbtStat -n command for example, shows the NetBIOS names that are in use by a device. The NbtStat -r command shows how many NetBIOS names the device has been able to resolve recently.



```
C:\Users\user>nbtstat -r

    NetBIOS Names Resolution and Registration Statistics
    ----------------------------------------------------

    Resolved By Broadcast     = 0
    Resolved By Name Server   = 0

    Registered By Broadcast   = 72
    Registered By Name Server = 0

C:\Users\user>
```

c)Hostname

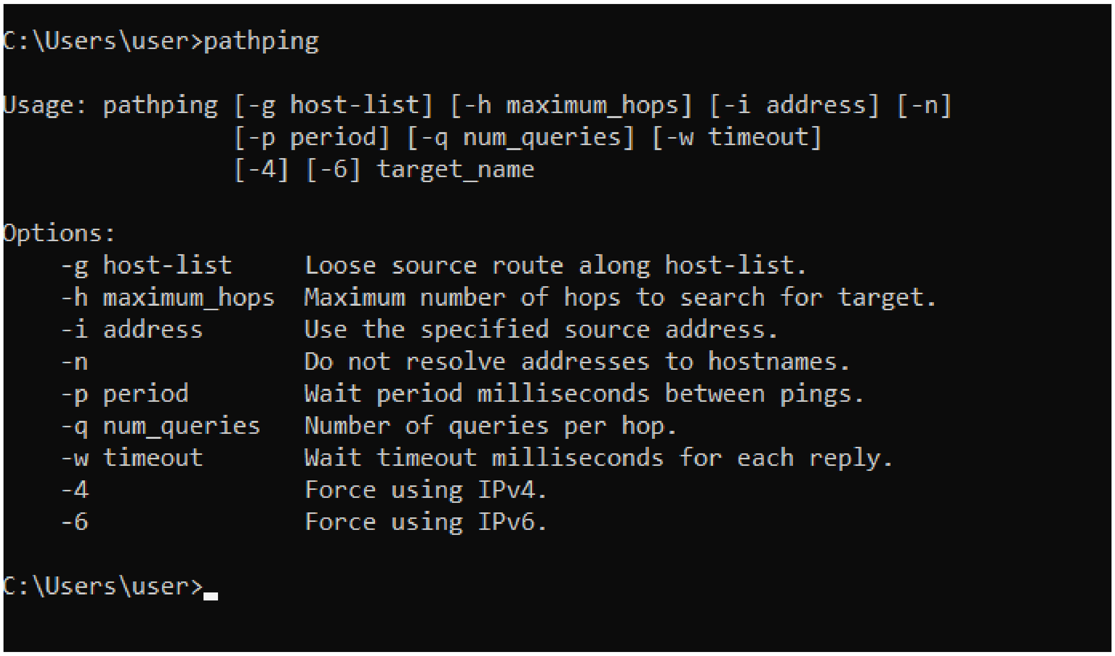
The previously discussed NbtStat command can provide you with the host name that has been assigned to a Windows device, if you know which switch to use with the command. However, if you're just looking for a fast and easy way of verifying a computer's name, then try using the Hostname command. Typing Hostname at the command prompt returns the local computer name.



```
C:\Users\user>hostname
DESKTOP-QVOH9LF

C:\Users\user>
```

d) PathPing

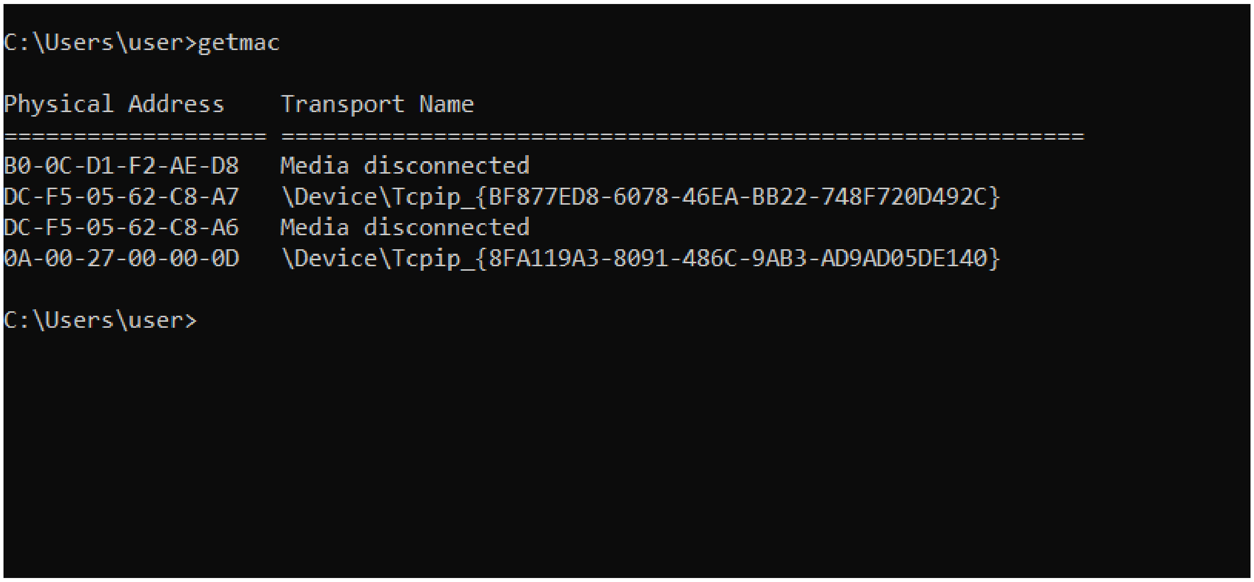
Earlier, I talked about the Ping utility and the Tracert utility, and the similarities between them. As you might have guessed, the PathPing tool is a utility that combines the best aspects of Tracert and Ping. Entering the PathPing command followed by a host name initiates what looks like a somewhat standard Tracert process. Once this process completes however, the tool takes 300 seconds (five minutes) to gather statistics, and then reports latency and packet loss statistics that are more detailed than those provided by Ping or Tracert.



```
C:\Users\user>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.

C:\Users\user>
```

e) getmac

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



```
C:\Users\user>getmac

Physical Address    Transport Name
=================== ==========================================================
B0-0C-D1-F2-AE-D8   Media disconnected
DC-F5-05-62-C8-A7   \Device\Tcpip_{BF877ED8-6078-46EA-BB22-748F720D492C}
DC-F5-05-62-C8-A6   Media disconnected
0A-00-27-00-00-0D   \Device\Tcpip_{8FA119A3-8091-486C-9AB3-AD9AD05DE140}

C:\Users\user>
```