Aim: Understanding of basic network commands

Theory:

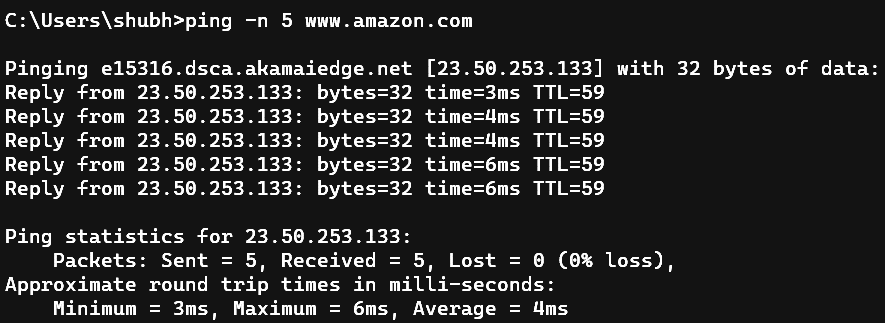
1. **Ping:** It is used to test the ability of the source computer to reach a specified destination computer. It’s a simple way to verify that a computer can communicate with another computer or network device.

The full form of Ping is Packet Internet or Inter-Network Groper.

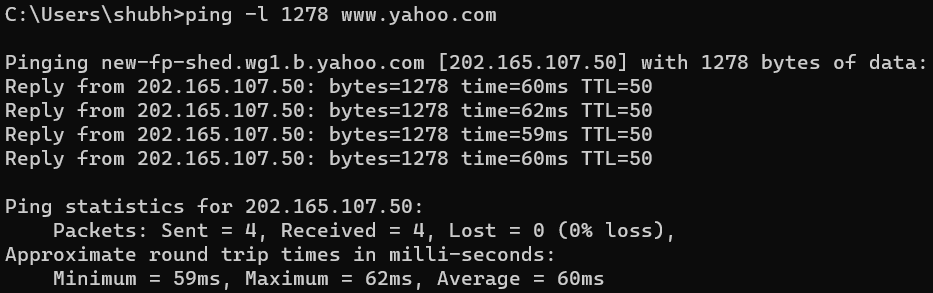
**How to run Ping command:**

1. First open the cmd (command prompt).
2. Type “ping” in the black box and hit the space bar.
3. Type the IP address you’d like to ping (e.g., ping [www.google.com](http://www.google.com))
4. Review the ping results displayed.

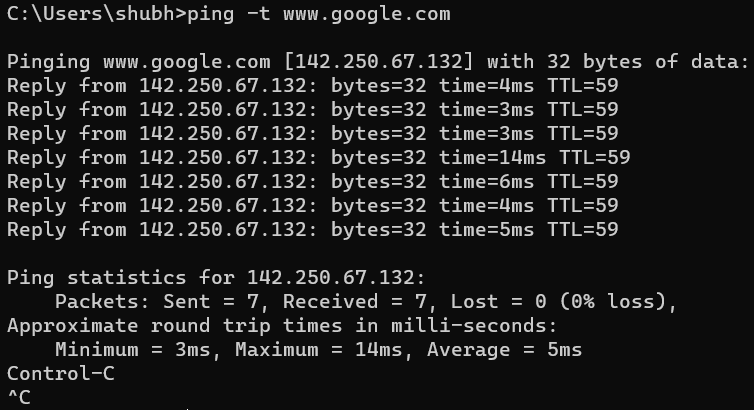
**-n :** The -n option tells the ping command to send 5 ICMP (Internet Control Message Protocol) Echo Requests instead of the default of 4.



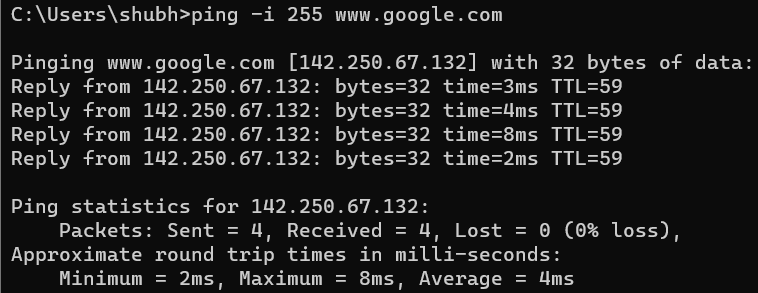
**-l :** The -l sets the packet size for each request to 1200 bytes instead of the default of 32 bytes



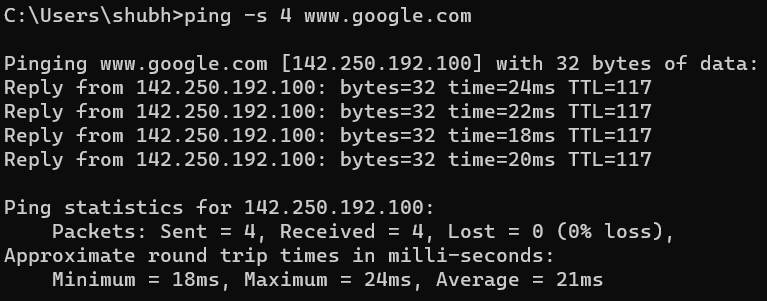
**-t :** The -t command ping indefinitely times. We can interrupt the ping manually with Ctrl+C

****

**-i :** We can increase and decrease ping time interval using -i.



**-s :** Specifies that the Internet Timestamp option in the IP header is used to record the time of arrival for the Echo Request message and corresponding Echo Reply message for each hop. **The Count must be a minimum of 1 and a maximum of 4**

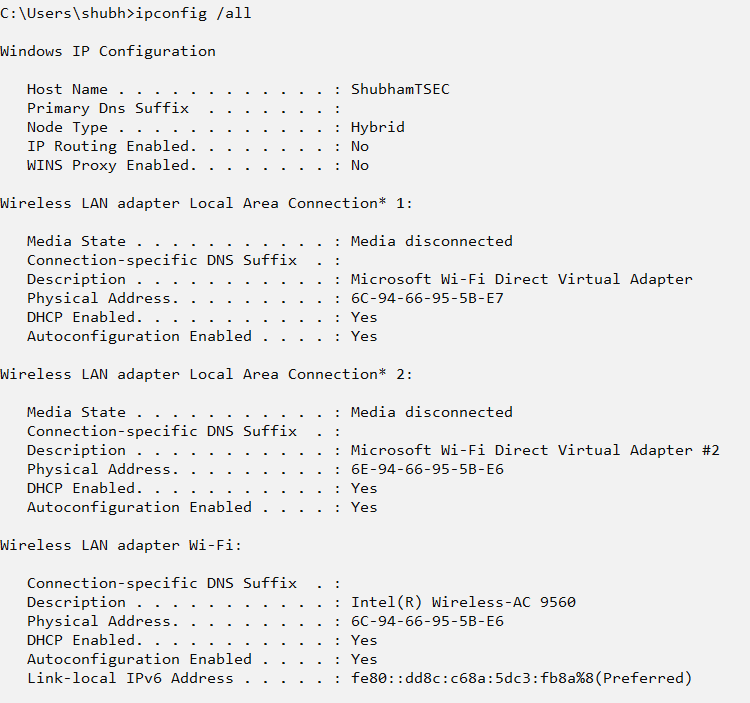
****

1. **‘ipconfig’:** Displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. Used without parameters, **ipconfig** displays Internet Protocol version 4 (IPv4) and IPv6 addresses, subnet mask, and default gateway for all adapters.

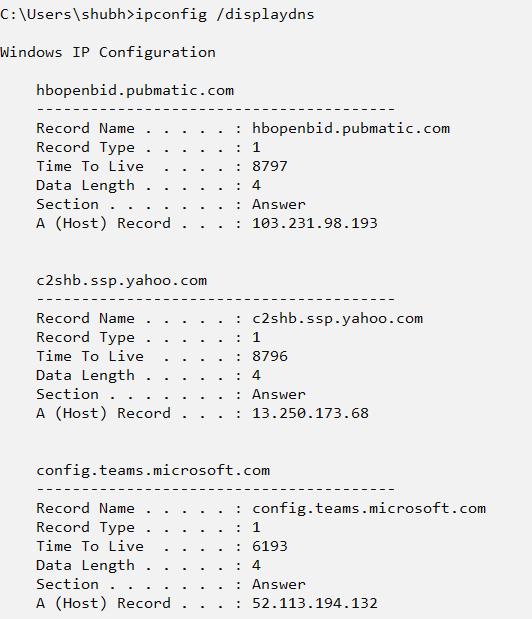
**How to run the ipconfig command:**

1. To use the Ip config command we will need to open Command Prompt or Power Shell.
2. Type ipconfig and press enter
3. This will show you the basic network information from your network adapters

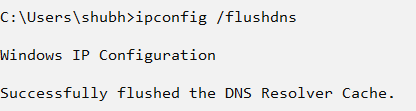
**/all** : Displays the full TCP/IP configuration for all adapters. Adapters can represent physical interfaces, such as installed network adapters, or logical interfaces, such as dial-up connections.

****

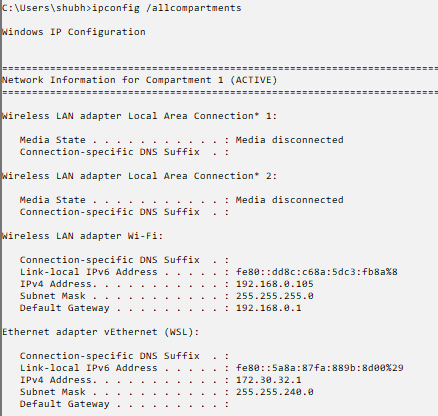
**/displaydns:** Displays the contents of the DNS client resolver cache, which includes both entries preloaded from the local Hosts file and any recently obtained resource records for name queries resolved by the computer. The DNS Client service uses this information to resolve frequently queried names quickly, before querying its configured DNS servers.



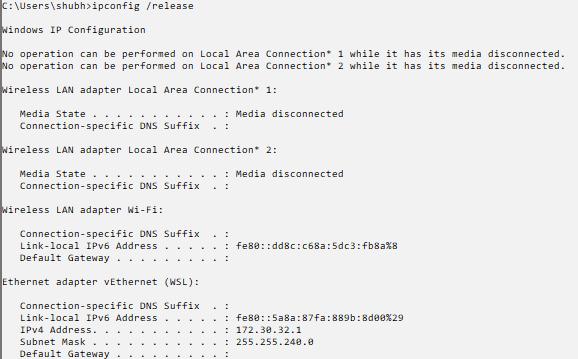
**/flushdns:** Flushes and resets the contents of the DNS client resolver cache. During DNS troubleshooting, you can use this procedure to discard negative cache entries from the cache, as well as any other entries that have been added dynamically.



**/allcompartments:**  It shows the output from my test server, which contains a single network adapter.

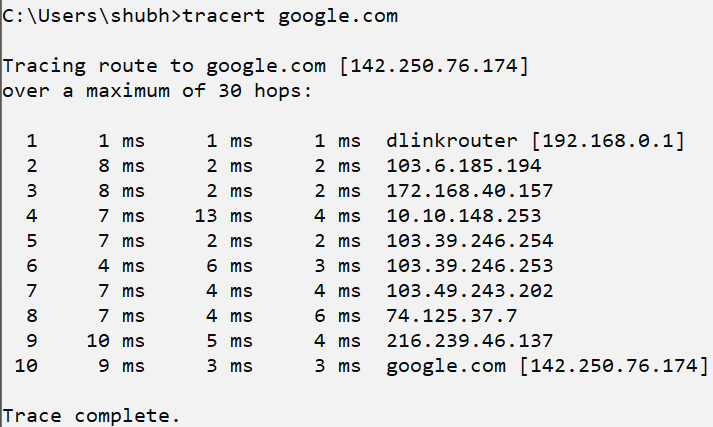


**/release:** This parameter sends a request to the DHCP server to abandon the active lease(s) and removes it (or them) from your system.

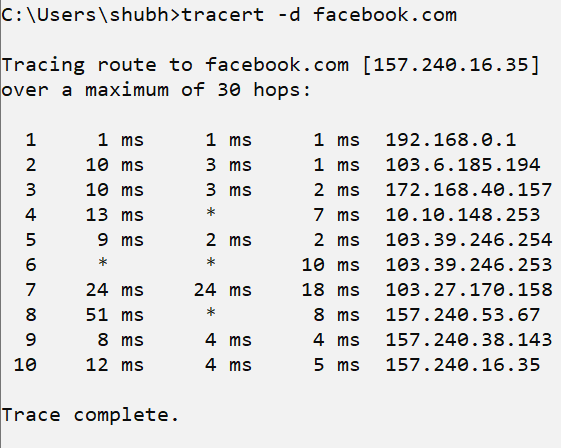
****

**Tracert:** This diagnostic tool determines the path taken to a destination by sending Internet Control Message Protocal (ICMP) echo Request or ICMPv6 messages to the destination with incrementally increasing time to live (TTL) field values.

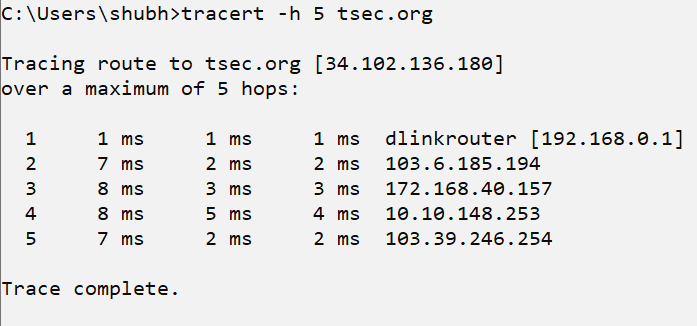
**tracert <domain> :** Traces the path from the local host to the specified domain.



**Tracert -d <domain> :** Traces the path without resolving the IP addresses of the intermediate hops to hostnames.



**tracert -h <max\_hops> <domain> :** Specifies the time-out in milliseconds to wait for a response from each hop.

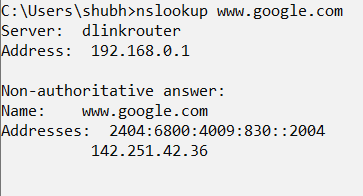


**Tracert -j <host-list> <domain> :** Traces the path and lists the IP addresses of the intermediate hops in the specified loose source route.

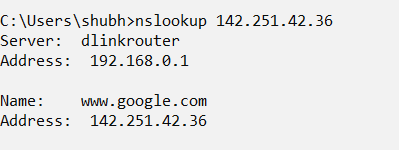


**Nslookup:** Displays information that you can use to diagnose Domain Name System (DNS) infrastructure. The nslookup command-line tool has two modes: interactive and noninteractive.

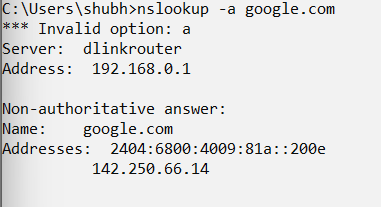
**Nslookup <hostname>:** This performs a lookup of the IP address associated with the specified hostname.



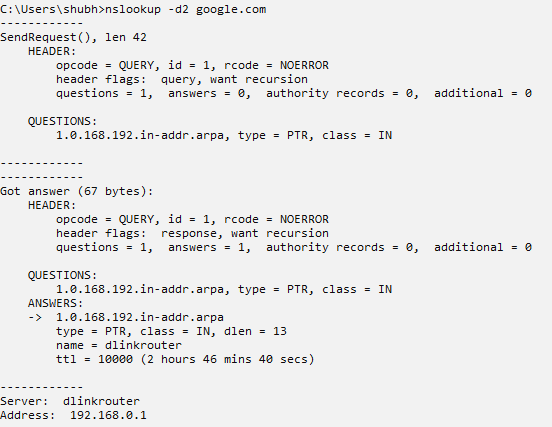
**nslookup <IP address> :** This performs a reverse lookup of the hostname associated with the specified IP address.



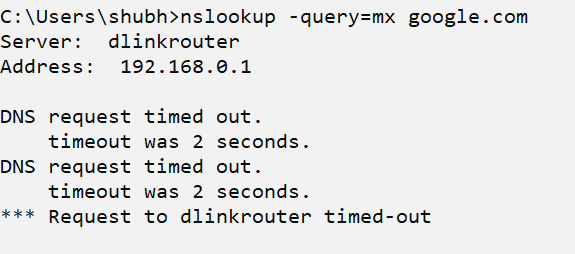
**Nslookup -a <hostname>:** This performs a lookup of all addresses associated with the specified hostname.



**Nslookup -d2:** This enables debug mode, which provides verbose output during the lookup process.



**Nslookup -query=mx <domain>:** This performs a lookup of the mail exchange (MX) records associated with the specified domain, which are used to route email for that domain.



**Netstat :** Netstat stands for “network statistics”. If you’re having difficulties accessing the internet, the netstat command can help you identify where the problem lies. Netstat will display all of your computer’s active network connections and the status of those connections. If a connection is not working, netstat can often provide more information about why it is not working.

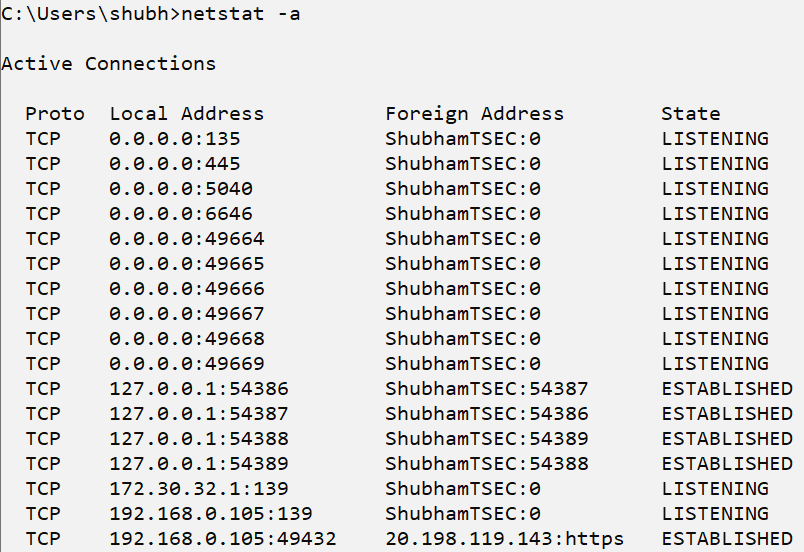
Netstat can also be used to monitor your computer for security threats.

**How do I run netstat command?**

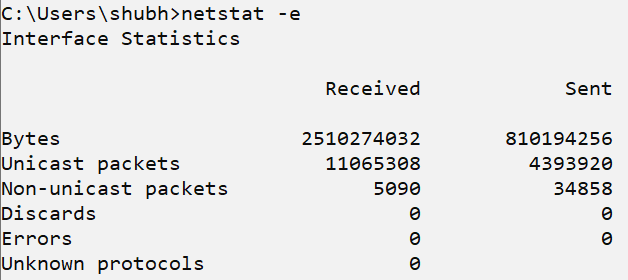
**Step 1:** Open the start menu, type cmd into the search box, and press Enter to launch the command prompt.

**Step 2:** Type netstat at the prompt and press Enter. The netstat command will now display a list of all active network connections.

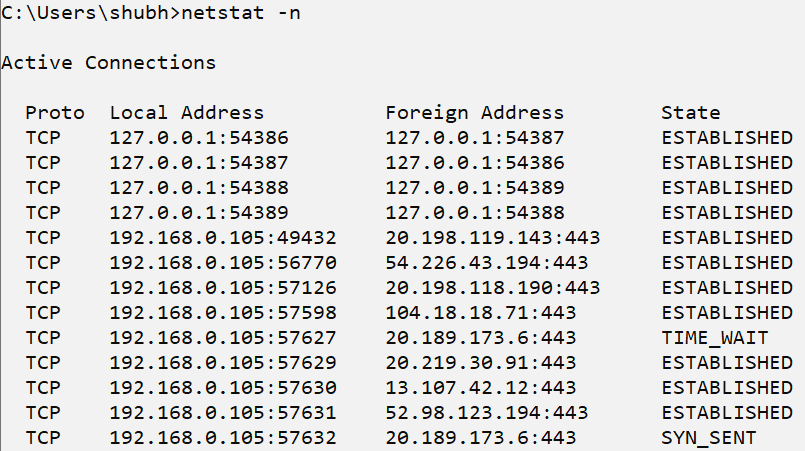
**‘netstat -a’ :** Shows all active connections and listening ports on the computer



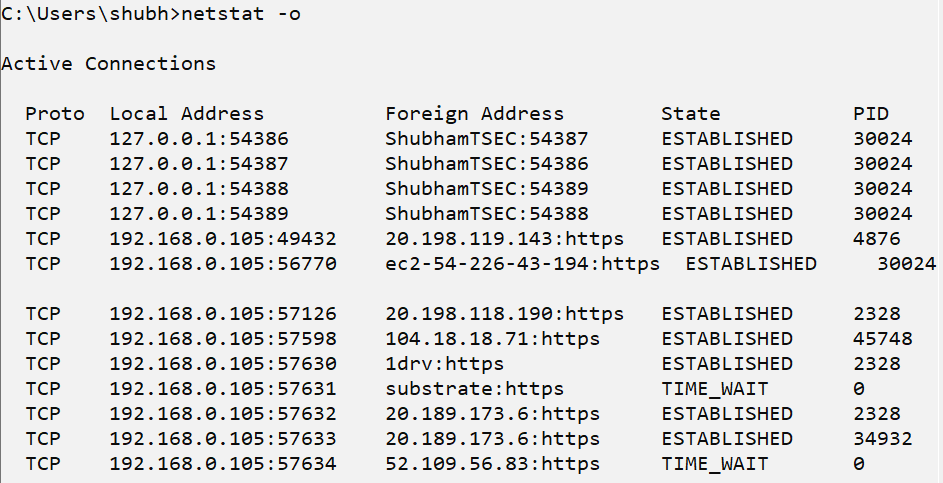
**‘netstat -e’ :** Displays Ethernet statistics, including the number of bytes and packets sent and received.



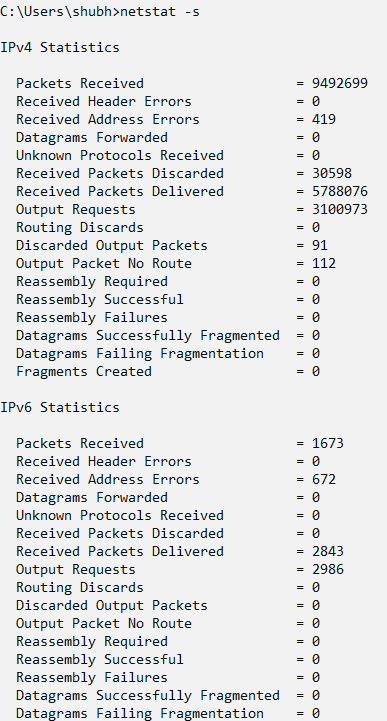
**‘netstat -n’ :** Shows active connections and their associated IP addresses and port numbers. The ‘-n’ option causes ‘netstat’ to display addresses and port numbers in numerical form, rather than resolving them to hostnames and service names.



‘**netstat -o’ :** Shows the process Id (PID) of each active connection, allowing you to see which process is responsible for each connection.



‘**netstat -s’ :** Displays a summary of all network statistics, including information on the number of segments received, errors, and more.



**Route command :**  The ‘route’ command is used to manipulate the IP routing table in Windows.

With the ‘route’ command, you can view the current routing table, add new routes, modify existing routes, and delete routes.

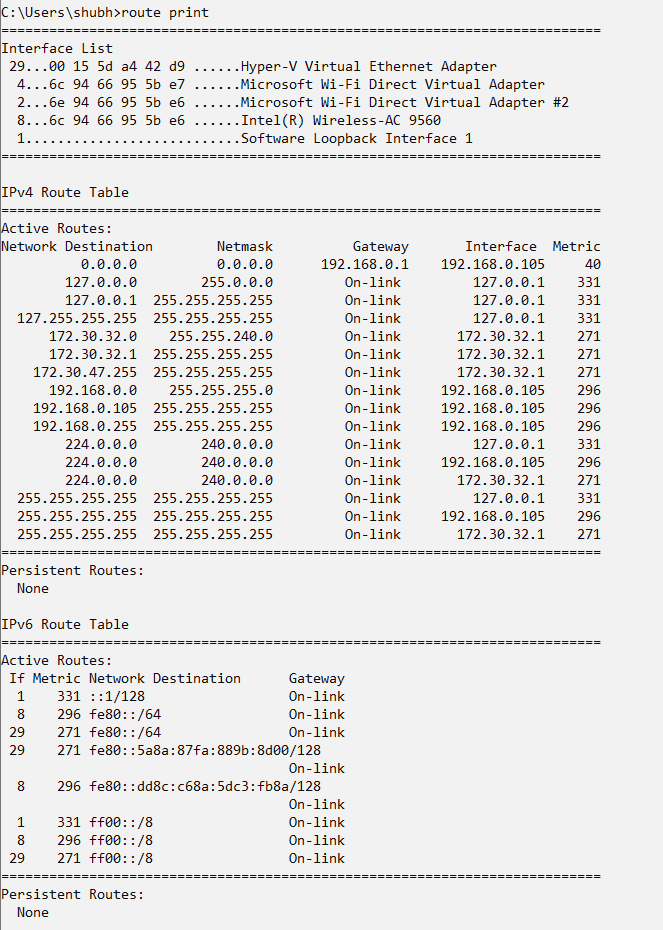
The ‘route’ command is often used in advanced network configuration scenarios, such as setting up VPN connections, specifying custom routes for specific networks, or resolving connectivity issues.

**How to use route command in windows?**

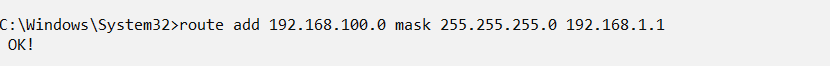
**Step 1 :** Open the command prompt.

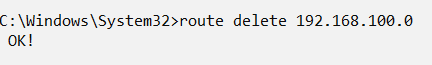
**Step 2 :** Write ‘route’ in the command prompt, you will see many options will be showing there after clicking enter. Now you can run your command according to your requirement.

**‘route print’** : Displays the current routing table on the computer, including information on the network interfaces, destinations, and gateways.



**‘route add <destination> mask <subnet mask> <gateway>’ :** Adds a new route to the routing table, specifying the destination network, subnet mask, and gateway.



**‘route delete <destination>’ :** Deletes an existing route from the routing table, specified by destination network. 

**‘route change <destination> mask <subnet mask> <gateway>’ :** Modifies an existing route in the routing table, changing the destination network, subnet mask, and/or gateway as specified.



**‘route -p add <destination> mask <subnet mask> <gateway>’ :** Adds a persistent route to the routing table, which will persist across reboots of the computer. This is useful for configuring static routes that are always present on the system.



**Hostname:** The ‘hostname’ command is used to display or set the hostname of a computer in windows 11. When run without any options, the ‘hostname’ command will display the current hostname of the computer.

**How to implement hostname command?**

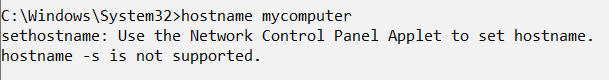
**Step 1:** Open the command prompt

**Step 2:** Write the hostname in the command prompt and you will see the name of the host in command prompt.

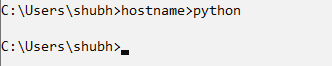
**‘hostname’ :** Displays the hostname of the current computer.



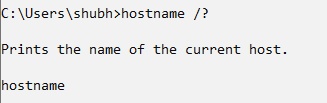
**‘hostname <new-hostname>’ :** Changes the hostname of the current computer to the specified value. This change is not permanent and will be lost upon reboot.



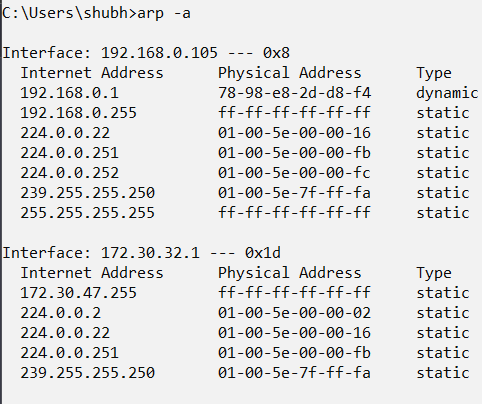
**‘hostname > filename’:** Writes the hostname of the current computer to a specified file.



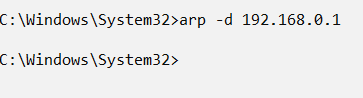
**‘hostname /?’ :** Displays the help information for the ‘hostname’ command.



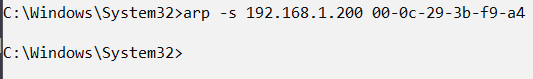
‘arp -a’ : Displays the current ARP (Address Resolution Protocol) cache, which maps IP addresses to MAC addresses on the local network.



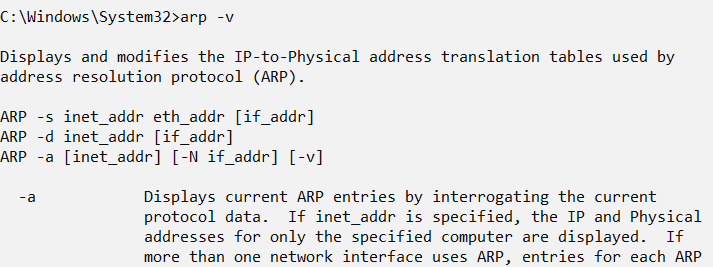
‘arp -d <ip-address>’ : Deletes a specific entry from the ARP cache, specified by IP address.



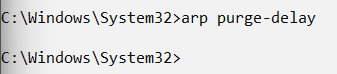
‘arp -s <ip-address> <mac-address>’ : Adds a new entry to the ARP cache, specifying the IP address and corresponding MAC address.



‘arp -v’ : Displays the ARP cache in verbose mode, including additional information such as the type of ARP entries (dynamic or static) and the interface used for each entry.

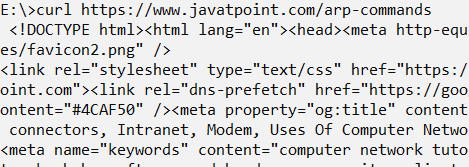


**arp purge-delay:** The arp purge-delay command delays the purging in the ARP entries in an ARP table/cache when the interface goes down or slows down. When the interface comes up within the delay time, the ARP entries are restored, and packet loss with ECMP (Equal Cost Multipath) is restricted.

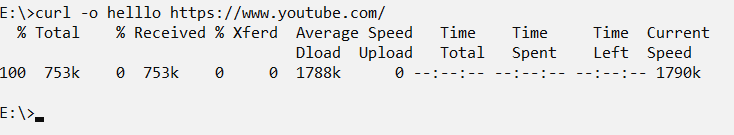


**Curl (client URL):** It is a command-line tool powered by the libcurl library to transfer data to and from the server using various protocols, such as HTTP, HTTPS, FTP, FTPS, IMAP, IMAPS, POP3, POP3S, SMTP, and SMTPS. It is highly popular for automation and scripts due to its wide range of features and protocol support.

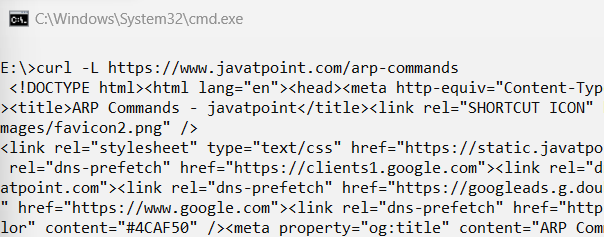
**‘curl <url>’ :** Downloads the content of the specified URL and displays it in the console.



**‘curl -o <filename> <url>’ :** Downloads the content of the specified URL and saves it to a file with the specified name.



**‘curl -I <url>’ :** Requests the HTTP headers of the specified URL, but not the actual content of the resource.



**‘curl -v’ :** The ‘curl -v’ command is used to show verbose output of a curl request. This can be useful for debugging or seeing the details of a request.



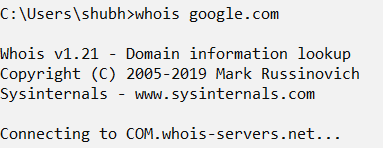
**Whois :** It allows you to perform lookup of owner information of a website by querying databases that store the registered users of a domain or IP address.

**How to run whois command?**

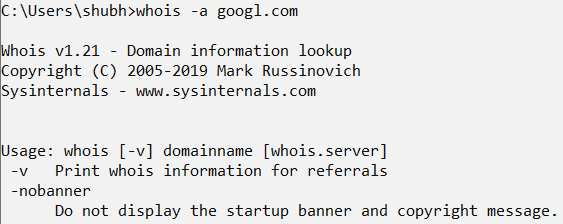
**Step 1: Open the command prompt**

**Step 2: Run the whois command with some domain name e.g. cmd> whois google.com**

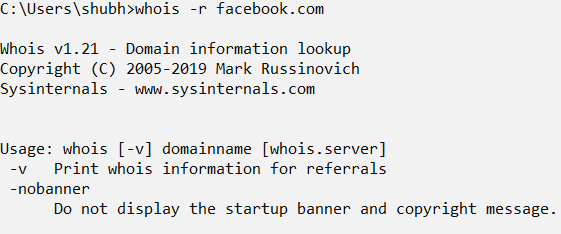
**‘whois <domain>’ :** Retrieves the WHOIS information for the specified domain.



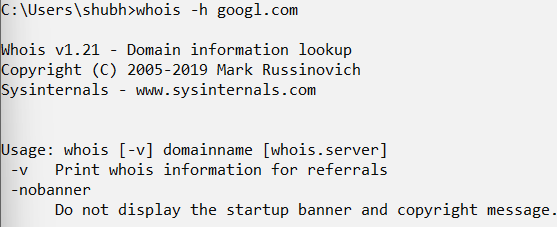
**‘whois -a <domain>’ :** Retrieves the WHOIS information for the specified domain, including the administrative and technical contact information.



**‘whois -r <domain>’ :** Retrieves the WHOIS information for the specified domain in a machine-readable format.



**‘whois -h <server> <domain>’ :** Retrieves the WHOIS information for the specified domain from the specified WHOIS server.



**‘whois -v <domain>’ :** Retrieves the WHOIS information for the specified domain and displays it in verbose mode, including detailed information about the domain registrar and registration dates.

