Date: 04/07/2023

Lab Practical #01:

Study of basic networking commands and IP configuration.

Practical Assignment #01:

1. Perform and explain various networking commands listed below:
    i. ipconfig
    ii. ping
    iii. getmac
    iv. systeminfo
    v. traceroute / tracert
    vi. netstat
    vii. nslookup
    viii. hostname
    ix. pathping
    x. Arp

Date: 04/07/2023

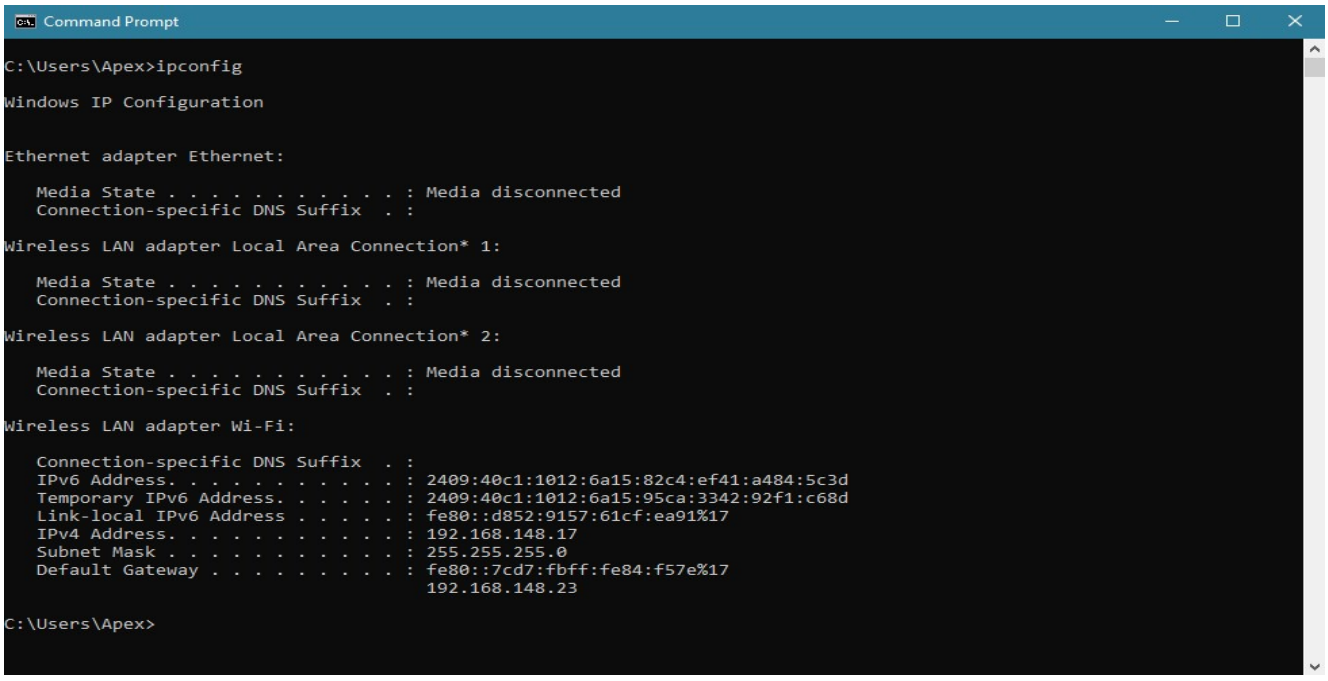
1. ipconfig

Description:

Ipconfig is a console application designed to run from the windows command prompt. This utility allows you to get the IP address of a windows computer. It also allows some control over your network adapters, IP addresses (DHCP – assigned specifically), even your DNS cache. The output of the default command contains the IP address, network mask, and gateway for all physical and virtual network adapters.

No.	Option	Description
1	*ipconfig /all*	*This option display the same IP addressing information for each adapter as the default option. Additionally, its displays DNS and WINS settings for each adapter as well as a whole host of additional information.*
2	*ipconfig /release*	*This option terminates any active TCP/IP connections on all network adapters and releases those IP addresses for use by other applications.* ***ipconfig /release*** *can be used with specific windows connection names.*
3	*ipconfig /renew*	*This option re-establishes TCP/IP connections on all network adapters. As with the release option,* ***ipconfig /renew*** *takes an optional connection name specifier. Both* ***/renew*** *and* ***/release*** *options only work on clients configured for dynamic (DHCP) addressing.*

Implementation:



Date: 04/07/2023

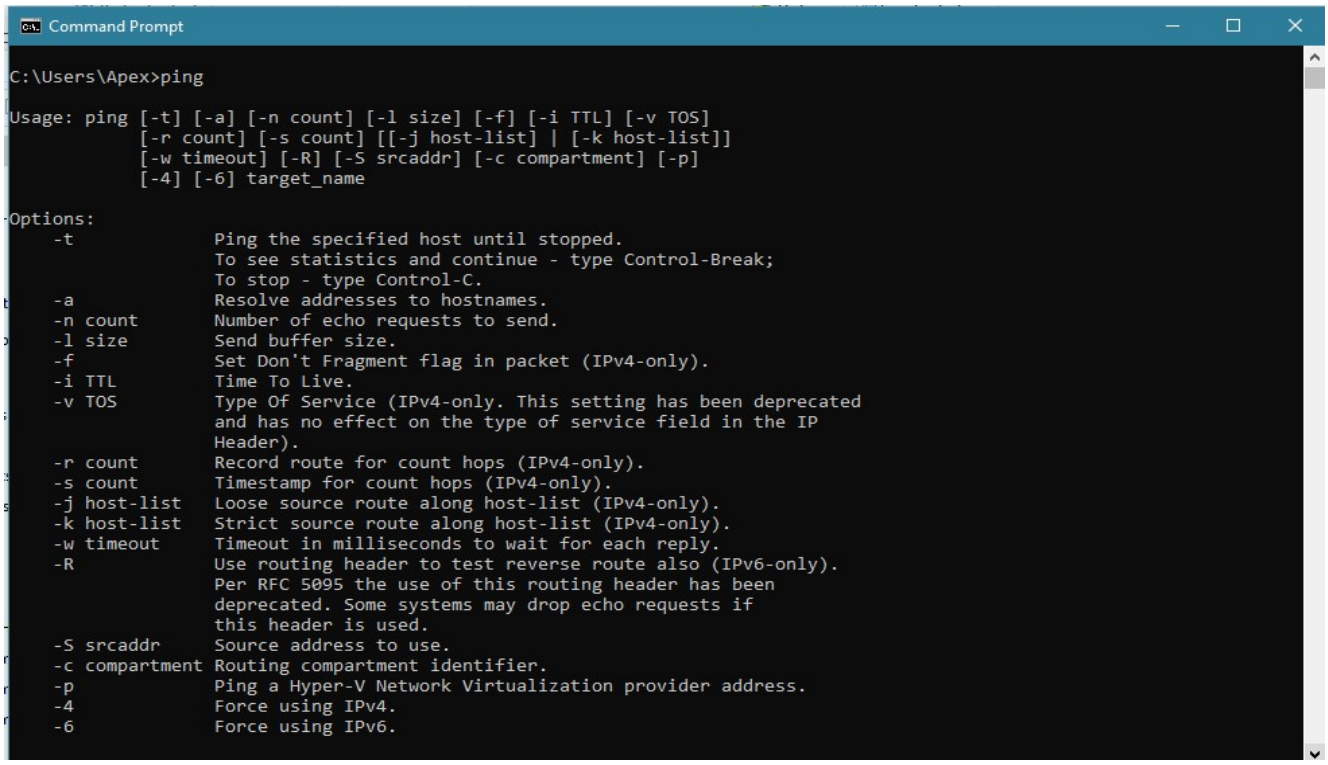
2. ping

Description:

Ping is used to test the network connectivity between two system. It's a simple way to verify that a computer can communicate with another computer or network device. Ping uses Internet Control Message Protocol (ICMP) for echo request and reply messages to check physical and logical connectivity of machines on an internet.

No.	Option	Description
1	*ping -n [count] [hostname]*	*This option sets the number of ICMP echo request to send, from 1 to 4294967295. The ping command will send 4 default if **-n** is not used.*
2	*ping -l [size] [hostname]*	*Use this option to set the size in bytes of the echo request packet from 32 to 65527. The ping will send a 32-bytes echo request if you don't use the **-l** option.*
3	*ping -t [hostname]*	*Using this option will ping the target until you force it to stop by using **CTRL + C .** Otherwise it will sent echo requests until do not you press **CTRL + C .***

Implementation:



Date: 04/07/2023

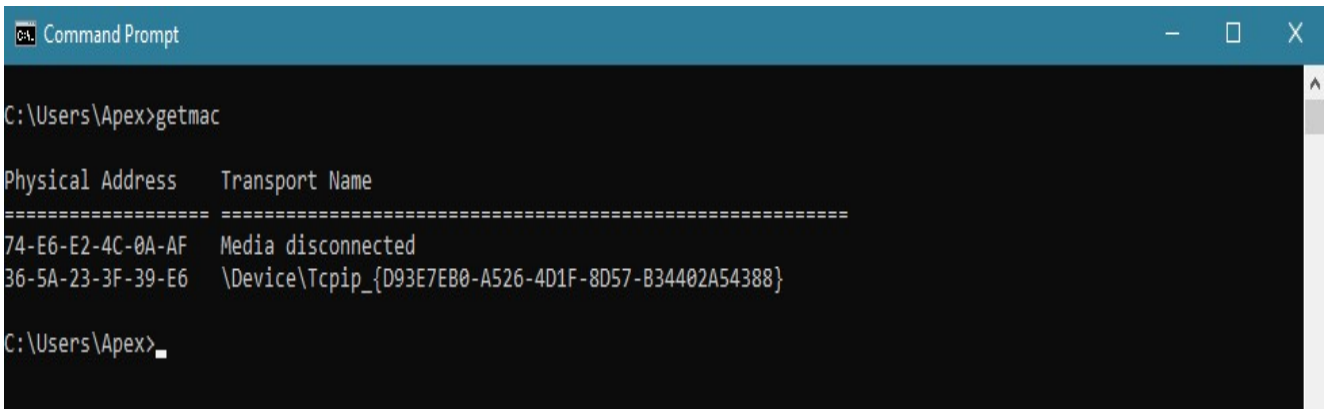
3. getmac

Description:

Getmac is a widows command used to display the Media Access Control (MAC) address for each network adapter in the computer. Using getmac command we could see the address of all media control like bluetooth, wi-fi etc.

No.	Option	Description
1	*getmac /s [hostname]*	*Specifies the remote system to connect. This can be either an IP address or a host name (do not use backslashes). The default is the local computer.*
2	*getmac /u [hostname]*	*Specifies the user context under which the command should execute. The default is the permissions of the current logged on user on the computer issuing the command.*
3	*getmac /fo [format]*	*Specifies the format in which the output is to be displayed. Valid format values: "TABLE", "LIST", "CSV". default is Table.*

Implementation:



Date: 04/07/2023

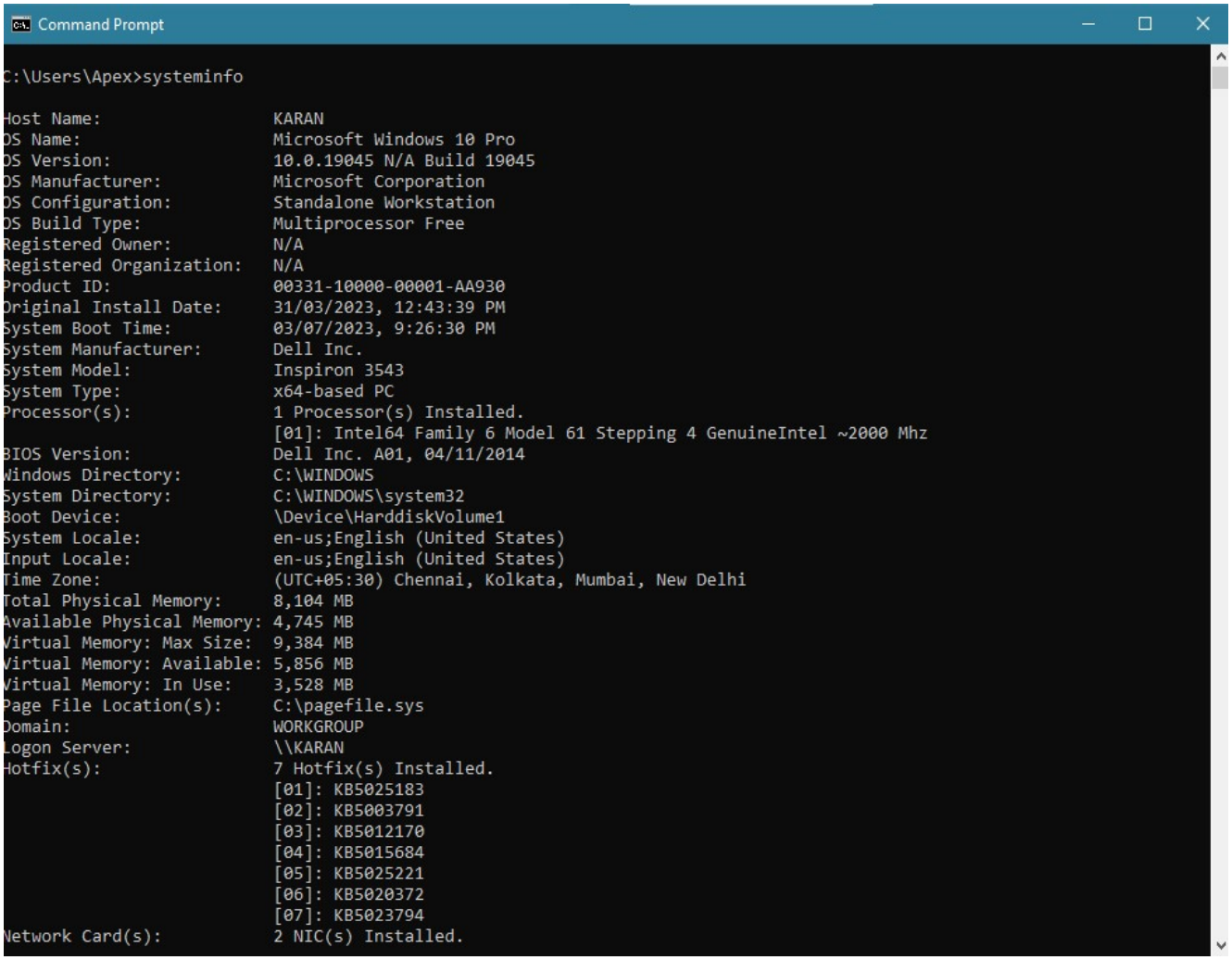
4. systeminfo

Description:

This command displays detailed configuration information about a computer and its operating system, including operating system configuration, security information, product ID and hardware properties (such as RAM, disk space and network cards.

No.	Option	Description
1	*systeminfo /s [hostname]*	*Specifies the name or IP address of a remote computer (do not use backslashes). The default is the local computer.*
2	*systeminfo /p [hostname]*	*Specifies the password of the user account that is specified in the **/u** parameter.*
3	*systeminfo /fo [format]*	*Specifies the format in which the output is to be displayed. Valid format values: "TABLE", "LIST", "CSV". default is List.*

Implementation:



Date: 04/07/2023

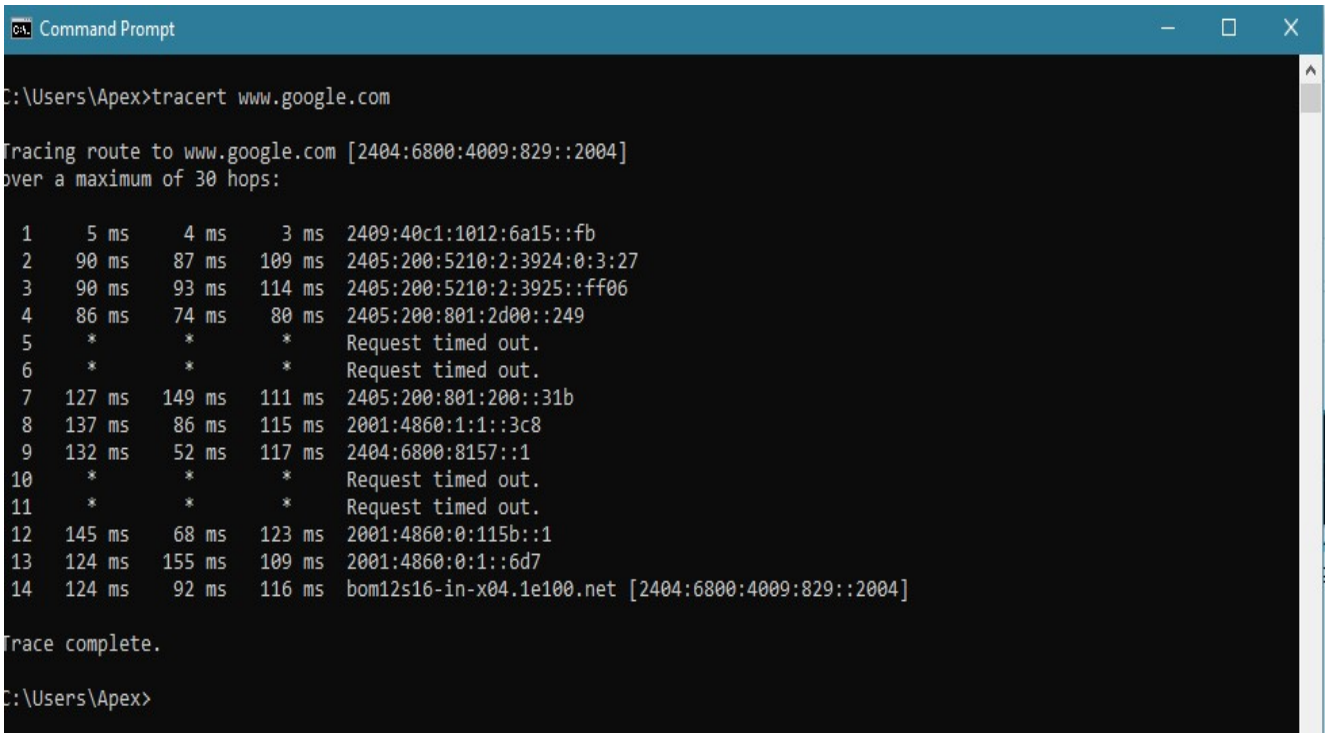
5. tracert / traceroute

Description:

The tracert command is a Command Prompt command that's used to show several details about the path that a packet takes from the computer or device you are on to whatever destination you specify. You might also sometimes see the tracert command referred to as the trace route command or traceroute command.

No.	Option	Description
1	*tracert -d [hostname]*	*This option prevents tracert from resolving IP addresses to hostnames, often resulting in much faster results..*
2	*tracert -h [number of hops] [hostname]*	*This tracert option specifies the maximum number of hops in the search for the target. If you do not specify MaxHops, and a target has not been found by 30 hops, tracert will stop looking.*
3	*tracert -w [mili-seconds] [hostname]*	*You can specify the time, in milliseconds, to allow each reply before timeout using this tracert option.*

Implementation:



Date: 04/07/2023

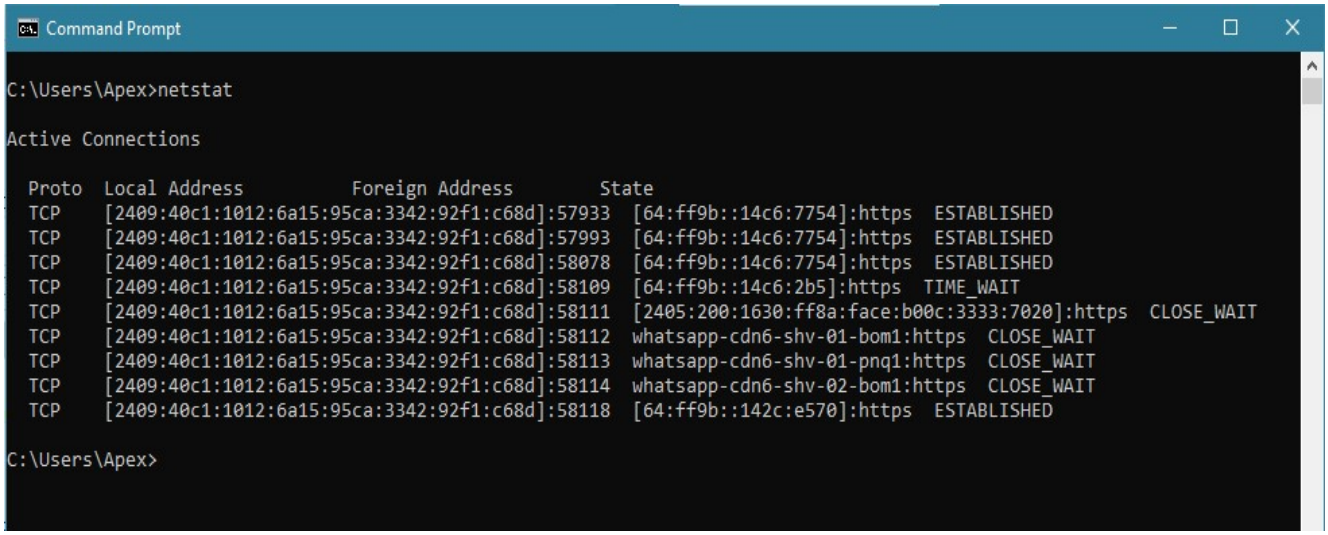
6. netstat

Description:

The netstat command generates displays that show network status and protocol statistics. You can display the status of TCP and UDP endpoints in table format, routing table information and interface information. Its used to display very detailed information about how your computer is communicating with other computers or network devices. Since netstat is a cross-platform command, it's also available in other operating systems like macOS and Linux.

No.	Option	Description
1	*netstat -a*	*This switch displays active TCP connections, TCP connections with the listening state, as well as UDP ports that are being listened to.*
2	*netstat -o*	*A handy option for many troubleshooting tasks, the **-o** switch displays the process identifier (PID) associated with each displayed connection.*
3	*netstat -r*	*Execute netstat with **-r** to show the IP routing table. This is the same as using the route command to execute **route print**.*

Implementation:



Date: 04/07/2023

7. nslookup

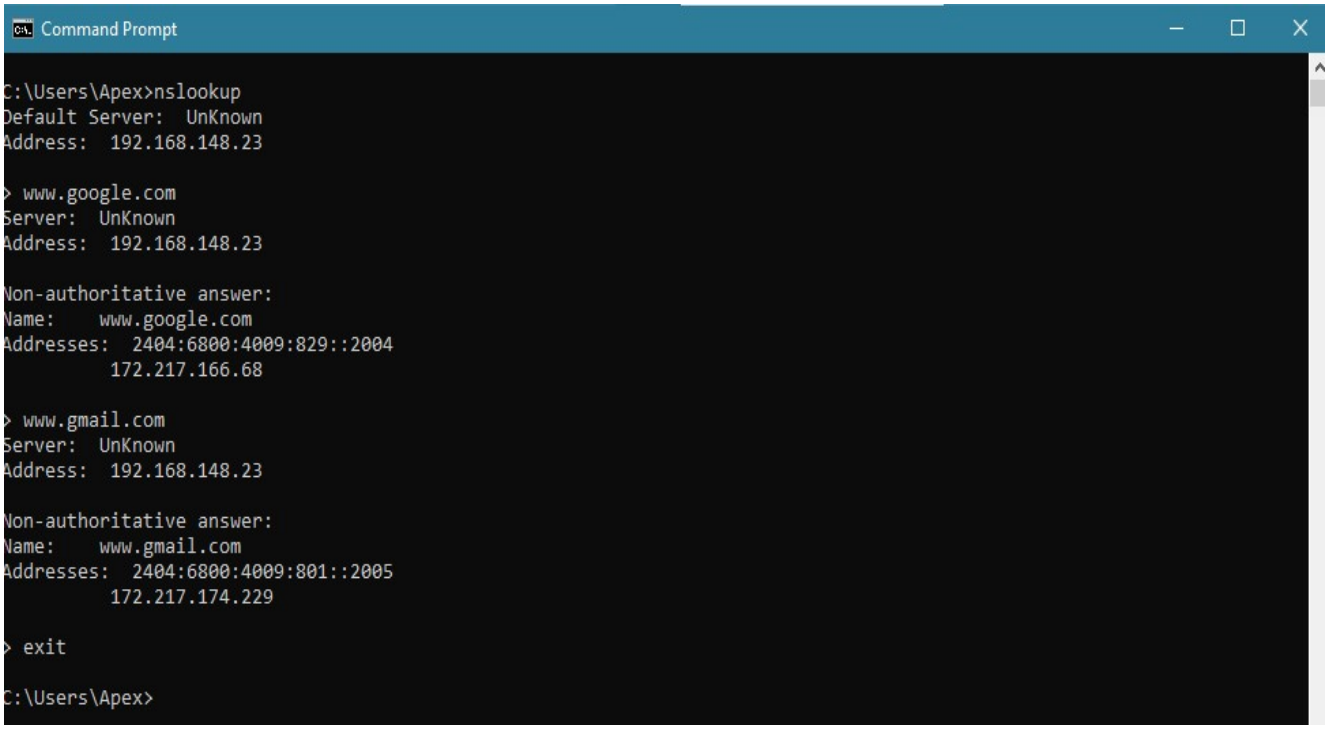
Description:

Microsoft Windows includes a tool called NSLOOKUP that you can use via the command prompt. This tool can be used to check DNS records propagation and resolution using different servers and perform other troubleshooting steps. NSLOOKUP can be use in interactive and non-interactive mode.

Its used to find the IP address of a host, domain name of an IP address and mail servers for a domain.

No.	Option	Description
1	*nslookup finger*	*Connects with the finger server on the current computer.*
2	*nslookup ls*	*Lists information for a DNS domain.*
3	*nslookup root*	*Changes the default server to the server for the root of the DNS domain name space.*

Implementation:



Date: 04/07/2023

8. hostname

Description:

Prints the name of the current host of the specific device

Implementation:

Date: 04/07/2023

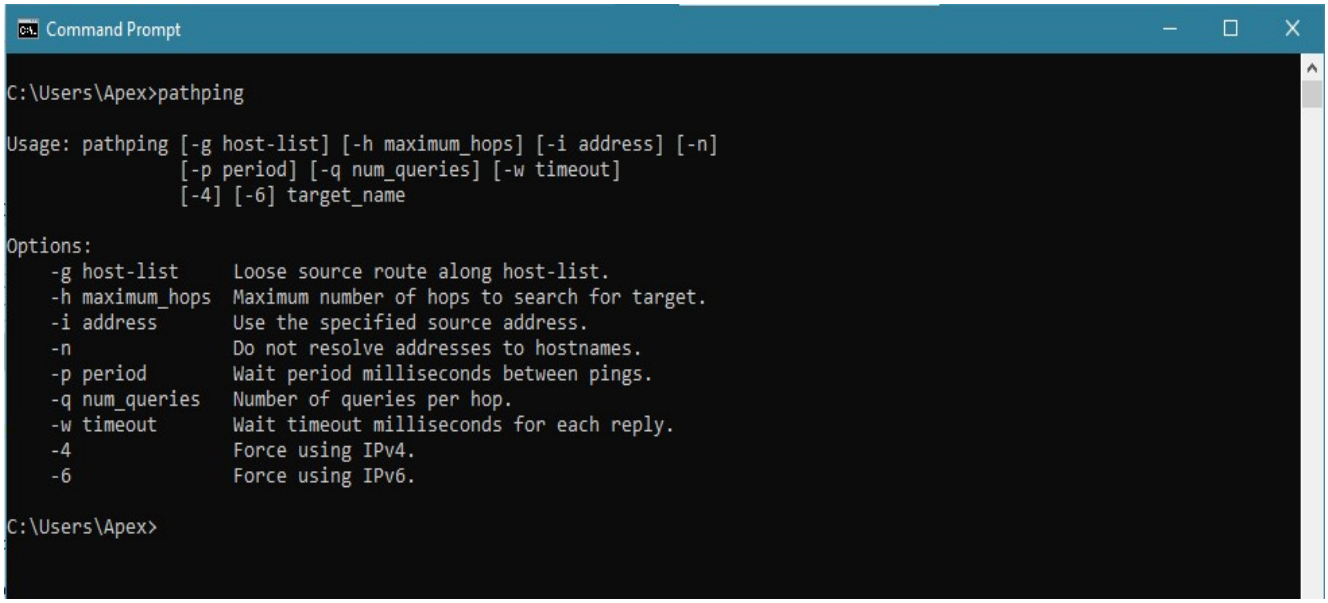
9. pathping

Description:

Provides information about network latency and network loss at intermediate hops between a source and destination. This command 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. Because this command displays the degree of packet loss at any given router or link, you can determine which routers or subnets might be having network problems. Used without parameters, this command displays help.

No.	Option	Description
1	*pathping /n [hostname]*	*Prevents **pathping** from attempting to resolve the IP addresses of intermediate routers to their names. This might expedite the display of **pathping** results.*
2	*pathping /q [hostname]*	*Specifies the number of echo Request messages sent to each router in the path. The default is 100 queries.*
3	*pathping /h [hostname]*	*Specifies the maximum number of hops in the path to search for the target (destination). The default is 30 hops.*

Implementation:



Date: 04/07/2023

10.arp

Description:

Displays and modifies entries in the Address Resolution Protocol (ARP) cache. The ARP cache contains one or more tables that are used to store IP addresses and their resolved Ethernet or Token Ring physical addresses. There is a separate table for each Ethernet or Token Ring network adapter installed on your computer. Used without parameters, ***arp*** *displays help information.*

No.	Option	Description
1	*arp -a*	*Displays current ARP entries by interrogating the current protocol data. If inet_addr is specified, the IP and Physical for only the specified computer are displayed. If more than one network interface uses ARP, entries for each ARP table are displayed.*
2	*arp -v*	*Displays current ARP entries in verbose mode. All invalid entries and entries on the loop-back interface will be shown.*
3	*arp -s*	*Adds the host and associates the Internet address inet_addr with the Physical address eth_addr. The Physical address is as 6 hexadecimal bytes separated by hyphens. The entry permanent.*

Implementation: