**Lab Practical #01:**

Study of basic networking commands and IP configuration.

**Practical Assignment #01:**

1. Perform and explain various networking commands listed below:
   1. ipconfig
   2. ping
   3. getmac
   4. systeminfo
   5. traceroute / tracert
   6. netstat
   7. nslookup
   8. hostname
   9. pathping
   10. arp

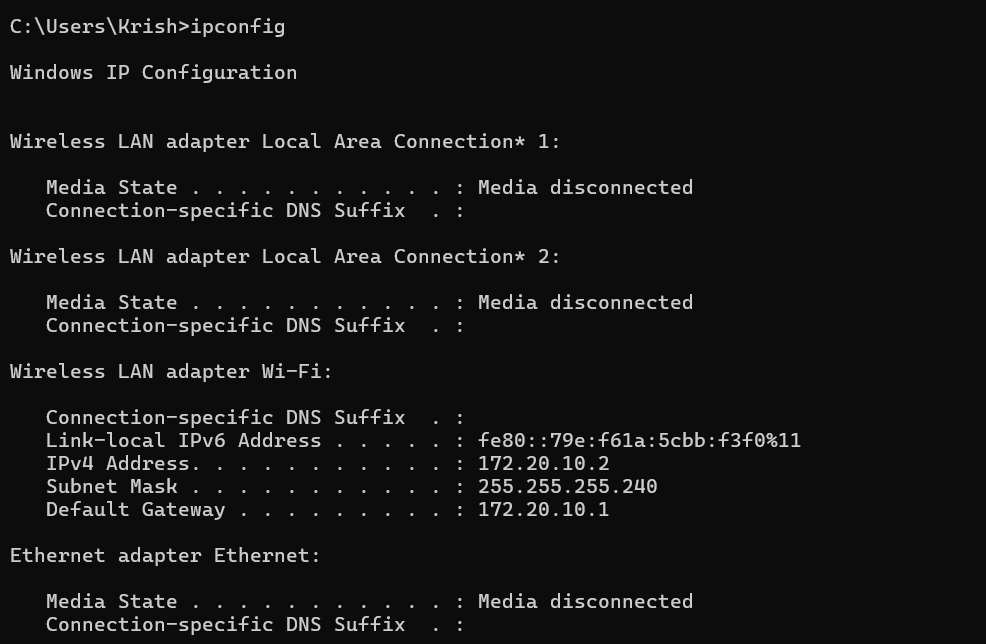
## ipconfig

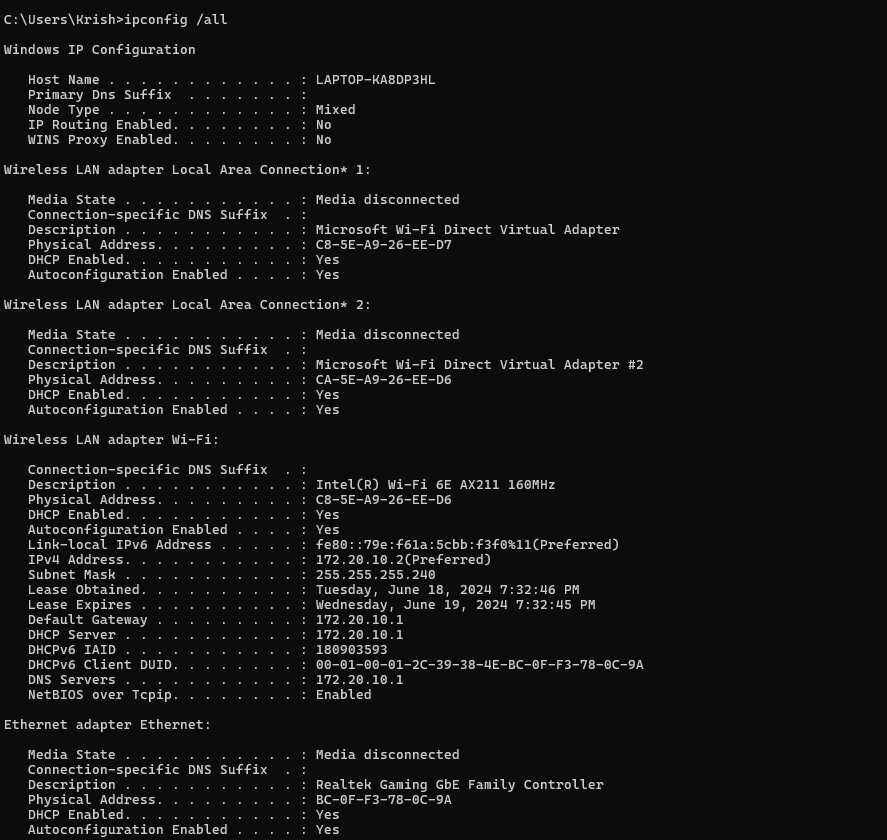
### Description:

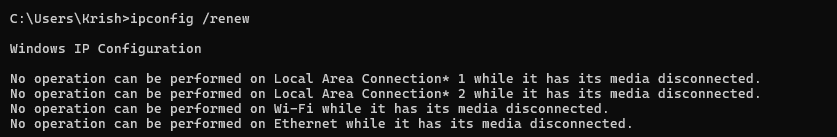
**The `ipconfig` command is used in Windows to display and manage the network configuration of the system. It provides detailed information about the IP addresses, subnet masks, default gateways, and other network settings of all network adapters in the system.**

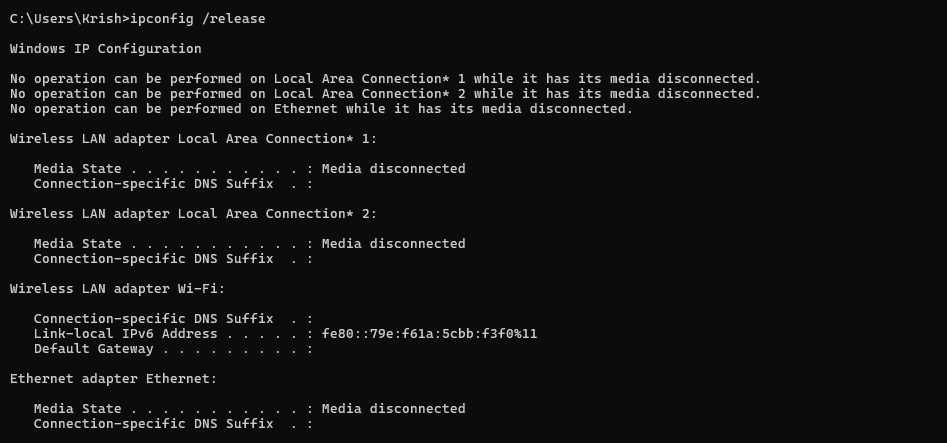
|  |  |  |
| --- | --- | --- |
| No. | Option | Description |
| 1 | /all | Displays the full TCP/IP configuration for all adapters. |
| 2 | /release | Releases the IPv4 address for the specified adapter. |
| 3 | /release6 | Releases the IPv6 address for the specified adapter. |
| 4 | /renew | Renews the IPv4 address for the specified adapter. |
| 5 | /renew | Renews the IPv6 address for the specified adapter. |

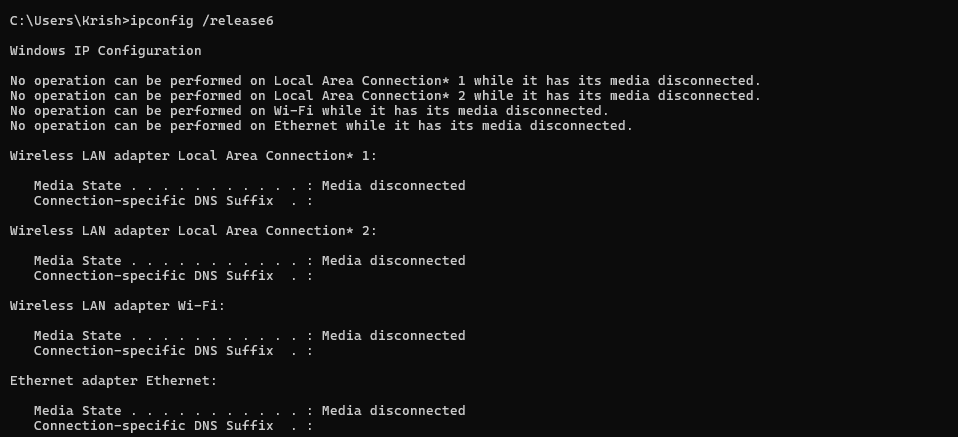
### Implementation:

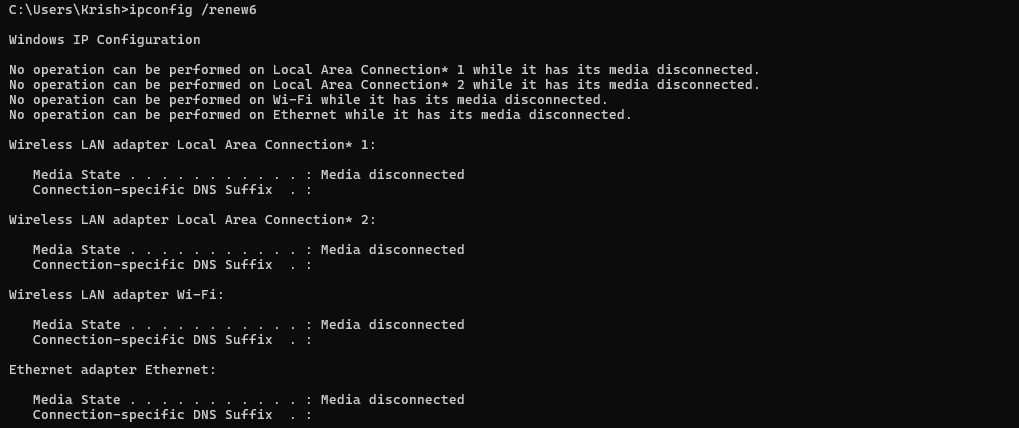












## ping

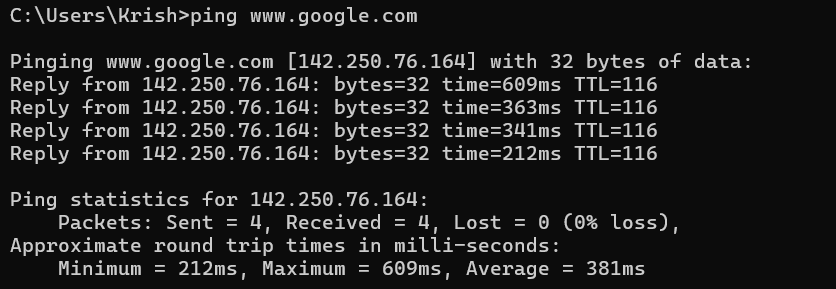
### Description:

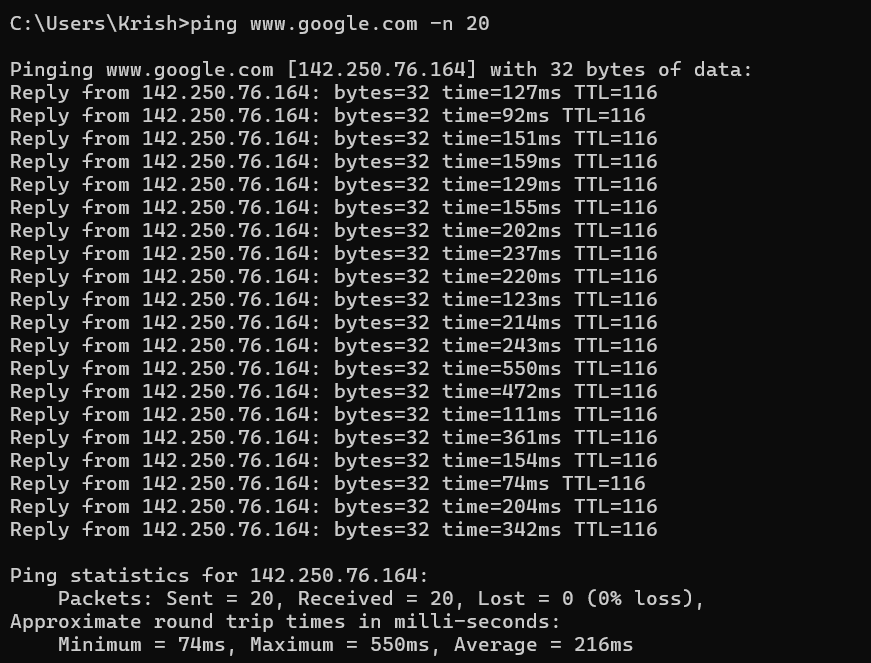
**The `ping` command is a network utility used to test the reachability of a host on an IP network. It sends ICMP Echo Request packets to the target host and listens for ICMP Echo Reply packets, measuring round-trip time and packet loss to diagnose network connectivity issues.**

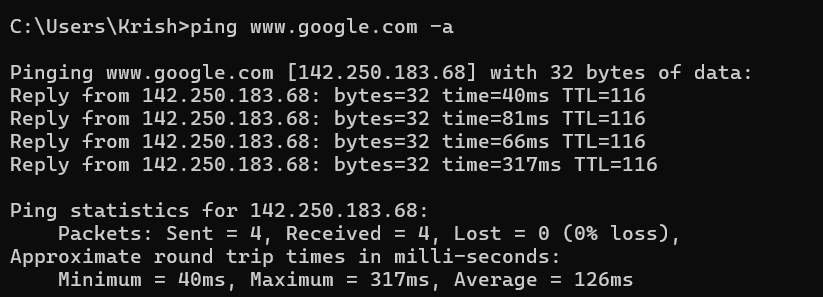
|  |  |  |
| --- | --- | --- |
| No. | Option | Description |
| 1 | -t | Ping the specified host until stopped. To stop, press “ctrl+c”. |
| 2 | -n | Specify the number of echo requests to send. |
| 3 | -a | Resolve addresses to hostnames. |
| 4 | -f | Set the "Don't Fragment" flag in the packet (IPv4-only). |
| 5 | -4 | Force using IPv4. |

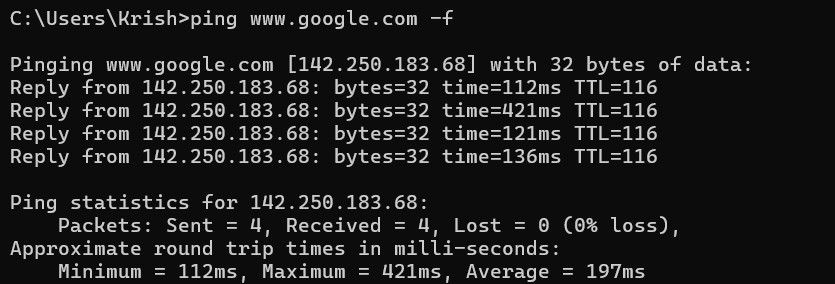
### Implementation:

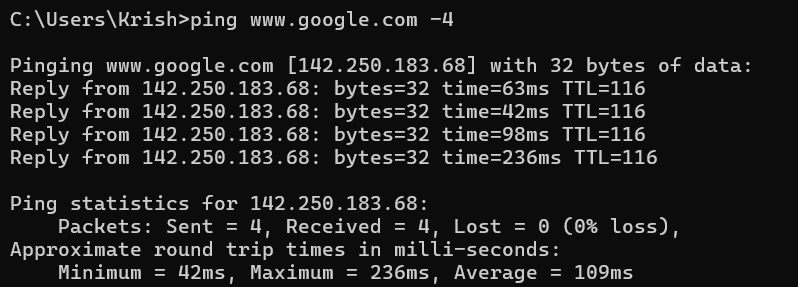
****

****

****

****

****

****

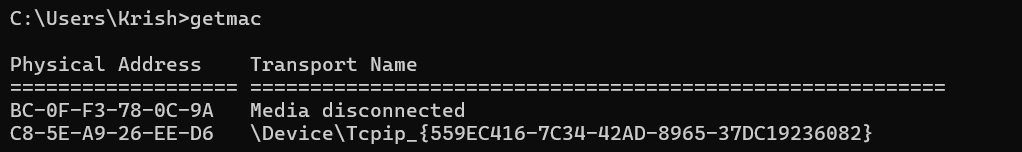
## Getmac

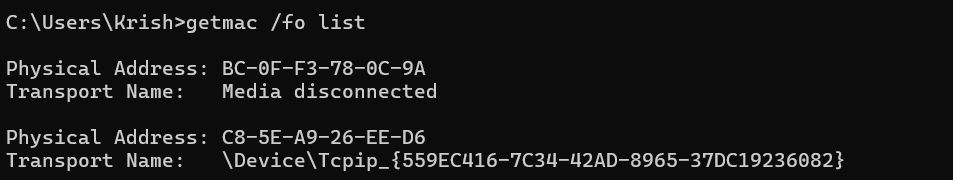
### Description:

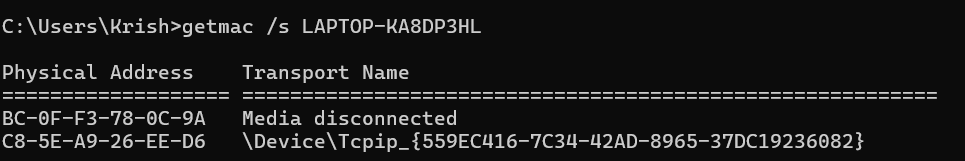
**The getmac command is a network utility used to display the Media Access Control (MAC) address for network adapters on a system. It provides a quick way to find the physical address associated with each network interface, which is essential for tasks such as network troubleshooting, security auditing, and network management.**

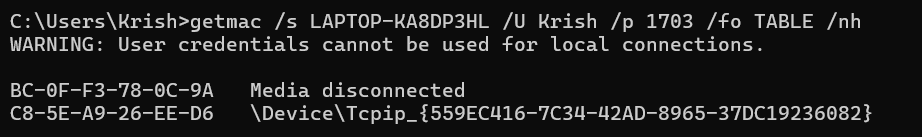
|  |  |  |
| --- | --- | --- |
| No. | Option | Description |
| 1 | /s | Connects to a remote system to retrieve MAC addresses.The default is the local computer. |
| 2 | /u | Specifies the user context for executing the command. |
| 3 | /p | Provides the password for the specified user account. |
| 4 | /fo | Sets the output format to TABLE, LIST, or CSV. |
| 5 | /nh | Omits the column header in the output. |

### Implementation:









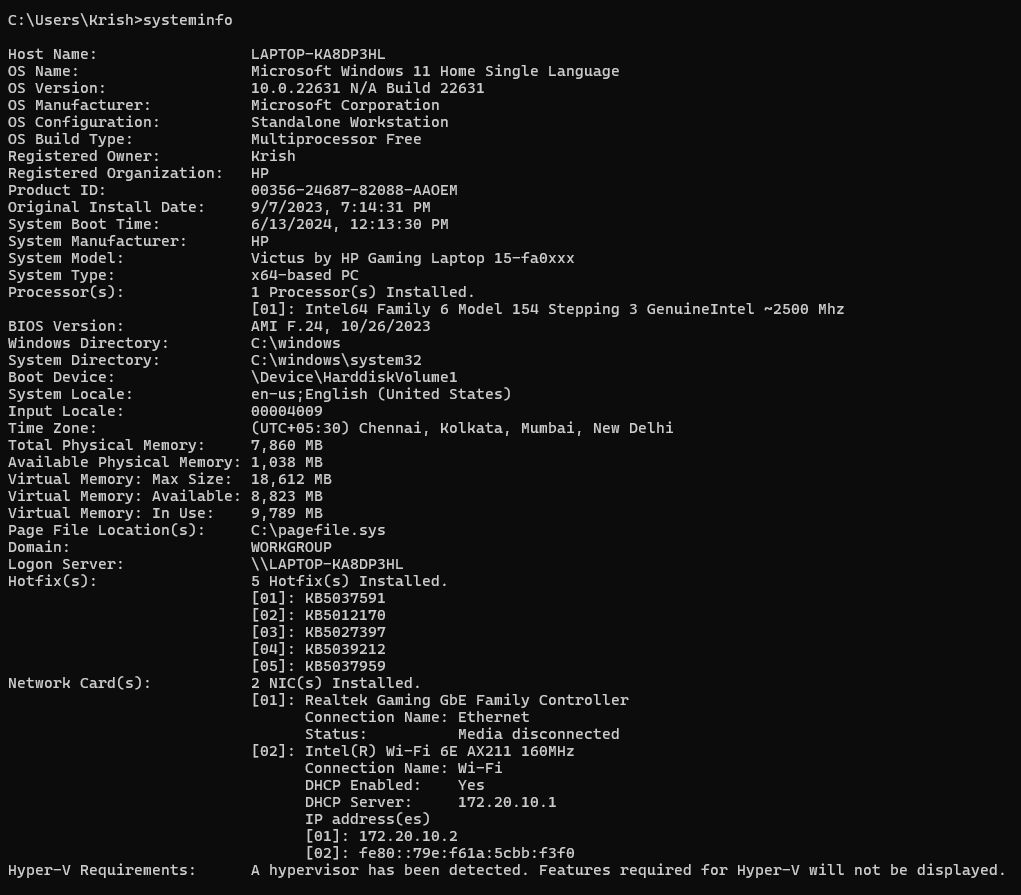
## systeminfo

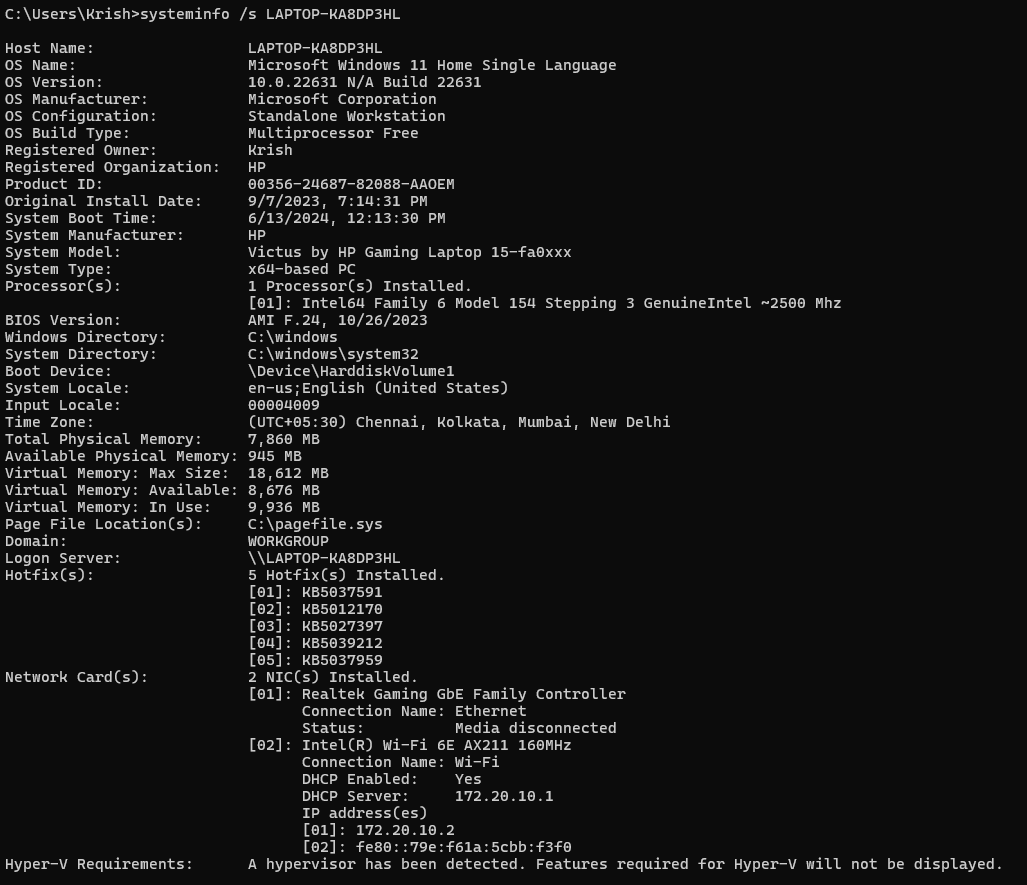
### Description:

**The systeminfo command is a system utility in Windows that provides detailed configuration information about a computer's operating system, hardware components, and software environment. This includes details such as OS version, memory, network adapters, and installed hotfixes.**

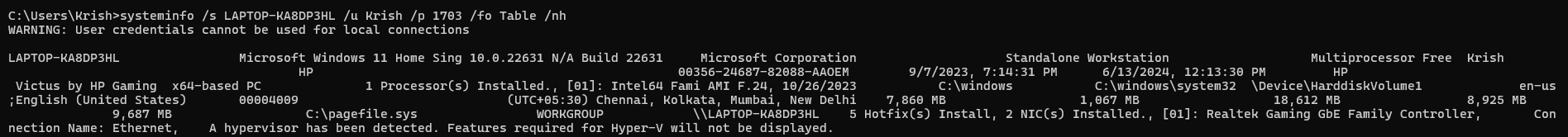
|  |  |  |
| --- | --- | --- |
| No. | Option | Description |
| 1 | /s | Connects to a specified remote system to retrieve system information. |
| 2 | /u | Specifies the user context under which the command should execute on the remote system. |
| 3 | /p | Provides the password for the specified user account on the remote system. |
| 4 | /fo | Sets the output format to TABLE, LIST, or CSV. |
| 5 | /nh | Omits the column headers in the output, useful for when the output is redirected to a file or used in scripts. |

### Implementation:









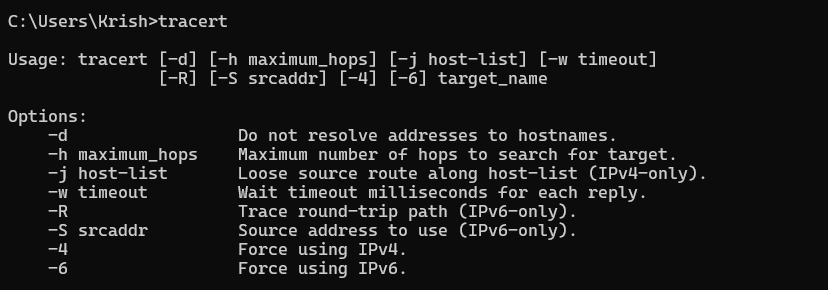
## tracert

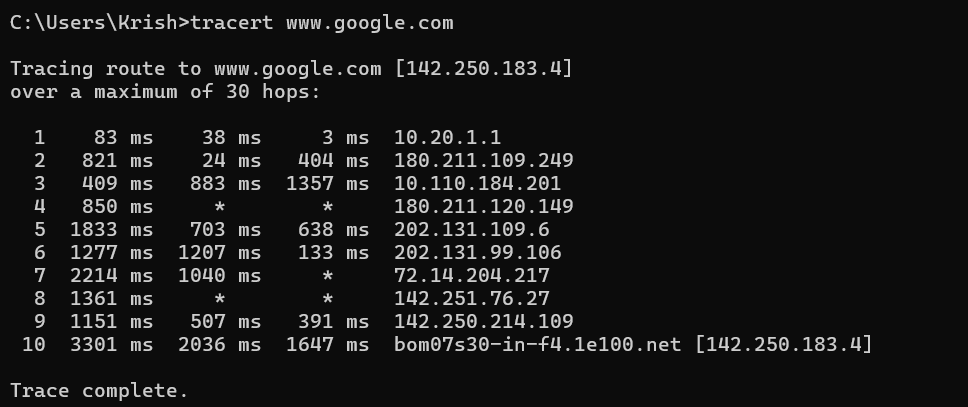
### Description:

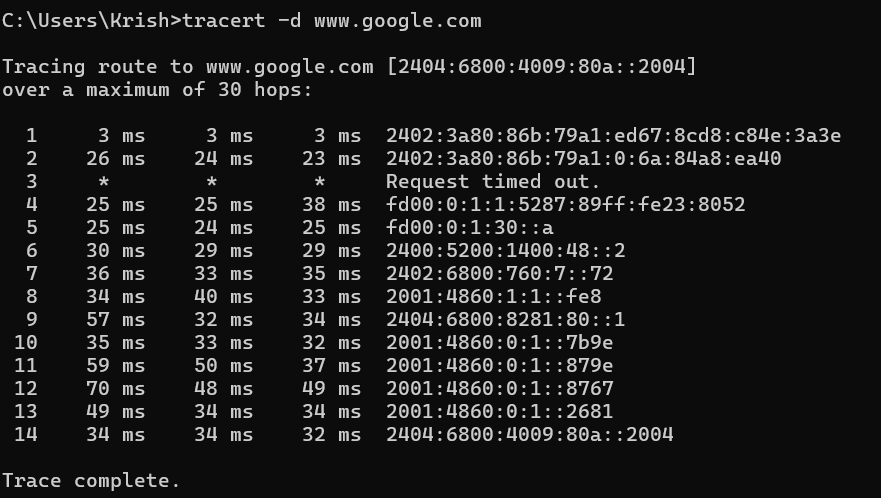
**The traceroute (on Unix-based systems) or tracert (on Windows) command is a network diagnostic tool used to track the path packets take from the source to the destination host across an IP network. It helps in identifying the route taken by packets and locating points of failure or high latency in the network path.**

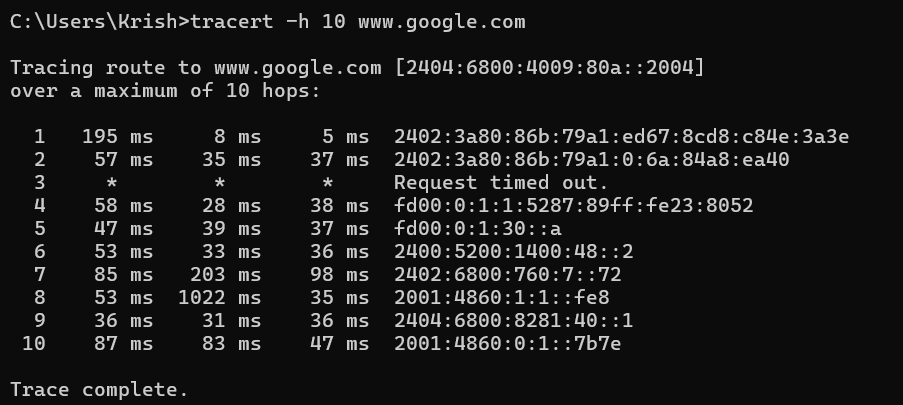
|  |  |  |
| --- | --- | --- |
| No. | Option | Description |
| 1 | -d | Do not resolve addresses to hostnames, displaying only IP addresses. |
| 2 | -h | Specifies the maximum number of hops (routing steps) to search for the target. The default is typically 30 hops. |
| 3 | -w | Specifies the timeout in milliseconds to wait for each reply. This helps in adjusting the waiting time for responses from each hop. |
| 4 | -4 | Force the use of IPv4 for the traceroute, even if the system is configured for IPv6. |
| 5 | -6 | Force the use of IPv6 for the traceroute, used in environments where IPv6 is deployed. |

### Implementation:

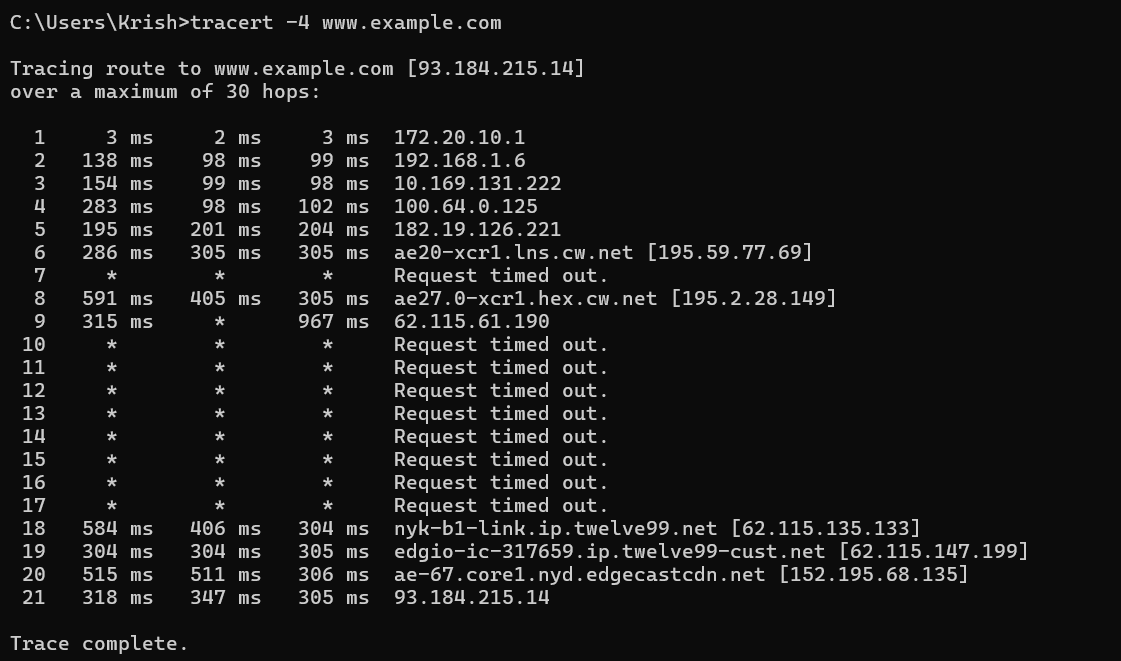












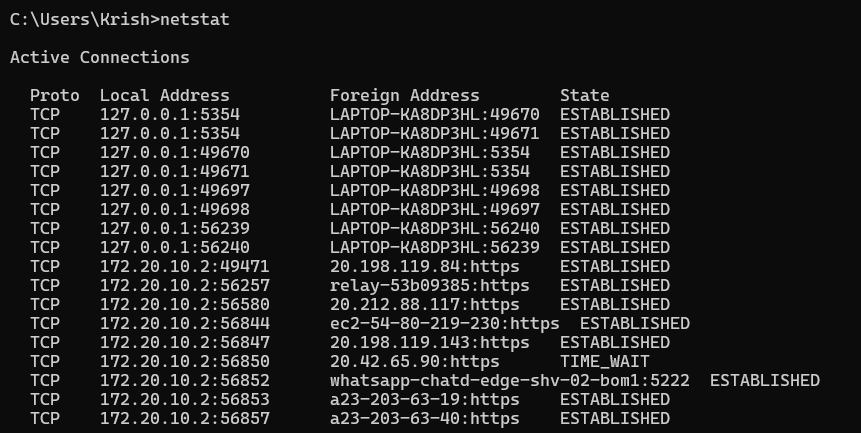
## netstat

### Description:

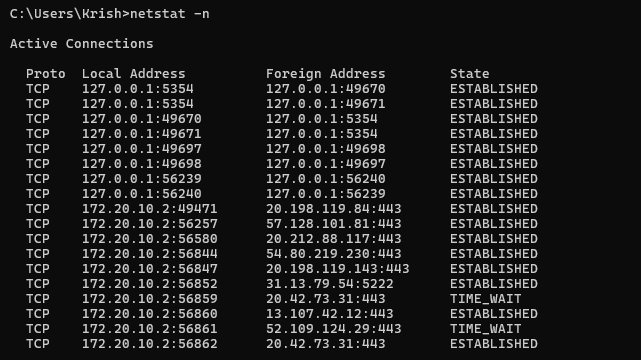
**The netstat command is a network utility used to display network connections (both incoming and outgoing), routing tables, interface statistics, masquerade connections, and multicast memberships. It is a valuable tool for diagnosing network issues and monitoring network activity.**

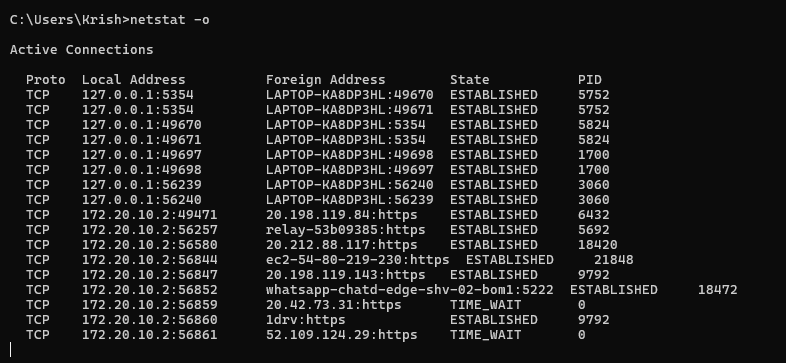
|  |  |  |
| --- | --- | --- |
| No. | Option | Description |
| 1 | -a | Displays all active connections and listening ports, including those on the listening state. |
| 2 | -n | Displays addresses and port numbers in numerical form, without resolving to hostnames or service names. |
| 3 | -o | Shows the owning process ID associated with each connection, which can be useful for identifying which processes are using which network connections. |
| 4 | -e | Displays Ethernet statistics, such as bytes sent and received. This can be useful for monitoring network interface activity. |
| 5 | -r | Displays the routing table, showing the paths that network traffic will take to reach its destination. |

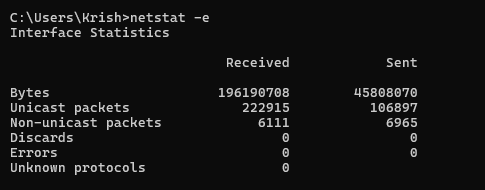
### Implementation:

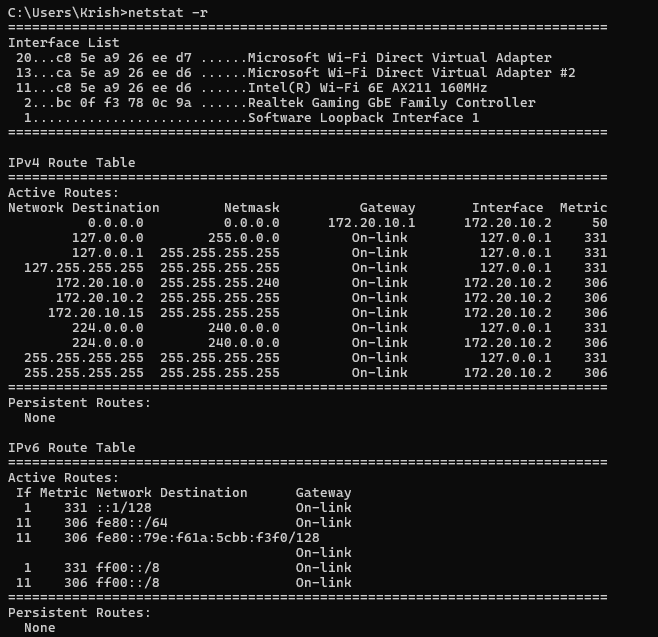












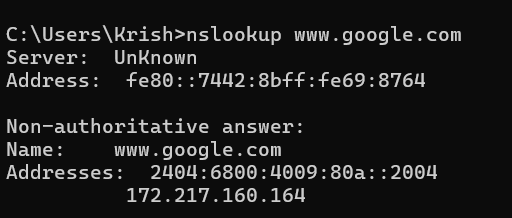
## nslookup

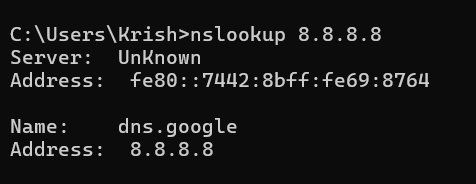
### Description:

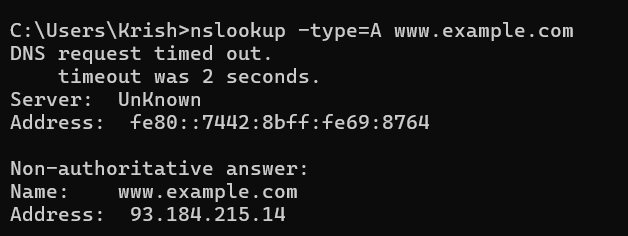
**The nslookup command is a network utility used to query Domain Name System (DNS) servers to obtain domain name or IP address mapping. It is commonly used to troubleshoot DNS issues, verify DNS configurations, and gather DNS-related information.**

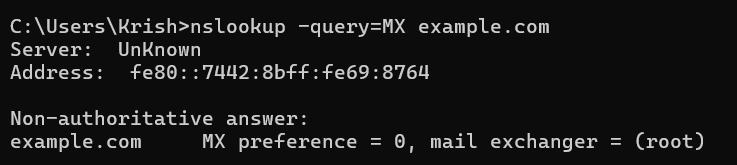
|  |  |  |
| --- | --- | --- |
| No. | Option | Description |
| 1 | < hostname> | Queries the specified hostname to find its corresponding IP address. |
| 2 | <IP address> | Queries the specified IP address to find its corresponding domain name. |
| 3 | server <DNS server> | Specifies a different DNS server to use for the query. Useful for checking DNS responses from specific DNS servers. |
| 4 | type=<record type> | Specifies the type of DNS record to query (e.g., A, AAAA, CNAME, MX, NS, PTR, SOA, SRV, TXT). This allows you to retrieve specific types of DNS information. |
| 5 | port | Specifies the DNS server port number. |
| 6 | timeout | Sets the initial timeout interval for waiting for a reply. |
| 7 | Debug | Turns on debug mode, which shows detailed information about the query. |

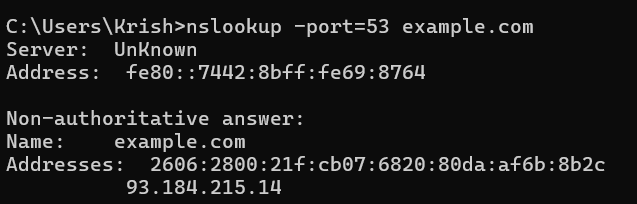
### Implementation:

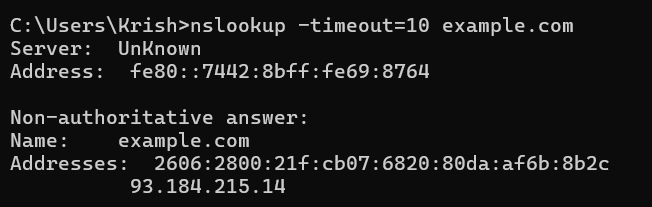














## hostname

### Description:

**The hostname command is a simple utility used to display or set the hostname of the system. The hostname is a unique name assigned to a computer on a network, which is used to identify the system in network communications.**

|  |  |  |
| --- | --- | --- |
| No. | Option | Description |
| 1 | -a | Displays the alias name of the host (if any). |
| 2 | -d | Shows the DNS domain name of the host. |
| 3 | -f | Displays the fully qualified domain name (FQDN). |
| 4 | -i | Displays the network addresses of the host (IP addresses). |
| 5 | -s | Shows the short hostname (the hostname up to the first dot). |



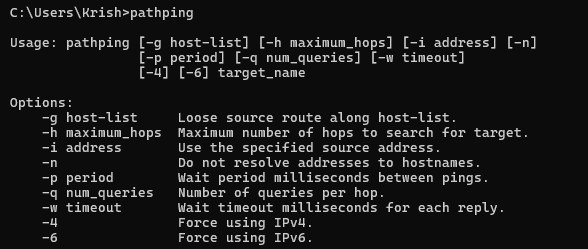
## pathping

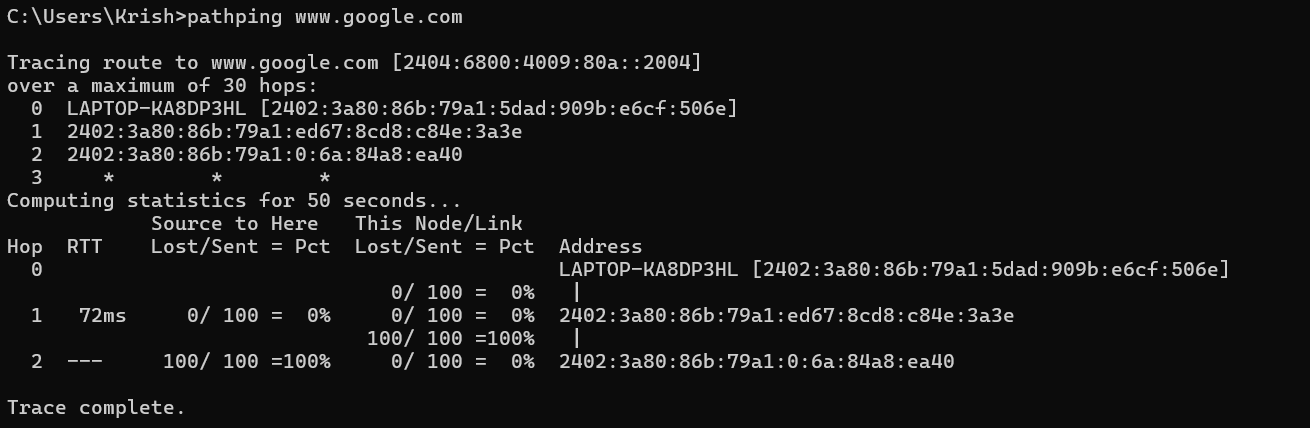
### Description:

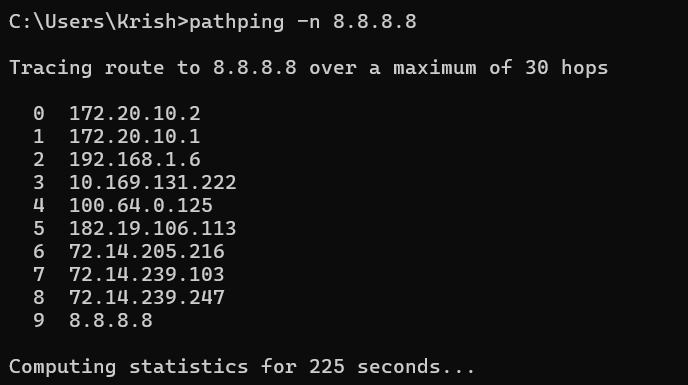
**The `ipconfig` command is used in Windows to display and manage the network configuration of the system. It provides detailed information about the IP addresses, subnet masks, default gateways, and other network settings of all network adapters in the system.**

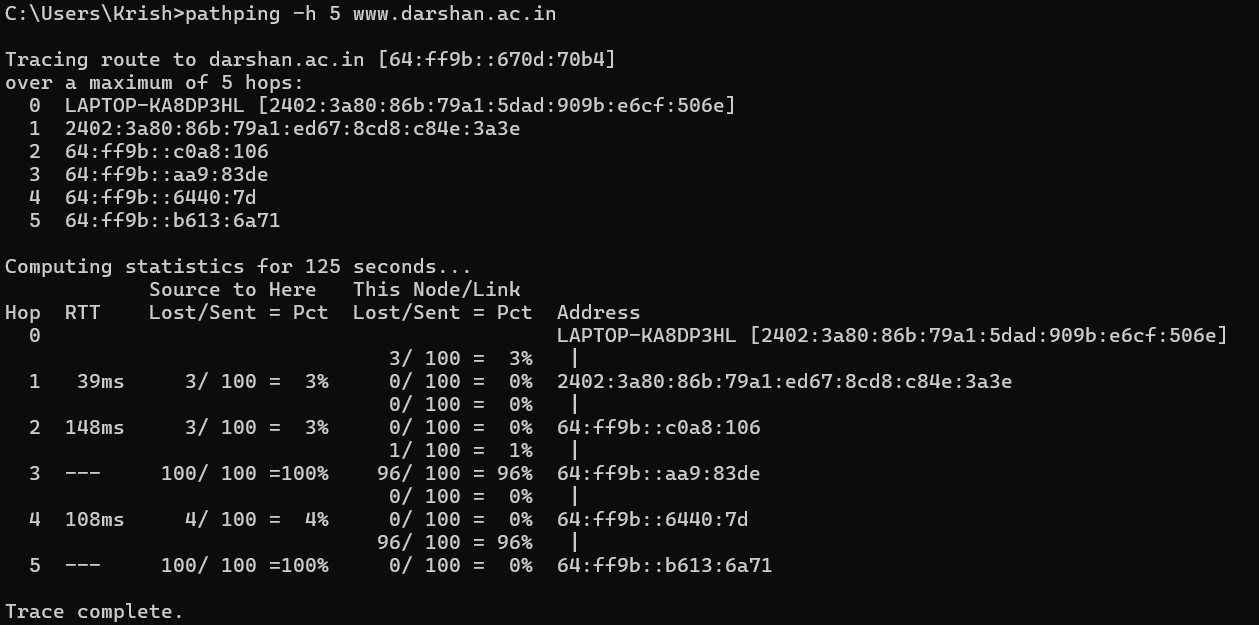
|  |  |  |
| --- | --- | --- |
| No. | Option | Description |
| 1 | -n | Does not resolve addresses to hostnames, displaying only IP addresses. |
| 2 | -h | Specifies the maximum number of hops (routing steps) to search for the target. The default is 30 hops. |
| 3 | -g | Allows for loose source routing along the specified list of hosts. |
| 4 | -p | Waits the specified number of milliseconds between pings. The default is 250 milliseconds. |
| 5 | -q | Specifies the number of queries per hop. The default is 100 queries. |

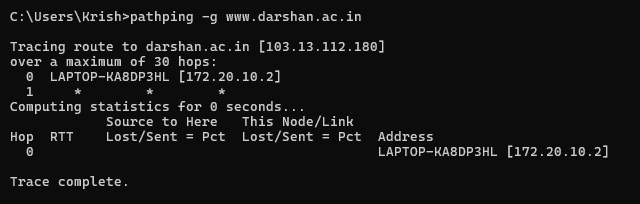
### Implementation:

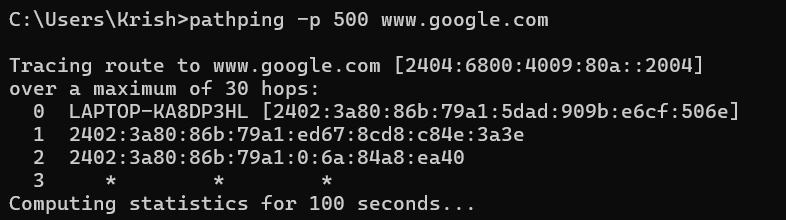


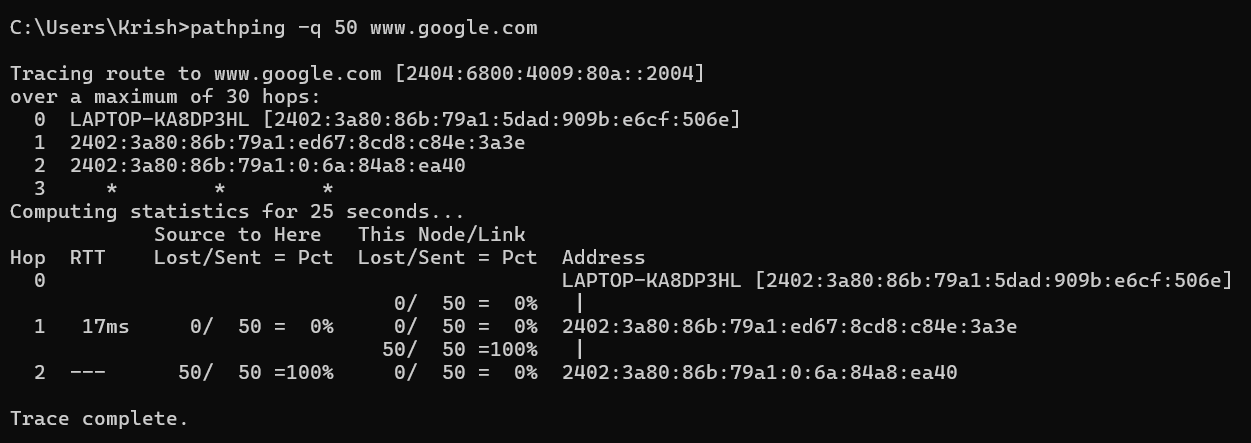


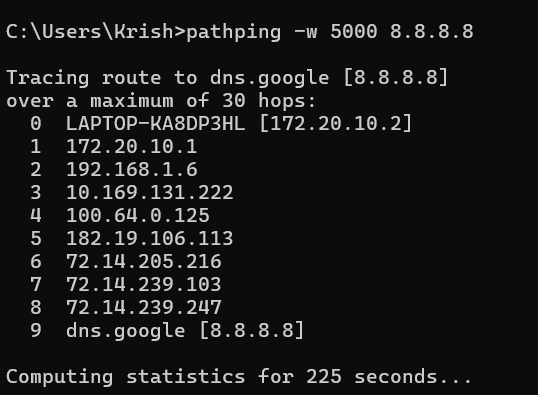












## arp

### Description:

**The arp command is used to display and manipulate the Address Resolution Protocol (ARP) cache, which maps IP addresses to physical MAC addresses on a local network. This is essential for network communication as it allows devices to find each other using their IP addresses by resolving them to the correct MAC addresses.**

|  |  |  |
| --- | --- | --- |
| No. | Option | Description |
| 1 | -a | Displays the current ARP entries in the ARP cache for all interfaces. |
| 2 | -g | Same as -a, displays the current ARP entries in the ARP cache for all interfaces. |
| 3 | -s | Adds a static ARP entry to the ARP cache that associates the specified IP address with the MAC address on an optional interface index. |
| 4 | -v | Displays current ARP entries in verbose mode. All invalid entries and entries on the loop-back interface will be shown. |
| 5 | -N | Displays the ARP entries for the specified network interface identified by its IP address. |

### Implementation:

