Date: 07/ 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

1. ipconfig

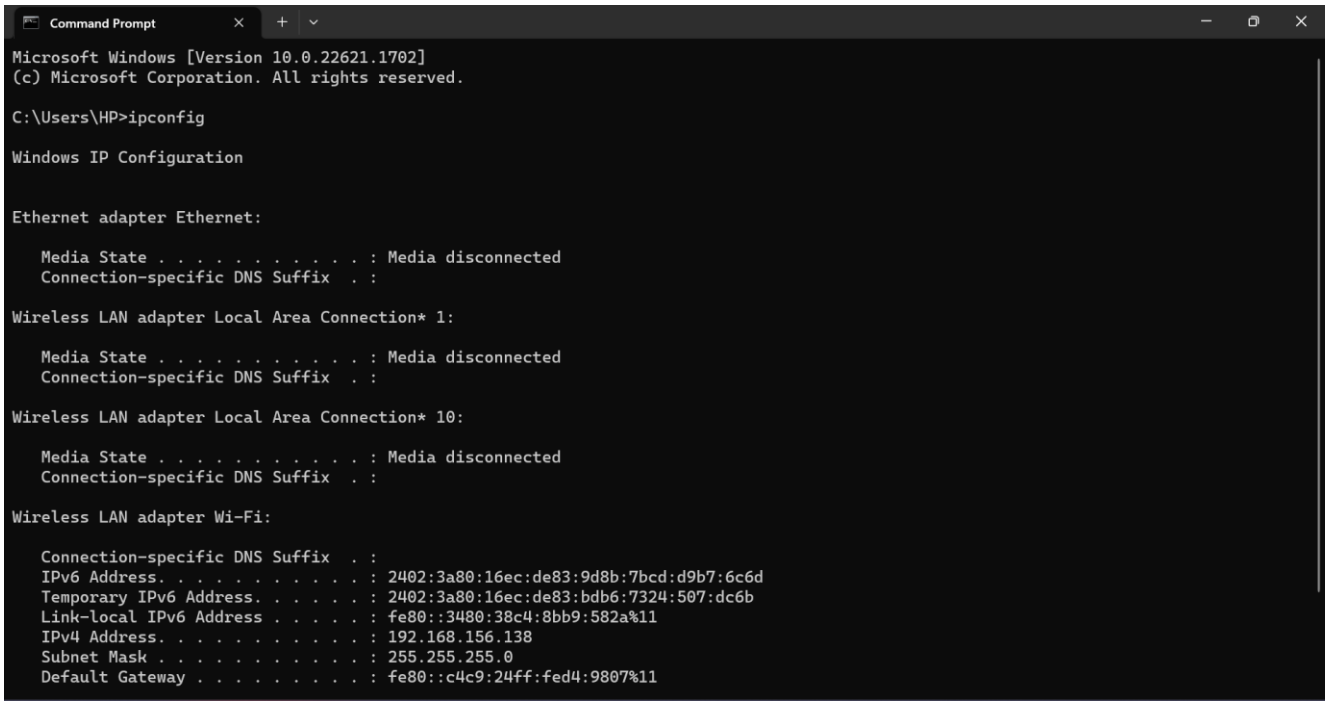
Description:

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.

No.	Option	Description
1	/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.
2	/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.
3	/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.

Date: 07/ 07 /2023

Implementation:



2. ping

Description:

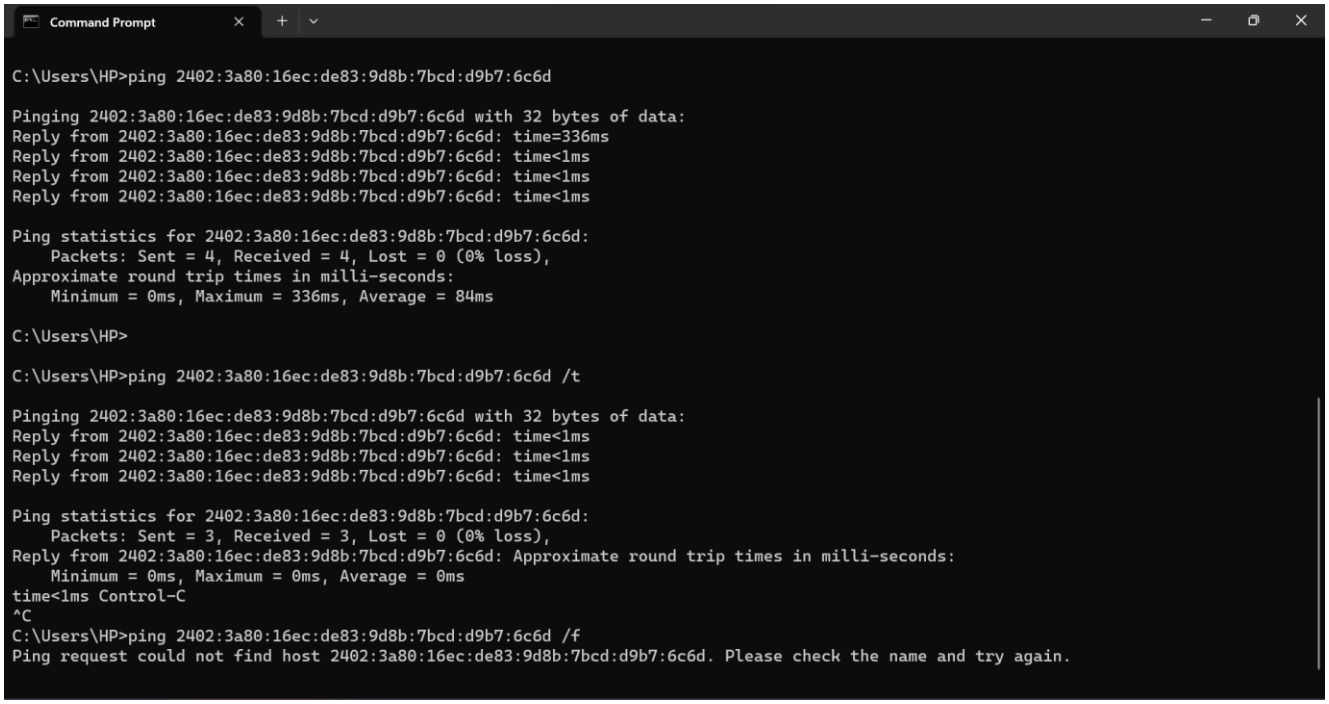
Verifies IP-level connectivity to another TCP/IP computer by sending Internet Control Message Protocol (ICMP) echo Request messages. The receipt of corresponding echo Reply messages are displayed, along with round-trip times. ping is the primary TCP/IP command used to troubleshoot connectivity, reachability, and name resolution. Used without parameters, this command displays Help content.

You can also use this command to test both the computer name and the IP address of the computer. If pinging the IP address is successful, but pinging the computer name isn't, you might have a name resolution problem. In this case, make sure the computer name you are specifying can be resolved through the local Hosts file, by using Domain Name System (DNS) queries, or through NetBIOS name resolution techniques.

No.	Option	Description
1	/t	Specifies ping continue sending echo Request messages to the destination until interrupted. To interrupt and display statistics, press CTRL+ENTER. To interrupt and quit this command, press CTRL+C.
2	/a	Specifies reverse name resolution be performed on the destination IP address. If this is successful, ping

		displays the corresponding host name.
3	/f	Specifies that echo Request messages are sent with the Do not Fragment flag in the IP header set to 1 (available on IPv4 only). The echo Request message can't be fragmented by routers in the path to the destination. This parameter is useful for troubleshooting path Maximum Transmission Unit (PMTU) problems.

Implementation:



3. getmac

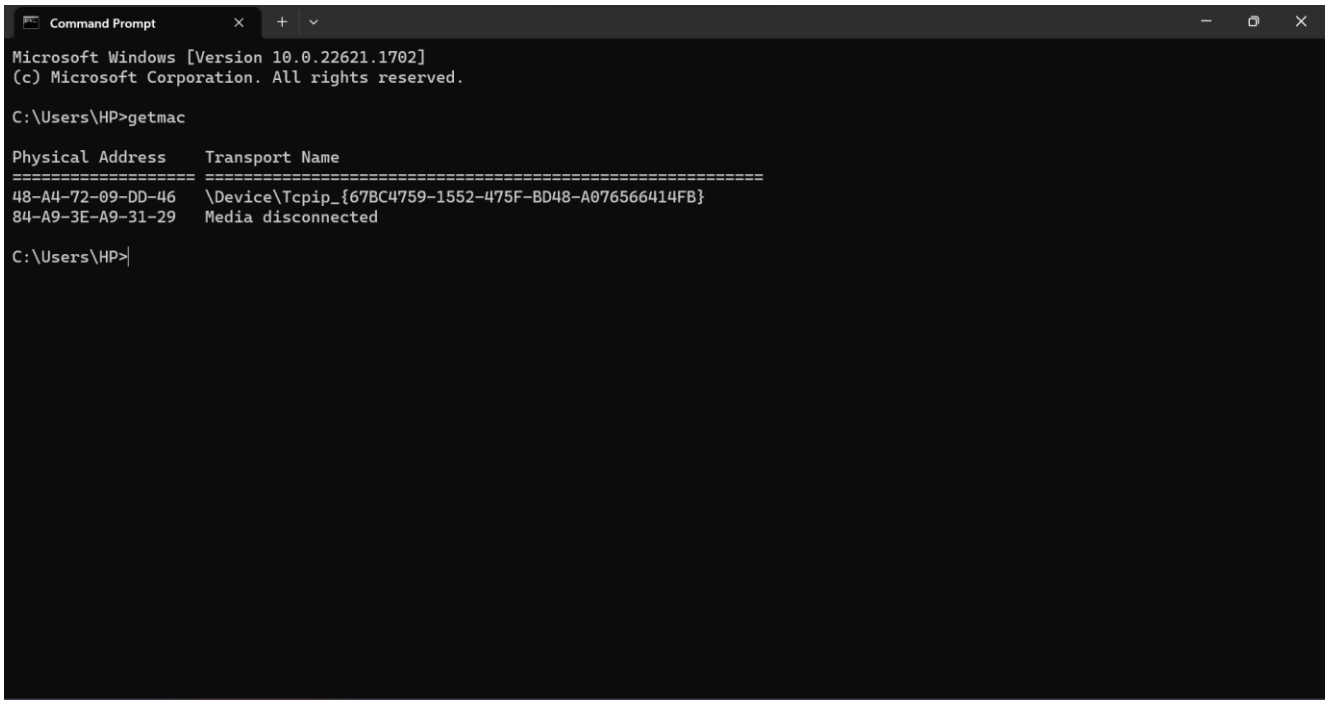
Description:

Returns the media access control (MAC) address and list of network protocols associated with each address for all network cards in each computer, either locally or across a network. This command is particularly useful either when you want to enter the MAC address into a network analyzer, or when you need to know what protocols are currently in use on each network adapter on a computer.

No.	Option	Description
1	/s <computer>	Specifies the name or IP address of a remote computer (do not use backslashes). The default is the local computer.
2	/u <domain>\<user>	Runs the command with the account permissions of the user specified by user or domain\user. The

		default is the permissions of the current logged on user on the computer issuing the command.
3	/v	Specifies that the output display verbose information.

Implementation:



4. Systeminfo

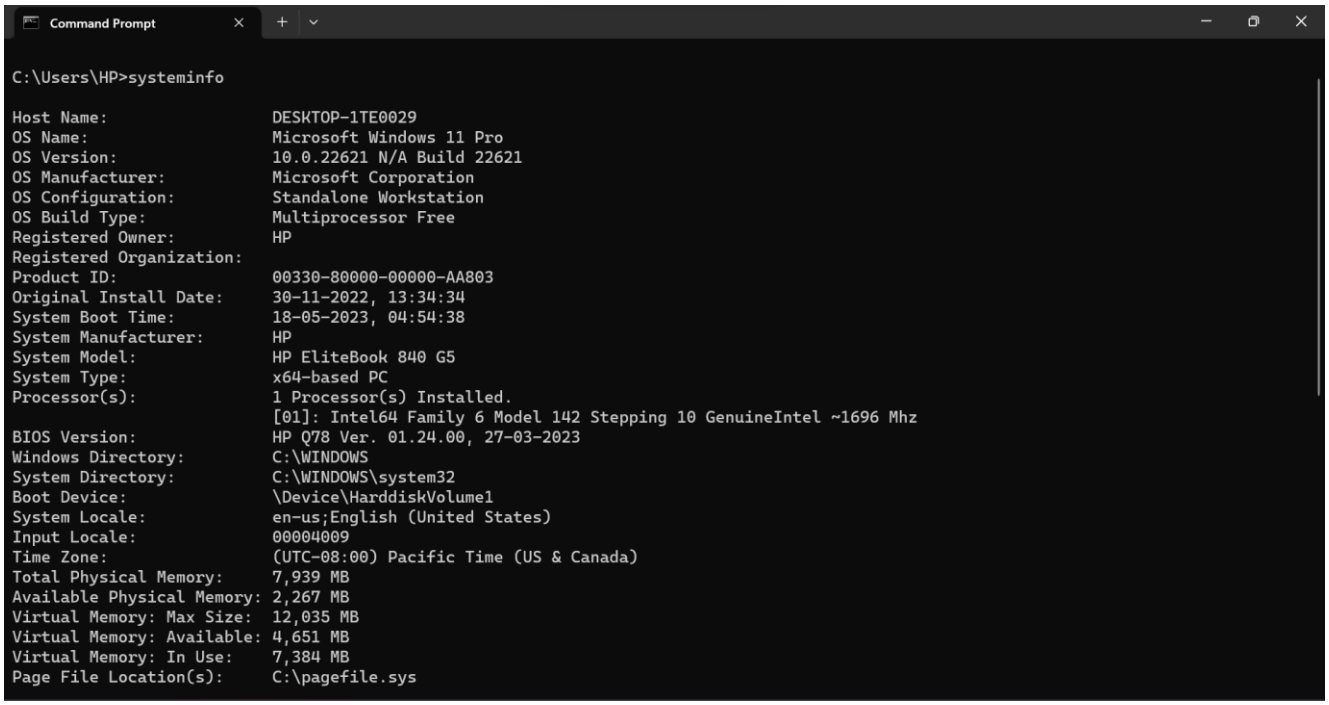
Description:

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	/s <computer>	Specifies the name or IP address of a remote computer (do not use backslashes). The default is the local computer.
2	/p <password>	Specifies the password of the user account that is specified in the /u parameter.
3	/nh	Suppresses column headers in the output. Valid when the /fo parameter is set to TABLE or CSV.

Date: 07/ 07 /2023

Implementation:



5. Traceroute/ tracert.

Description:

This diagnostic tool determines the path taken to a destination by sending Internet Control Message Protocol (ICMP) echo Request or ICMPv6 messages to the destination with incrementally increasing time to live (TTL) field values. Each router along the path is required to decrement the TTL in an IPpacket by at least 1 before forwarding it. Effectively, the TTL is a maximum link counter. When theTTL on a packet reaches 0, the router is expected to return an ICMP time Exceeded message to the source computer.

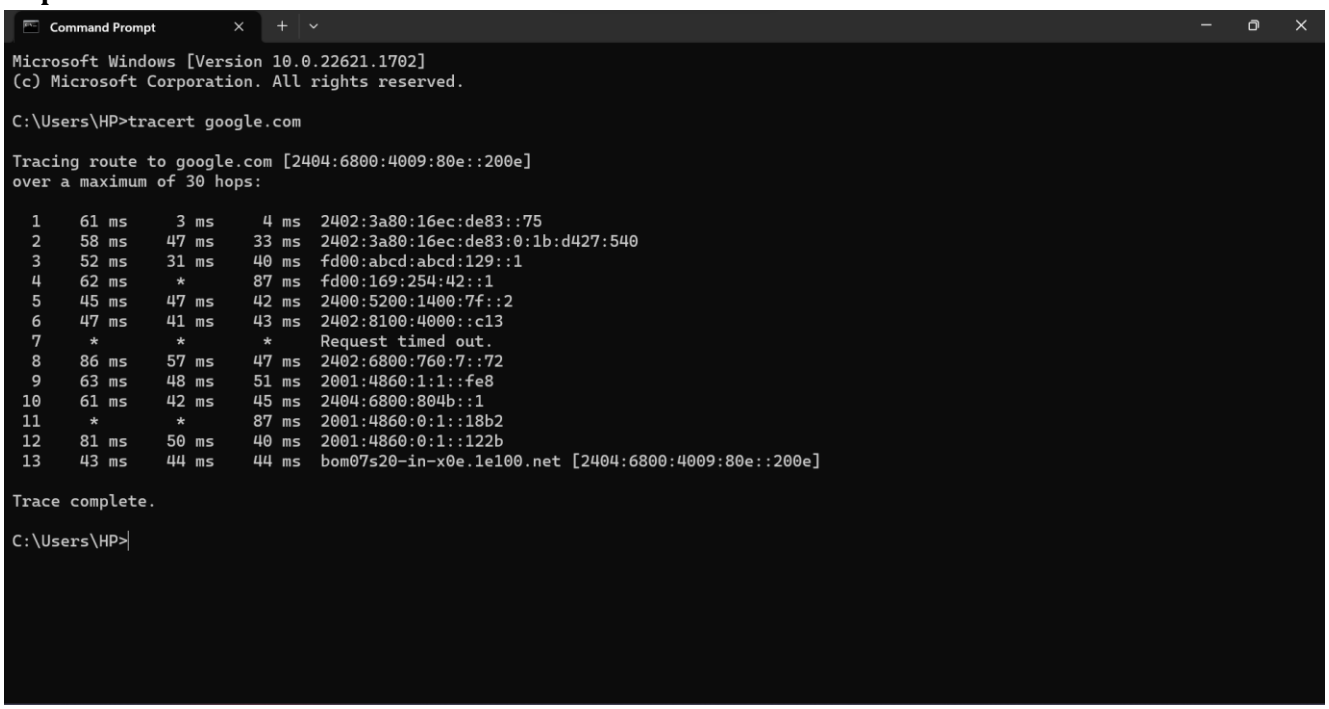
This command determines the path by sending the first echo Request message with a TTL of 1 and incrementing the TTL by 1 on each subsequent transmission until the target responds or the maximum number of hops is reached. The maximum number of hops is 30 by default and can be specified using the /h parameter.

The path is determined by examining the ICMP time Exceeded messages returned by intermediate routers and the echo Reply message returned by the destination. However, some routers do not return time Exceeded messages for packets with expired TTL values and are invisible to the tracert command. In this case, a row of asterisks (*) is displayed for that hop. The path displayed is the list of near/side router interfaces of the routers in the path between a source host and a destination. The near/side interface is the interface of the router that is closest to the sending host in the path.

Date: 07/ 07 /2023

No.	Option	Description
1	/d	Stops attempts to resolve the IP addresses of intermediate routers to their names. This can speed up the return of results.
2	/h <maximumhops>	Specifies the maximum number of hops in the path to search for the target (destination). The default is 30 hops.
3	/R	Specifies that the IPv6 Routing extension header be used to send an echo Request message to the local host, using the destination as an intermediate destination and testing the reverse route.

Implementation:



6. netstat

Description:

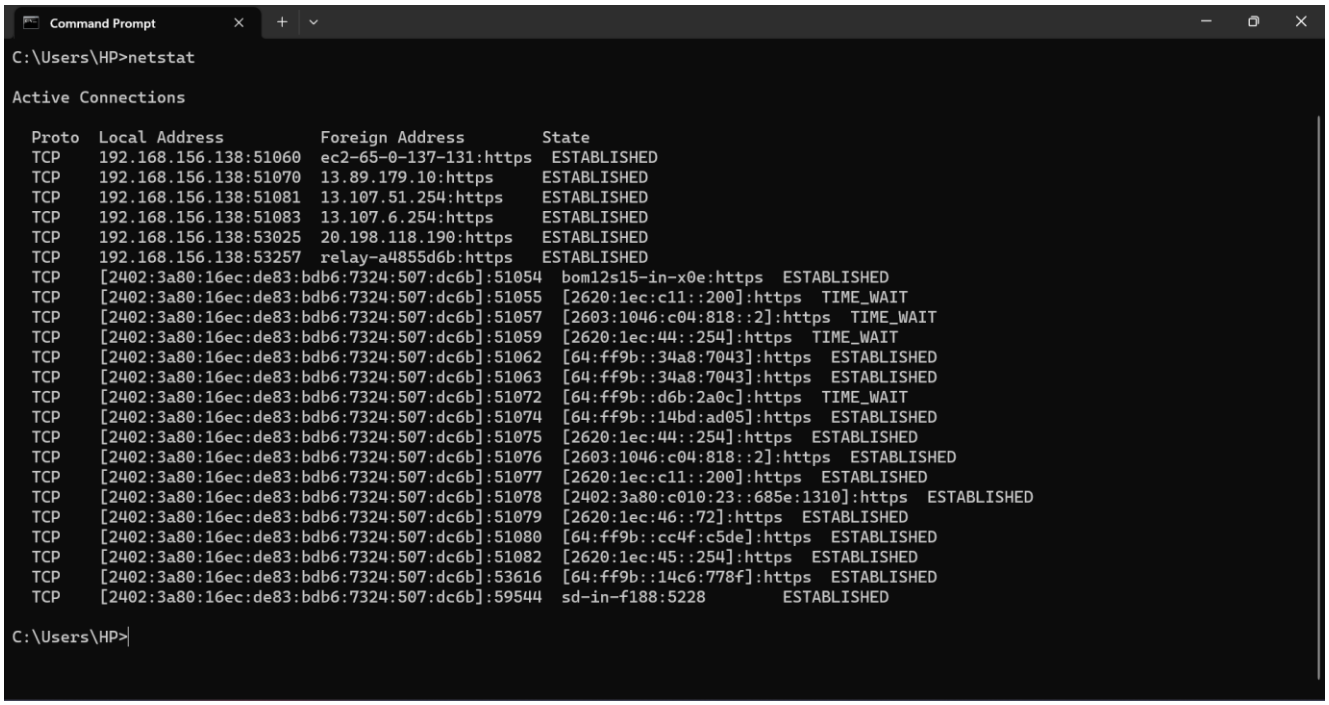
Displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols). Used without parameters, this command displays active TCP connections.

No.	Option	Description
1	-a	Displays all active TCP connections and the TCP and UDP ports on which the computer is listening.

Date: 07/ 07 /2023

2	-e	Displays Ethernet statistics, such as the number of bytes and packets sent and received. This parameter can be combined with -s.
3	-n	Displays active TCP connections, however, addresses and port numbers are expressed numerically and no attempt is made to determine names.

Implementation:



7. nslookup

Description:

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.

The nslookup command-line tool has two modes: interactive and noninteractive.

If you need to look up only a single piece of data, we recommend using the non-interactive mode. For the first parameter, type the name or IP address of the computer that you want to look up. For the second parameter, type the name or IP address of a DNS name server. If you omit the second argument, nslookup uses the default DNS name server.

If you need to look up more than one piece of data, you can use interactive mode. Type a hyphen (-) for the first parameter and the name or IP address of a DNS name server for the second parameter. If you omit both parameters, the tool uses the default DNS name server. While using the interactive mode, you can:

Date: 07/ 07 /2023

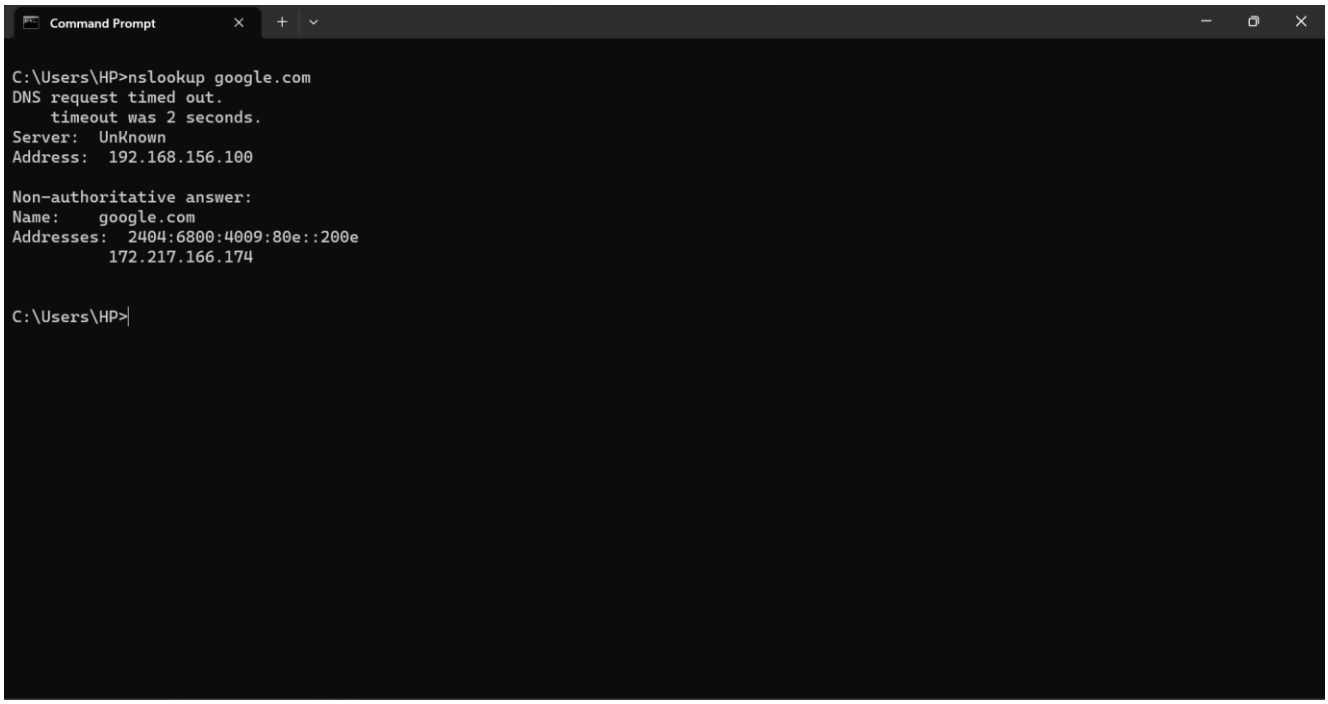
Interrupt interactive commands at any time, by pressing CTRL+B.

Exit, by typing exit.

Treat a built-in command as a computer name, by preceding it with the escape character (\). An unrecognized command is interpreted as a computer name.

No.	Option	Description
1	nslookup root	Changes the default server to the server for the root of the DNS domain name space.
2	nslookup set all	Prints the current values of the configuration settings.
3	nslookup set domain	Changes the default DNS domain name to the name specified.

Implementation:



Date: 07/ 07 /2023

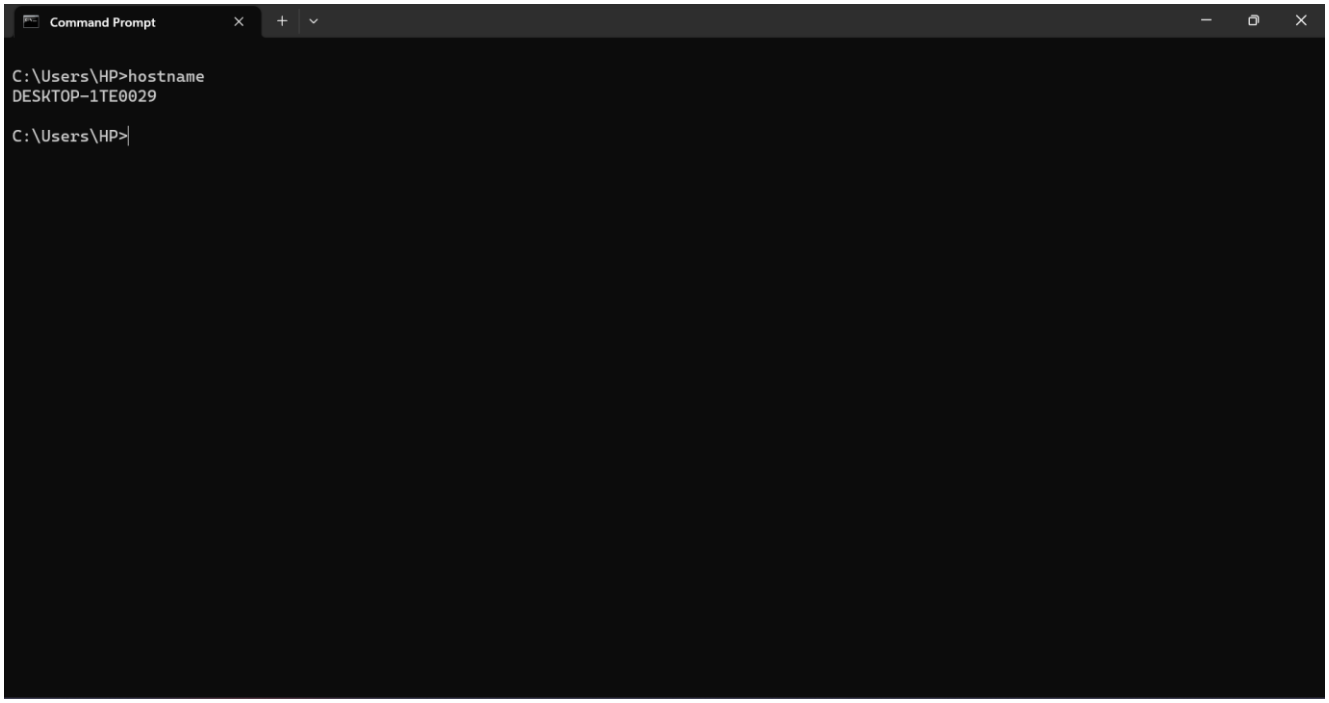
8. hostname

Description:

Displays the host name portion of the full computer name of the computer.

No.	Option	Description
1	/?	Displays help at the command prompt.

Implementation:



9. pathping

Description:

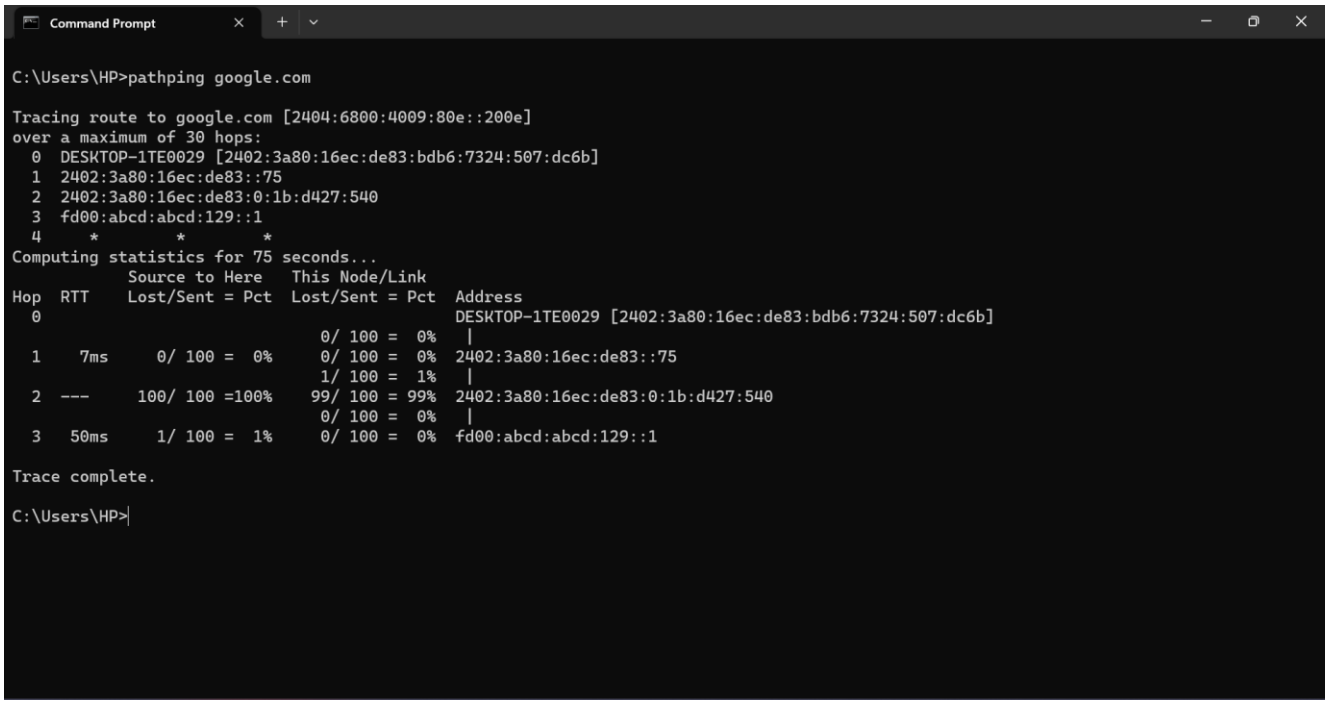
Provides information about network latency and network loss at intermediate hops between a source and destination. This command sends multiple echo Request messages to each router between a source and destination, over a period of time, and then computes results based on the packets returned from each 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	/q <numqueries>	Specifies the number of echo Request messages sent to each router in the path. The default is 100 queries.

Date: 07/ 07 /2023

2	/i <IPaddress>	Specifies the source address.
3	/w <timeout>	Specifies the number of milliseconds to wait for each reply. The default is 3000 milliseconds (3 seconds). This parameter sends multiple pings in parallel. Because of this, the amount of time specified in the timeout parameter isn't bounded by the amount of time specified in the period parameter for waiting between pings.

Implementation:



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	[/a [<inetaddr>] [/n <ifaceaddr>]	Displays current arp cache tables for all interfaces. The /n parameter is case-sensitive. To display the arp cache entry for a specific IP address, use arp /a with the inetaddr parameter, where inetaddr is an IP address. If inetaddr is not specified, the first applicable interface is used. To display the arp

Date: 07/ 07 /2023

		cache table for a specific interface, use the /n ifaceaddr parameter in conjunction with the /a parameter where inetaddr is the IP address assigned to the interface.
2	[/s <inetaddr> <etheraddr> [<ifaceaddr>]	Adds a static entry to the arp cache that resolves the IP address inetaddr to the physical address etheraddr. To add a static arp cache entry to the table for a specific interface, use the ifaceaddr parameter where ifaceaddr is an IP address assigned to the interface.
3	[/d <inetaddr> [<ifaceaddr>]	Deletes an entry with a specific IP address, where inetaddr is the IP address. To delete an entry in a table for a specific interface, use the ifaceaddr parameter where ifaceaddr is the IP address assigned to the interface. To delete all entries, use the asterisk (*) wildcard character in place of inetaddr.

Implementation: