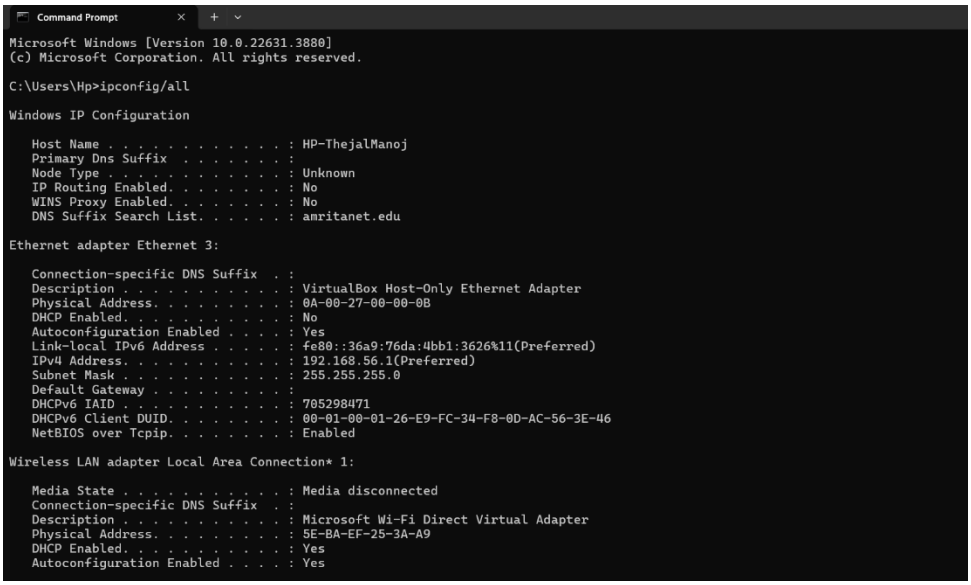
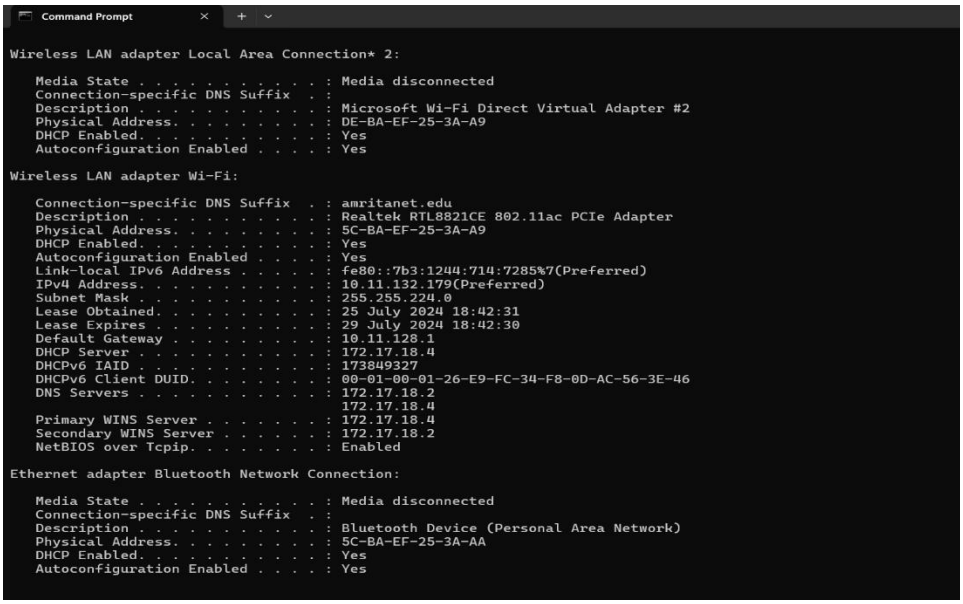
LAB 1:

BASIC NETWORK ADMINISTRATION AND TROUBLESHOOTING USING WINDOWS COMMAND LINE UTILITIES

1. **Ipconfig/all**: Internet protocol configuration (ipconfig) command is used to dispay network details of a system.



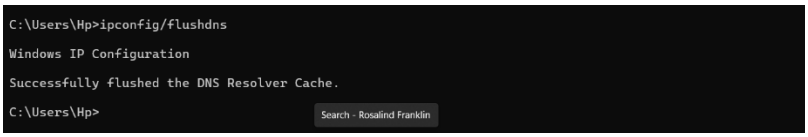


Here we have three network adapters – Ethernet, Wifi, and Bluetooth.

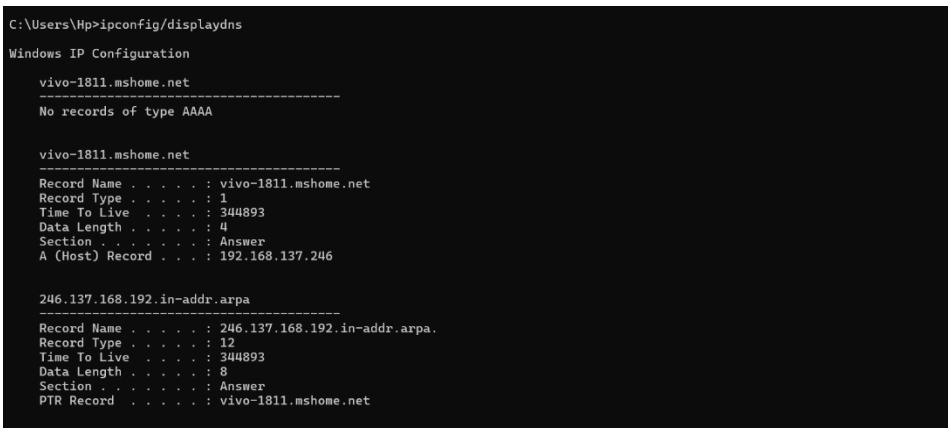
- Hostname : Name of the system.
- Node type : Type of node (System)
- IPv6 Address : 128 bits hexa-decimal address, separated by columns.
- IPv4 Address : 32 bits decimal address, separated by dots.

- DHCP : Dynamic Host Configuration Protocol is a network management protocol in which DHCP server manages IP address and network configuration parameters.
- Subnet mask : 32 bits IP address having internal usage with in a network. It helps routers to route data packets in to correct destination.
- DNS Suffix : Set of characters added at the end of the domain name that helps to identify particular domain.
- Default gateway : Gateway is a software component that acts as a entry point between 2 networks.

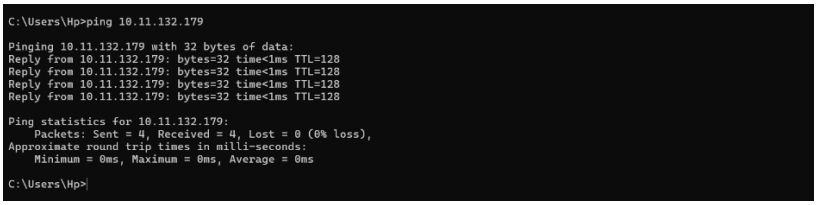
2. **Ipconfig/flushdns:** It is a troubleshooting command to resolve DNS related issues by flushing DNS cache.



3. **Ipconfig/displaydns:** Displays DNS cache contents (records of recent DNS lookups)

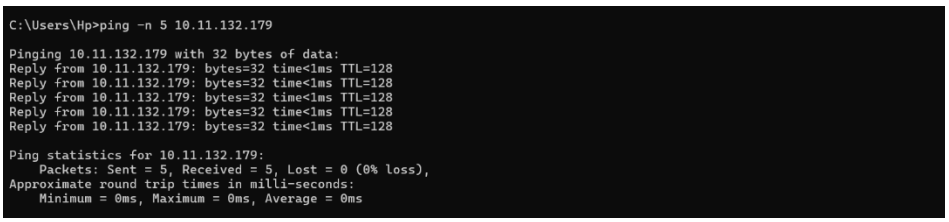


4. **Ping:** It sends Internet Control Message Protocol (ICMP) echo requests to the specified IP address and waits for the reply packets.



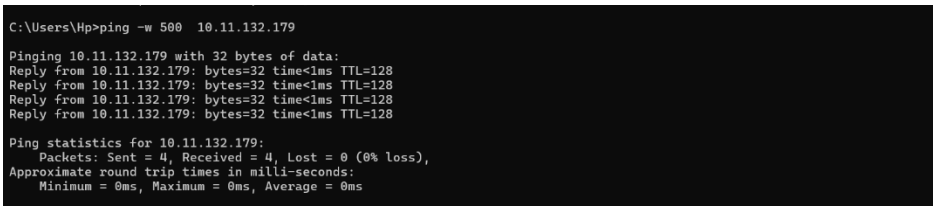
- Here, the first line indicates, the host is pinging and the size of data packet is 32 bytes.
- Line 2 to 5 indicates, received reply from the host , packet size , how long the packet takes to go destination and come back (Round Trip Time) and Time To Live (TTL) value of the packet.
- The remaining session shows ping statistics that includes number of packets sent, received and lost.

5. **ping -n <Count> <IP_Address>:** Determines the number of ICMP packets to sent to the destination. Here count indicates the desired number of packets and IP_Address indicates the IP address of target system.

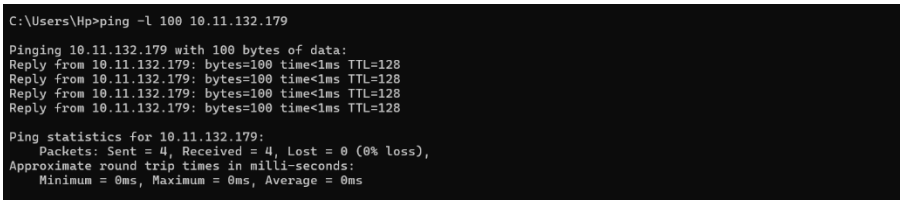


Output shows the statistics of each packets.

6. **ping -w <time_out> <IP_Address>:** Specifies the time out period for each ICMP packets.

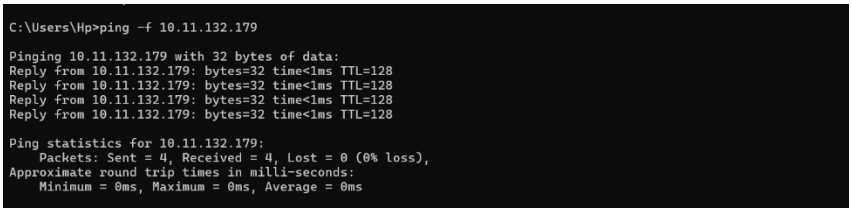


7. **ping -l <Size> <Ip_address> :** specifies the size of ICMP packets send to the target.Default size of a packet is 32 bytes.



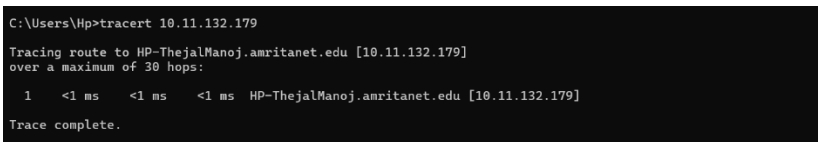
Here, user changes the packet size to 100 bytes.

8. **ping -f <IP_Address>:** f stands for “don’t fragment (DF)” flag. It determines whether fragmentation of packets are permitted or not.



By default, the packets are transmitted after fragmentation. Here, -f indicates that DF flag is set to 1. That means fragmentation is prevented. And so, packets are transmitted without fragmentation.

9. **tracert:** trace route command is used to determine the path selected by the data packet from source to destination by sending ICMP echo packets.



Here, the data packets have only one route and also displays the round trip times having 3 different values. That indicates, three different packets are send to the host. And we have a completion message also.

10. **nslookup <domain_name>:** name server lookup is used to obtain domain name/ip address from DNS.

- Server indicates the DNS server used for the query.
- Address indicates the IP address of the DNS
- Name indicates the domain we asked.
- Address indicates the associated IP address.

11. netstat -a: Displays all the TCP connections in the network. It shows the statistics of network connections including,

- protocol: The used protocol (TCP/UDP)
- local address: Local IP address and port number.
- foreign address: Remote IP address and port number.
- state: State of a connection.

1)Listening: The state in which the network service is waiting for incoming connections.

2)Established: Connection has been established between client and server.

```
C:\Users\Hp>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            HP-ThejalManoj:0       LISTENING
  TCP    0.0.0.0:445            HP-ThejalManoj:0       LISTENING
  TCP    0.0.0.0:3306           HP-ThejalManoj:0       LISTENING
  TCP    0.0.0.0:5040           HP-ThejalManoj:0       LISTENING
  TCP    0.0.0.0:7070           HP-ThejalManoj:0       LISTENING
  TCP    0.0.0.0:7680           HP-ThejalManoj:0       LISTENING
  TCP    0.0.0.0:33060          HP-ThejalManoj:0       LISTENING
  TCP    0.0.0.0:49664          HP-ThejalManoj:0       LISTENING
  TCP    0.0.0.0:49665          HP-ThejalManoj:0       LISTENING
  TCP    0.0.0.0:49666          HP-ThejalManoj:0       LISTENING
  TCP    0.0.0.0:49667          HP-ThejalManoj:0       LISTENING
  TCP    0.0.0.0:49668          HP-ThejalManoj:0       LISTENING
  TCP    0.0.0.0:49670          HP-ThejalManoj:0       LISTENING
  TCP    10.11.132.179:139      HP-ThejalManoj:0       LISTENING
  TCP    10.11.132.179:64214    relay-6287bd7e:https   ESTABLISHED
  TCP    10.11.132.179:64217    20.198.119.84:https    ESTABLISHED
  TCP    10.11.132.179:64238    20.249.115.161:https   ESTABLISHED
  TCP    10.11.132.179:64642    20.212.88.117:https    ESTABLISHED
  TCP    10.11.132.179:64645    maa05s17-in-f10:https  ESTABLISHED
  TCP    10.11.132.179:64646    maa05s17-in-f10:https  ESTABLISHED
  TCP    10.11.132.179:64655    lax31s01-in-f3:https   ESTABLISHED
  TCP    10.11.132.179:64735    20.249.115.161:https   ESTABLISHED
  TCP    10.11.132.179:64765    52.123.249.144:https   ESTABLISHED
  TCP    10.11.132.179:64824    lax17s46-in-f10:https  TIME_WAIT
  TCP    10.11.132.179:64825    lax31s11-in-f14:https  TIME_WAIT
  TCP    10.11.132.179:64826    lax31s11-in-f10:https  TIME_WAIT
  TCP    10.11.132.179:64838    maa03s43-in-f3:https   ESTABLISHED
  TCP    10.11.132.179:64839    dy-in-f84:https        ESTABLISHED
  TCP    10.11.132.179:64844    maa05s22-in-f10:https  ESTABLISHED
  TCP    10.11.132.179:64848    104.208.16.92:https    TIME_WAIT
  TCP    10.11.132.179:64854    a23-217-111-51:https   CLOSE_WAIT
  TCP    10.11.132.179:64857    52.109.124.29:https    TIME_WAIT
  TCP    10.11.132.179:64858    104.18.30.2:https      ESTABLISHED
  TCP    10.11.132.179:64859    104.18.31.2:https      ESTABLISHED
  TCP    10.11.132.179:64860    ec2-3-233-158-24:https  ESTABLISHED
```

12. netstat -e: Displays the number of packets sent and received.

```
C:\Users\Hp>netstat -e
Interface Statistics

                           Received            Sent

Bytes                    3706204383       189884758
Unicast packets             337799          199388
Non-unicast packets        32193903           24367
Discards                         0               0
Errors                           0               0
Unknown protocols                0
```

- Byetes: Total number of bytes sent and received.
- Unicast packets: Number of packets sent and received to a single destination.
- Non unicast packets: Number of packets broadcasted.
- Discards: Number of packets dropped due to errors.
- Errors: Number of errors occurred during the processing.

13. netstat -n: Displays active TCP connections and the port numbers are expressed numerically. Here, the protocol used is tcp.

- Local address: IP address and port number of local machine.
- Foreign address: IP address and port number of remote machine.
- State: State of current connection – Established (Successfully established client server connection),Time Wait (Connection has been closed

beforeport is released) and Listening (The state in which the network service is waiting for incoming connections)

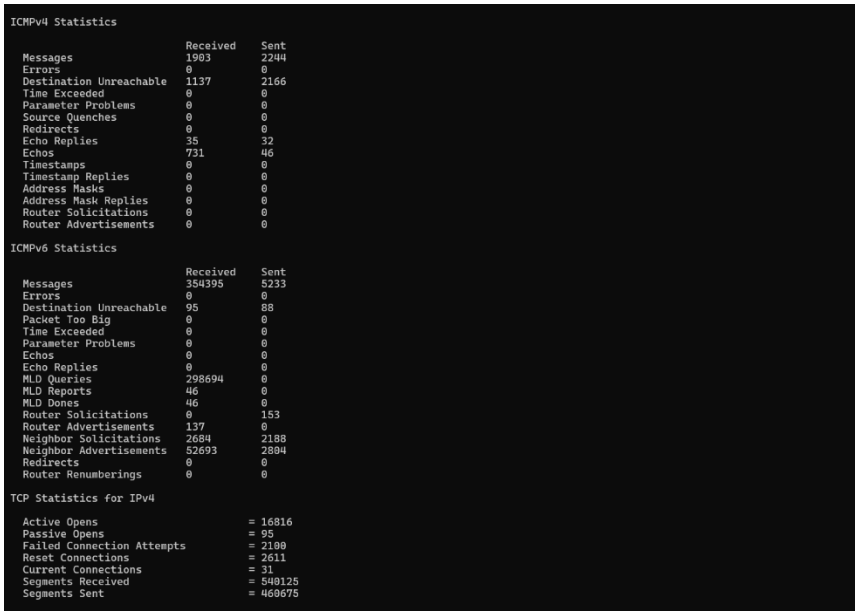
```
C:\Users\Hp>netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    10.11.132.179:65053    52.96.66.226:443       ESTABLISHED
  TCP    10.11.132.179:65103    20.249.115.164:443     ESTABLISHED
  TCP    10.11.132.179:65110    203.17.244.53:443      ESTABLISHED
  TCP    10.11.132.179:65113    20.198.119.143:443     ESTABLISHED
  TCP    10.11.132.179:65125    48.218.107.40:443      ESTABLISHED
  TCP    10.11.132.179:65132    142.250.196.3:443      TIME_WAIT
  TCP    10.11.132.179:65134    142.250.196.74:443     TIME_WAIT
  TCP    10.11.132.179:65135    142.250.196.74:443     ESTABLISHED
  TCP    10.11.132.179:65154    142.251.12.84:443      TIME_WAIT
  TCP    10.11.132.179:65155    172.217.163.170:443    TIME_WAIT
  TCP    10.11.132.179:65156    142.250.72.174:443     TIME_WAIT
  TCP    10.11.132.179:65165    51.104.18.253:443      TIME_WAIT
  TCP    10.11.132.179:65167    13.89.179.11:443       ESTABLISHED
  TCP    10.11.132.179:65168    20.212.88.117:443      ESTABLISHED
  TCP    127.0.0.1:49706        127.0.0.1:49707        ESTABLISHED
  TCP    127.0.0.1:49707        127.0.0.1:49706        ESTABLISHED
```

14. netstat -o: Displaying Displays active TCP connections along with their process id. Process id is an unique number used to identify each process.

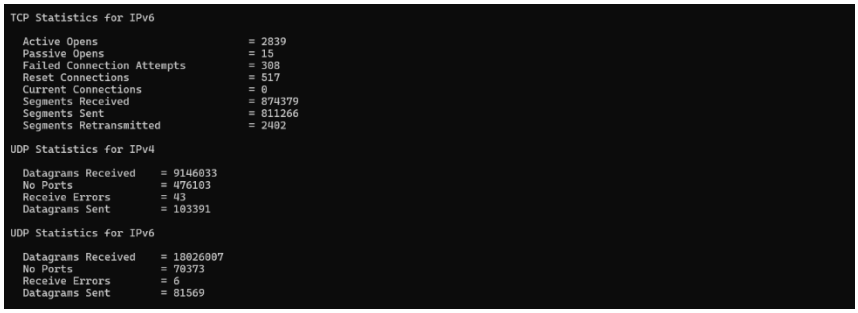
```
C:\Users\Hp>netstat -o

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    10.11.132.179:49628    maa05s28-in-f10:https  ESTABLISHED     37232
  TCP    10.11.132.179:49632    maa05s28-in-f10:https  ESTABLISHED     37232
  TCP    10.11.132.179:49635    maa05s24-in-f3:https   ESTABLISHED     37232
  TCP    10.11.132.179:49985    52.123.253.86:https    ESTABLISHED     11756
  TCP    10.11.132.179:49995    maa05s05-in-f14:https  ESTABLISHED     37232
  TCP    10.11.132.179:50011    104.18.31.2:https      ESTABLISHED     37232
  TCP    10.11.132.179:50012    104.18.30.2:https      ESTABLISHED     37232
  TCP    10.11.132.179:50019    maa05s19-in-f10:https  TIME_WAIT       0
  TCP    10.11.132.179:50026    maa05s19-in-f10:https  TIME_WAIT       0
  TCP    10.11.132.179:50031    maa05s24-in-f3:https   ESTABLISHED     37232
  TCP    10.11.132.179:50033    52.123.253.136:https   ESTABLISHED     31888
  TCP    10.11.132.179:50034    52.168.112.67:https    ESTABLISHED     11756
  TCP    10.11.132.179:50035    lax17s38-in-f5:https   ESTABLISHED     37232
  TCP    10.11.132.179:50038    a104-90-5-146:https    TIME_WAIT       0
  TCP    10.11.132.179:50043    maa03s45-in-f14:https  ESTABLISHED     37232
  TCP    10.11.132.179:50044    sb-in-f84:https        ESTABLISHED     37232
  TCP    10.11.132.179:50049    a104-71-60-41:http     TIME_WAIT       0
  TCP    10.11.132.179:50050    152.195.38.76:http     TIME_WAIT       0
  TCP    10.11.132.179:50051    104.46.162.227:https   TIME_WAIT       0
  TCP    10.11.132.179:50055    49.44.116.178:http     TIME_WAIT       0
  TCP    10.11.132.179:50058    ec2-3-233-158-24:https  ESTABLISHED    37232
  TCP    10.11.132.179:50059    maa03s38-in-f4:https   CLOSE_WAIT      37232
  TCP    10.11.132.179:50060    172.17.143.38:ms-do    SYN_SENT        8316
  TCP    10.11.132.179:65103    20.249.115.164:https   ESTABLISHED     11088
  TCP    10.11.132.179:65110    relay-ea245132:https   ESTABLISHED     6052
  TCP    10.11.132.179:65113    20.198.119.143:https   ESTABLISHED     5752
  TCP    10.11.132.179:65125    48.218.107.40:https    ESTABLISHED     31888
  TCP    10.11.132.179:65168    20.212.88.117:https    ESTABLISHED     11756
  TCP    127.0.0.1:49706        HP-ThejalManoj:49707   ESTABLISHED     7832
  TCP    127.0.0.1:49707        HP-ThejalManoj:49706   ESTABLISHED     7832
```

15. netstat -s: Displays configuration details of different protocols. Each section of the output gives relevant details of particular protocol.

```
C:\Users\Hp>netstat -s

IPv4 Statistics

  Packets Received                   = 6614856
  Received Header Errors             = 0
  Received Address Errors            = 1466308
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 0
  Received Packets Discarded         = 3951192
  Received Packets Delivered         = 4742513
  Output Requests                    = 616906
  Routing Discards                   = 0
  Discarded Output Packets           = 5596
  Output Packet No Route             = 348
  Reassembly Required                = 105145
  Reassembly Successful              = 25004
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 30472
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 162364

IPv6 Statistics

  Packets Received                   = 18281821
  Received Header Errors             = 135
  Received Address Errors            = 11003102
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 46
  Received Packets Discarded         = 2065896
  Received Packets Delivered         = 7223605
  Output Requests                    = 905968
  Routing Discards                   = 0
  Discarded Output Packets           = 448
  Output Packet No Route             = 41
  Reassembly Required                = 20635
  Reassembly Successful              = 5750
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 0
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 0
```



```
ICMPv4 Statistics

                        Received    Sent
  Messages              1903        2244
  Errors                0           0
  Destination Unreachable 1137      2166
  Time Exceeded         0           0
  Parameter Problems    0           0
  Source Quenches       0           0
  Redirects             0           0
  Echo Replies          35          32
  Echos                 731         46
  Timestamps            0           0
  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              354395      5233
  Errors                0           0
  Destination Unreachable 95        88
  Packet Too Big        0           0
  Time Exceeded         0           0
  Parameter Problems    0           0
  Echos                 0           0
  Echo Replies          0           0
  MLD Queries           298694      0
  MLD Reports           46          0
  MLD Dones             46          0
  Router Solicitations  0           153
  Router Advertisements 137         0
  Neighbor Solicitations 2684       2188
  Neighbor Advertisements 52693     2804
  Redirects             0           0
  Router Renumberings   0           0

TCP Statistics for IPv4

  Active Opens                        = 16816
  Passive Opens                       = 95
  Failed Connection Attempts          = 2100
  Reset Connections                   = 2611
  Current Connections                 = 31
  Segments Received                   = 540125
  Segments Sent                       = 460675
```

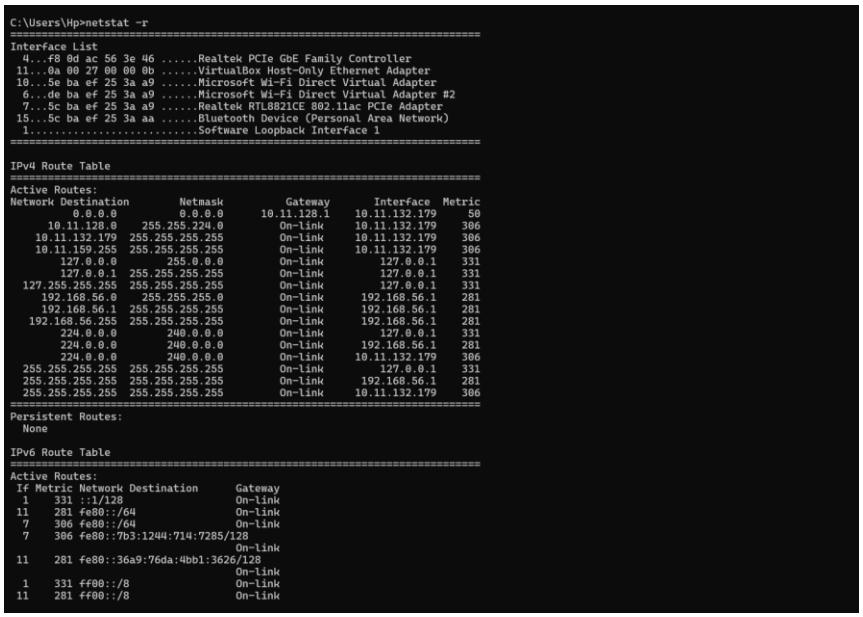


```
TCP Statistics for IPv6

  Active Opens                        = 2839
  Passive Opens                       = 15
  Failed Connection Attempts          = 308
  Reset Connections                   = 517
  Current Connections                 = 0
  Segments Received                   = 874379
  Segments Sent                       = 811266
  Segments Retransmitted              = 2402

UDP Statistics for IPv4

  Datagrams Received    = 9146033
  No Ports              = 476103
  Receive Errors        = 43
  Datagrams Sent        = 103391

UDP Statistics for IPv6

  Datagrams Received    = 18026007
  No Ports              = 70373
  Receive Errors        = 6
  Datagrams Sent        = 81569
```

- Packets received: Number of packets received
- Received header errors: Number of packets having header errors.
- Received address errors: Number of packets having address errors.
- Datagram forwarded: The number of “datagrams”(Basic unit of data used in UDP protocol).
- Routing discards: Number of packets discarded due to routing issue.
- Echo: A type of ICMP message sent by source to check whether it is reachable or not.
- Echo reply: Response from the destination that ensures it is reachable.
- MLD Query: Query send by a router to check which host is interested to receive the message in a broadcast.
- MLD Report: Reply from the host to indicate its interest to receive the message.
- MLD Done: Message from a host to router to informs that it is leaving from the broadcast group.
- Active opens: Number of times a connection was initiated.
- Passive opens: Number of times a connection was accepted.
- Segments received: Number of TCP connection received.
- Segments sent: Number of TCP connection sent.

- Segments retransmitted – Number of packets retransmitted due to packet lose.
- Datagram received: Number of datagrams received.

16. netstat -r: Displays the routing table



```
C:\Users\Hp>netstat -r
===========================================================================
Interface List
  4...f8 0d ac 56 3e 46 ......Realtek PCIe GbE Family Controller
 11...0a 00 27 00 00 0b ......VirtualBox Host-Only Ethernet Adapter
 10...5e ba ef 25 3a a9 ......Microsoft Wi-Fi Direct Virtual Adapter
  6...de ba ef 25 3a a9 ......Microsoft Wi-Fi Direct Virtual Adapter #2
  7...5c ba ef 25 3a a9 ......Realtek RTL8821CE 802.11ac PCIe Adapter
 15...5c ba ef 25 3a aa ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     10.11.128.1    10.11.132.179     50
      10.11.128.0    255.255.224.0         On-link     10.11.132.179    306
    10.11.132.179  255.255.255.255         On-link     10.11.132.179    306
    10.11.159.255  255.255.255.255         On-link     10.11.132.179    306
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
     192.168.56.0    255.255.255.0         On-link      192.168.56.1    281
     192.168.56.1  255.255.255.255         On-link      192.168.56.1    281
   192.168.56.255  255.255.255.255         On-link      192.168.56.1    281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link      192.168.56.1    281
        224.0.0.0        240.0.0.0         On-link     10.11.132.179    306
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link      192.168.56.1    281
  255.255.255.255  255.255.255.255         On-link     10.11.132.179    306
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    331 ::1/128                  On-link
 11    281 fe80::/64                On-link
  7    306 fe80::/64                On-link
  7    306 fe80::7b3:1244:714:7285/128
                                    On-link
 11    281 fe80::36a9:76da:4bb1:3626/128
                                    On-link
  1    331 ff00::/8                 On-link
 11    281 ff00::/8                 On-link
```

- Network destination: IP address of destination
- Netmask: The subnet applied to the host network.
- Gateway: Network node that connects 2 different networks using different protocols.
- Metric: Defines cost of each route. Route having lower cost will be the preferred one.
- Interface: IP address of the network interface that used to reach the destination.

17. arp -a: view and manages address resolution protocol (ARP) cache. It maps IP address to MAC address.

- Interface: IP address of the network interface where the ARP table is being displayed.
- Physical address: The MAC address associated with the IP address.
- Type: Defines type of ARP entry – Dynamic (Managed by OS based on the ARP requests and response) and Static (Manually configured).

```
C:\Users\Hp>arp -a

Interface: 10.11.132.179 --- 0x7
  Internet Address      Physical Address      Type
  10.11.128.1           00-00-5e-00-01-fe     dynamic
  10.11.128.11          44-31-92-8f-64-97     dynamic
  10.11.129.19          14-13-33-8a-60-35     dynamic
  10.11.131.70          50-5a-65-fa-70-dc     dynamic
  10.11.132.114         14-85-7f-26-fb-f1     dynamic
  10.11.137.78          a0-b3-39-f1-bc-92     dynamic
  10.11.138.182         20-4e-f6-79-e5-e1     dynamic
  10.11.139.222         a8-41-f4-c3-b3-91     dynamic
  10.11.159.254         40-a8-f0-81-05-00     dynamic
  10.11.159.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.113           01-00-5e-00-00-71     static
  224.0.0.250           01-00-5e-00-00-fa     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  224.0.1.60            01-00-5e-00-01-3c     static
  224.77.77.77          01-00-5e-4d-4d-4d     static
  230.0.0.1             01-00-5e-00-00-01     static
  230.86.6.15           01-00-5e-56-06-0f     static
  239.0.0.8             01-00-5e-00-00-08     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

Interface: 192.168.56.1 --- 0xb
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.250           01-00-5e-00-00-fa     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  224.0.1.60            01-00-5e-00-01-3c     static
  224.77.77.77          01-00-5e-4d-4d-4d     static
  230.0.0.1             01-00-5e-00-00-01     static
  230.86.6.15           01-00-5e-56-06-0f     static
  239.0.0.8             01-00-5e-00-00-08     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

18. Gpresult: To display resultant set of policy information for users and systems.

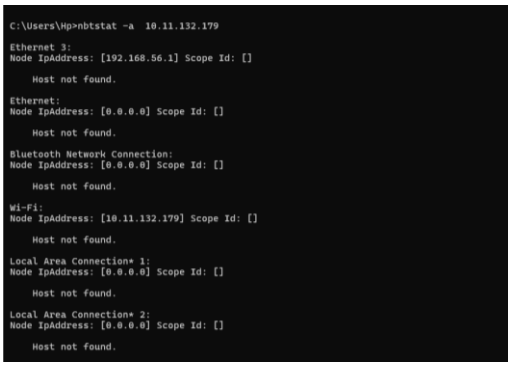
```
C:\Users\Hp>Gpresult

GPRESULT [/S system [/U username [/P [password]]]] [/SCOPE scope]
         [/USER targetusername] [/R | /V | /Z]

Description:
    This command line tool displays the Resultant Set of Policy (RSoP)
    information for a target user and computer.

Parameter List:
    /S        system           Specifies the remote system to connect to.

    /U        [domain\]user    Specifies the user context under which the
                               command should run.
    /P        [password]       Specifies the password for the given user
                               context. Prompts for input if omitted.
    /SCOPE    scope            Specifies whether the user or the
                               computer settings need to be displayed.
                               Valid values: "USER", "COMPUTER".

    /USER     [domain\]user    Specifies the user name for which the
                               RSoP data is to be displayed.

    /R                         Displays RSoP summary data.

    /V                         Specifies that verbose information should
                               be displayed. Verbose information provides
                               additional detailed settings that have
                               been applied with a precedence of 1.

    /Z                         Specifies that the super-verbose
                               information should be displayed. Super-
                               verbose information provides additional
                               detailed settings that have been applied
                               with a precedence of 1 and higher. This
                               allows you to see if a setting was set in
                               multiple places. See the Group Policy
                               online help topic for more information.

    /?                         Displays this help message.


Examples:
    GPRESULT /R
    GPRESULT /USER targetusername /V
    GPRESULT /S system /USER targetusername /SCOPE COMPUTER /Z
    GPRESULT /S system /U username /P password /SCOPE USER /V
```

- /S system: Specifies the remote system to query.
- /U username: User context for the command.
- /P password: Password for user account
- /USER [domain\]user: Specifies the user for whom the policy information is to be displayed.
- /R: Summary of RSoP summary.
- /V: Detailed information about the group policy settings applied to the user and system.

19. nbstat -a <IP_Address> : To display NetBIOS over TCP/IP statistics for a system. The out will shows

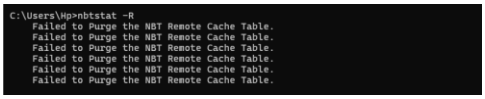
- Name: NetBIOS names registered by the system.

- Type: Type of NetBIOS name – Unique(Unique name for specific system) and Group(Group of NetBIOS name for a group of systems)
- Status: Defines whether the name is registered or not.



In this output, the there is no host details. It may be due the system might not be running NetBIOS over TCP.

20. nbtstat -R: To reload NetBIOS name cache.



21. Set U: Shows which user is logged in.