**INVESTIGATING NETWORKS**

**LAB # 02**



**Fall 2024**

Submitted by: **Mohsin Sajjad**

Registration No: **22pwsce2149**

Class Section: **A**

“On my honor, as student of University of Engineering and Technology, I have neither given nor received unauthorized assistance on this academic work.”



Student Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Submitted to:

**Dr. Yasir Saleem Afridi**

Month Day, Year (26 02, 2025)

Department of Computer Systems Engineering

University of Engineering and Technology, Peshawar

## ABOUT PING

The original PING command stood for "Packet Internet Groper", and was a package of diagnostic utilities used by DARPA personnel to test the performance of the ARPANET. However, the modern Internet Ping command refers to a program written by Mike Muss in December, 1983, which has since become one of the most versatile and widely used diagnostic tools on the Internet.

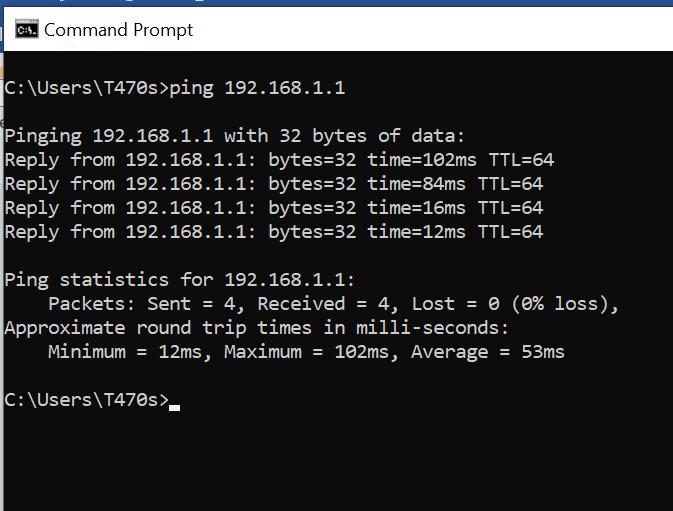
Typical Diagnostic Tests Performed By Ping Command

Some of the internet diagnostic tests performed by ping command are:

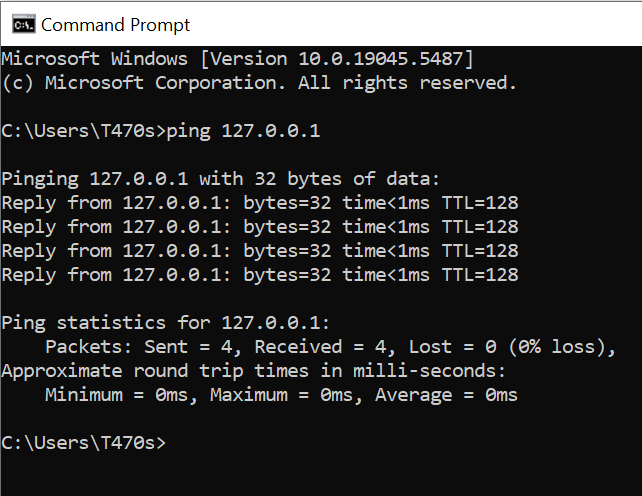
* **Access –** Ping is used to determine whether the remote host is active or inactive. If a certain site is not pinged, but the other sites can, then it's a pretty good sign that your Internet network is fine and that site is down. On the other hand, if you can't ping any site, then likely your entire network connection is down that needs rebooting.
* **Time & distance –** Another use of Ping command is to determine how long it takes to bounce a packet off of another site. Thereby giving Internet distance in network terms. For example, a web site hosted on your neighbor's computer with a different Internet service provider (ISP) might go through more routers and be farther away in network distance than a site on the other side of the ocean with a direct connection to the Internet backbone. If a site seems slow, then ping distance of that site can be compared with that of other Internet sites to find out whether it is the site, the network, or your system that is slow. You can also compare ping times to get an idea of which sites have the fastest network access and would be most efficient for downloading, chatting, and other applications.
* **Domain IP address –** Typically, Ping command is used to probe either a domain name or an IP address; if a domain name is pinged, and then it displays the corresponding IP address in its response.

**--------------------------------------------TASK 01--------------------------------------------**

1. Ping the IP address of the Default Gateway and DNS Servers. Was the result successful?



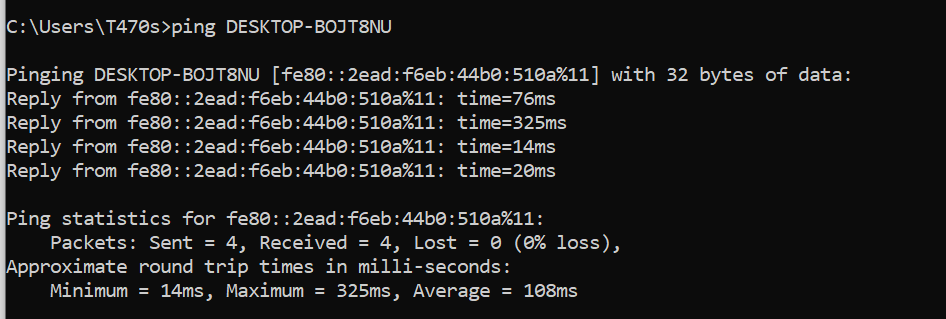
1. Ping the computer’s loop-back address. Type the following command: **>> ping 127.0.0.1**



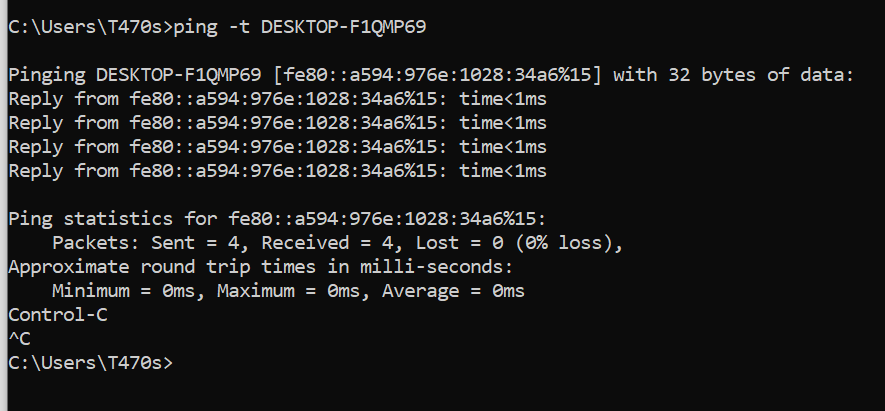
1. What is the IP Address of [www.yahoo.com](http://www.yahoo.com): **212.82.117.205**

How much time did our ping took to reach [www.yahoo.com](http://www.yahoo.com): **252ms**

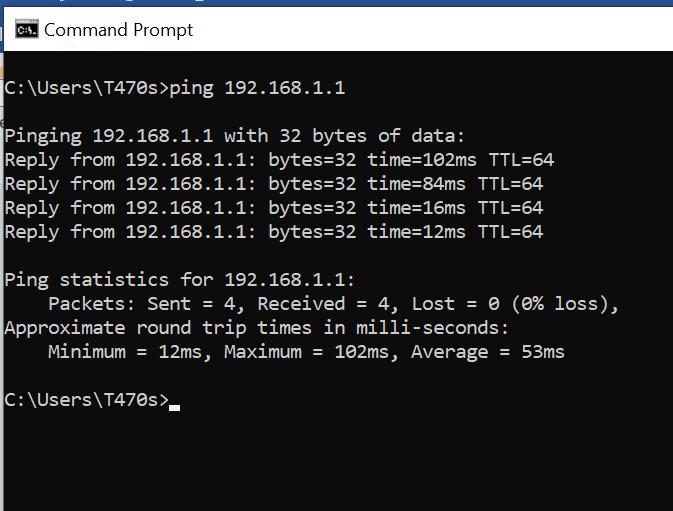
1. Ping the hostname of another computer**.** Try to ping the hostname of the computer that was recorded in the previous lab.



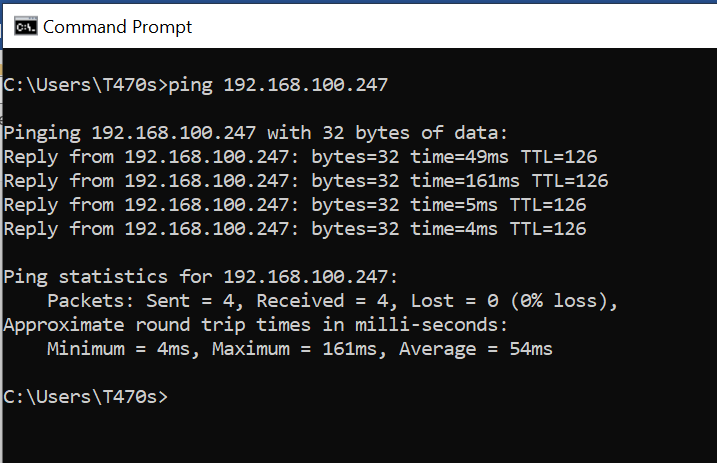
1. Ping the hostname of another computer using –t. Try to ping repetitively, the hostname of the computer.



1. How can we stop the ping**? Ctrl + C**
2. ping the IP address of the default gateway



1. ping the IP address of a DHCP or DNS server.

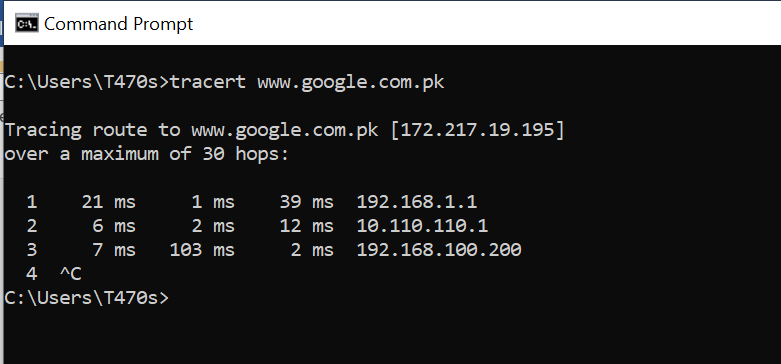


**--------------------------------------------TASK 03--------------------------------------------**

1. Trace the route to the GOOGLE PAKISTAN website by typing:

**>> tracert www.google.com.pk**

The result shows the complete route to the site, along with the number of hops in the path.



1. Trace the route to the UET website using options listed in option description table.

**Option Description**

===================================================

**-d (Do Not Resolve** Displays the route using numeric addresses only

**Addresses)** rather than showing both IP address and host

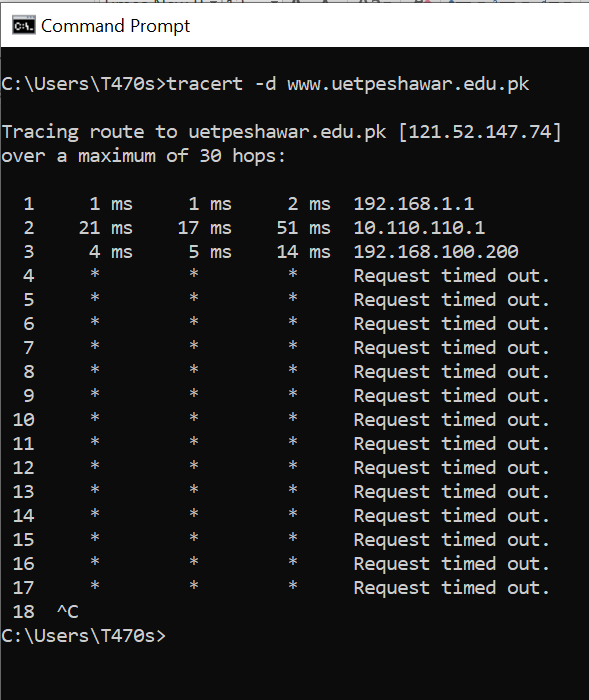
names, for faster display.

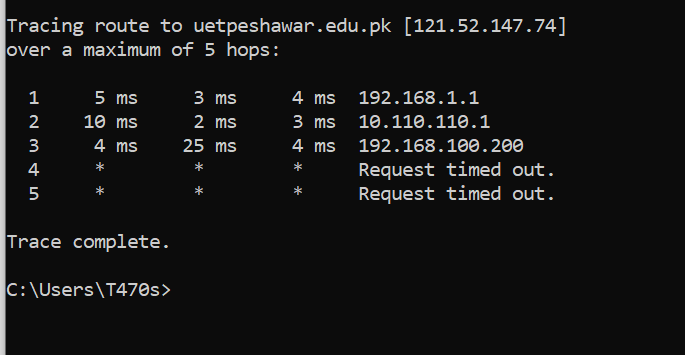
**-h maximum\_hops (Max.** Specifies the maximum number of hops to use for

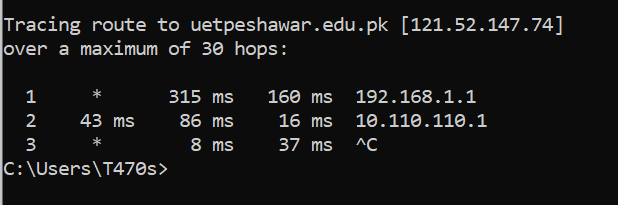
**Hops)** tracing; Default is 30

**-w timeout** Specifies how long to wait for a reply to each

Request in milliseconds; Default is 4000 [for 4 sec]







c) What is the difference between the following commands?

Tracert [www.yahoo.com](http://www.yahoo.com)

Tracert –h 20 [www.yahoo.com](http://www.yahoo.com)

Ans: Tracert [www.yahoo.com](http://www.yahoo.com): The trace will attempt to reach the destination with up to **30 hops** by default.

Tracert –h 20 [www.yahoo.com](http://www.yahoo.com): This command adds the -h option to limit the maximum number of hops in the traceroute to **20 hops**.

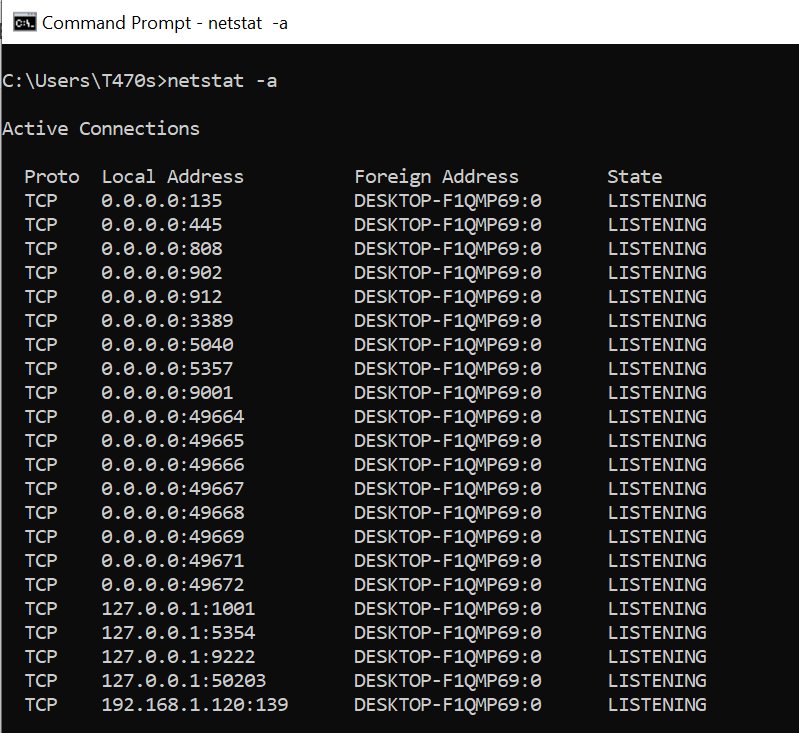
**Task 04 (Long Life Learning)**

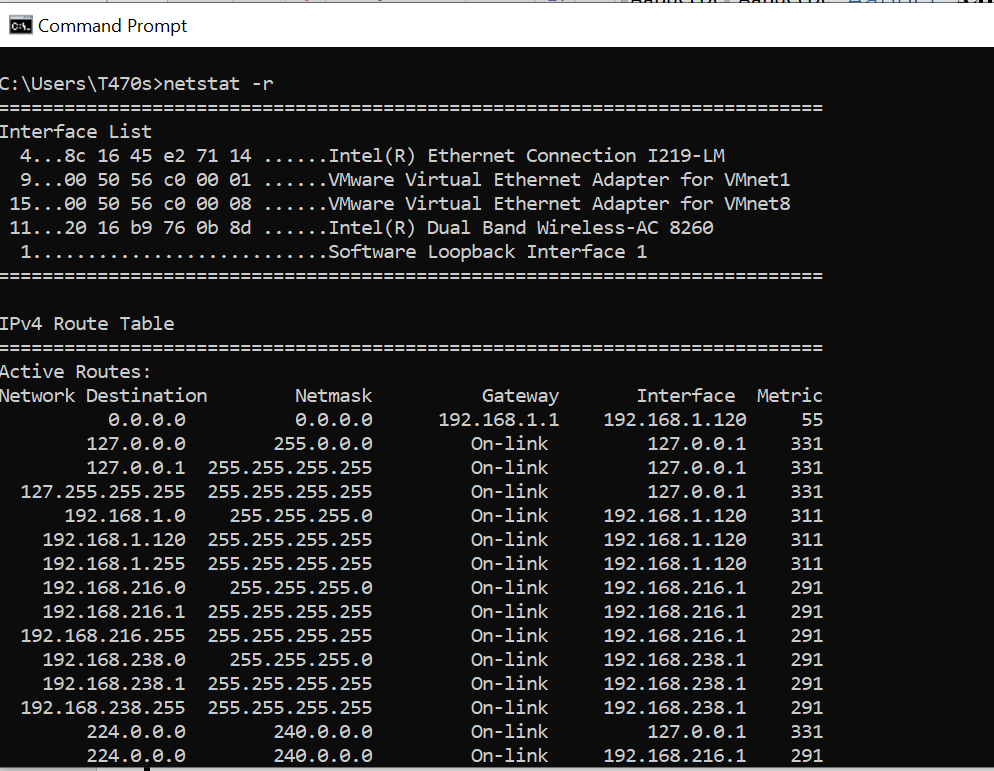
Practice the following network commands and understand/report their usage

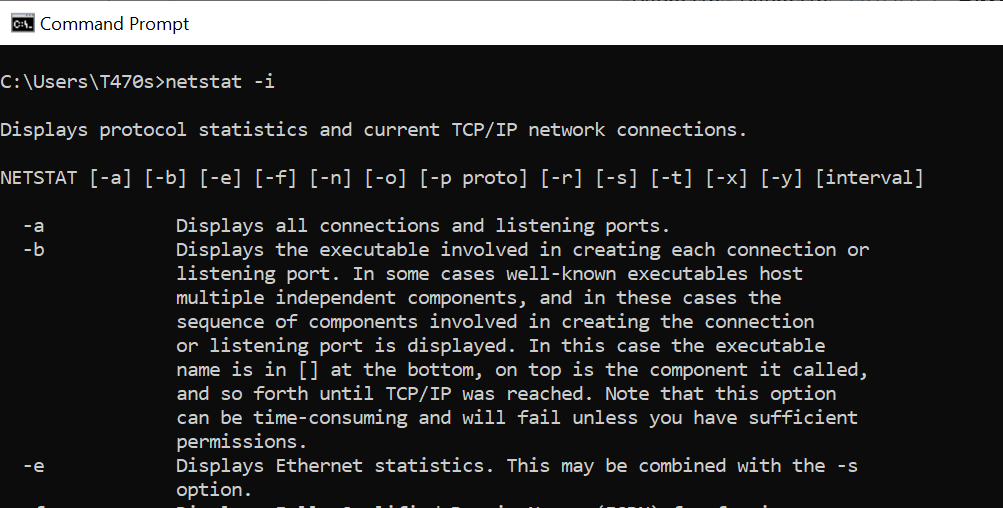
1. **netstat**  
   Displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the [IP](http://whirlpool.net.au/wiki/IP) routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols). Used without parameters, netstat displays active TCP connections.

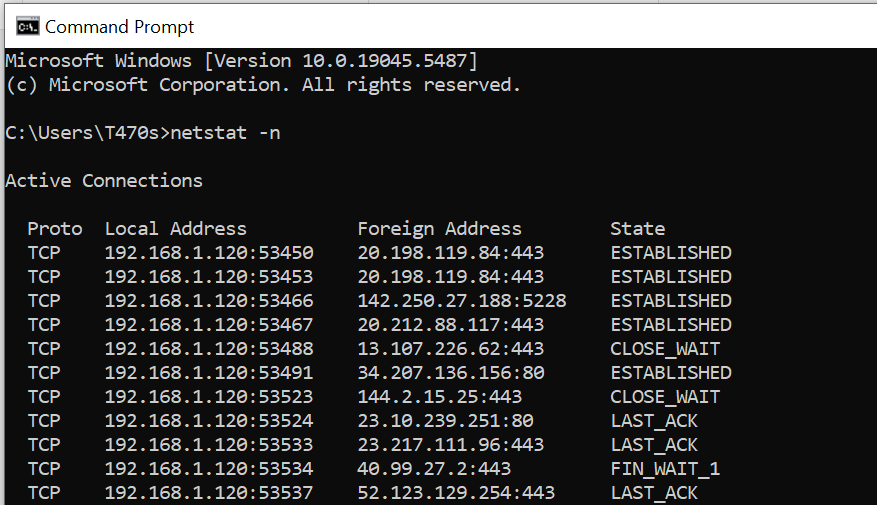
**Try the following**

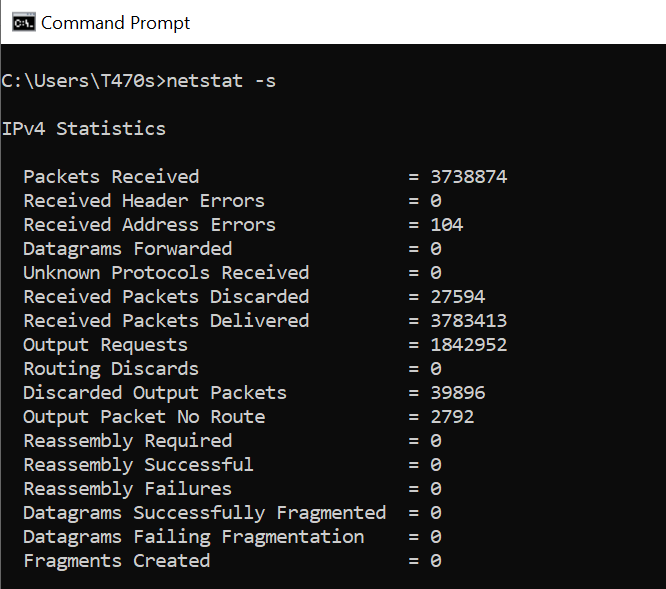
* 1. \_ **netstat -a**: Shows the state of all sockets, routing table entries, and interfaces.
  2. \_ **netstat -r**: Displays the routing table.
  3. \_ **netstat -i**: Displays the interface information.
  4. \_ **netstat -n**: Displays numbers instead of names.
  5. \_ **netstat -s**: Displays per-protocol statistics.



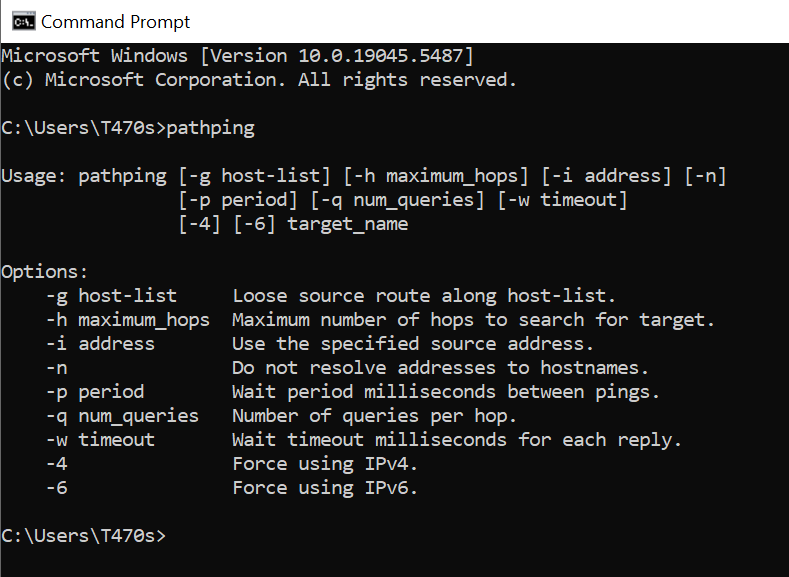




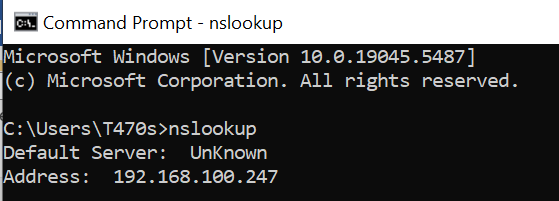




1. **pathping**  
   Provides information about network latency and network loss at intermediate hops between a source and destination. Pathping sends multiple Echo Request messages to each router between a source and destination over a period of time and then computes results based on the packets returned from each router.



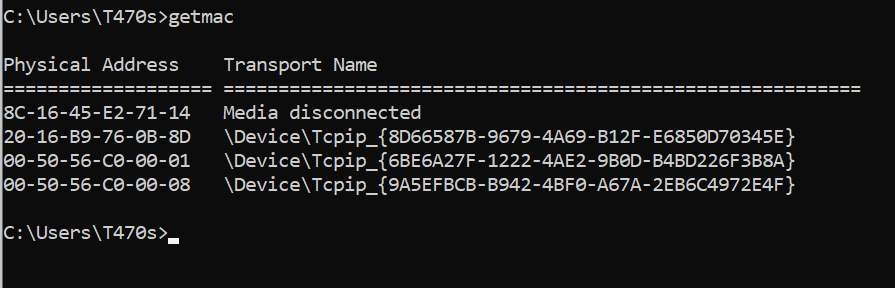
1. **telnet**  
   Telnet is software that allows users to remotely access another computer such as a server, network device, or other computer. With telnet users can connect to a device or computer, manage a network device, setup a device, transfer files, etc.
2. **nslookup**  
   Displays information that you can use to diagnose Domain Name System (DNS) infrastructure. Before using this tool, you should be familiar with how DNS works. The Nslookup command-line tool is available only if you have installed the TCP/IP protocol.



1. **getmac**

Command used to show both local and remote MAC addresses. When run with no parameters (ie. getmac) it displays MAC addresses for the local system. When run with the /s parameter (eg. getmac /s \\foo) it displays MAC addresses for the remote computer. When the /v parameter is used, it also displays the associated connection name and network adapter name.

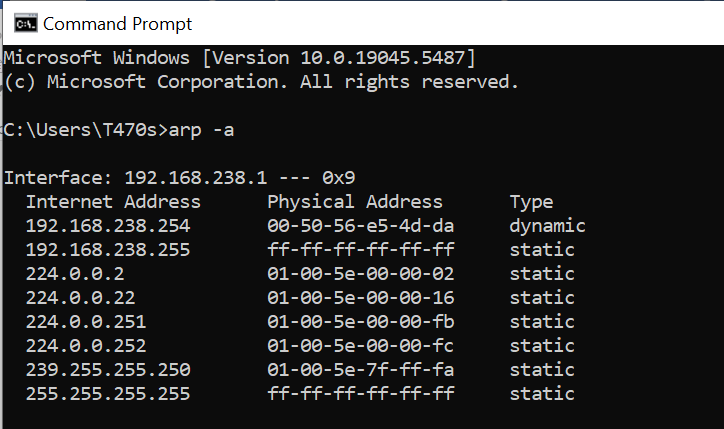
* **getmac /s 192.168.1.1** – Get MAC Address by IP Address
* **getmac /s localhost** – Get local MAC Address



1. **ARP Command**.

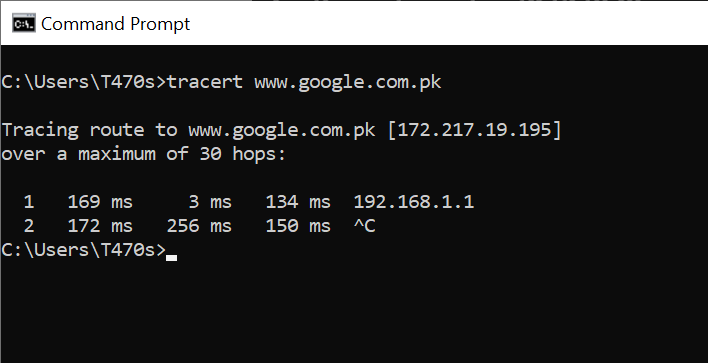
Using the arp command allows you to display and modify the Address Resolution Protocol (ARP) cache. An ARP cache is a simple mapping of IP addresses to MAC addresses

Use **arp -a** to see the entire ARP table.



1. **Tracert Command:**

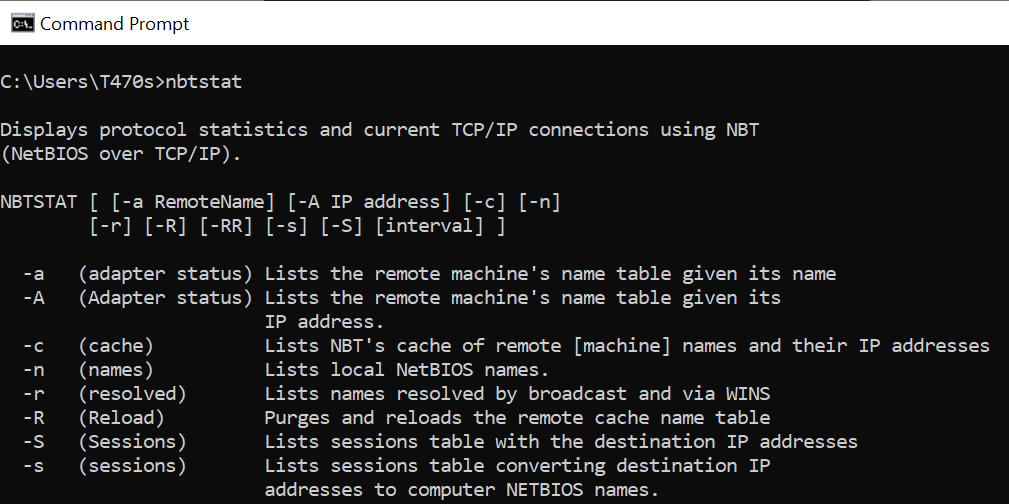
Traces the route packets take to reach a destination, showing each "hop" along the way (e.g., tracert google.com).



1. **nbtstat Command:**

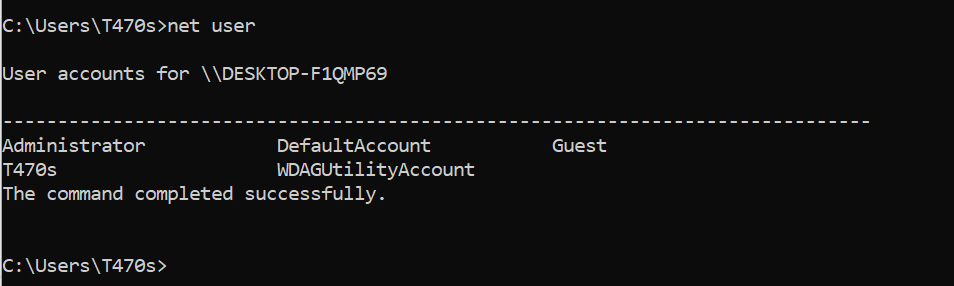
Displays NetBIOS over TCP/IP statistics and connections.

Other Useful Commands



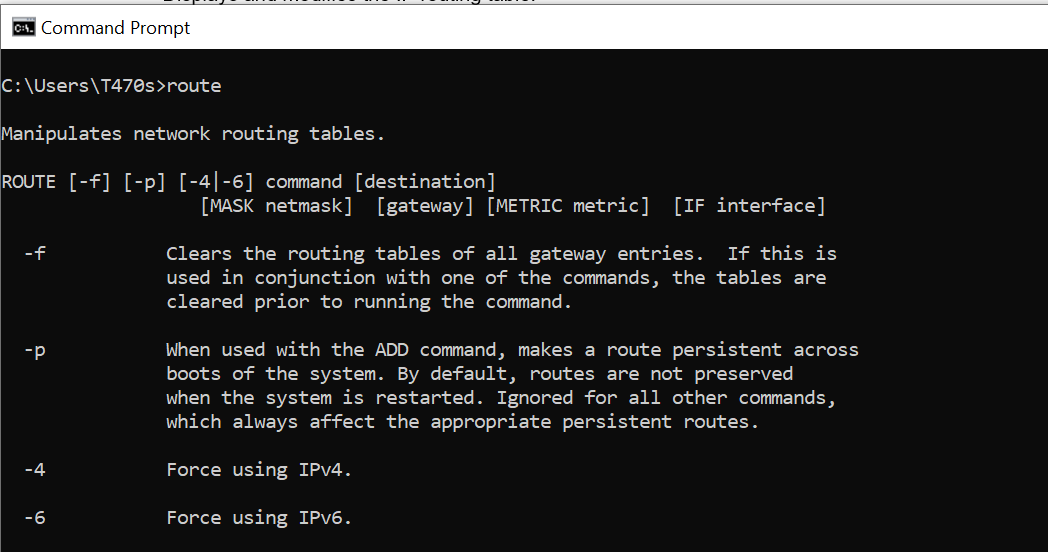
1. **net command:**

A powerful command for managing various network aspects, including shares, users, and services.



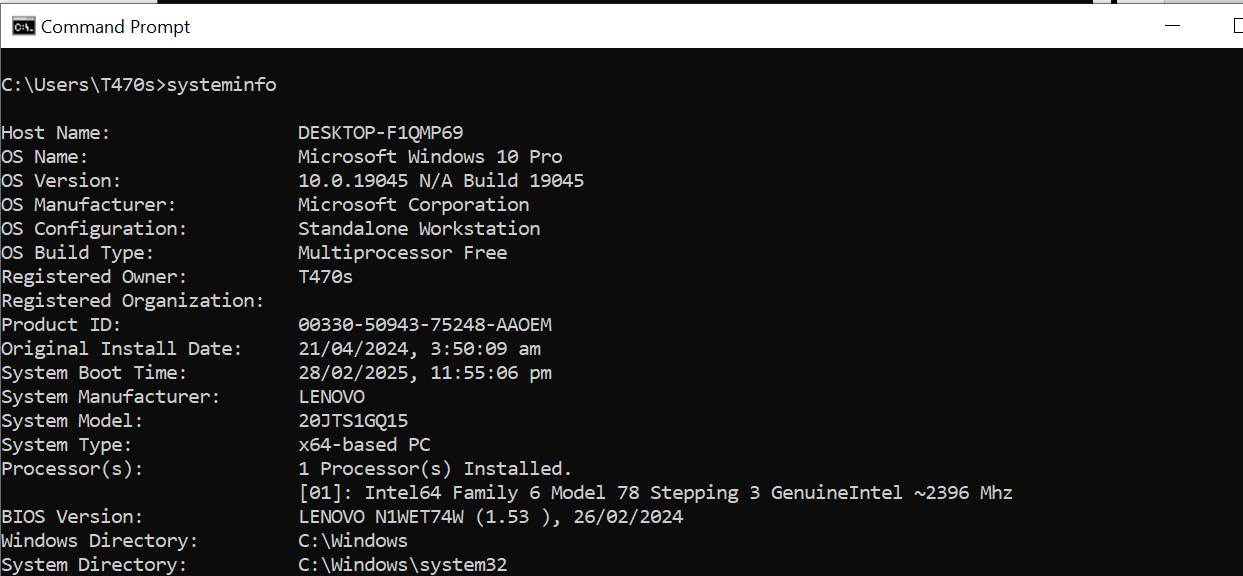
1. **route command:**

Displays and modifies the IP routing table.



1. **Systeminfo command**:

Provides detailed information about your system configuration, including network adapters.



1. **Hostname command:**

Shows your computer's name.

