21CY681 IP Lab-Assignment 1

Basic Network Administration using windows command line utilities

Name:Ramya Ajay

Roll No:CB.EN.P2CYS22004

Date:03-10-2022

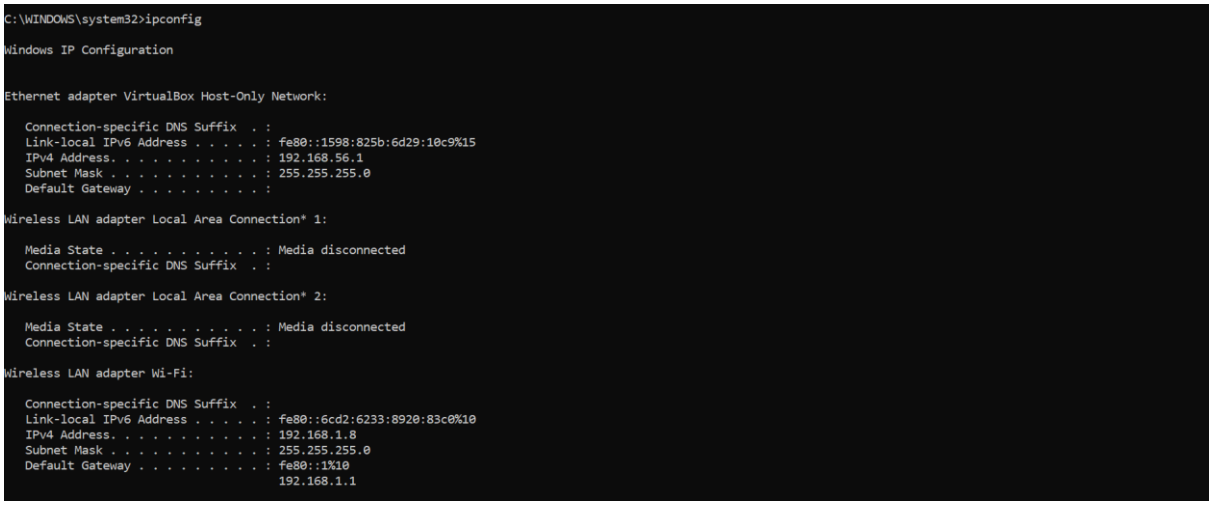
AIM: To analyze and use the basic Windows command line utilities to perform troubleshooting in the network.

Tools:

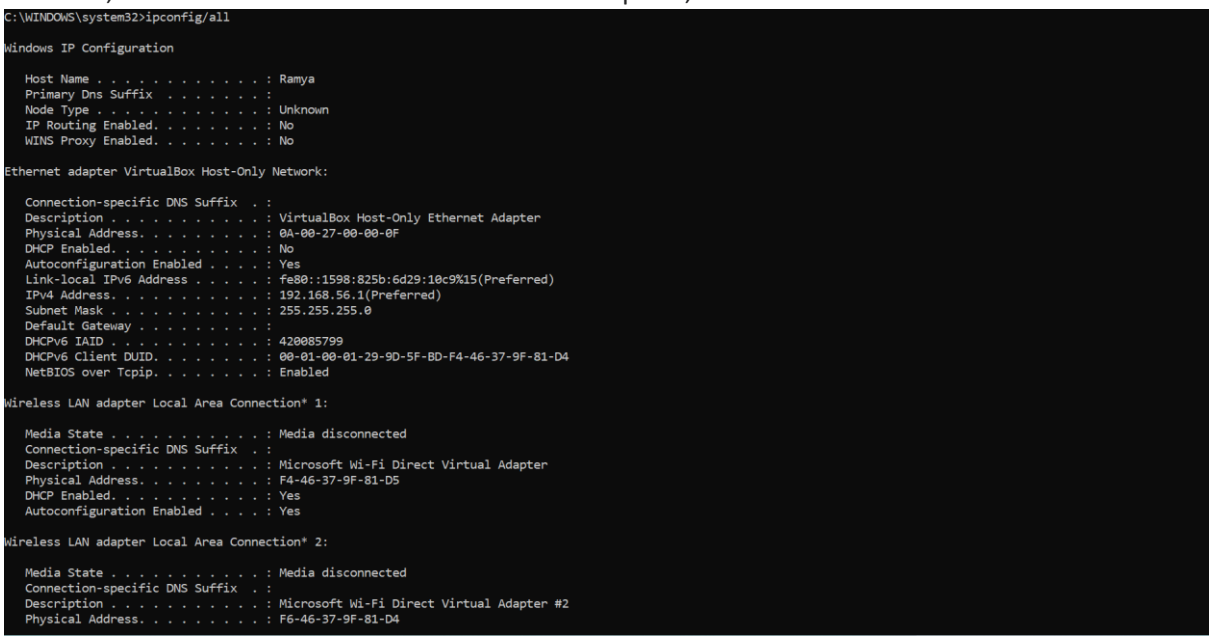
- Windows OS
- Command Prompt(Administrator Privileges to run the tools)

TASK 1:Verifying IP Configuration Settings

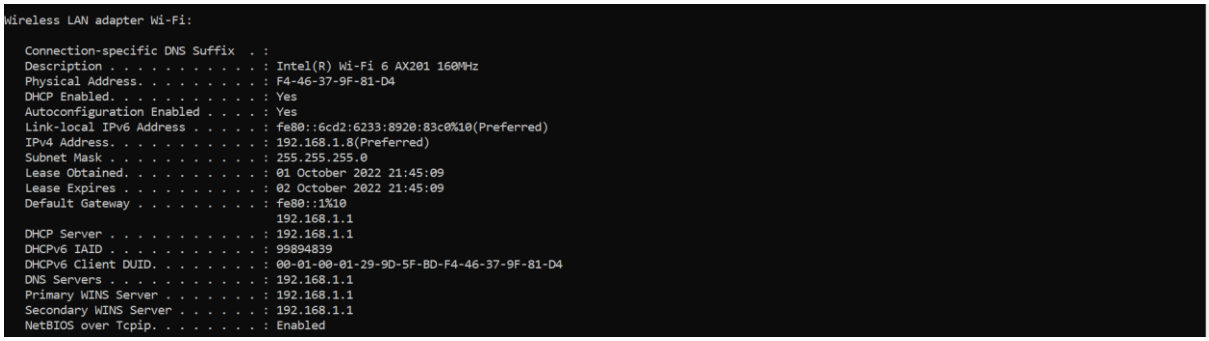
1)ipconfig –The output of this command displays, the MAC, IP address, subnet mask and gateway for all the physical and virtual network adapter.



1.1) ipconfig/all- It gives out a detailed description of the Network Adapters connected to the machine, with additional information like the Description, DNS Servers and all.

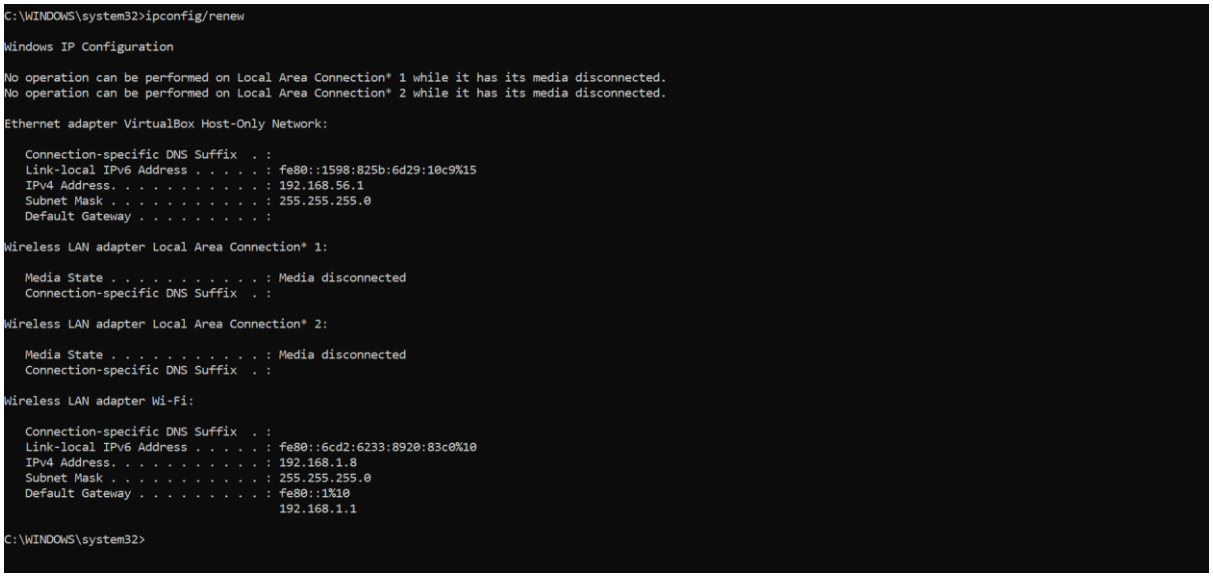


```
C:\WINDOWS\system32>ipconfig/all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Ramya
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Unknown
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter
   Physical Address. . . . . . . . . : 0A-00-27-00-00-0F
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::1598:825b:6d29:10c9%15(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.56.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 420085799
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-29-9D-5F-BD-F4-46-37-9F-81-D4
   NetBIOS over Tcpip. . . . . . . . : Enabled

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : F4-46-37-9F-81-D5
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : F6-46-37-9F-81-D4
```



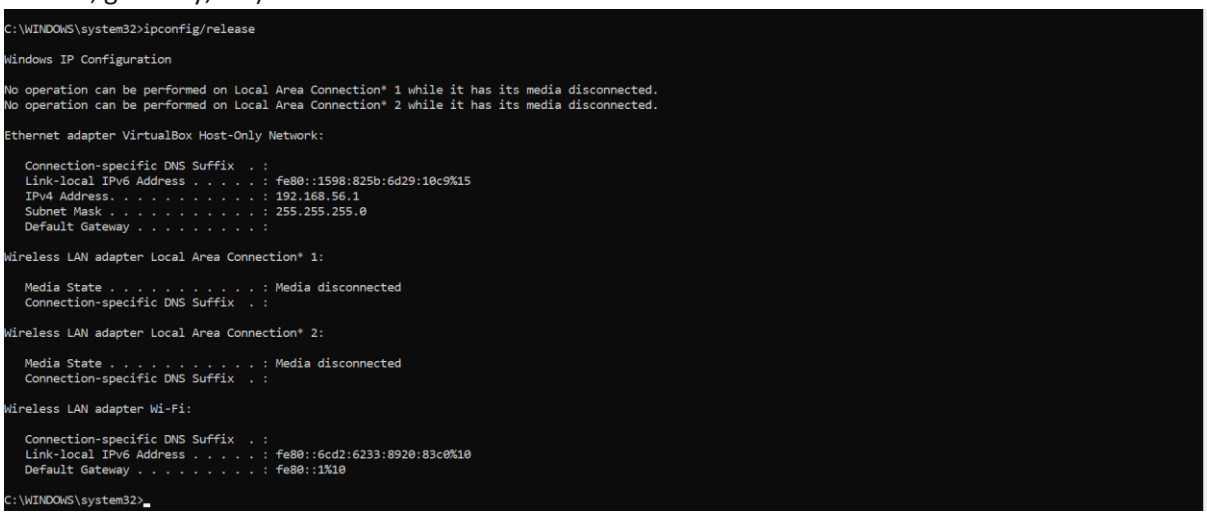
```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
   Physical Address. . . . . . . . . : F4-46-37-9F-81-D4
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::6cd2:6233:8920:83c0%10(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.8(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 01 October 2022 21:45:09
   Lease Expires . . . . . . . . . . : 02 October 2022 21:45:09
   Default Gateway . . . . . . . . . : fe80::1%10
                                       192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 99894839
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-29-9D-5F-BD-F4-46-37-9F-81-D4
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   Primary WINS Server . . . . . . . : 192.168.1.1
   Secondary WINS Server . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

1.2)ipconfig/renew- It will instruct the computer to request a new IP address from the DHCP server as well as DNS, gateway, and other information the DHCP server is set to configure.



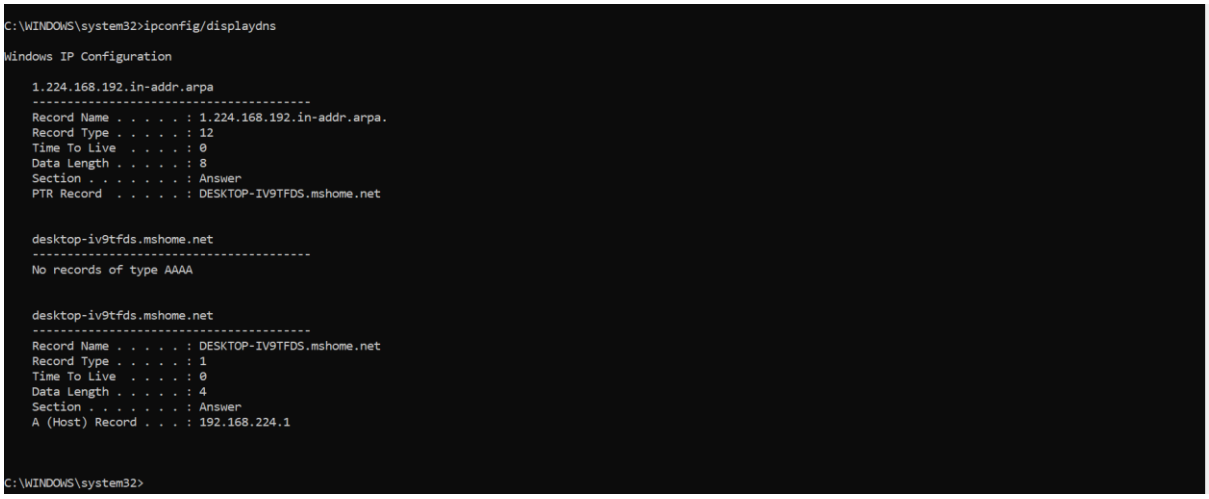
```
C:\WINDOWS\system32>ipconfig/renew

Windows IP Configuration

No operation can be performed on Local Area Connection* 1 while it has its media disconnected.
No operation can be performed on Local Area Connection* 2 while it has its media disconnected.

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::1598:825b:6d29:10c9%15
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::6cd2:6233:8920:83c0%10
   IPv4 Address. . . . . . . . . . . : 192.168.1.8
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::1%10
                                       192.168.1.1

C:\WINDOWS\system32>
```

1.3)ipconfig/release- It sends a command to the DHCP server instructing it to dump the network configuration, and then deletes the current network configuration for all adapters (IP address, DNS servers, gateway, etc).



1.4)ipconfig/flushdns- This command can flush and reset the DNS Resolver Cache

1.5)ipconfig/displaydns- Displays the contents of the DNS Resolver Cache



1.6)ipconfig/registerdns: it initiates manual dynamic registration for the DNS names and IP addresses that are configured at a computer.

```
C:\WINDOWS\system32>ipconfig/registerdns

Windows IP Configuration

Registration of the DNS resource records for all adapters of this computer has been initiated. Any errors will be reported in the Event Viewer in 15 minutes.
```

1.7)ipconfig/showclassid “Wi-Fi”

```
C:\WINDOWS\system32>ipconfig/showclassid "Wi-Fi"

Windows IP Configuration

There are no DHCPv4 classes defined for Wi-Fi.

C:\WINDOWS\system32>
```

1.8)ipconfig/?-Displays Help at the command prompt

```
C:\WINDOWS\system32>ipconfig/?

USAGE:
    ipconfig [/allcompartments] [/? | /all |
                                 /renew [adapter] | /release [adapter] |
                                 /renew6 [adapter] | /release6 [adapter] |
                                 /flushdns | /displaydns | /registerdns |
                                 /showclassid adapter |
                                 /setclassid adapter [classid] |
                                 /showclassid6 adapter |
                                 /setclassid6 adapter [classid] ]

where
    adapter             Connection name
                       (wildcard characters * and ? allowed, see examples)

    Options:
       /?               Display this help message
       /all             Display full configuration information.
       /release         Release the IPv4 address for the specified adapter.
       /release6        Release the IPv6 address for the specified adapter.
       /renew           Renew the IPv4 address for the specified adapter.
       /renew6          Renew the IPv6 address for the specified adapter.
       /flushdns        Purges the DNS Resolver cache.
       /registerdns     Refreshes all DHCP leases and re-registers DNS names
       /displaydns      Display the contents of the DNS Resolver Cache.
       /showclassid     Displays all the dhcp class IDs allowed for adapter.
       /setclassid      Modifies the dhcp class id.
       /showclassid6    Displays all the IPv6 DHCP class IDs allowed for adapter.
       /setclassid6     Modifies the IPv6 DHCP class id.


The default is to display only the IP address, subnet mask and
default gateway for each adapter bound to TCP/IP.

For Release and Renew, if no adapter name is specified, then the IP address
leases for all adapters bound to TCP/IP will be released or renewed.

For Setclassid and Setclassid6, if no ClassId is specified, then the ClassId is removed.
```

1.9)ipconfig/setclassid “Wi-Fi” 1- Configures the DHCP class ID for a specified adapter

```
C:\WINDOWS\system32>ipconfig/setclassid "Wi-Fi" 1

Windows IP Configuration

Successfully set the DHCPv4 class id for adapter Wi-Fi.

C:\WINDOWS\system32>
```

TASK 2:Checking IP Level connectivity using ping command

2)ping ‘IP Address’- it tests and verifies if a particular IP address exists and can accept requests.

```
C:\WINDOWS\system32>ping 192.168.56.1

Pinging 192.168.56.1 with 32 bytes of data:
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.56.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\WINDOWS\system32>
```

ping ‘IP Address’ -n 2 : Here the ping command send 2 ICMP echo request instead of default 4.

2.1) ping ‘IP Address’ -w 1000 : When executing the ping command it adjusts the amount of time, in milliseconds, that ping waits for each reply. Here the timeout value of 1000 is used, which is 1 second.

```
C:\WINDOWS\system32>ping 192.168.56.1 -w 1000

Pinging 192.168.56.1 with 32 bytes of data:
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.56.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

2.2) ping ‘IP Address’ -f: sets the Do Not Fragment bit.

```
C:\WINDOWS\system32>ping 192.168.56.1 -f

Pinging 192.168.56.1 with 32 bytes of data:
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.56.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\WINDOWS\system32>
```

2.3)ping ‘IP Address’ -l size: Sets the packet size for each request

Here the packet size is taken as 1800 bytes.

```
C:\WINDOWS\system32>ping -l 1800 192.168.56.1

Pinging 192.168.56.1 with 1800 bytes of data:
Reply from 192.168.56.1: bytes=1800 time<1ms TTL=128
Reply from 192.168.56.1: bytes=1800 time<1ms TTL=128
Reply from 192.168.56.1: bytes=1800 time<1ms TTL=128
Reply from 192.168.56.1: bytes=1800 time<1ms TTL=128

Ping statistics for 192.168.56.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

TASK 3:Tracking the route of the packets using tracert command

3)tracert ‘IP Address’ - It traces the path an IP packet takes across one or many networks.Here the destination was reached in one hop itself.

```
C:\WINDOWS\system32>tracert 192.168.56.1

Tracing route to Ramya [192.168.56.1]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  Ramya [192.168.56.1]

Trace complete.

C:\WINDOWS\system32>
```

In the below example,it took 7 hops to reach the destination .

```
C:\WINDOWS\system32>tracert 8.8.8.8

Tracing route to dns.google [8.8.8.8]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  192.168.1.1
  2     7 ms     9 ms     6 ms  100.89.0.1
  3    23 ms    21 ms    21 ms  10.1.6.2
  4    26 ms    20 ms    22 ms  as15169.maa.extreme-ix.net [45.120.251.135]
  5    30 ms    22 ms    21 ms  74.125.242.145
  6    30 ms    22 ms    22 ms  74.125.252.209
  7    34 ms    24 ms    24 ms  dns.google [8.8.8.8]

Trace complete.
```

TASK 4:Resolving Domain names with using nslookup command

4)nslookup www.bing.com: It stands for name server lookup and it queries a DNS server to obtain domain name and the associate IP Address. Here the IP address record for the domain www.bing.com is 13.107.21.200 .

```
C:\WINDOWS\system32>nslookup www.bing.com
Server:  UnKnown
Address:  192.168.1.1

Non-authoritative answer:
Name:    dual-a-0001.a-msedge.net
Addresses:  2620:1ec:c11::200
          13.107.21.200
          204.79.197.200
Aliases:  www.bing.com
          www-www.bing.com.trafficmanager.net
          www-bing-com.dual-a-0001.a-msedge.net

C:\WINDOWS\system32>
```

4.1)nslookup -type=A www.bing.com – It gives a non authorative name server listed below.

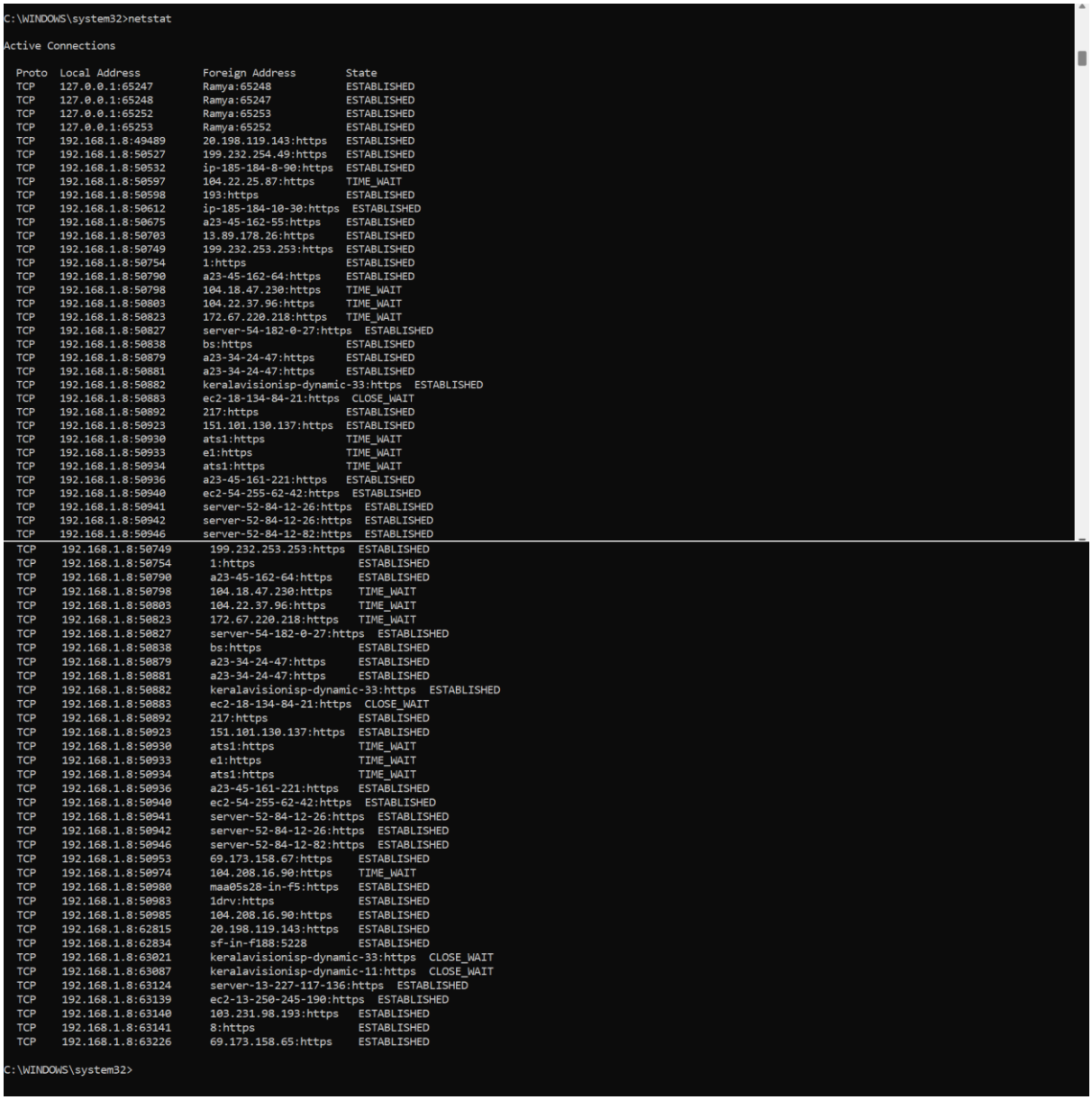
```
C:\WINDOWS\system32>nslookup -type=A www.bing.com
Server:  UnKnown
Address:  192.168.1.1

Non-authoritative answer:
Name:    dual-a-0001.a-msedge.net
Addresses:  13.107.21.200
          204.79.197.200
Aliases:  www.bing.com
          www-www.bing.com.trafficmanager.net
          www-bing-com.dual-a-0001.a-msedge.net
```

4.2)nslookup -type=soa www.bing.com :Start of Authority (SOA) records provide authoritative information about the domain and the server, such as the email address of the administrator, serial number, refresh interval, query expiration time

```
C:\WINDOWS\system32>nslookup -type=soa www.bing.com
Server:  UnKnown
Address:  192.168.1.1

Non-authoritative answer:
www.bing.com    canonical name = www-www.bing.com.trafficmanager.net
www-www.bing.com.trafficmanager.net     canonical name = www-bing-com.dual-a-0001.a-msedge.net
www-bing-com.dual-a-0001.a-msedge.net   canonical name = dual-a-0001.a-msedge.net

a-msedge.net
        primary name server = ns1.a-msedge.net
        responsible mail addr = msnhst.microsoft.com
        serial  = 2016092901
        refresh = 1800 (30 mins)
        retry   = 900 (15 mins)
        expire  = 2419200 (28 days)
        default TTL = 240 (4 mins)

C:\WINDOWS\system32>
```

TASK 5: Checking network configuration and statistics using netstat command

5)netstat: It display very detailed information about how your computer is communicating with other computers or network devices.



```
C:\WINDOWS\system32>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:65247        Ramya:65248            ESTABLISHED
  TCP    127.0.0.1:65248        Ramya:65247            ESTABLISHED
  TCP    127.0.0.1:65252        Ramya:65253            ESTABLISHED
  TCP    127.0.0.1:65253        Ramya:65252            ESTABLISHED
  TCP    192.168.1.8:49489      20.198.119.143:https   ESTABLISHED
  TCP    192.168.1.8:50527      199.232.254.49:https   ESTABLISHED
  TCP    192.168.1.8:50532      ip-185-184-8-90:https  ESTABLISHED
  TCP    192.168.1.8:50597      104.22.25.87:https     TIME_WAIT
  TCP    192.168.1.8:50598      193:https              ESTABLISHED
  TCP    192.168.1.8:50612      ip-185-184-10-30:https  ESTABLISHED
  TCP    192.168.1.8:50675      a23-45-162-55:https    ESTABLISHED
  TCP    192.168.1.8:50703      13.89.178.26:https     ESTABLISHED
  TCP    192.168.1.8:50749      199.232.253.253:https  ESTABLISHED
  TCP    192.168.1.8:50754      1:https                ESTABLISHED
  TCP    192.168.1.8:50790      a23-45-162-64:https    ESTABLISHED
  TCP    192.168.1.8:50798      104.18.47.230:https    TIME_WAIT
  TCP    192.168.1.8:50803      104.22.37.96:https     TIME_WAIT
  TCP    192.168.1.8:50823      172.67.220.218:https   TIME_WAIT
  TCP    192.168.1.8:50827      server-54-182-0-27:https  ESTABLISHED
  TCP    192.168.1.8:50838      bs:https               ESTABLISHED
  TCP    192.168.1.8:50879      a23-34-24-47:https     ESTABLISHED
  TCP    192.168.1.8:50881      a23-34-24-47:https     ESTABLISHED
  TCP    192.168.1.8:50882      keralavisionisp-dynamic-33:https  ESTABLISHED
  TCP    192.168.1.8:50883      ec2-18-134-84-21:https  CLOSE_WAIT
  TCP    192.168.1.8:50892      217:https              ESTABLISHED
  TCP    192.168.1.8:50923      151.101.130.137:https  ESTABLISHED
  TCP    192.168.1.8:50930      ats1:https             TIME_WAIT
  TCP    192.168.1.8:50933      e1:https               TIME_WAIT
  TCP    192.168.1.8:50934      ats1:https             TIME_WAIT
  TCP    192.168.1.8:50936      a23-45-161-221:https   ESTABLISHED
  TCP    192.168.1.8:50940      ec2-54-255-62-42:https  ESTABLISHED
  TCP    192.168.1.8:50941      server-52-84-12-26:https  ESTABLISHED
  TCP    192.168.1.8:50942      server-52-84-12-26:https  ESTABLISHED
  TCP    192.168.1.8:50946      server-52-84-12-82:https  ESTABLISHED
  TCP    192.168.1.8:50749      199.232.253.253:https  ESTABLISHED
  TCP    192.168.1.8:50754      1:https                ESTABLISHED
  TCP    192.168.1.8:50790      a23-45-162-64:https    ESTABLISHED
  TCP    192.168.1.8:50798      104.18.47.230:https    TIME_WAIT
  TCP    192.168.1.8:50803      104.22.37.96:https     TIME_WAIT
  TCP    192.168.1.8:50823      172.67.220.218:https   TIME_WAIT
  TCP    192.168.1.8:50827      server-54-182-0-27:https  ESTABLISHED
  TCP    192.168.1.8:50838      bs:https               ESTABLISHED
  TCP    192.168.1.8:50879      a23-34-24-47:https     ESTABLISHED
  TCP    192.168.1.8:50881      a23-34-24-47:https     ESTABLISHED
  TCP    192.168.1.8:50882      keralavisionisp-dynamic-33:https  ESTABLISHED
  TCP    192.168.1.8:50883      ec2-18-134-84-21:https  CLOSE_WAIT
  TCP    192.168.1.8:50892      217:https              ESTABLISHED
  TCP    192.168.1.8:50923      151.101.130.137:https  ESTABLISHED
  TCP    192.168.1.8:50930      ats1:https             TIME_WAIT
  TCP    192.168.1.8:50933      e1:https               TIME_WAIT
  TCP    192.168.1.8:50934      ats1:https             TIME_WAIT
  TCP    192.168.1.8:50936      a23-45-161-221:https   ESTABLISHED
  TCP    192.168.1.8:50940      ec2-54-255-62-42:https  ESTABLISHED
  TCP    192.168.1.8:50941      server-52-84-12-26:https  ESTABLISHED
  TCP    192.168.1.8:50942      server-52-84-12-26:https  ESTABLISHED
  TCP    192.168.1.8:50946      server-52-84-12-82:https  ESTABLISHED
  TCP    192.168.1.8:50953      69.173.158.67:https    ESTABLISHED
  TCP    192.168.1.8:50974      104.208.16.90:https    TIME_WAIT
  TCP    192.168.1.8:50980      maa05s28-in-f5:https   ESTABLISHED
  TCP    192.168.1.8:50983      1drv:https             ESTABLISHED
  TCP    192.168.1.8:50985      104.208.16.90:https    ESTABLISHED
  TCP    192.168.1.8:62815      20.198.119.143:https   ESTABLISHED
  TCP    192.168.1.8:62834      sf-in-f188:5228        ESTABLISHED
  TCP    192.168.1.8:63021      keralavisionisp-dynamic-33:https  CLOSE_WAIT
  TCP    192.168.1.8:63087      keralavisionisp-dynamic-11:https  CLOSE_WAIT
  TCP    192.168.1.8:63124      server-13-227-117-136:https  ESTABLISHED
  TCP    192.168.1.8:63139      ec2-13-250-245-190:https  ESTABLISHED
  TCP    192.168.1.8:63140      103.231.98.193:https   ESTABLISHED
  TCP    192.168.1.8:63141      8:https                ESTABLISHED
  TCP    192.168.1.8:63226      69.173.158.65:https    ESTABLISHED

C:\WINDOWS\system32>
```

5.1)netstat -a :It displays active TCP connections, TCP connections with the listening state, as well as UDP ports that are being listened to.

```
C:\WINDOWS\system32>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            Ramya:0                LISTENING
  TCP    0.0.0.0:445            Ramya:0                LISTENING
  TCP    0.0.0.0:5040           Ramya:0                LISTENING
  TCP    0.0.0.0:6646           Ramya:0                LISTENING
  TCP    0.0.0.0:49664          Ramya:0                LISTENING
  TCP    0.0.0.0:49665          Ramya:0                LISTENING
  TCP    0.0.0.0:49666          Ramya:0                LISTENING
  TCP    0.0.0.0:49667          Ramya:0                LISTENING
  TCP    0.0.0.0:49668          Ramya:0                LISTENING
  TCP    0.0.0.0:49670          Ramya:0                LISTENING
  TCP    0.0.0.0:49671          Ramya:0                LISTENING
  TCP    0.0.0.0:49672          Ramya:0                LISTENING
  TCP    127.0.0.1:65247        Ramya:65248            ESTABLISHED
  TCP    127.0.0.1:65248        Ramya:65247            ESTABLISHED
  TCP    127.0.0.1:65252        Ramya:65253            ESTABLISHED
  TCP    127.0.0.1:65253        Ramya:65252            ESTABLISHED
  TCP    192.168.1.8:139        Ramya:0                LISTENING
  TCP    192.168.1.8:49489      20.198.119.143:https   ESTABLISHED
  TCP    192.168.1.8:50532      ip-185-184-8-90:https  ESTABLISHED
  TCP    192.168.1.8:50598      193:https              TIME_WAIT
  TCP    192.168.1.8:50754      1:https                TIME_WAIT
  TCP    192.168.1.8:50838      bs:https               ESTABLISHED
  TCP    192.168.1.8:50892      217:https              ESTABLISHED
  TCP    192.168.1.8:50923      151.101.130.137:https  ESTABLISHED
  TCP    192.168.1.8:50940      ec2-54-255-62-42:https  ESTABLISHED
  TCP    192.168.1.8:50953      69.173.158.67:https    TIME_WAIT
  TCP    192.168.1.8:50980      maa05s28-in-f5:https   TIME_WAIT
  TCP    192.168.1.8:50985      104.208.16.90:https    TIME_WAIT
  TCP    192.168.1.8:50986      219:https              ESTABLISHED
  TCP    192.168.1.8:50990      13.107.21.200:https    ESTABLISHED
  TCP    192.168.1.8:50992      1drv:https             ESTABLISHED
  TCP    192.168.1.8:50993      maa05s28-in-f5:https   ESTABLISHED
  TCP    192.168.1.8:50994      13.89.179.9:https      ESTABLISHED
  TCP    192.168.1.8:50995      13.89.179.9:https      ESTABLISHED
  TCP    [::]:49666             Ramya:0                LISTENING
  TCP    [::]:49667             Ramya:0                LISTENING
  TCP    [::]:49668             Ramya:0                LISTENING
  TCP    [::]:49672             Ramya:0                LISTENING
  TCP    [::1]:49669            Ramya:0                LISTENING
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:4500           *:*
  UDP    0.0.0.0:5050           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5355           *:*
  UDP    0.0.0.0:6646           *:*
  UDP    0.0.0.0:50060          142.250.195.234:443
  UDP    0.0.0.0:50369          216.58.200.138:443
  UDP    0.0.0.0:63988          142.250.195.234:443
  UDP    127.0.0.1:1900         *:*
  UDP    127.0.0.1:55068        127.0.0.1:55068
  UDP    127.0.0.1:60397        *:*
  UDP    127.0.0.1:63814        127.0.0.1:63814
  UDP    192.168.1.8:137        *:*
  UDP    192.168.1.8:138        *:*
  UDP    192.168.1.8:1900       *:*
  UDP    192.168.1.8:60396      *:*
  UDP    192.168.56.1:137       *:*
  UDP    192.168.56.1:138       *:*
  UDP    192.168.56.1:1900      *:*
  UDP    192.168.56.1:60395     *:*
  UDP    [::]:500               *:*
  UDP    [::]:4500              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5353              *:*
```

5.2)netstat -e: It show statistics about network connection and this data includes bytes, unicast packets, non-unicast packets, discards, errors, and unknown protocols received and sent since the connection was established.

```
C:\WINDOWS\system32>netstat -e
Interface Statistics

                           Received            Sent

Bytes                     505009358        97168631
Unicast packets              510566          214242
Non-unicast packets            1722            3430
Discards                          0               0
Errors                            0               0
Unknown protocols                 0

C:\WINDOWS\system32>
```

5.3)netstat -n: It displays active tcp connections.

```
C:\WINDOWS\system32>netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:65247        127.0.0.1:65248        ESTABLISHED
  TCP    127.0.0.1:65248        127.0.0.1:65247        ESTABLISHED
  TCP    127.0.0.1:65252        127.0.0.1:65253        ESTABLISHED
  TCP    127.0.0.1:65253        127.0.0.1:65252        ESTABLISHED
  TCP    192.168.1.8:49489      20.198.119.143:443     ESTABLISHED
  TCP    192.168.1.8:50532      185.184.8.90:443       ESTABLISHED
  TCP    192.168.1.8:50838      77.88.21.90:443        ESTABLISHED
  TCP    192.168.1.8:50892      35.186.202.217:443     TIME_WAIT
  TCP    192.168.1.8:50923      151.101.130.137:443    ESTABLISHED
  TCP    192.168.1.8:50986      35.247.144.219:443     ESTABLISHED
  TCP    192.168.1.8:50990      13.107.21.200:443      ESTABLISHED
  TCP    192.168.1.8:50993      142.250.205.229:443    ESTABLISHED
  TCP    192.168.1.8:50994      13.89.179.9:443        ESTABLISHED
  TCP    192.168.1.8:50997      204.79.197.239:443     ESTABLISHED
  TCP    192.168.1.8:50998      13.107.42.12:443       ESTABLISHED
  TCP    192.168.1.8:50999      20.189.173.10:443      ESTABLISHED
  TCP    192.168.1.8:62815      20.198.119.143:443     ESTABLISHED
  TCP    192.168.1.8:62834      74.125.24.188:5228     ESTABLISHED
  TCP    192.168.1.8:63141      35.244.159.8:443       ESTABLISHED

C:\WINDOWS\system32>
```

5.4)netstat -o: It displays the process identifier (PID) associated with each active TCP connections.

```
C:\WINDOWS\system32>netstat -o

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    127.0.0.1:65247        Ramya:65248            ESTABLISHED     1080
  TCP    127.0.0.1:65248        Ramya:65247            ESTABLISHED     1080
  TCP    127.0.0.1:65252        Ramya:65253            ESTABLISHED     1080
  TCP    127.0.0.1:65253        Ramya:65252            ESTABLISHED     1080
  TCP    192.168.1.8:49489      20.198.119.143:https   ESTABLISHED     5244
  TCP    192.168.1.8:50532      ip-185-184-8-90:https  ESTABLISHED     5368
  TCP    192.168.1.8:50838      bs:https               ESTABLISHED     5368
  TCP    192.168.1.8:50892      217:https              TIME_WAIT       0
  TCP    192.168.1.8:50923      151.101.130.137:https  ESTABLISHED     5368
  TCP    192.168.1.8:50986      219:https              ESTABLISHED     6152
  TCP    192.168.1.8:50990      13.107.21.200:https    ESTABLISHED     596
  TCP    192.168.1.8:50993      maa05s28-in-f5:https   ESTABLISHED     5368
  TCP    192.168.1.8:50994      13.89.179.9:https      ESTABLISHED     596
  TCP    192.168.1.8:50997      204.79.197.239:https   ESTABLISHED     596
  TCP    192.168.1.8:50998      1drv:https             ESTABLISHED     19652
  TCP    192.168.1.8:50999      20.189.173.10:https    ESTABLISHED     19652
  TCP    192.168.1.8:62815      20.198.119.143:https   ESTABLISHED     19652
  TCP    192.168.1.8:62834      sf-in-f188:5228        ESTABLISHED     5368
  TCP    192.168.1.8:63141      8:https                ESTABLISHED     5368

C:\WINDOWS\system32>
```

5.5)netstat -p protocol : Displays connection for the specified protocol. Here it shows connections or statistics for the mentioned protocol ie, TCP

```
C:\WINDOWS\system32>netstat -p tcp

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:65247        Ramya:65248            ESTABLISHED
  TCP    127.0.0.1:65248        Ramya:65247            ESTABLISHED
  TCP    127.0.0.1:65252        Ramya:65253            ESTABLISHED
  TCP    127.0.0.1:65253        Ramya:65252            ESTABLISHED
  TCP    192.168.1.8:49489      20.198.119.143:https   ESTABLISHED
  TCP    192.168.1.8:50838      bs:https               ESTABLISHED
  TCP    192.168.1.8:50923      151.101.130.137:https  ESTABLISHED
  TCP    192.168.1.8:50986      219:https              ESTABLISHED
  TCP    192.168.1.8:50990      13.107.21.200:https    ESTABLISHED
  TCP    192.168.1.8:50993      maa05s28-in-f5:https   ESTABLISHED
  TCP    192.168.1.8:50994      13.89.179.9:https      ESTABLISHED
  TCP    192.168.1.8:50997      204.79.197.239:https   ESTABLISHED
  TCP    192.168.1.8:50998      1drv:https             TIME_WAIT
  TCP    192.168.1.8:50999      20.189.173.10:https    TIME_WAIT
  TCP    192.168.1.8:51000      1drv:https             ESTABLISHED
  TCP    192.168.1.8:51001      20.189.173.10:https    ESTABLISHED
  TCP    192.168.1.8:62815      20.198.119.143:https   ESTABLISHED
  TCP    192.168.1.8:62834      sf-in-f188:5228        ESTABLISHED
  TCP    192.168.1.8:63141      8:https                TIME_WAIT

C:\WINDOWS\system32>
```

5.6) netstat-s: It show detailed statistics by protocol and by default it shows TCP,UDP,ICMP and IP Protocols.

```
C:\WINDOWS\system32>netstat -s

IPv4 Statistics

  Packets Received                   = 3401582
  Received Header Errors             = 0
  Received Address Errors            = 128674
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 0
  Received Packets Discarded         = 765861
  Received Packets Delivered         = 3274129
  Output Requests                    = 1285596
  Routing Discards                   = 0
  Discarded Output Packets           = 4194
  Output Packet No Route             = 126
  Reassembly Required                = 191
  Reassembly Successful              = 95
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 0
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 0

IPv6 Statistics

  Packets Received                   = 961727
  Received Header Errors             = 0
  Received Address Errors            = 115
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 0
  Received Packets Discarded         = 110359
  Received Packets Delivered         = 965978
  Output Requests                    = 7930
  Routing Discards                   = 0
  Discarded Output Packets           = 0
  Output Packet No Route             = 0
  Reassembly Required                = 0
  Reassembly Successful              = 0
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 0
  Datagrams Failing Fragmentation    = 0
```

```
TCP Statistics for IPv4

  Active Opens                       = 25215
  Passive Opens                      = 397
  Failed Connection Attempts         = 1077
  Reset Connections                  = 4748
  Current Connections                = 18
  Segments Received                  = 1201881
  Segments Sent                      = 1072718
  Segments Retransmitted             = 83829

TCP Statistics for IPv6

  Active Opens                       = 120
  Passive Opens                      = 4
  Failed Connection Attempts         = 116
  Reset Connections                  = 8
  Current Connections                = 0
  Segments Received                  = 1910
  Segments Sent                      = 1678
  Segments Retransmitted             = 232

UDP Statistics for IPv4

  Datagrams Received    = 2173420
  No Ports              = 80310
  Receive Errors        = 14
  Datagrams Sent        = 78707

UDP Statistics for IPv6

  Datagrams Received    = 1415031
  No Ports              = 349
  Receive Errors        = 0
  Datagrams Sent        = 3471

C:\WINDOWS\system32>
```

5.7)netstat -r :It displays the IP routing table contents or kernel routing information.

```
C:\WINDOWS\system32>netstat -r
===========================================================================
Interface List
 15...0a 00 27 00 00 0f ......VirtualBox Host-Only Ethernet Adapter
 17...f4 46 37 9f 81 d5 ......Microsoft Wi-Fi Direct Virtual Adapter
 13...f6 46 37 9f 81 d4 ......Microsoft Wi-Fi Direct Virtual Adapter #2
 10...f4 46 37 9f 81 d4 ......Intel(R) Wi-Fi 6 AX201 160MHz
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.1.1      192.168.1.8     40
        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
      192.168.1.0    255.255.255.0         On-link       192.168.1.8    296
      192.168.1.8  255.255.255.255         On-link       192.168.1.8    296
    192.168.1.255  255.255.255.255         On-link       192.168.1.8    296
     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       192.168.1.8    296
  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       192.168.1.8    296
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
 10    296 ::/0                     fe80::1
  1    331 ::1/128                  On-link
```

```
        224.0.0.0        240.0.0.0         On-link       192.168.1.8    296
  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       192.168.1.8    296
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
 10    296 ::/0                     fe80::1
  1    331 ::1/128                  On-link
 15    281 fe80::/64                On-link
 10    296 fe80::/64                On-link
 15    281 fe80::1598:825b:6d29:10c9/128
                                    On-link
 10    296 fe80::6cd2:6233:8920:83c0/128
                                    On-link
  1    331 ff00::/8                 On-link
 15    281 ff00::/8                 On-link
 10    296 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

5.8): netstat /?: It show details about the netstat command's several options.

```
C:\WINDOWS\system32>netstat /?

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-f] [-i] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [interval]

  -a            Displays all connections and listening ports.
  -b            Displays the executable involved in creating each connection or
                listening port. In some cases well-known executables host
                multiple independent components, and in these cases the
                sequence of components involved in creating the connection
                or listening port is displayed. In this case the executable
                name is in [] at the bottom, on top is the component it called,
                and so forth until TCP/IP was reached. Note that this option
                can be time-consuming and will fail unless you have sufficient
                permissions.
  -e            Displays Ethernet statistics. This may be combined with the -s
                option.
  -f            Displays Fully Qualified Domain Names (FQDN) for foreign
                addresses.
  -i            Displays the time spent by a TCP connection in its current state.
  -n            Displays addresses and port numbers in numerical form.
  -o            Displays the owning process ID associated with each connection.
  -p proto      Shows connections for the protocol specified by proto; proto
                may be any of: TCP, UDP, TCPv6, or UDPv6.  If used with the -s
                option to display per-protocol statistics, proto may be any of:
                IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
  -q            Displays all connections, listening ports, and bound
                nonlistening TCP ports. Bound nonlistening ports may or may not
                be associated with an active connection.
  -r            Displays the routing table.
  -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 default.
  -t            Displays the current connection offload state.
  -x            Displays NetworkDirect connections, listeners, and shared
                endpoints.
  -y            Displays the TCP connection template for all connections.
                Cannot be combined with the other options.
  interval      Redisplays selected statistics, pausing interval seconds
```

TASK 6: Displaying ARP cache using arp command

6)arp-a : It is used to find out the hardware (MAC) address of a device from an IP address.

```
C:\WINDOWS\system32>arp -a

Interface: 192.168.1.8 --- 0xa
  Internet Address      Physical Address      Type
  192.168.1.1           bc-62-d2-16-78-08     dynamic
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     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 --- 0xf
  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
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\WINDOWS\system32>
```

7)Gpresult: It displays the resulting set of policy settings that were enforced on the computer for the specified user when the user logged on.

```
C:\WINDOWS\system32>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.
```

8)netstat -ab:The b switch links each used port with its application. [Need more Clarity]

```
C:\WINDOWS\system32>netstat -ab

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            Ramya:0                LISTENING
  RpcEptMapper
 [svchost.exe]
  TCP    0.0.0.0:445            Ramya:0                LISTENING
 Can not obtain ownership information
  TCP    0.0.0.0:5040           Ramya:0                LISTENING
  CDPSvc
 [svchost.exe]
  TCP    0.0.0.0:6646           Ramya:0                LISTENING
 [MMSSHOST.EXE]
  TCP    0.0.0.0:49664          Ramya:0                LISTENING
 [lsass.exe]
  TCP    0.0.0.0:49665          Ramya:0                LISTENING
 Can not obtain ownership information
  TCP    0.0.0.0:49666          Ramya:0                LISTENING
  Schedule
 [svchost.exe]
  TCP    0.0.0.0:49667          Ramya:0                LISTENING
  EventLog
 [svchost.exe]
  TCP    0.0.0.0:49668          Ramya:0                LISTENING
 [spoolsv.exe]
  TCP    0.0.0.0:49670          Ramya:0                LISTENING
 [AsusLinkNear.exe]
  TCP    0.0.0.0:49671          Ramya:0                LISTENING
 [AsusLinkNear.exe]
  TCP    0.0.0.0:49672          Ramya:0                LISTENING
 Can not obtain ownership information
  TCP    127.0.0.1:65247        Ramya:65248            ESTABLISHED
 [MFEAvSvc.exe]
  TCP    127.0.0.1:65248        Ramya:65247            ESTABLISHED
 [MFEAvSvc.exe]
  TCP    127.0.0.1:65252        Ramya:65253            ESTABLISHED
 [MFEAvSvc.exe]
  TCP    127.0.0.1:65253        Ramya:65252            ESTABLISHED
```

9)netstat -an: It displays all the open ports

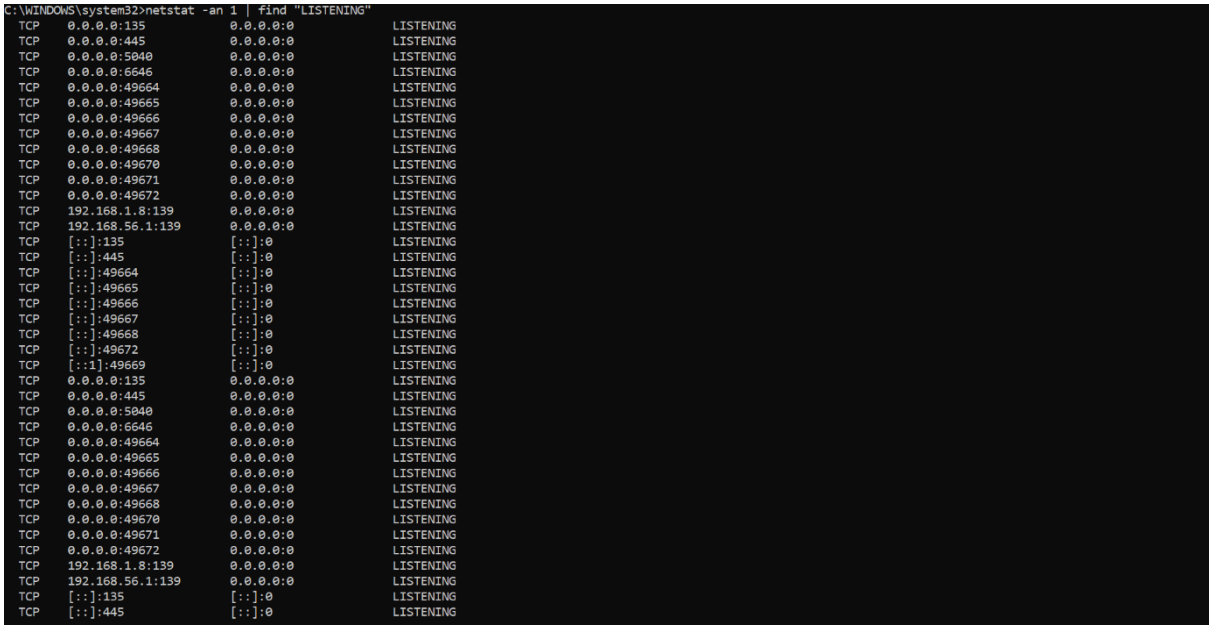
```
C:\WINDOWS\system32>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:6646           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49671          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49672          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:65247        127.0.0.1:65248        ESTABLISHED
  TCP    127.0.0.1:65248        127.0.0.1:65247        ESTABLISHED
  TCP    127.0.0.1:65252        127.0.0.1:65253        ESTABLISHED
  TCP    127.0.0.1:65253        127.0.0.1:65252        ESTABLISHED
  TCP    192.168.1.8:139        0.0.0.0:0              LISTENING
  TCP    192.168.1.8:49496      20.198.119.143:443     ESTABLISHED
  TCP    192.168.1.8:49498      20.198.119.143:443     ESTABLISHED
  TCP    192.168.1.8:61675      20.198.119.143:443     ESTABLISHED
  TCP    192.168.1.8:61685      142.250.182.138:443    CLOSE_WAIT
  TCP    192.168.1.8:61688      142.250.4.109:993      ESTABLISHED
  TCP    192.168.1.8:61705      13.69.116.104:443      ESTABLISHED
  TCP    192.168.1.8:61713      35.247.144.219:443     ESTABLISHED
  TCP    192.168.1.8:61722      13.107.21.239:443      ESTABLISHED
  TCP    192.168.1.8:61731      108.159.15.78:443      ESTABLISHED
  TCP    192.168.1.8:61739      3.227.190.204:443      ESTABLISHED
  TCP    192.168.1.8:61749      40.79.150.120:443      ESTABLISHED
  TCP    192.168.1.8:61761      20.120.124.64:443      ESTABLISHED
  TCP    192.168.1.8:61770      13.107.213.58:443      ESTABLISHED
  TCP    192.168.1.8:61774      117.18.232.200:443     ESTABLISHED
  TCP    192.168.1.8:61781      103.165.166.34:443     ESTABLISHED
  TCP    192.168.1.8:61783      40.99.31.130:443       ESTABLISHED
  TCP    192.168.1.8:61784      40.99.31.130:443       ESTABLISHED
  TCP    192.168.1.8:61785      13.107.21.200:443      ESTABLISHED
```

```
  UDP    0.0.0.0:56703          *:*
  UDP    127.0.0.1:1900         *:*
  UDP    127.0.0.1:55068        127.0.0.1:55068
  UDP    127.0.0.1:57351        *:*
  UDP    127.0.0.1:63814        127.0.0.1:63814
  UDP    192.168.1.8:137        *:*
  UDP    192.168.1.8:138        *:*
  UDP    192.168.1.8:1900       *:*
  UDP    192.168.1.8:57350      *:*
  UDP    192.168.56.1:137       *:*
  UDP    192.168.56.1:138       *:*
  UDP    192.168.56.1:1900      *:*
  UDP    192.168.56.1:57349     *:*
  UDP    [::]:500               *:*
  UDP    [::]:4500              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5353              *:*
  UDP    [::]:5355              *:*
  UDP    [::]:56703             *:*
  UDP    [::1]:1900             *:*
  UDP    [::1]:57348            *:*
  UDP    [fe80::1598:825b:6d29:10c9%15]:1900  *:*
  UDP    [fe80::1598:825b:6d29:10c9%15]:57346  *:*
  UDP    [fe80::6cd2:6233:8920:83c0%10]:1900  *:*
  UDP    [fe80::6cd2:6233:8920:83c0%10]:57347  *:*

C:\WINDOWS\system32>
```

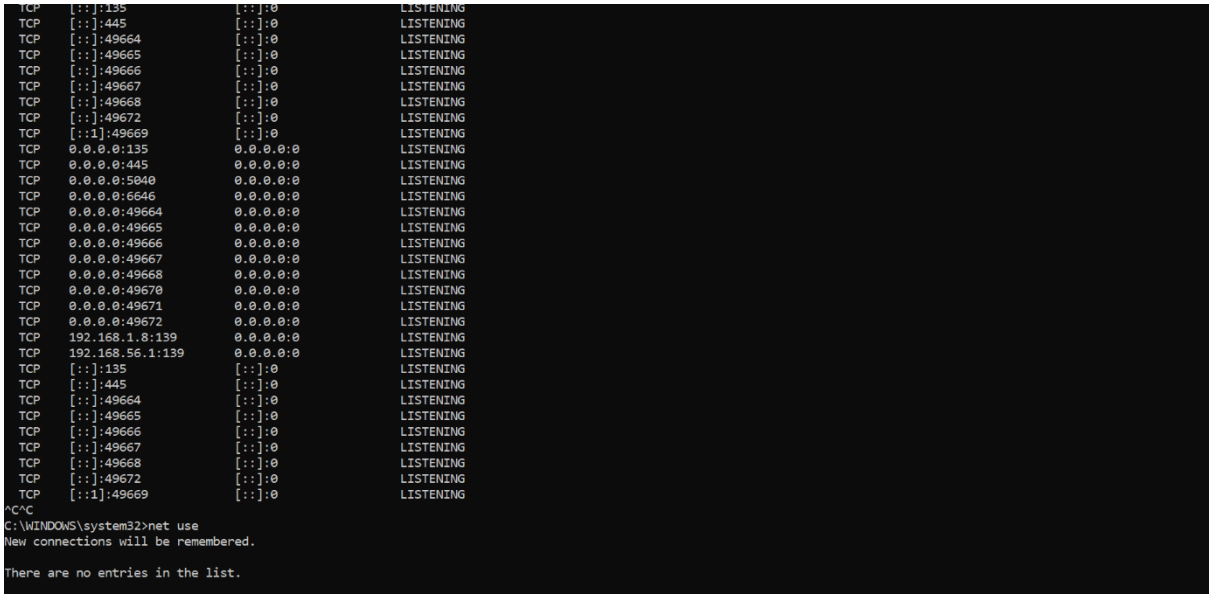
10)netstat -an 1|find ‘LineNo’: Here,It locates the line with number 153 and redisplays every second.

```
C:\WINDOWS\system32>netstat -an 1 | find "153"
  TCP    192.168.1.8:62153      52.98.123.210:443      ESTABLISHED
  TCP    192.168.1.8:62153      52.98.123.210:443      ESTABLISHED
  TCP    192.168.1.8:62153      52.98.123.210:443      ESTABLISHED
  TCP    192.168.1.8:62153      52.98.123.210:443      ESTABLISHED
  TCP    192.168.1.8:62153      52.98.123.210:443      ESTABLISHED
  TCP    192.168.1.8:62153      52.98.123.210:443      ESTABLISHED
  TCP    192.168.1.8:62153      52.98.123.210:443      ESTABLISHED
  TCP    192.168.1.8:62153      52.98.123.210:443      ESTABLISHED
  TCP    192.168.1.8:62153      52.98.123.210:443      ESTABLISHED
  TCP    192.168.1.8:62153      52.98.123.210:443      ESTABLISHED
  TCP    192.168.1.8:62153      52.98.123.210:443      ESTABLISHED
  TCP    192.168.1.8:62153      52.98.123.210:443      ESTABLISHED
  TCP    192.168.1.8:62153      52.98.123.210:443      ESTABLISHED
  TCP    192.168.1.8:62153      52.98.123.210:443      ESTABLISHED
  TCP    192.168.1.8:62153      52.98.123.210:443      ESTABLISHED
  TCP    192.168.1.8:62153      52.98.123.210:443      ESTABLISHED
  TCP    192.168.1.8:62153      52.98.123.210:443      ESTABLISHED
  TCP    192.168.1.8:62153      52.98.123.210:443      ESTABLISHED
  TCP    192.168.1.8:62153      52.98.123.210:443      TIME_WAIT
  TCP    192.168.1.8:62153      52.98.123.210:443      TIME_WAIT
  TCP    192.168.1.8:62153      52.98.123.210:443      TIME_WAIT
  TCP    192.168.1.8:62153      52.98.123.210:443      TIME_WAIT
  TCP    192.168.1.8:62153      52.98.123.210:443      TIME_WAIT
  TCP    192.168.1.8:62153      52.98.123.210:443      TIME_WAIT
  TCP    192.168.1.8:62153      52.98.123.210:443      TIME_WAIT
  TCP    192.168.1.8:62153      52.98.123.210:443      TIME_WAIT
  TCP    192.168.1.8:62153      52.98.123.210:443      TIME_WAIT
  TCP    192.168.1.8:62153      52.98.123.210:443      TIME_WAIT
  TCP    192.168.1.8:62153      52.98.123.210:443      TIME_WAIT
  TCP    192.168.1.8:62153      52.98.123.210:443      TIME_WAIT
  TCP    192.168.1.8:62153      52.98.123.210:443      TIME_WAIT
  TCP    192.168.1.8:62153      52.98.123.210:443      TIME_WAIT
  TCP    192.168.1.8:62153      52.98.123.210:443      TIME_WAIT
  TCP    192.168.1.8:62153      52.98.123.210:443      TIME_WAIT
  TCP    192.168.1.8:62153      52.98.123.210:443      TIME_WAIT
  TCP    192.168.1.8:62153      52.98.123.210:443      TIME_WAIT
  TCP    192.168.1.8:62153      52.98.123.210:443      TIME_WAIT
  TCP    192.168.1.8:62153      52.98.123.210:443      TIME_WAIT
```

11)netstat -an 1|find “status” :It displays all the open ports with Listening status.



```
C:\WINDOWS\system32>netstat -an 1 | find "LISTENING"
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:6646           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49671          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49672          0.0.0.0:0              LISTENING
  TCP    192.168.1.8:139        0.0.0.0:0              LISTENING
  TCP    192.168.56.1:139       0.0.0.0:0              LISTENING
  TCP    [::]:135               [::]:0                 LISTENING
  TCP    [::]:445               [::]:0                 LISTENING
  TCP    [::]:49664             [::]:0                 LISTENING
  TCP    [::]:49665             [::]:0                 LISTENING
  TCP    [::]:49666             [::]:0                 LISTENING
  TCP    [::]:49667             [::]:0                 LISTENING
  TCP    [::]:49668             [::]:0                 LISTENING
  TCP    [::]:49672             [::]:0                 LISTENING
  TCP    [::1]:49669            [::]:0                 LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:6646           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49671          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49672          0.0.0.0:0              LISTENING
  TCP    192.168.1.8:139        0.0.0.0:0              LISTENING
  TCP    192.168.56.1:139       0.0.0.0:0              LISTENING
  TCP    [::]:135               [::]:0                 LISTENING
  TCP    [::]:445               [::]:0                 LISTENING
```



```
  TCP    [::]:135               [::]:0                 LISTENING
  TCP    [::]:445               [::]:0                 LISTENING
  TCP    [::]:49664             [::]:0                 LISTENING
  TCP    [::]:49665             [::]:0                 LISTENING
  TCP    [::]:49666             [::]:0                 LISTENING
  TCP    [::]:49667             [::]:0                 LISTENING
  TCP    [::]:49668             [::]:0                 LISTENING
  TCP    [::]:49672             [::]:0                 LISTENING
  TCP    [::1]:49669            [::]:0                 LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:6646           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49671          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49672          0.0.0.0:0              LISTENING
  TCP    192.168.1.8:139        0.0.0.0:0              LISTENING
  TCP    192.168.56.1:139       0.0.0.0:0              LISTENING
  TCP    [::]:135               [::]:0                 LISTENING
  TCP    [::]:445               [::]:0                 LISTENING
  TCP    [::]:49664             [::]:0                 LISTENING
  TCP    [::]:49665             [::]:0                 LISTENING
  TCP    [::]:49666             [::]:0                 LISTENING
  TCP    [::]:49667             [::]:0                 LISTENING
  TCP    [::]:49668             [::]:0                 LISTENING
  TCP    [::]:49672             [::]:0                 LISTENING
  TCP    [::1]:49669            [::]:0                 LISTENING
^C^C
C:\WINDOWS\system32>net use
New connections will be remembered.

There are no entries in the list.
```

12)net user: It displays user accounts on a computer

```
C:\WINDOWS\system32>net user

User accounts for \\RAMYA

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
moona                    WDAGUtilityAccount
The command completed successfully.


C:\WINDOWS\system32>
```

13)ping -a ‘IP Address’: Resolves IP address to hostnames

```
C:\WINDOWS\system32>ping -a 192.168.56.1

Pinging Ramya [192.168.56.1] with 32 bytes of data:
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.56.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\WINDOWS\system32>
```

14)ping -t ‘IP Address’:Pings host until stopped.

```
C:\WINDOWS\system32>ping -t 192.168.56.1

Pinging 192.168.56.1 with 32 bytes of data:
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
```

```
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.56.1:
    Packets: Sent = 57, Received = 57, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\WINDOWS\system32>
```

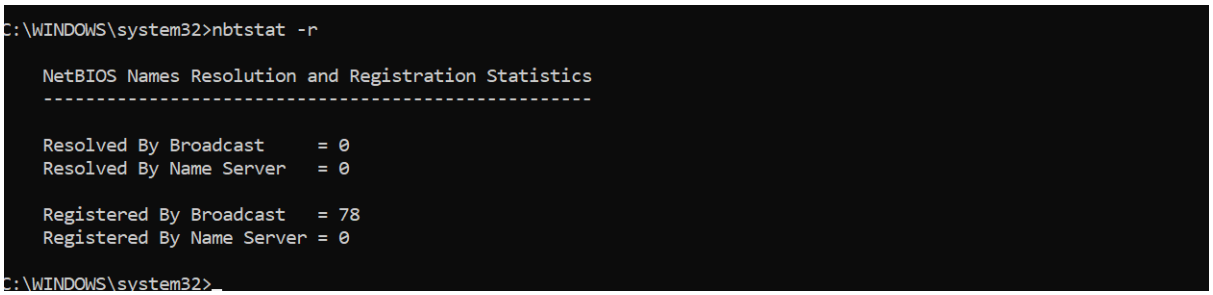
15)pathping: Displays route and ping information

```
C:\WINDOWS\system32>pathping

Usage: pathping [-g host-list] [-h maximum_hops] [-i address] [-n]
                [-p period] [-q num_queries] [-w timeout]
                [-4] [-6] target_name

Options:
    -g host-list     Loose source route along host-list.
    -h maximum_hops  Maximum number of hops to search for target.
    -i address       Use the specified source address.
    -n               Do not resolve addresses to hostnames.
    -p period        Wait period milliseconds between pings.
    -q num_queries   Number of queries per hop.
    -w timeout       Wait timeout milliseconds for each reply.
    -4               Force using IPv4.
    -6               Force using IPv6.

C:\WINDOWS\system32>
```

16)set U: Shows which user is logged on and other user information like User domain, Username and User profile.

17)set L: Displays the logon server

18)nbtstat -r: List names resolved by broadcast and via wins



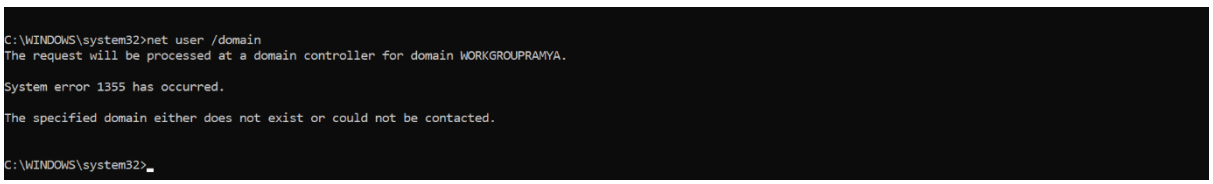
19)net use: Retrieves a list of network connections.

For the below example, there is no list of domains, computers, or resources that are being shared by the computer hence it shows “There are no entries in the list”

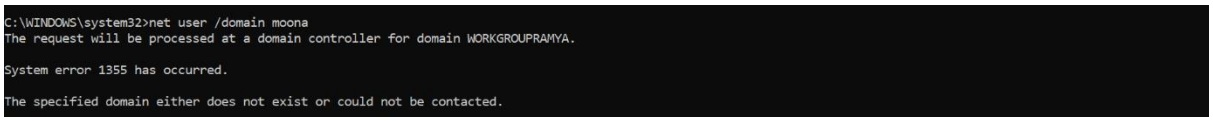
20)net view: It displays the computers in the current domain or network.

For the below ss, there are no shared computers in this network so it says that the list of servers for the workgroup is not currently available.

21)net user/domain[Need more clarity]



22)net user /domain <username>[Need more clarity]



23)net group /domain[Need more clarity]

```
C:\WINDOWS\system32>net group /domain
The request will be processed at a domain controller for domain WORKGROUPRAMYA.

System error 1355 has occurred.

The specified domain either does not exist or could not be contacted.
```

24)net view /domain: Specifies computer available in a specific domain.For the below ss, there are no shared computers in this network so it says that the list of servers for the workgroup is not currently available.

```
C:\WINDOWS\system32>net view /domain
System error 6118 has occurred.

The list of servers for this workgroup is not currently available


C:\WINDOWS\system32>
```

25)net view /cache: Displays the offline client cache settings for resources on the specified computer

net view /domain:<DomainName> | More:It shows user accounts from specific domain.

For the below ss, there are no shared computers in this network so it says that the list of servers for the workgroup is not currently available.

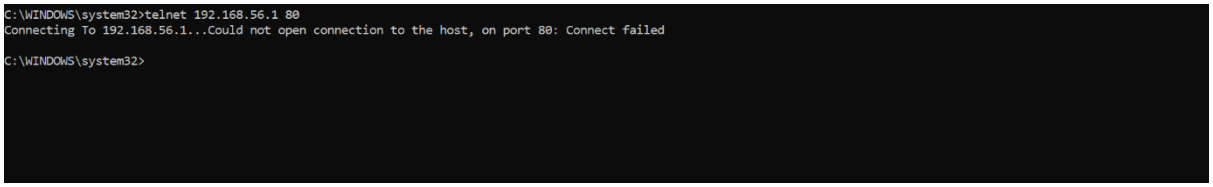
```
C:\WINDOWS\system32>net view /cache
System error 6118 has occurred.

The list of servers for this workgroup is not currently available


C:\WINDOWS\system32>echo %userdomain%
RAMYA

C:\WINDOWS\system32>wmic computersystem get domain
Domain
WORKGROUPRAMYA


C:\WINDOWS\system32>systeminfo | findstr /B /C:"Domain
Domain:                   WORKGROUPRAMYA

C:\WINDOWS\system32>net view /domain:WORKGROUPRAMYA | more
System error 6118 has occurred.

The list of servers for this workgroup is not currently available
```

26)nbtstat -n: Lists out locally registered NetBios names

```
C:\WINDOWS\system32>nbtstat -n

VirtualBox Host-Only Network:
Node IpAddress: [192.168.56.1] Scope Id: []

               NetBIOS Local Name Table

       Name               Type         Status
    ---------------------------------------------
    RAMYA          <20>  UNIQUE      Registered
    RAMYA          <00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered

Wi-Fi:
Node IpAddress: [192.168.1.8] Scope Id: []

               NetBIOS Local Name Table

       Name               Type         Status
    ---------------------------------------------
    RAMYA          <20>  UNIQUE      Registered
    RAMYA          <00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered

Local Area Connection* 1:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache

Local Area Connection* 2:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache
```

27)nbtstat -R: Purges the contents of the NetBIOS name cache and then reloads.

28)telnet <IP><Port>: It confirms whether a port is open or not.



Result

Learned and used basic Windows command line utilities to perform troubleshooting in the network.