Date: 28/6/2024

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

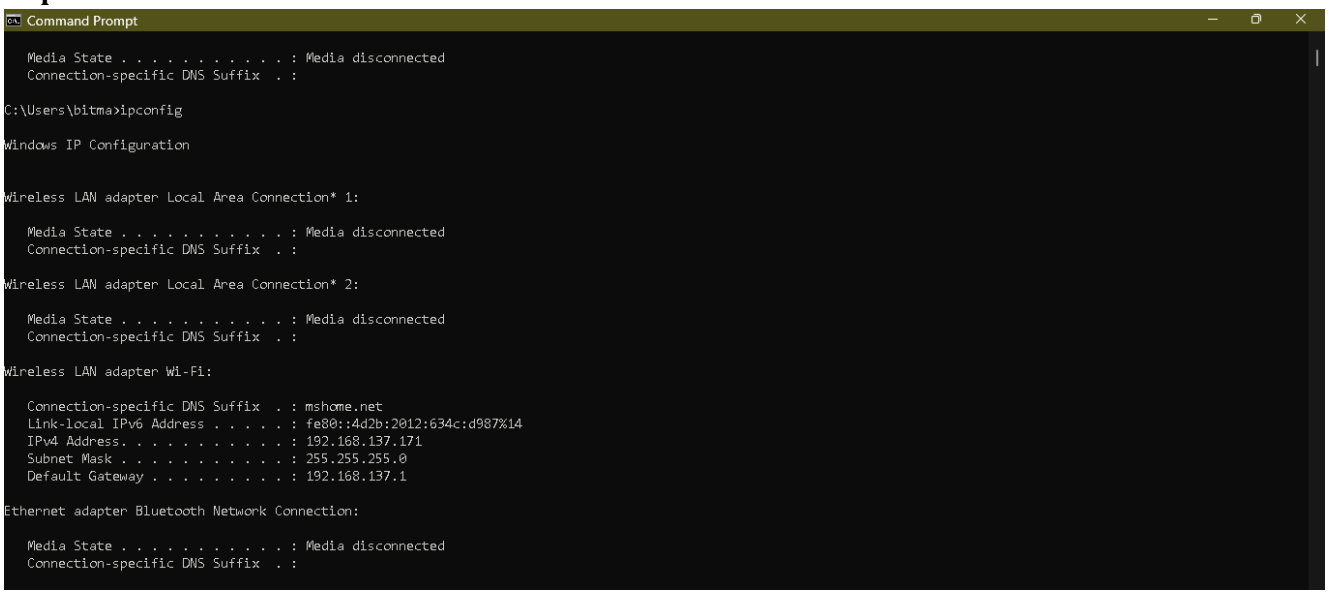
Description:

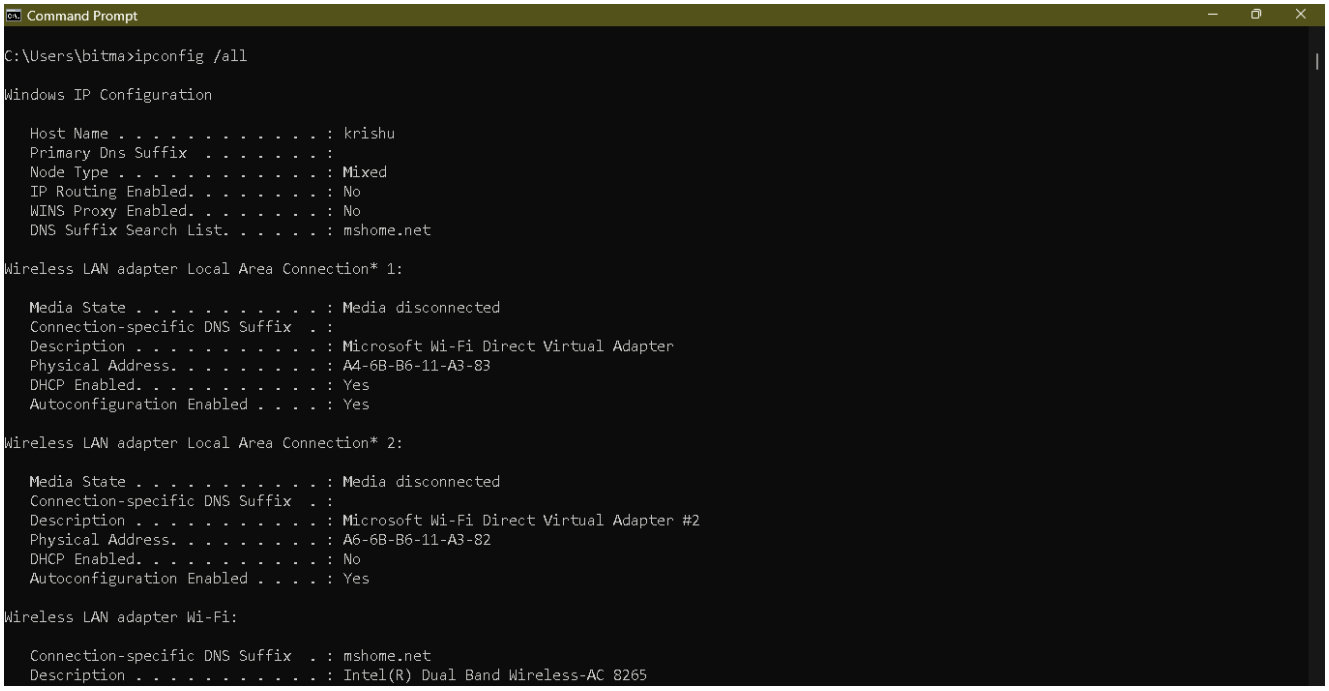
The ipconfig command in Windows is a useful tool for network troubleshooting and configuration. It displays the current configuration of the installed IP stack on a networked computer using TCP/IP. Displays the IP address, subnet mask, and default gateway for all network adapters.

No.	Option	Description
1	ipconfig /all	Shows detailed information about all network interfaces, including DNS and DHCP details.
2	ipconfig /release	Release the IPv4 address for the specified adapter.
3	ipconfig /release6	Release the IPv6 address for the specified adapter.
4	ipconfig /renew	Renew the IPv4 address for the specified adapter.
5	ipconfig /renew6	Renew the IPv6 address for the specified adapter.

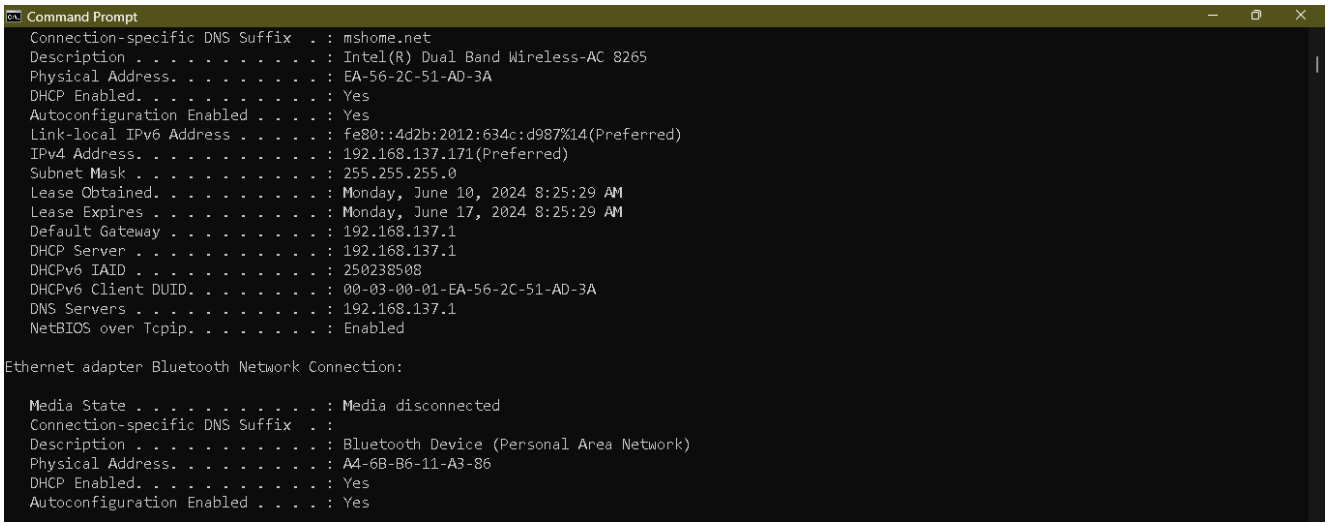
Date: 28/6/2024

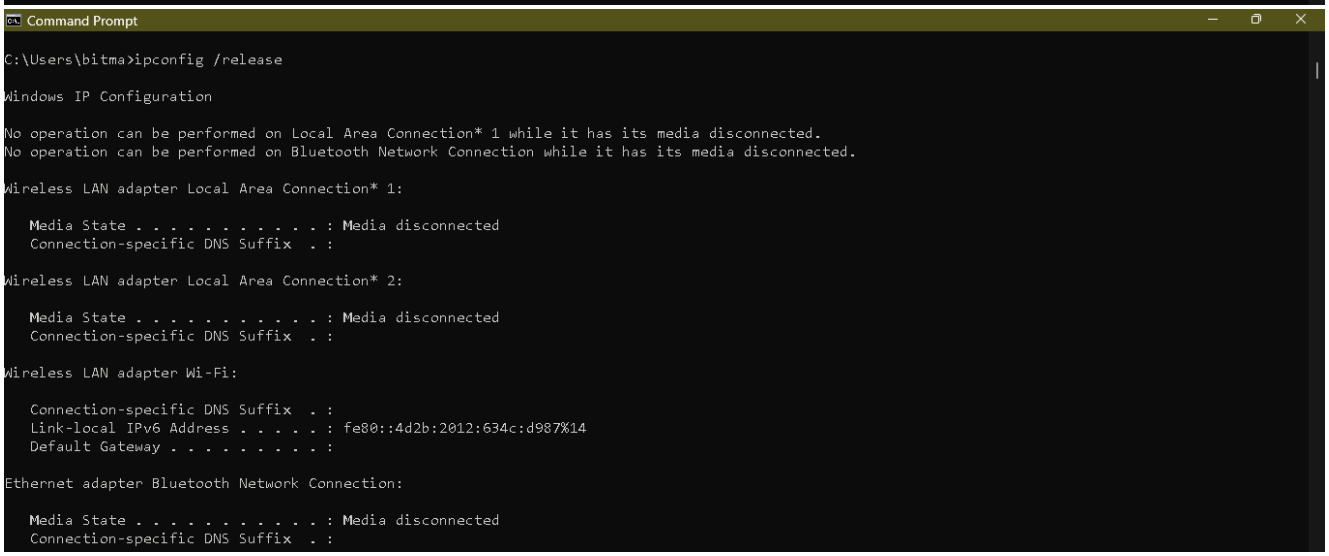
Implementation:

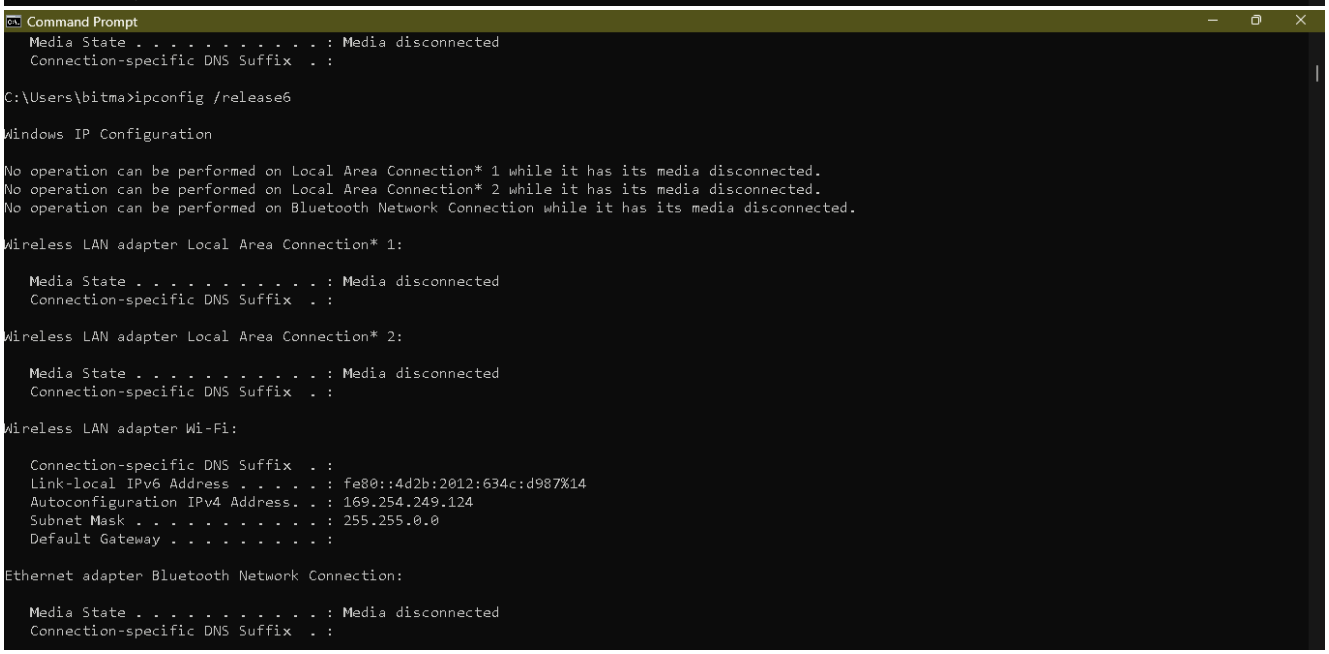




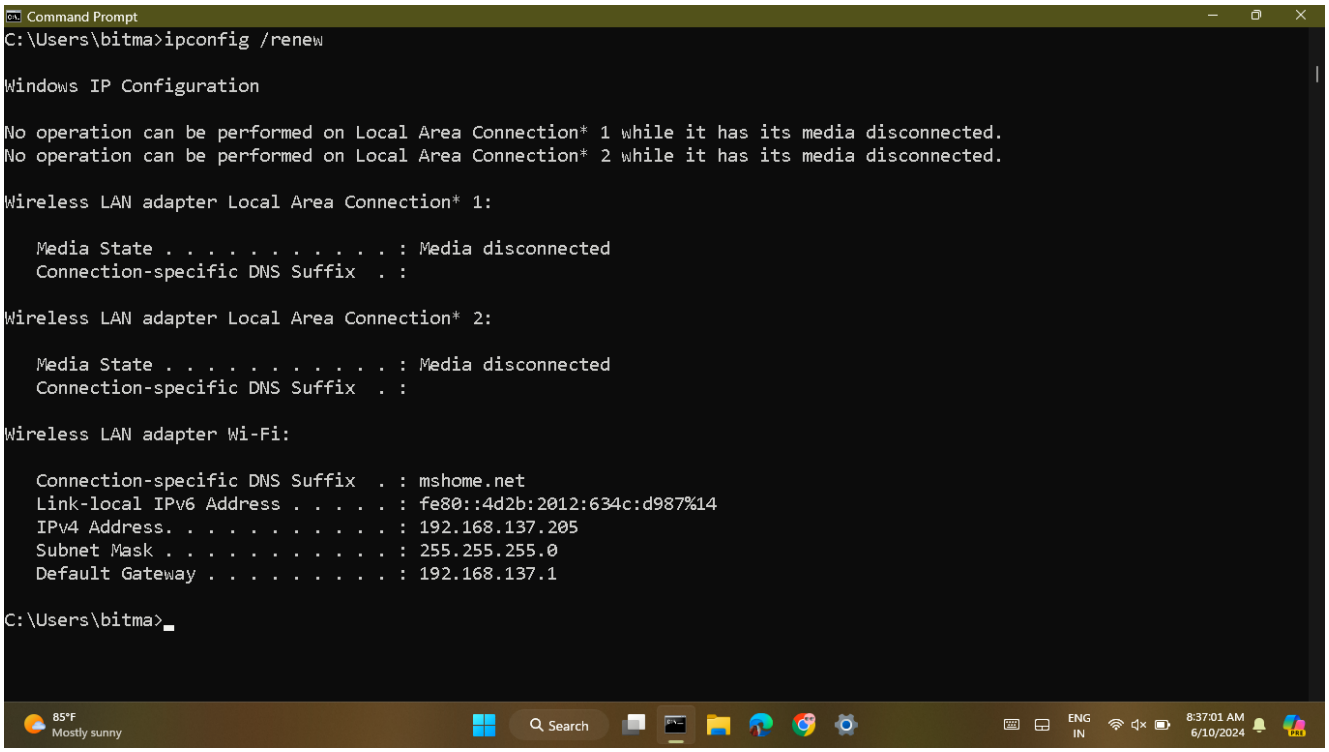
Date: 28/6/2024

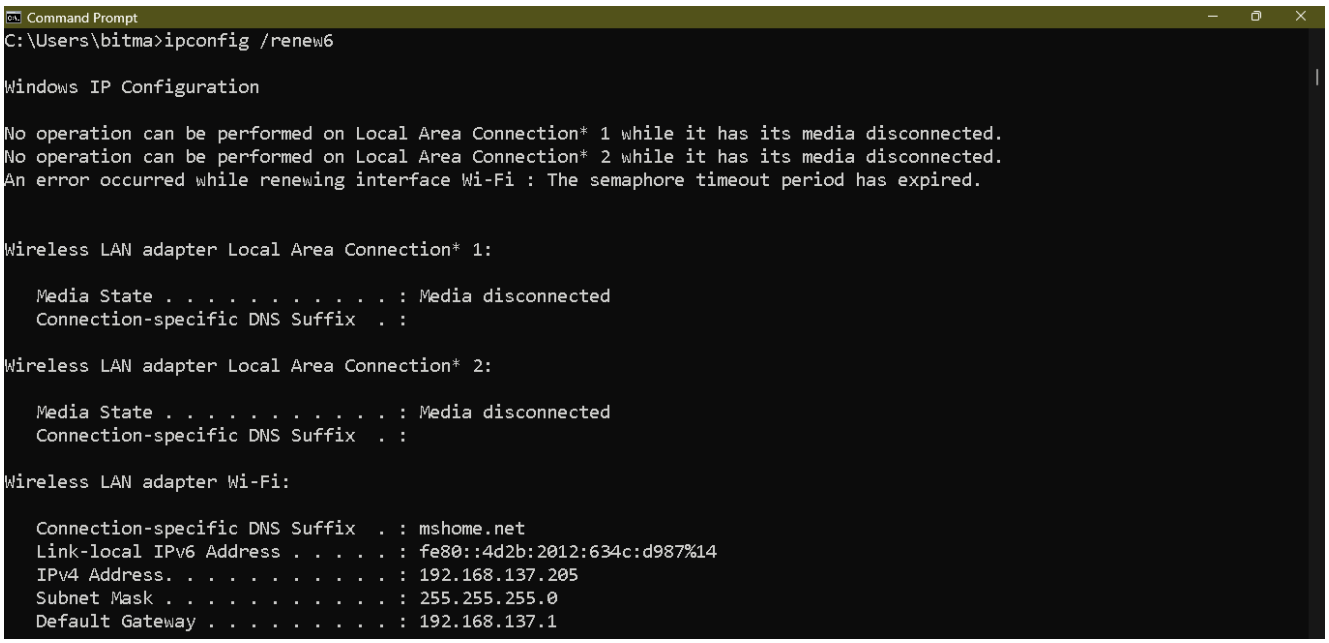






Date: 28/6/2024





2. ping

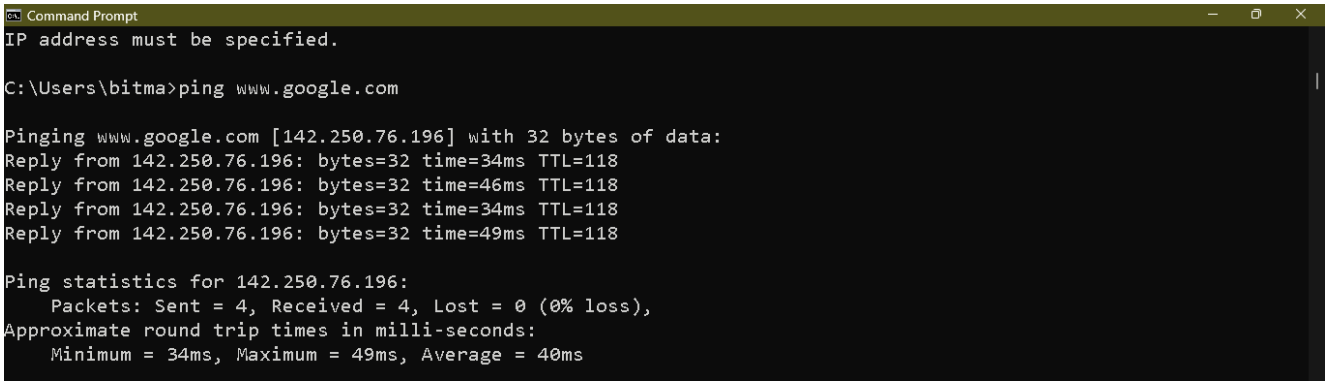
Description:

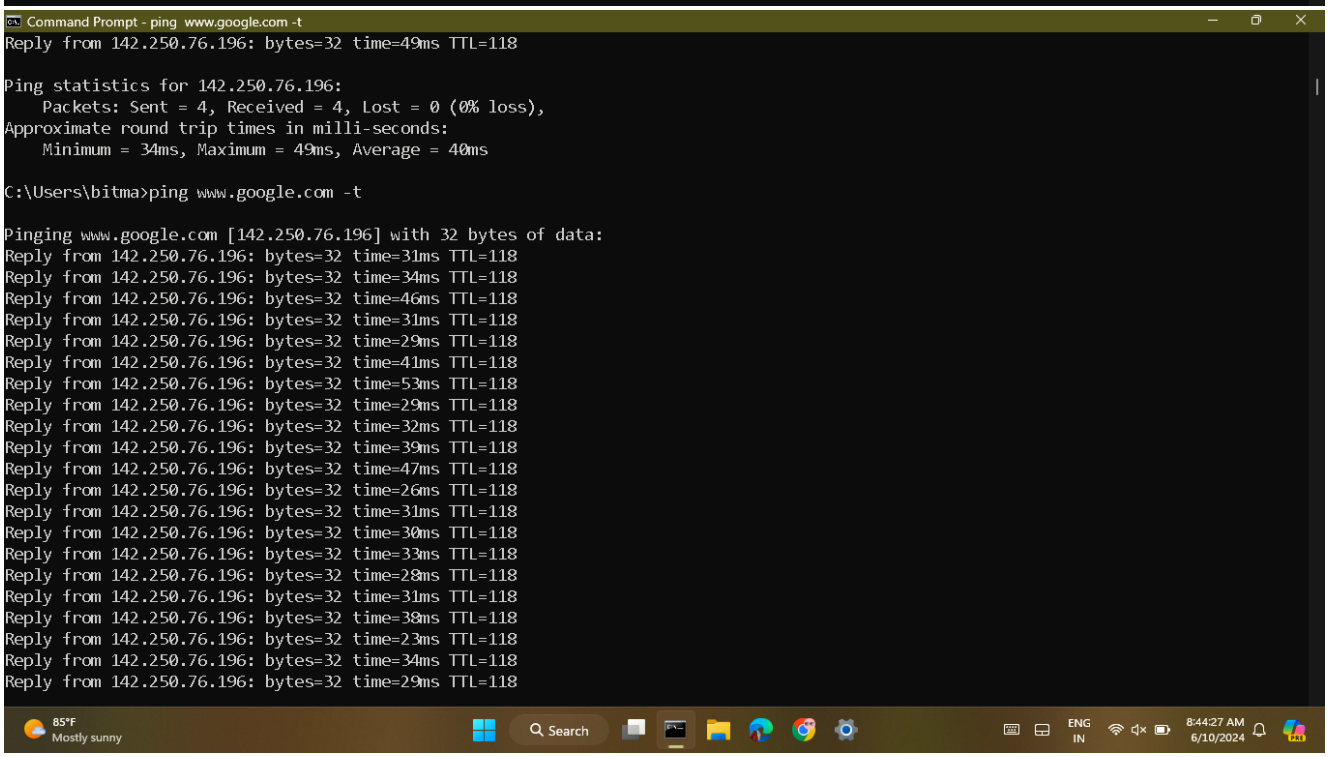
The ping command in Windows (and other operating systems) is used to test the reachability of a host on an IP network and to measure the round-trip time for messages sent from the originating host to a destination computer.

Date: 28/6/2024

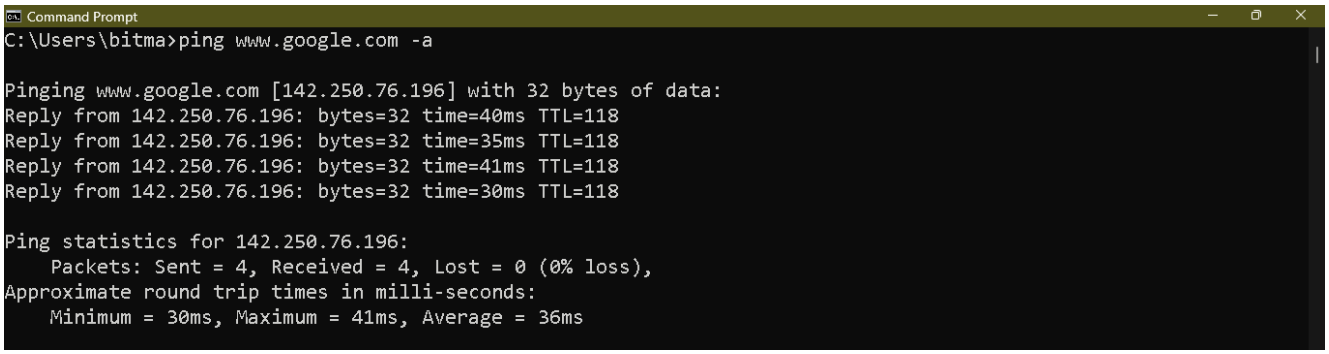
No.	Option	Description
1	ping -t [hostname or IP address]	Ping the specified host until stopped.To see statistics and continue - type Control-Break;
2	ping -n [count] [hostname or IP address]	Number of echo requests to send.
3	ping -l [size] [hostname or IP address]	Send buffer size.
4	ping -f	Set Don't Fragment flag in packet (IPv4-only).
5	ping -a	Resolve addresses to hostnames.

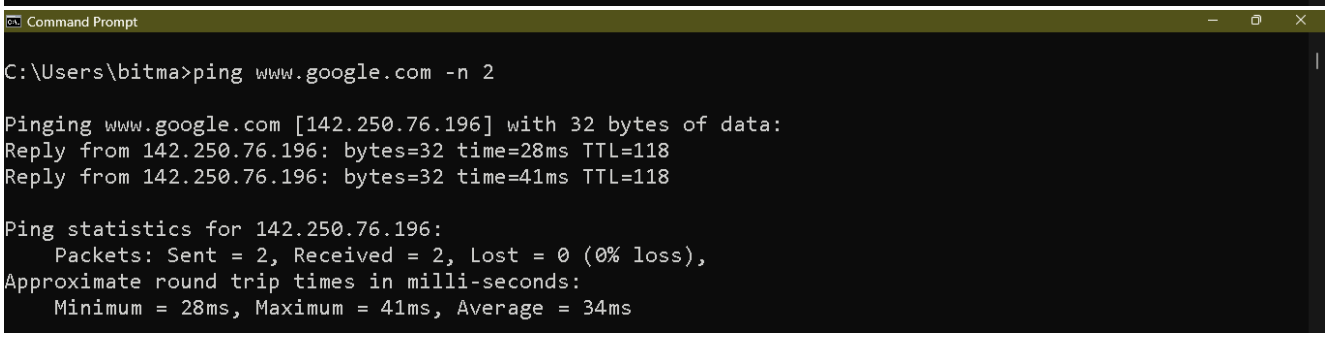
Implementation:

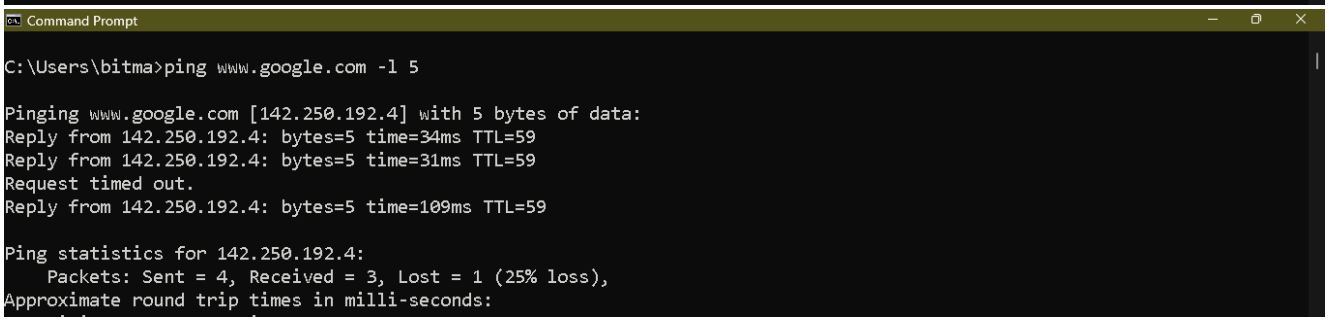


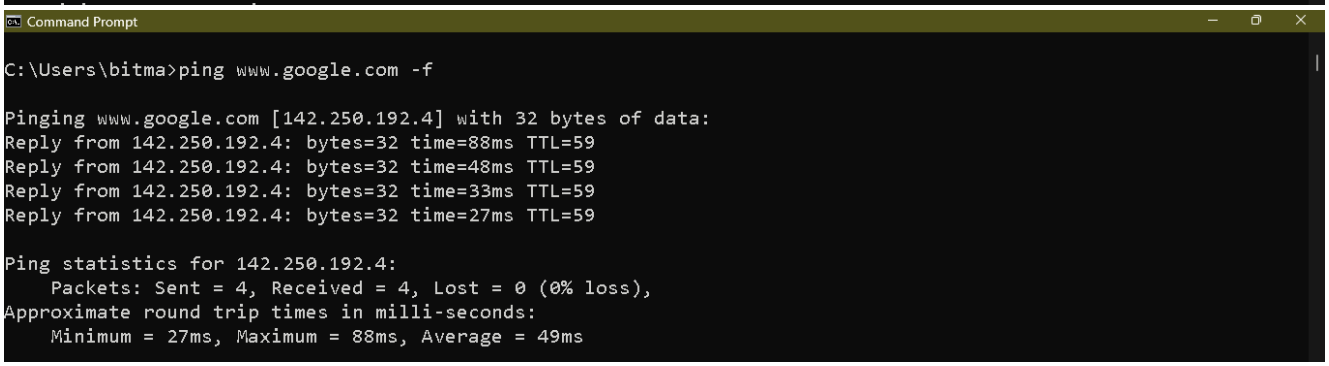


Date: 28/6/2024









3.getmac

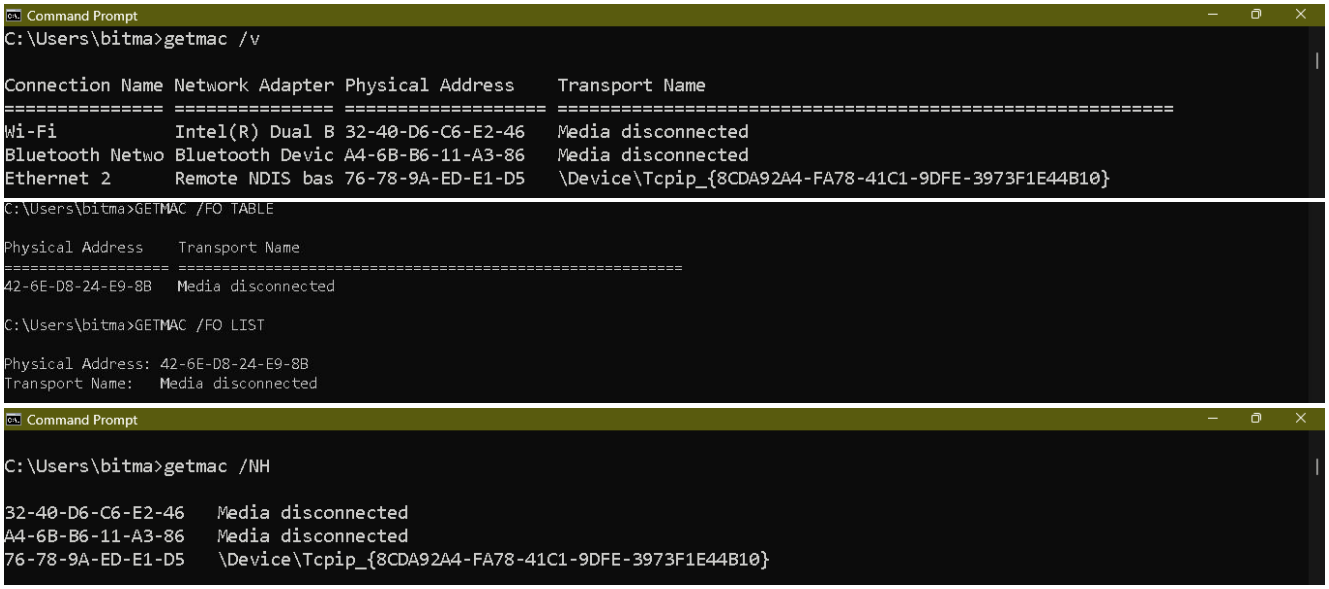
Description:

The getmac command in Windows is used to display the MAC addresses (Media Access Control addresses) for network adapters on a system. A MAC address is a unique identifier assigned to network interfaces for communications at the data link layer of a network segment. Displays the MAC addresses and associated network transport names for all network adapters on the system.

Date: 28/6/2024

No.	Option	Description
1	getmac /s	Specifies the remote system to connect to.
2	getmac /v	Specifies that verbose output is displayed.
3	getmac /fo [format]	Specifies the format in which the output is to be displayed. Valid values: "TABLE", "LIST", "CSV".
4	getmac /nh	Specifies that the "Column Header" should not be displayed in the output. Valid only for TABLE and CSV formats.
5	getmac/u [domain\]user	Specifies the user context under which the command should execute.

Implementation:



4.systeminfo

Description:

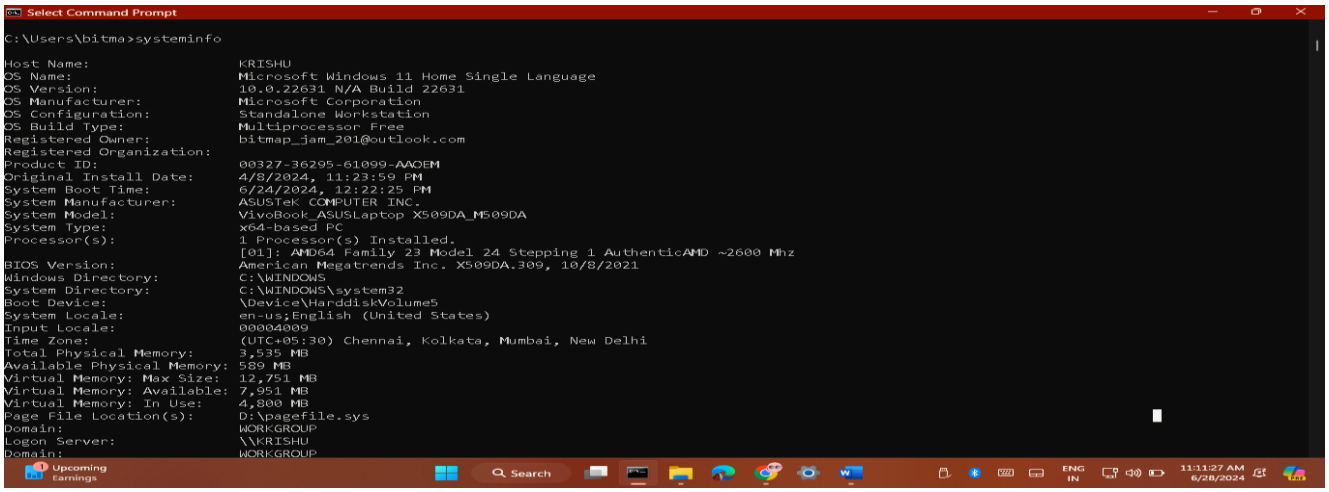
The systeminfo command in Windows provides detailed information about the system configuration, including the operating system version, hardware resources, and network settings. It's a powerful tool for gathering comprehensive details about a computer.

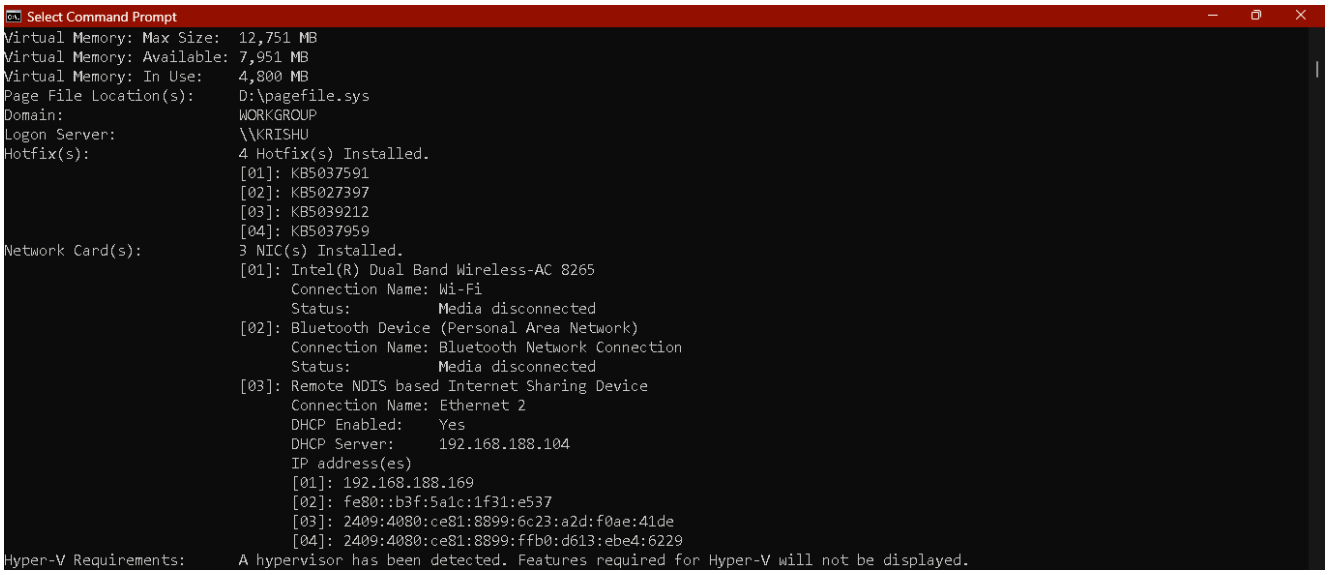
No.	Option	Description
1	systeminfo /s	Specifies the remote system to connect to.
2	systeminfo /u [domain\]user	Specifies the user context under which the command should execute.
3	systeminfo /fo [format]	Specifies the format in which the output is to be displayed. Valid values: "TABLE", "LIST", "CSV".
4	systeminfo /nh	Specifies that the "Column Header" should

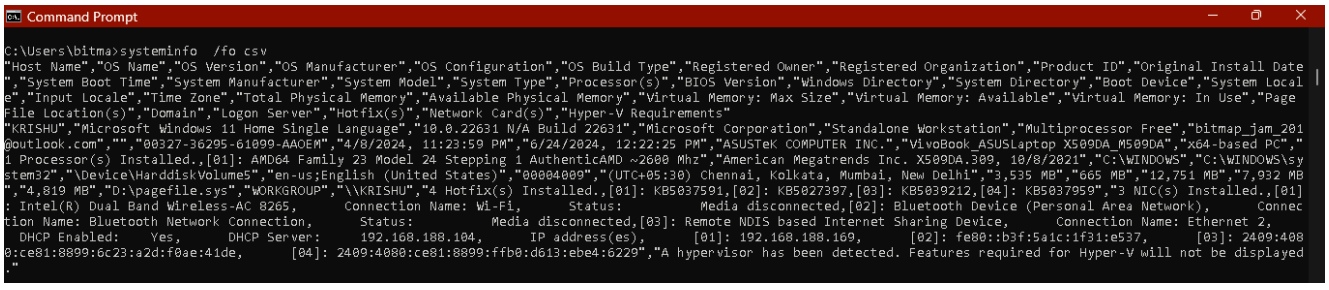
Date: 28/6/2024

		not be displayed in the output. Valid only for "TABLE" and "CSV" formats.
5	systeminfo /p [password]	Specifies the password for the given user context. Prompts for input if omitted.

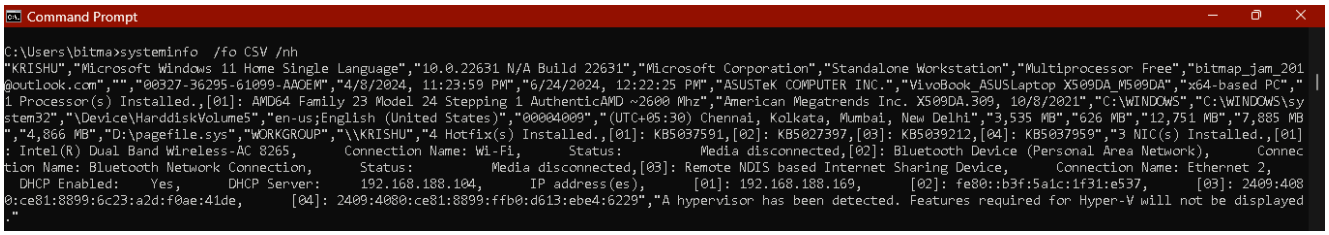
Implementation:







Date: 28/6/2024



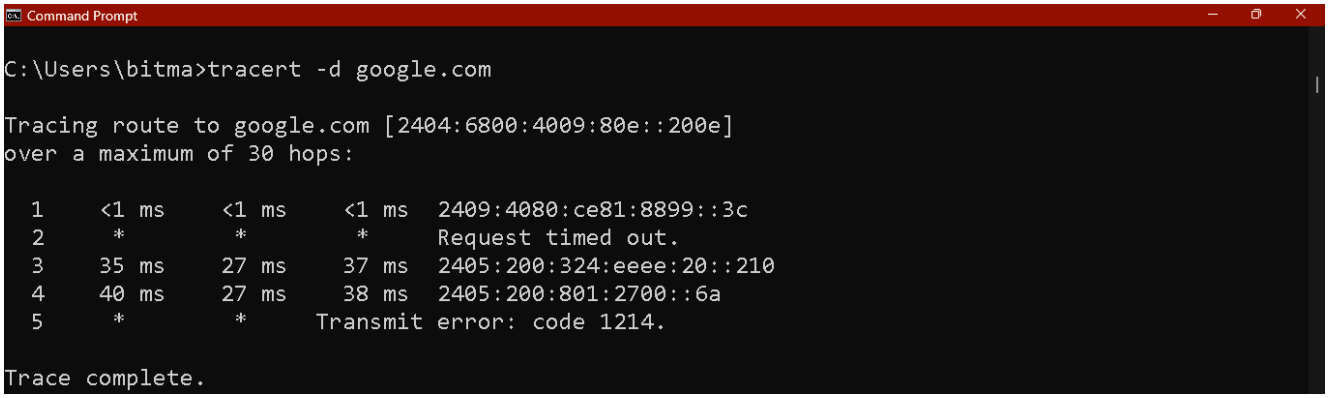
5. tracert/traceroute

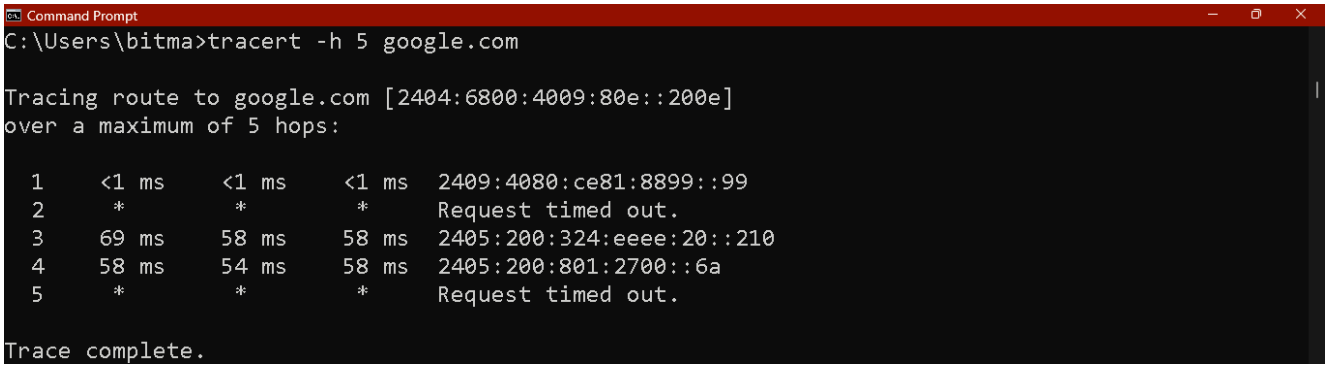
Description:

The traceroute (Linux/macOS) or `tracert` (Windows) command is a network diagnostic tool used to trace the path that data packets take from one computer to another over a network. It helps identify the route and measure transit delays of packets across an IP network.

No.	Option	Description
1	tracert -d [hostname or IP address]	Do not resolve addresses to hostnames.
2	tracert -h [maximum_hops] [hostname or IP address]	Maximum number of hops to search for target.
3	tracert -w [timeout] [hostname or IP address]	Wait timeout milliseconds for each reply.
4	Tracert -6	Force using IPv6.
5	Tracert -4	Force using IPv4.

Implementation:





Date: 28/6/2024

Command Prompt

```
C:\Users\bitma>tracert -w 1000 google.com

Tracing route to google.com [2404:6800:4009:82c::200e]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  2409:4080:ce81:8899::99
  2     *        *        *     Request timed out.
  3    40 ms    37 ms    37 ms  2405:200:324:eeee:20::210
  4    48 ms    46 ms    35 ms  2405:200:801:2700::6c
  5     *        *        *     Request timed out.
  6    73 ms    70 ms    79 ms  2405:200:801:200::31b
  7    65 ms    57 ms    53 ms  2001:4860:1:1::3c8
  8    69 ms    62 ms    58 ms  2404:6800:80eb::1
  9    70 ms    58 ms    57 ms  2001:4860:0:1::49e4
 10    66 ms    65 ms    59 ms  2001:4860:0:1::876a
 11    56 ms    62 ms    61 ms  2001:4860:0:1::3fe5
 12    54 ms    56 ms    60 ms  2001:4860:0:1::269d
 13    58 ms    57 ms    58 ms  bom07s35-in-x0e.1e100.net [2404:6800:4009:82c::200e]

Trace complete.
```

Command Prompt

```
C:\Users\bitma>tracert -4 google.com

Tracing route to google.com [142.250.66.14]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.188.104
  2     *        *        *     Request timed out.
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.
  5    44 ms    41 ms    48 ms  172.17.185.2
  6    38 ms    37 ms    56 ms  192.168.168.10
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9    61 ms    64 ms    59 ms  173.194.121.8
 10    72 ms   147 ms   161 ms  192.178.111.159
 11    62 ms    65 ms    57 ms  72.14.236.219
 12    67 ms    66 ms    70 ms  bom07s35-in-f14.1e100.net [142.250.66.14]

Trace complete.
```

Command Prompt

```
C:\Users\bitma>tracert -6 google.com

Tracing route to google.com [2404:6800:4009:82f::200e]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  2409:4080:ce81:8899::99
  2     *        *        *     Request timed out.
  3    50 ms    37 ms    40 ms  2405:200:324:eeee:20::210
  4    48 ms    37 ms    43 ms  2405:200:801:2700::6c
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7    80 ms    57 ms    66 ms  2405:200:802:760::8
  8    71 ms    57 ms    69 ms  2405:200:802:760::8
  9     *        *        *     Request timed out.
 10    75 ms    77 ms    78 ms  2001:4860:1:1::a14
 11    73 ms    65 ms    57 ms  2404:6800:8113::1
 12    74 ms   132 ms    77 ms  2001:4860:0:1::fb4
 13   105 ms    72 ms    77 ms  2001:4860:0:1::443
 14    67 ms    71 ms    65 ms  bom12s19-in-x0e.1e100.net [2404:6800:4009:82f::200e]

Trace complete.
```

Date: 28/6/2024

6.netstat

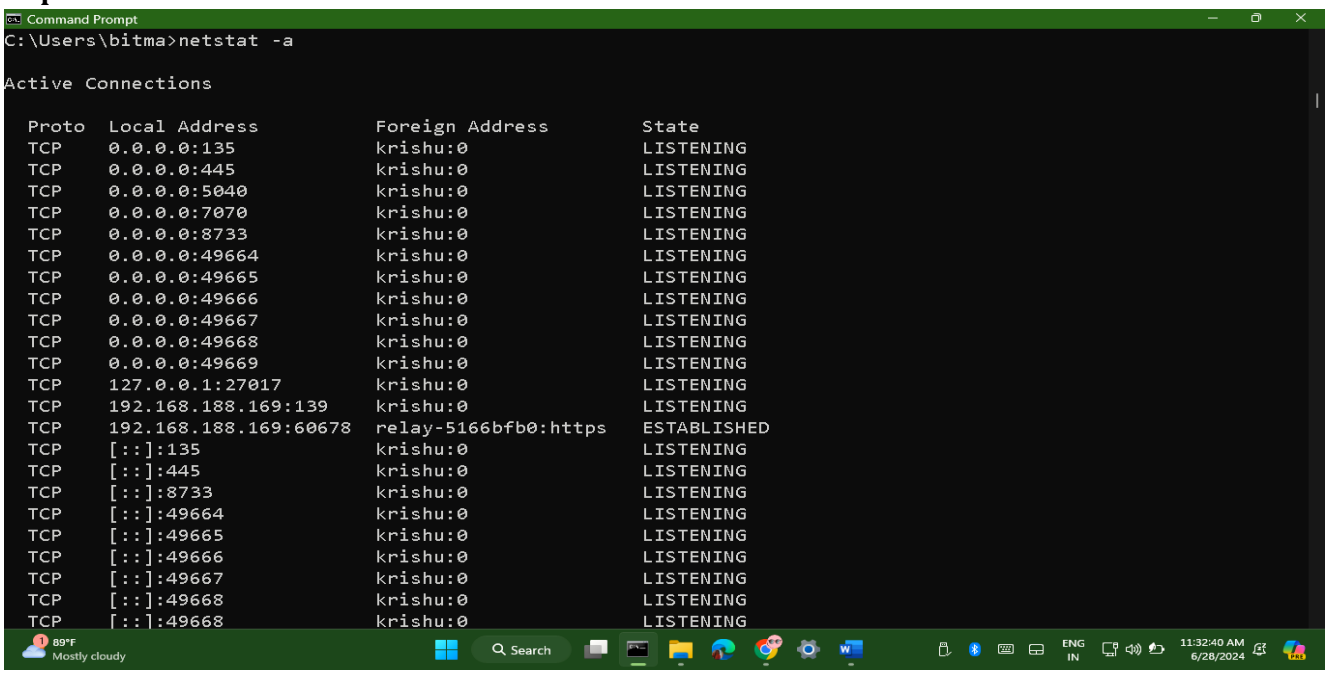
Description:

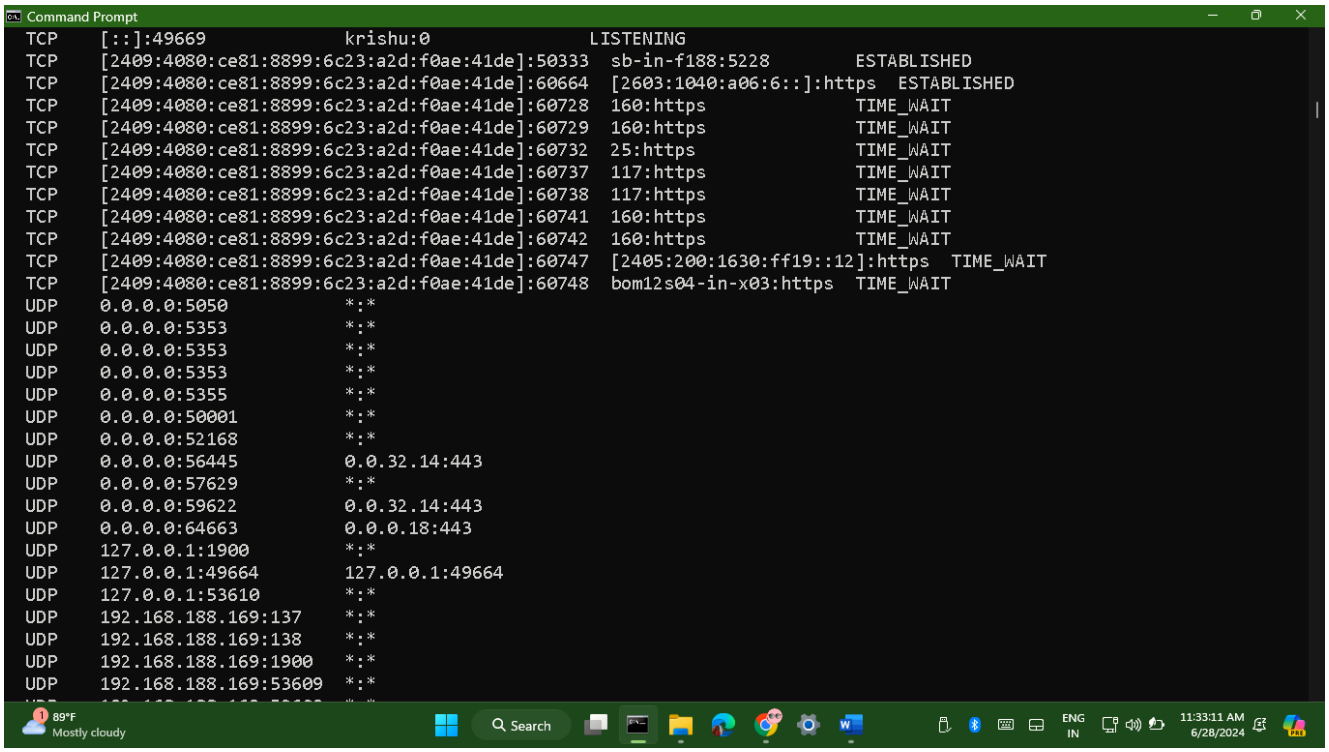
The netstat command in Windows, Linux, and macOS is a network utility that provides information about network connections, routing tables, interface statistics, masquerade connections, and multicast memberships. It is useful for network troubleshooting and performance measurement. Displays a list of active connections and listening ports.

No.	Option	Description
1	Netstat -a	Displays all connections and listening ports.
2	netstat -x	Displays NetworkDirect connections, listeners, and shared endpoints.
3	netstat -t	Displays the current connection offload state.
4	netstat -s	Displays per-protocol statistics. By default, statistics are shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6; the -p option may be used to specify a subset of the default002E
5	netstat -r	Displays the routing table.

Date: 28/6/2024

Implementation:





Date: 28/6/2024

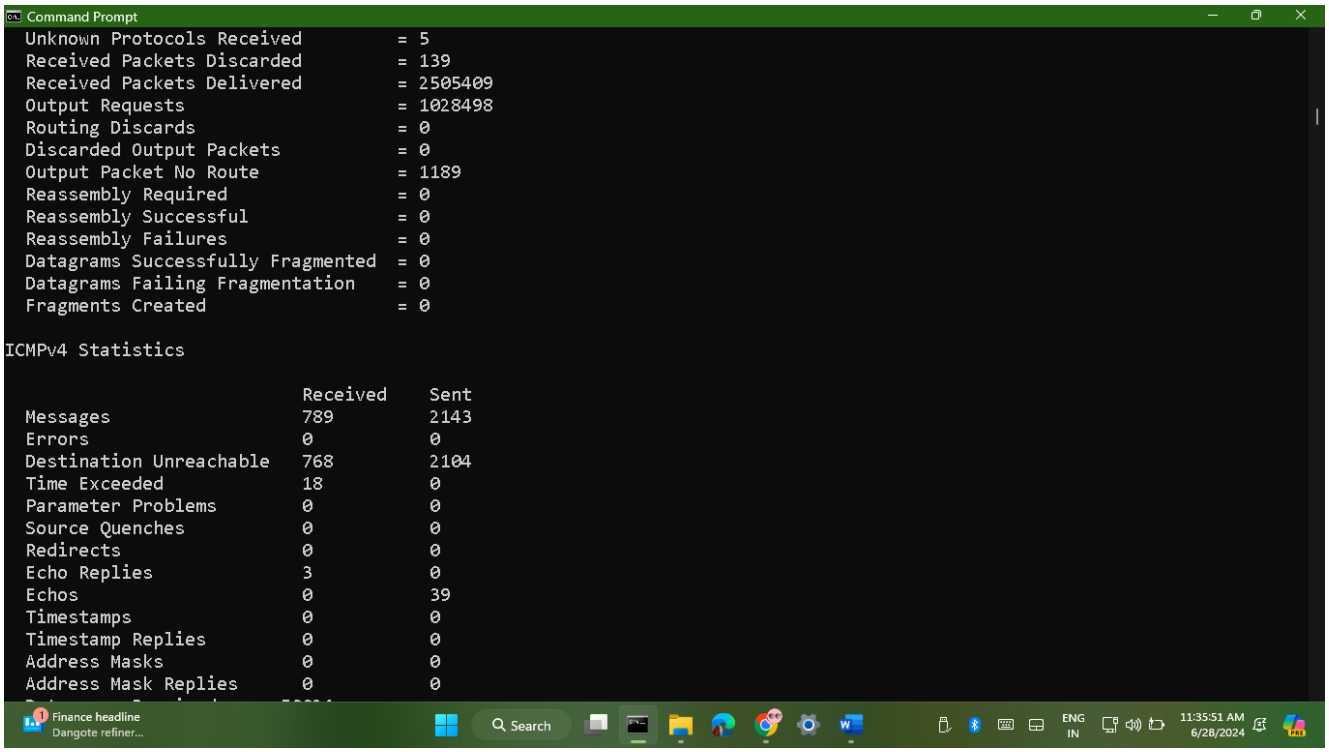
```
Command Prompt
  UDP    0.0.0.0:52168          *:*
  UDP    0.0.0.0:56445          0.0.32.14:443
  UDP    0.0.0.0:57629          *:*
  UDP    0.0.0.0:59622          0.0.32.14:443
  UDP    0.0.0.0:64663          0.0.0.18:443
  UDP    127.0.0.1:1900         *:*
  UDP    127.0.0.1:49664        127.0.0.1:49664
  UDP    127.0.0.1:53610        *:*
  UDP    192.168.188.169:137    *:*
  UDP    192.168.188.169:138    *:*
  UDP    192.168.188.169:1900   *:*
  UDP    192.168.188.169:53609  *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5355              *:*
  UDP    [::]:52168             *:*
  UDP    [::]:56445             [2404:6800:4009:81f::200e]:443
  UDP    [::]:57629             *:*
  UDP    [::]:59622             [2404:6800:4009:81e::200e]:443
  UDP    [::]:64663             [2405:200:1630:ff19::12]:443
  UDP    [::1]:1900             *:*
  UDP    [::1]:53608            *:*
  UDP    [fe80::b3f:5a1c:1f31:e537%15]:1900  *:*
  UDP    [fe80::b3f:5a1c:1f31:e537%15]:53607  *:*
```

```
Command Prompt
C:\Users\bitma>netstat -x

Active NetworkDirect Connections, Listeners, SharedEndpoints

  Mode   IfIndex Type           Local Address          Foreign Address        PID
```

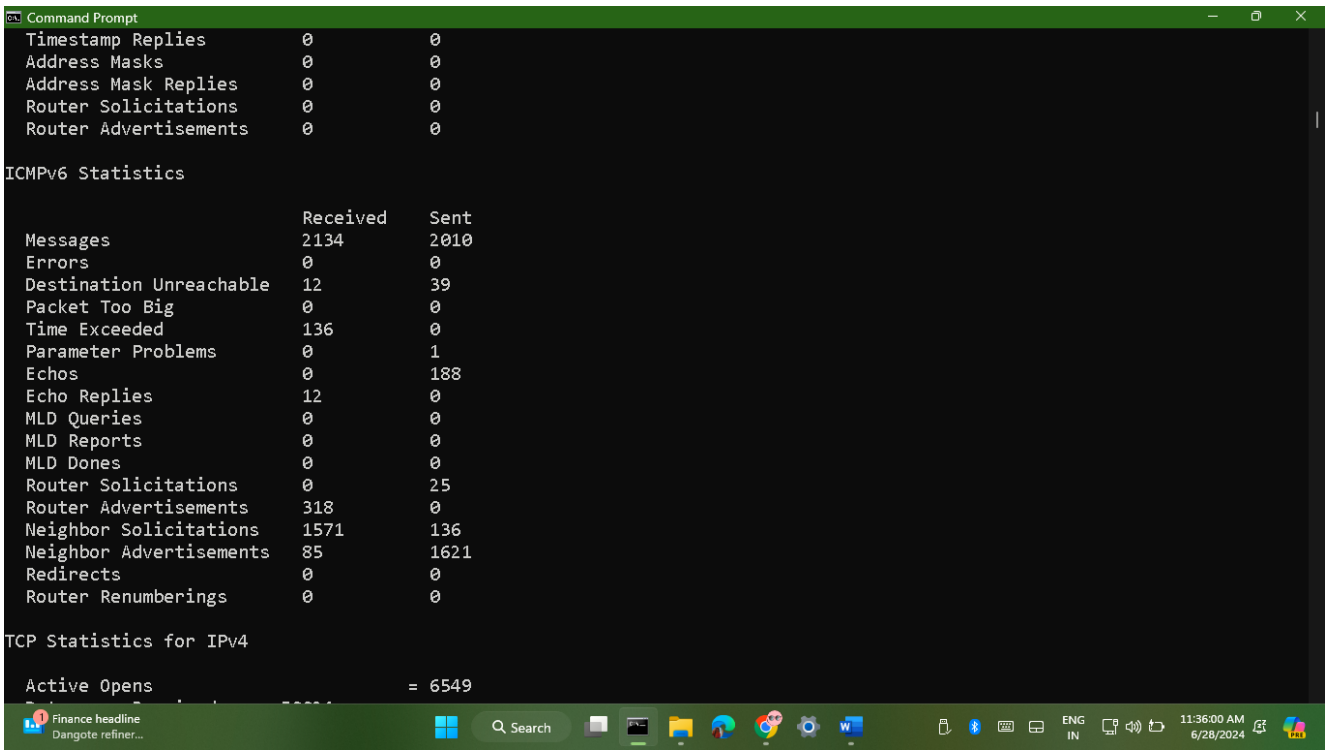
```
Command Prompt
C:\Users\bitma>netstat -t

Active Connections

  Proto  Local Address          Foreign Address        State           Offload State

  TCP    192.168.188.169:60678  relay-5166bfb0:https   ESTABLISHED     InHost
  TCP    [2409:4080:ce81:8899:6c23:a2d:f0ae:41de]:50333  sb-in-f188:5228        ESTABLISHED     InHost
  TCP    [2409:4080:ce81:8899:6c23:a2d:f0ae:41de]:60664  [2603:1040:a06:6::]:https  ESTABLISHED     InHost
  TCP    [2409:4080:ce81:8899:6c23:a2d:f0ae:41de]:60760  [64:ff9b::348c:761c]:https  TIME_WAIT       InHost
  TCP    [2409:4080:ce81:8899:6c23:a2d:f0ae:41de]:60765  [2603:1046:1406::5]:https  TIME_WAIT       InHost
  TCP    [2409:4080:ce81:8899:6c23:a2d:f0ae:41de]:60769  [2620:1ec:bdf::72]:https  TIME_WAIT       InHost
  TCP    [2409:4080:ce81:8899:6c23:a2d:f0ae:41de]:60771  [2603:1046:1400::1]:https  ESTABLISHED     InHost
  TCP    [2409:4080:ce81:8899:6c23:a2d:f0ae:41de]:60775  os-in-x5e:https        TIME_WAIT       InHost
  TCP    [2409:4080:ce81:8899:6c23:a2d:f0ae:41de]:60777  [64:ff9b::312c:8ce3]:https  ESTABLISHED     InHost
```

```
Command Prompt
C:\Users\bitma>netstat -s

IPv4 Statistics

  Packets Received                   = 522761
  Received Header Errors             = 6
  Received Address Errors            = 1
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 0
  Received Packets Discarded         = 4896
  Received Packets Delivered         = 628184
  Output Requests                    = 502610
  Routing Discards                   = 0
  Discarded Output Packets           = 24
  Output Packet No Route             = 251
  Reassembly Required                = 0
  Reassembly Successful              = 0
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 0
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 0

IPv6 Statistics

  Packets Received                   = 2501240
  Received Header Errors             = 0
  Received Address Errors            = 10
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 5
```

Date: 28/6/2024

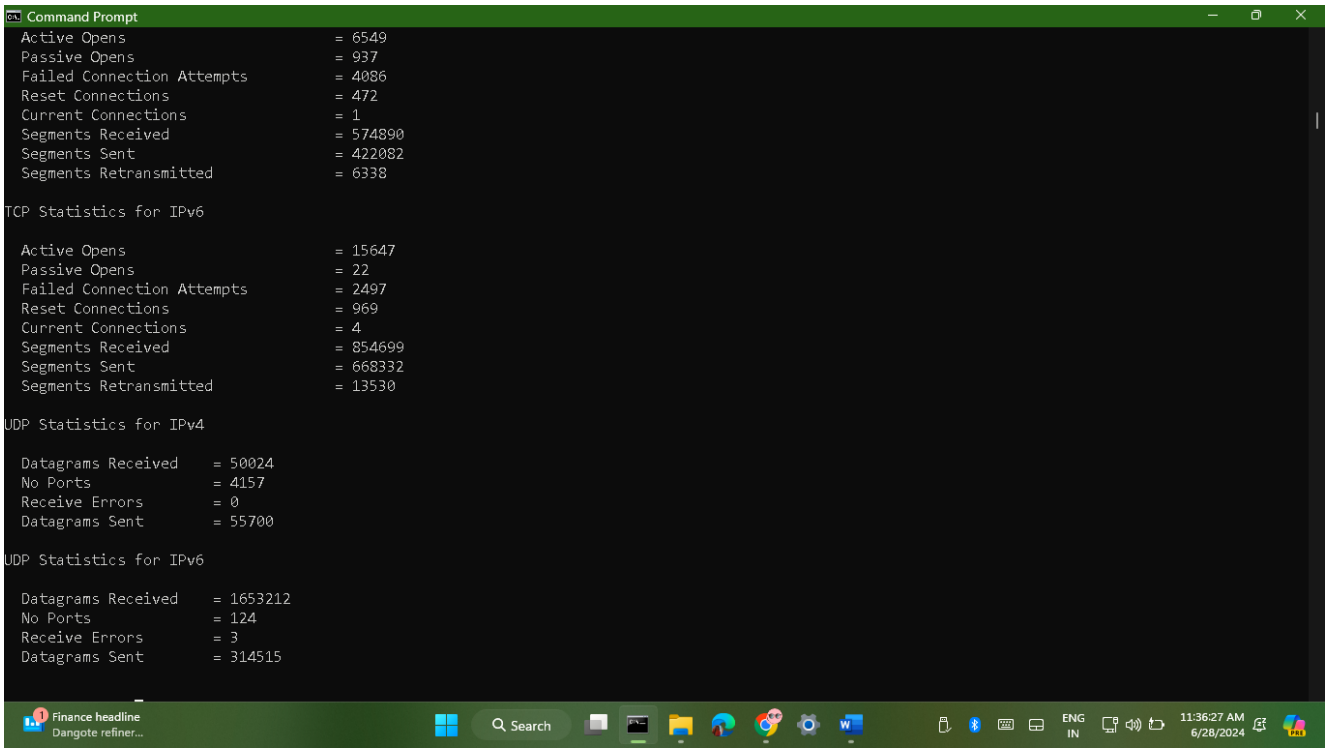


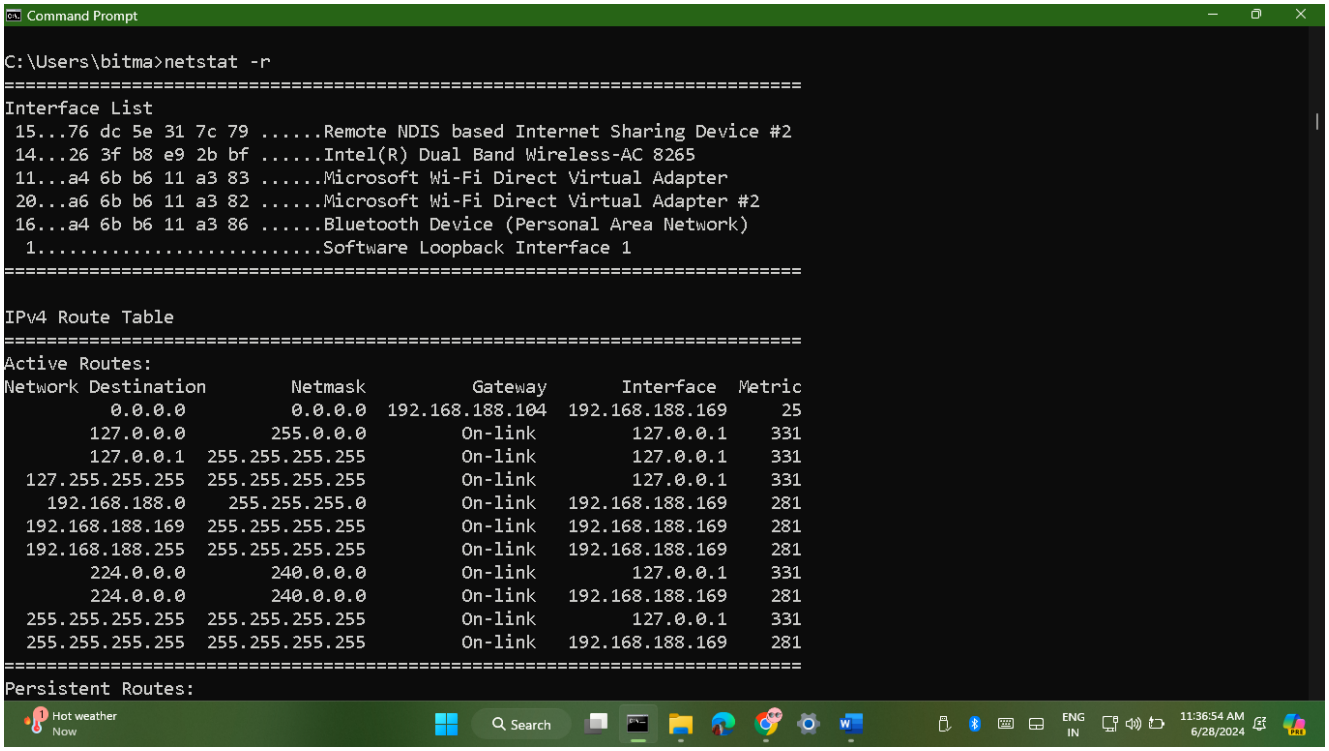
```
Command Prompt
  Unknown Protocols Received         = 5
  Received Packets Discarded         = 139
  Received Packets Delivered         = 2505409
  Output Requests                    = 1028498
  Routing Discards                   = 0
  Discarded Output Packets           = 0
  Output Packet No Route             = 1189
  Reassembly Required                = 0
  Reassembly Successful              = 0
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 0
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 0

ICMPv4 Statistics

                        Received    Sent
  Messages              789         2143
  Errors                0           0
  Destination Unreachable 768       2104
  Time Exceeded         18          0
  Parameter Problems    0           0
  Source Quenches       0           0
  Redirects             0           0
  Echo Replies          3           0
  Echos                 0           39
  Timestamps            0           0
  Timestamp Replies     0           0
  Address Masks         0           0
  Address Mask Replies  0           0
```



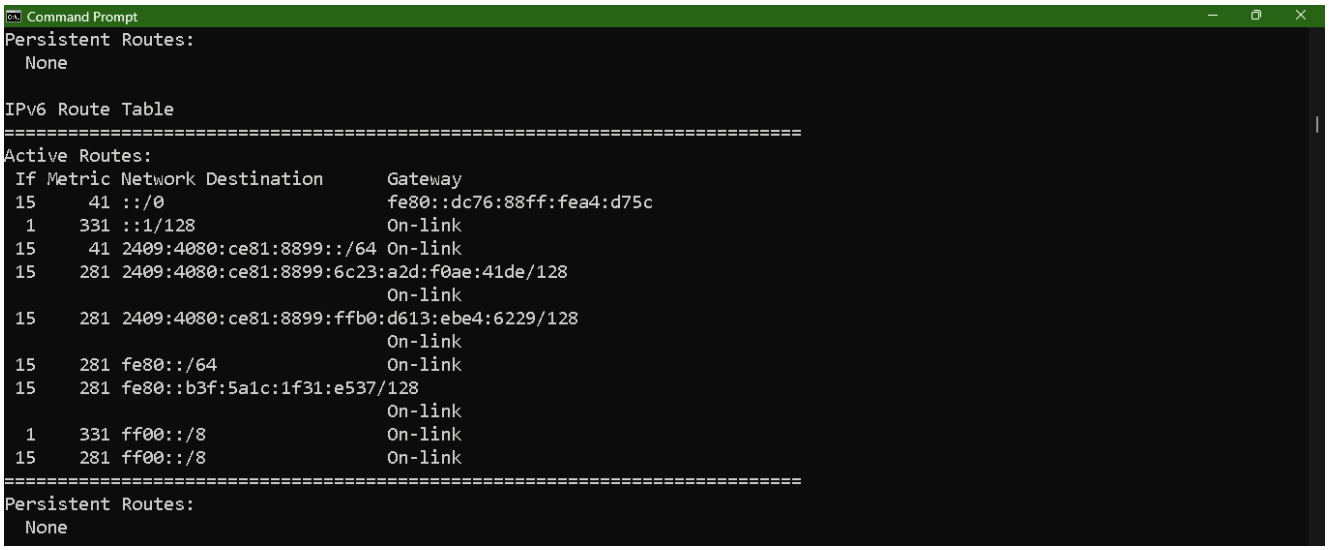
```
Command Prompt
  Timestamp Replies     0           0
  Address Masks         0           0
  Address Mask Replies  0           0
  Router Solicitations  0           0
  Router Advertisements 0           0

ICMPv6 Statistics

                        Received    Sent
  Messages              2134        2010
  Errors                0           0
  Destination Unreachable 12        39
  Packet Too Big        0           0
  Time Exceeded         136         0
  Parameter Problems    0           1
  Echos                 0           188
  Echo Replies          12          0
  MLD Queries           0           0
  MLD Reports           0           0
  MLD Dones             0           0
  Router Solicitations  0           25
  Router Advertisements 318         0
  Neighbor Solicitations 1571       136
  Neighbor Advertisements 85        1621
  Redirects             0           0
  Router Renumberings   0           0

TCP Statistics for IPv4

  Active Opens                      = 6549
```

Date: 28/6/2024





Date: 28/6/2024



7.nslookup

Description:

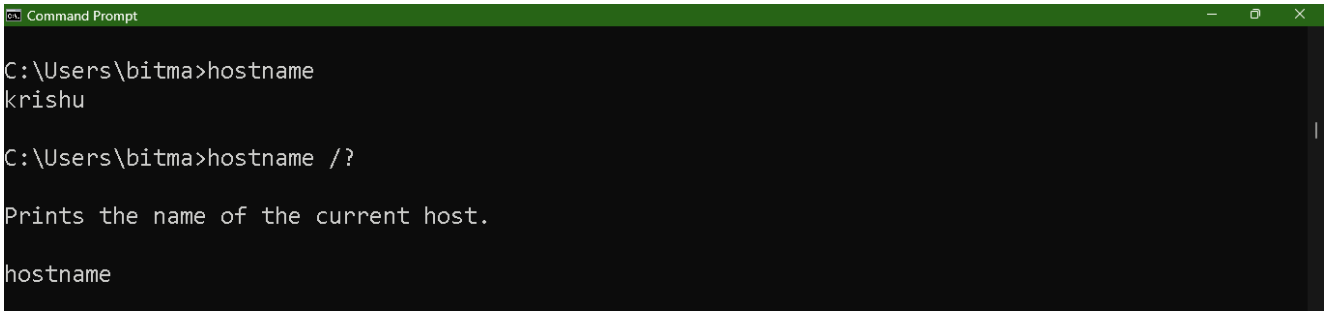
The nslookup command is a network utility used for querying the Domain Name System (DNS) to obtain domain name or IP address mapping information. It helps troubleshoot DNS-related issues by allowing users to look up the IP address associated with a domain name and vice versa.

8.hostname

Description:

The hostname command is used to display the name of the current host (the computer you are using). It's a simple utility that shows the network name of the machine.

Implementation:



Date: 28/6/2024

9.pathping

Description:

The pathping command is a network utility in Windows that combines the functionality of `ping` and tracert to provide detailed information about network latency and packet loss at each hop between a source and destination.

No.	Option	Description
1	Pathping -n	Do not resolve addresses to hostnames.
2	Pathping -4	Force using IPv4.
3	Pathping -6	Force using IPv6.
4	Pathping -g	Loose source route along host-list.
5	Pathping -p peroid	Wait period milliseconds between pings.

Date: 28/6/2024

Implementation:

```
Command Prompt
C:\Users\bitma>pathping -n youtube.com

Tracing route to youtube.com [2404:6800:4009:805::200e]
over a maximum of 30 hops:
  0  2409:4080:ce81:8899:6c23:a2d:f0ae:41de
  1  2409:4080:ce81:8899::99
  2     *        *        *
Computing statistics for 25 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           2409:4080:ce81:8899:6c23:a2d:f0ae:41de
                                    0/ 100 =  0%   |
  1    0ms     0/ 100 =  0%     0/ 100 =  0%  2409:4080:ce81:8899::99

Trace complete.
```

```
Command Prompt
C:\Users\bitma>pathping -4 youtube.com

Tracing route to youtube.com [142.250.70.110]
over a maximum of 30 hops:
  0  krishu [192.168.188.169]
  1  192.168.188.104
  2     *        *        *
Computing statistics for 25 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           krishu [192.168.188.169]
                                    0/ 100 =  0%   |
  1    0ms     0/ 100 =  0%     0/ 100 =  0%  192.168.188.104

Trace complete.
```

```
Select Command Prompt
C:\Users\bitma>pathping -6 youtube.com

Tracing route to youtube.com [2404:6800:4009:81f::200e]
over a maximum of 30 hops:
  0  krishu [2409:4080:ce81:8899:6c23:a2d:f0ae:41de]
  1  2409:4080:ce81:8899::99
  2     *        *        *
Computing statistics for 25 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           krishu [2409:4080:ce81:8899:6c23:a2d:f0ae:41de]
                                    0/ 100 =  0%   |
  1    0ms     0/ 100 =  0%     0/ 100 =  0%  2409:4080:ce81:8899::99

Trace complete.
```

```
Command Prompt

C:\Users\bitma>pathping -g youtube.com

Tracing route to youtube.com [142.250.70.110]
over a maximum of 30 hops:
  0  krishu [192.168.188.169]
  1     *        *        *
Computing statistics for 0 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           krishu [192.168.188.169]

Trace complete.
```

Date: 28/6/2024

```
Command Prompt

C:\Users\bitma>pathping -p 1000 youtube.com

Tracing route to youtube.com [2404:6800:4009:81f::200e]
over a maximum of 30 hops:
  0  krishu [2409:4080:ce81:8899:6c23:a2d:f0ae:41de]
  1  2409:4080:ce81:8899::99
  2     *        *        *
Computing statistics for 100 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           krishu [2409:4080:ce81:8899:6c23:a2d:f0ae:41de]
                                    0/ 100 =  0%   |
  1    0ms     0/ 100 =  0%     0/ 100 =  0%  2409:4080:ce81:8899::99

Trace complete.
```

10.arp

Description:

The arp command is used to display and modify the ARP (Address Resolution Protocol) cache, which contains mappings of IP addresses to MAC (Media Access Control) addresses.

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 addresses for only the specified computer are displayed. If more than one network interface uses ARP, entries for each ARP table are displayed.
2	arp -g	Same as -a

Implementation:

```
Command Prompt

C:\Users\bitma>arp -a

Interface: 192.168.188.169 --- 0xf
  Internet Address      Physical Address      Type
  192.168.188.104       de-76-88-a4-d7-5c     dynamic
  192.168.188.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.102.18        01-00-5e-7f-66-12     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

```
Command Prompt
C:\Users\bitma>arp -g

Interface: 192.168.188.169 --- 0xf
  Internet Address      Physical Address      Type
  192.168.188.104       de-76-88-a4-d7-5c     dynamic
  192.168.188.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.102.18        01-00-5e-7f-66-12     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```