21CY681– Internet Protocol lab

Name: B.Shebu

Register Number : CYS22005

Title: Network Administration and Troubleshooting Using Windows Command Line Utilities.

Date of Assignment provided: 26/09/2022

Aim: To study more various Windows command-line utilities to perform troubleshooting in the network.

Tools Required: Command Prompt with administrative privileges,

Procedure :

1. **ipconfig** – This command displays all the ip configuration details of the system

```
C:\Users\shebu> ipconfig

Windows IP Configuration


Unknown adapter Local Area Connection:

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

Ethernet adapter Ethernet:

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

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4ff:3f85:f619:a2d3%16
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

Ipconfig /all – Displays full TCP/IP configuration for all the adapters

```
C:\Users\shebu>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : shebu
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Unknown
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : amritanet.edu

Unknown adapter Local Area Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : TAP-Windows Adapter V9 for OpenVPN Connect
   Physical Address. . . . . . . . . : 00-FF-F7-92-B8-D2
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : amritanet.edu
   Description . . . . . . . . . . . : Realtek Gaming GbE Family Controller
   Physical Address. . . . . . . . . : 9C-7B-EF-1F-50-CF
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```

Ipconfig /renew [adapter_name] – This parameter renews an IPv4 address. For IPv6 we need to specify /renew6.

```
C:\Users\shebu>ipconfig /release Wi-Fi

Windows IP Configuration


Unknown adapter Local Area Connection:

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

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : amritanet.edu
```

Ipconfig /release - The /release parameter sends a request to the DHCP server to abandon the active lease(s) and removes it (or them) from your system.

```
C:\Windows\System32>ipconfig /release Wi-Fi

Windows IP Configuration


Unknown adapter Local Area Connection:

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

Ethernet adapter Ethernet:

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

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::2059:c484:1167:b78%17
   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  . :
```

Ipconfig /flushdns - The /flushdns parameter will flush the DNS resolver cache. This can be useful when you are troubleshooting or when you want to get rid of defective or obsolete DNS records. The cache will be repopulated as you browse the Internet or during normal system activity.

```
C:\Windows\System32>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

Ipconfig /displaydns – This command displays the DNS resolver cache of your system.

```
safebrowsing.googleapis.com
----------------------------------------
Record Name . . . . . : safebrowsing.googleapis.com
Record Type . . . . . : 1
Time To Live  . . . . : 189
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 142.250.77.106


ml314.com
----------------------------------------
Record Name . . . . . : ml314.com
Record Type . . . . . : 1
Time To Live  . . . . : 100
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 34.111.234.236
```

Ipconfig /registerdns – It refreshes all DHCP leases and re-registers DNS names for all your system's network adapters. It might take some time for this to happen. It helps to resolve problems between your system and the DNS server.

```
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 report
ed in the Event Viewer in 15 minutes.
```

ipconfig /showclassid <ADAPTER> - The /showclassid parameter will display the DHCP class ID for a specified adapter.

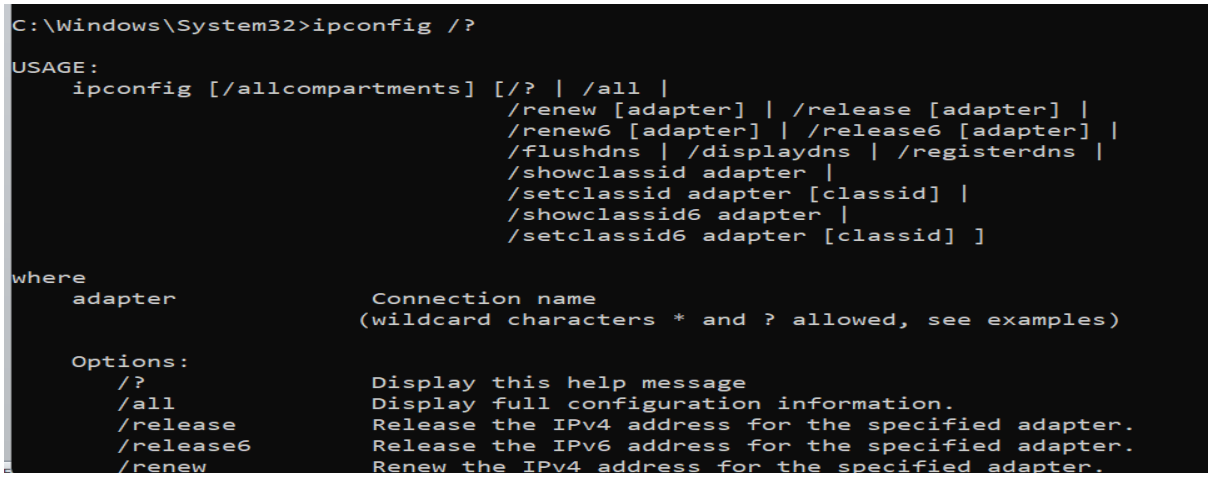
```
C:\Windows\System32>ipconfig /showclassid Wi-Fi

Windows IP Configuration

There are no DHCPv4 classes defined for Wi-Fi.
```

NOTE – Here it shows an error that there is no dhcp classes defined for wifi

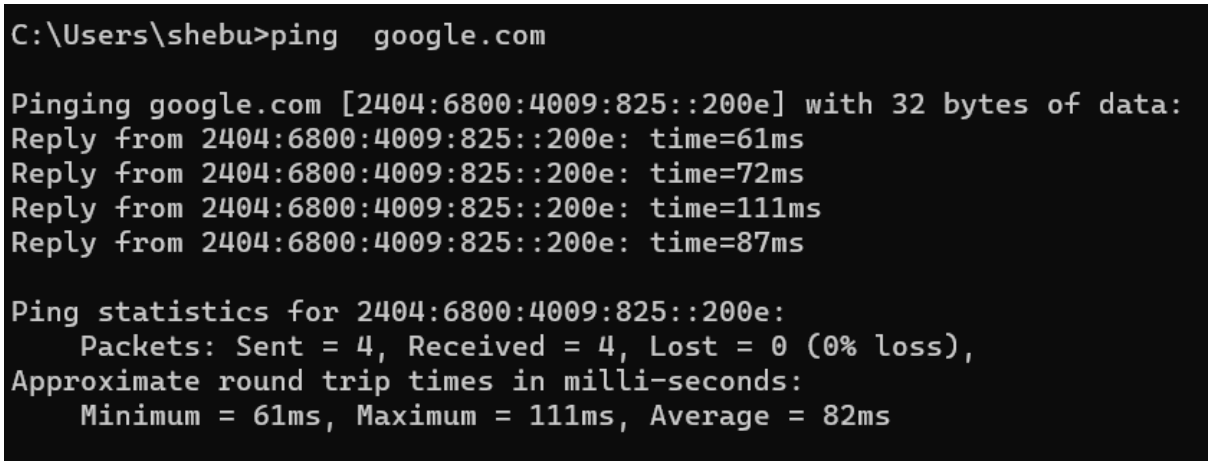
ipconfig /setclassid [classid] - The /setclassid parameter lets you assign a class ID to one or more of your system's adapters.

Note - Since /showclassid parameter tells there is no dhcp classes defined this command does not work

ipconfig /? - The /? parameter displays all available commands and tips on how to use it.



2. **ping google.com**



Ping –n count google.com

```
C:\Users\shebu>ping -n 4 google.com

Pinging google.com [2404:6800:4007:819::200e] with 32 bytes of data:
Reply from 2404:6800:4007:819::200e: time=223ms
Reply from 2404:6800:4007:819::200e: time=60ms
Reply from 2404:6800:4007:819::200e: time=76ms
Reply from 2404:6800:4007:819::200e: time=64ms

Ping statistics for 2404:6800:4007:819::200e:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 60ms, Maximum = 223ms, Average = 105ms
```

Ping –w timeout

```
C:\Users\shebu>ping -w 5 google.com

Pinging google.com [2404:6800:4009:825::200e] with 32 bytes of data:
Reply from 2404:6800:4009:825::200e: time=76ms
Reply from 2404:6800:4009:825::200e: time=191ms
Reply from 2404:6800:4009:825::200e: time=96ms
Reply from 2404:6800:4009:825::200e: time=177ms

Ping statistics for 2404:6800:4009:825::200e:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 76ms, Maximum = 191ms, Average = 135ms
```

Ping –l size – This command is used to send buffer size of the packet

```
C:\Windows\System32>ping -l 1000 8.8.8.8

Pinging 8.8.8.8 with 1000 bytes of data:
Reply from 8.8.8.8: bytes=68 (sent 1000) time=365ms TTL=53
Reply from 8.8.8.8: bytes=68 (sent 1000) time=353ms TTL=53
Reply from 8.8.8.8: bytes=68 (sent 1000) time=363ms TTL=53
Reply from 8.8.8.8: bytes=68 (sent 1000) time=173ms TTL=53

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 173ms, Maximum = 365ms, Average = 313ms
```

NOTE - Here we send the buffer size as 1000

Ping –f – It sets DON’T-FRAMENT flag in packet

```
C:\Windows\System32>ping -f google.com

Pinging google.com [172.217.166.46] with 32 bytes of data:
Reply from 172.217.166.46: bytes=32 time=233ms TTL=53
Reply from 172.217.166.46: bytes=32 time=101ms TTL=53
Reply from 172.217.166.46: bytes=32 time=96ms TTL=53
Reply from 172.217.166.46: bytes=32 time=97ms TTL=53

Ping statistics for 172.217.166.46:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 96ms, Maximum = 233ms, Average = 131ms
```

3. **tracert**

```
C:\Users\shebu>tracert facebook.com

Tracing route to facebook.com [2a03:2880:f12f:183:face:b00c:0:25de]
over a maximum of 30 hops:

  1     3 ms     3 ms     3 ms  2409:4072:6d80:1829::71
  2     *        *        *     Request timed out.
  3    81 ms    30 ms    38 ms  2405:200:369:eeee:20::744
  4    38 ms    35 ms    36 ms  2405:200:801:2300::52c
  5    69 ms    33 ms    34 ms  2405:200:801:2300::529
  6    51 ms    35 ms    35 ms  2405:200:801:2300::499
  7   113 ms    91 ms    75 ms  ae5.pr02.bom1.tfbnw.net [2620:0:1cff:dead:beee::6a]
  8    76 ms    68 ms    64 ms  ae5.pr02.bom1.tfbnw.net [2620:0:1cff:dead:beee::6a]
  9    75 ms    53 ms    62 ms  po102.psw03.bom1.tfbnw.net [2620:0:1cff:dead:bef0::17f]
 10    70 ms    75 ms    75 ms  po3.msw1av.02.bom1.tfbnw.net [2a03:2880:f02f:ffff::293]
 11    85 ms    76 ms    81 ms  edge-star-mini6-shv-02-bom1.facebook.com [2a03:2880:f12f:183:face:b00c:0:25de]

Trace complete.
```

4. **nslookup google.com**

```
C:\Users\shebu>nslookup google.com
Server:  UnKnown
Address:  192.168.119.43

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4009:823::200e
          142.250.182.14
```

nslookup –type=[name server] google.com

```
C:\Users\shebu>nslookup -type=soa google.com
Server:  UnKnown
Address:  192.168.119.43

Non-authoritative answer:
google.com
        primary name server = ns1.google.com
        responsible mail addr = dns-admin.google.com
        serial  = 477406428
        refresh = 900 (15 mins)
        retry   = 900 (15 mins)
        expire  = 1800 (30 mins)
        default TTL = 60 (1 min)
```

5. **netstat** - The **netstat** command displays the contents of various network-related data for active connections.

```
C:\Users\shebu>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:56105        checkhost:65001        ESTABLISHED
  TCP    127.0.0.1:65001        checkhost:56105        ESTABLISHED
  TCP    192.168.119.150:56476  20.198.118.190:https   ESTABLISHED
  TCP    192.168.119.150:56479  20.198.118.190:https   ESTABLISHED
  TCP    192.168.119.150:56499  stackoverflow:https    ESTABLISHED
  TCP    [2409:4072:6d80:1829:ac7b:9f9d:d20f:5e93]:56478  whatsapp-cdn6-shv-01-tir2:https  ESTABLISHED
  TCP    [2409:4072:6d80:1829:ac7b:9f9d:d20f:5e93]:56485  sa-in-xbc:5228         ESTABLISHED
  TCP    [2409:4072:6d80:1829:ac7b:9f9d:d20f:5e93]:56561  maa03s26-in-x04:https  ESTABLISHED
  TCP    [2409:4072:6d80:1829:ac7b:9f9d:d20f:5e93]:65386  maa03s38-in-x0e:https  ESTABLISHED
  TCP    [2409:4072:6d80:1829:ac7b:9f9d:d20f:5e93]:65391  bom12s18-in-x03:https  ESTABLISHED
  TCP    [2409:4072:6d80:1829:ac7b:9f9d:d20f:5e93]:65392  maa03s42-in-x0e:https  ESTABLISHED
```

netstat –a - The **netstat -a** command shows the state of all sockets.

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

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            shebu:0                LISTENING
  TCP    0.0.0.0:445            shebu:0                LISTENING
  TCP    0.0.0.0:903            shebu:0                LISTENING
  TCP    0.0.0.0:913            shebu:0                LISTENING
  TCP    0.0.0.0:5040           shebu:0                LISTENING
  TCP    0.0.0.0:5357           shebu:0                LISTENING
  TCP    0.0.0.0:8733           shebu:0                LISTENING
  TCP    0.0.0.0:49664          shebu:0                LISTENING
  TCP    0.0.0.0:49665          shebu:0                LISTENING
  TCP    0.0.0.0:49666          shebu:0                LISTENING
  TCP    0.0.0.0:49667          shebu:0                LISTENING
  TCP    0.0.0.0:49668          shebu:0                LISTENING
  TCP    0.0.0.0:49670          shebu:0                LISTENING
  TCP    127.0.0.1:55215        shebu:0                LISTENING
  TCP    127.0.0.1:56105        checkhost:65001        ESTABLISHED
  TCP    127.0.0.1:65001        shebu:0                LISTENING
  TCP    127.0.0.1:65001        checkhost:56105        ESTABLISHED
  TCP    169.254.166.209:139    shebu:0                LISTENING
  TCP    169.254.200.239:139    shebu:0                LISTENING
  TCP    172.22.160.1:139       shebu:0                LISTENING
  TCP    192.168.56.1:139       shebu:0                LISTENING
  TCP    192.168.119.150:139    shebu:0                LISTENING
  TCP    192.168.119.150:56476  20.198.118.190:https   ESTABLISHED
```

netstat –e – It displays Ethernet statistics

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

                           Received            Sent

Bytes                     279055809       134580766
Unicast packets              338617          190472
Non-unicast packets            4502          123258
Discards                          0               0
Errors                            0               0
Unknown protocols                 0
```

netstat –n – It displays addresses and port numbers in numerical form.

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

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:56105        127.0.0.1:65001        ESTABLISHED
  TCP    127.0.0.1:65001        127.0.0.1:56105        ESTABLISHED
  TCP    192.168.119.150:56476  20.198.118.190:443     ESTABLISHED
  TCP    192.168.119.150:56479  20.198.118.190:443     ESTABLISHED
  TCP    192.168.119.150:56499  198.252.206.25:443     ESTABLISHED
  TCP    192.168.119.150:65503  108.159.10.64:443      ESTABLISHED
  TCP    192.168.119.150:65504  3.220.9.191:443        ESTABLISHED
  TCP    [2409:4072:6d80:1829:ac7b:9f9d:d20f:5e93]:56478  [2a03:2880:f268:c1:face:b00c:0:167]:443  ESTABLISHED
  TCP    [2409:4072:6d80:1829:ac7b:9f9d:d20f:5e93]:56485  [2404:6800:4003:c00::bc]:5228  ESTABLISHED
  TCP    [2409:4072:6d80:1829:ac7b:9f9d:d20f:5e93]:65485  [2404:6800:4009:800::200e]:443  ESTABLISHED
  TCP    [2409:4072:6d80:1829:ac7b:9f9d:d20f:5e93]:65488  [2404:6800:4009:804::200e]:443  ESTABLISHED
  TCP    [2409:4072:6d80:1829:ac7b:9f9d:d20f:5e93]:65492  [2404:6800:4007:811::200a]:443  TIME_WAIT
  TCP    [2409:4072:6d80:1829:ac7b:9f9d:d20f:5e93]:65496  [2404:6800:4007:825::2003]:443  TIME_WAIT
  TCP    [2409:4072:6d80:1829:ac7b:9f9d:d20f:5e93]:65497  [2404:6800:4007:82a::2004]:443  ESTABLISHED
  TCP    [2409:4072:6d80:1829:ac7b:9f9d:d20f:5e93]:65498  [2620:1ec:12::239]:443  ESTABLISHED
  TCP    [2409:4072:6d80:1829:ac7b:9f9d:d20f:5e93]:65502  [2404:6800:4009:822::200e]:443  ESTABLISHED
```

netstat –o – This displays the process ID associated with each connection.

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

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    127.0.0.1:56105        checkhost:65001        ESTABLISHED     5460
  TCP    127.0.0.1:65001        checkhost:56105        ESTABLISHED     5460
  TCP    192.168.119.150:56476  20.198.118.190:https   ESTABLISHED     10292
  TCP    192.168.119.150:56479  20.198.118.190:https   ESTABLISHED     6020
  TCP    192.168.119.150:56499  stackoverflow:https    ESTABLISHED     9924
  TCP    192.168.119.150:65503  server-108-159-10-64:https  ESTABLISHED     9924
  TCP    192.168.119.150:65504  ec2-3-220-9-191:https  ESTABLISHED     9924
  TCP    [2409:4072:6d80:1829:ac7b:9f9d:d20f:5e93]:56478  whatsapp-cdn6-shv-01-tir2:https  ESTABLISHED     9924
  TCP    [2409:4072:6d80:1829:ac7b:9f9d:d20f:5e93]:56485  sa-in-xbc:5228         ESTABLISHED     9924
  TCP    [2409:4072:6d80:1829:ac7b:9f9d:d20f:5e93]:65485  bom07s15-in-x0e:https  ESTABLISHED     9924
  TCP    [2409:4072:6d80:1829:ac7b:9f9d:d20f:5e93]:65488  bom12s04-in-x0e:https  TIME_WAIT       0
  TCP    [2409:4072:6d80:1829:ac7b:9f9d:d20f:5e93]:65496  maa03s40-in-x03:https  TIME_WAIT       0
  TCP    [2409:4072:6d80:1829:ac7b:9f9d:d20f:5e93]:65497  maa03s45-in-x04:https  ESTABLISHED     9924
  TCP    [2409:4072:6d80:1829:ac7b:9f9d:d20f:5e93]:65502  bom12s12-in-x0e:https  ESTABLISHED     9924
  TCP    [2409:4072:6d80:1829:ac7b:9f9d:d20f:5e93]:65506  bom05s12-in-x03:https  ESTABLISHED     9924
  TCP    [2409:4072:6d80:1829:ac7b:9f9d:d20f:5e93]:65507  bom05s12-in-x03:https  ESTABLISHED     9924
  TCP    [2409:4072:6d80:1829:ac7b:9f9d:d20f:5e93]:65508  bom07s28-in-x0e:https  ESTABLISHED     9924
```

netstat –p - The netstat –p command shows the statistics about the value specified for te protocol (udp,tcp,sctp,ip,icmp)

```
C:\Windows\System32>netstat -p tcp

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49674        checkhost:65001        ESTABLISHED
  TCP    127.0.0.1:50393        checkhost:50394        ESTABLISHED
  TCP    127.0.0.1:50394        checkhost:50393        ESTABLISHED
  TCP    127.0.0.1:50408        checkhost:50409        ESTABLISHED
  TCP    127.0.0.1:50409        checkhost:50408        ESTABLISHED
  TCP    127.0.0.1:65001        checkhost:49674        ESTABLISHED
  TCP    192.168.160.150:49695  20.198.118.190:https   ESTABLISHED
  TCP    192.168.160.150:49735  20.198.118.190:https   ESTABLISHED
```

netstat –s - This command displays statistics of each proocol.

```
C:\Windows\System32>netstat -s

IPv4 Statistics

  Packets Received                    = 15213
  Received Header Errors              = 0
  Received Address Errors             = 0
  Datagrams Forwarded                 = 0
  Unknown Protocols Received          = 0
  Received Packets Discarded          = 71
  Received Packets Delivered          = 16769
  Output Requests                     = 18980
  Routing Discards                    = 0
  Discarded Output Packets            = 0
  Output Packet No Route              = 49
  Reassembly Required                 = 0
  Reassembly Successful               = 0
  Reassembly Failures                 = 0
  Datagrams Successfully Fragmented   = 0
  Datagrams Failing Fragmentation     = 0
  Fragments Created                   = 0

IPv6 Statistics

  Packets Received                    = 40933
  Received Header Errors              = 0
```

netstat –r – This command displays the entire routing table

```
C:\Windows\System32>netstat -r
===========================================================================
Interface List
 23...00 ff f7 92 b8 d2 ......TAP-Windows Adapter V9 for OpenVPN Connect
 13...9c 7b ef 1f 50 cf ......Realtek Gaming GbE Family Controller
 17...0a 00 27 00 00 11 ......VirtualBox Host-Only Ethernet Adapter
 18...3c f0 11 18 a1 a1 ......Microsoft Wi-Fi Direct Virtual Adapter
 12...3e f0 11 18 a1 a0 ......Microsoft Wi-Fi Direct Virtual Adapter #2
 15...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
 16...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
 10...3c f0 11 18 a1 a0 ......Intel(R) Wireless-AC 9560 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  192.168.160.254  192.168.160.150      35
        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
      169.254.0.0      255.255.0.0         On-link   169.254.200.239     291
      169.254.0.0      255.255.0.0         On-link   169.254.166.209     291
  169.254.166.209  255.255.255.255         On-link   169.254.166.209     291
  169.254.200.239  255.255.255.255         On-link   169.254.200.239     291
  169.254.255.255  255.255.255.255         On-link   169.254.200.239     291
```

netstat interval [EG -netstat –n 5] - Redisplays selected statistics for specified interval seconds between each display.

NOTE - Press ctrl+c to stop redisplaying the statistics

```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49674        127.0.0.1:65001        ESTABLISHED
  TCP    127.0.0.1:50393        127.0.0.1:50394        ESTABLISHED
  TCP    127.0.0.1:50394        127.0.0.1:50393        ESTABLISHED
  TCP    127.0.0.1:50408        127.0.0.1:50409        ESTABLISHED
  TCP    127.0.0.1:50409        127.0.0.1:50408        ESTABLISHED
  TCP    127.0.0.1:65001        127.0.0.1:49674        ESTABLISHED
  TCP    192.168.160.150:49695  20.198.118.190:443     ESTABLISHED
  TCP    192.168.160.150:49735  20.198.118.190:443     ESTABLISHED
  TCP    192.168.160.150:49919  117.18.237.29:80       CLOSE_WAIT
  TCP    192.168.160.150:58248  162.125.19.131:443     ESTABLISHED
  TCP    192.168.160.150:58256  162.125.36.2:443       ESTABLISHED
  TCP    192.168.160.150:58265  108.159.10.72:443      ESTABLISHED
  TCP    192.168.160.150:58276  151.101.158.114:443    ESTABLISHED
  TCP    192.168.160.150:58281  8.241.132.122:443      ESTABLISHED
  TCP    192.168.160.150:58283  8.241.132.122:443      ESTABLISHED
```

netstat /? – Displays help command which includes decriptions of each flag that can be used.

```
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
```

6. **arp –a**

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

Interface: 10.11.136.109 --- 0x9
  Internet Address      Physical Address      Type
  10.11.128.1           00-00-5e-00-01-fe     dynamic
  10.11.128.11          44-31-92-56-07-97     dynamic
  10.11.129.81          30-d1-6b-e9-7f-9b     dynamic
  10.11.129.95          10-6f-d9-ba-92-0b     dynamic
  10.11.131.76          58-00-e3-ac-da-6f     dynamic
  10.11.131.187         9c-fc-e8-69-d7-7d     dynamic
  10.11.131.237         80-45-dd-c1-50-75     dynamic
  10.11.132.28          90-e8-68-d4-67-d5     dynamic
  10.11.132.206         d0-ab-d5-a6-eb-4a     dynamic
  10.11.132.209         84-3a-4b-ad-52-7e     dynamic
  10.11.133.9           f8-89-d2-85-aa-53     dynamic
  10.11.133.57          b0-52-16-0b-2c-bf     dynamic
  10.11.133.81          3c-a0-67-a1-f4-c3     dynamic
  10.11.136.9           44-e5-17-f8-6d-cb     dynamic
  10.11.136.124         ec-2e-98-ba-62-0d     dynamic
  10.11.139.132         28-56-5a-87-44-55     dynamic
  10.11.139.236         98-8d-46-a0-44-9d     dynamic
  10.11.159.255         ff-ff-ff-ff-ff-ff     static
  10.12.37.110          34-c9-3d-86-65-55     dynamic
  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
```

7. **Gpresult** – It is a tool displays the Resultant Set of Policy (RSoP) information for a target user and computer.

```
C:\Windows\System32>Gpresult /R

Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.
© Microsoft Corporation. All rights reserved.

Created on  01- 10- 2022 at 16:59:30


RSOP data for SHEBU\shebu on SHEBU : Logging Mode
-------------------------------------------------

OS Configuration:            Standalone Workstation
OS Version:                  10.0.22622
Site Name:                   N/A
Roaming Profile:             N/A
Local Profile:               C:\Users\shebu
Connected over a slow link?: No


COMPUTER SETTINGS
------------------

    Last time Group Policy was applied: 01-10-2022 at 12:30:49
    Group Policy was applied from:      N/A
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        SHEBU
    Domain Type:                        <Local Computer>

    Applied Group Policy Objects
```

8. **ipconfig /flushdns** – This command flushes the DNS entries ie. clear any IP addresses or other DNS records from te system cache

```
C:\Windows\System32>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

9. **nbtstat –a [remotemachine_ip]** – This command shows the NETBIOS name table of the remote computer

```
C:\Windows\System32>nbtstat -a 2409:4072:6e0d:dbc:b5ba:8683:8764:52a9

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

    Host not found.

VMware Network Adapter VMnet1:
Node IpAddress: [169.254.200.239] Scope Id: []

    Host not found.

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

    Host not found.

VMware Network Adapter VMnet8:
Node IpAddress: [169.254.166.209] Scope Id: []
```

10. **nbtstat –R** This command reloads the remote cache name table

```
C:\Windows\System32>nbtstat -R
    Successful purge and preload of the NBT Remote Cache Name Table.
```

11. **nbtstat –n** - This command lists the local netbios names

```
C:\Windows\System32>nbtstat -n

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

    No names in cache

VMware Network Adapter VMnet1:
Node IpAddress: [169.254.200.239] Scope Id: []

                NetBIOS Local Name Table

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

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

12. **nbtstat –r** – This command lists the names resolved by WINS(**Windows Internet Name Service**)

```
C:\Windows\System32>nbtstat -r

    NetBIOS Names Resolution and Registration Statistics
    ----------------------------------------------------

    Resolved By Broadcast     = 0
    Resolved By Name Server   = 0

    Registered By Broadcast   = 12
    Registered By Name Server = 0
```

13. **nbtstat /ab - /a displays all the connection and listening ports where as /b displays all the executables involved in creating a connection**

```
C:\Windows\System32>netstat /ab

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            shebu:0                LISTENING
  RpcEptMapper
 [svchost.exe]
  TCP    0.0.0.0:445            shebu:0                LISTENING
 Can not obtain ownership information
  TCP    0.0.0.0:903            shebu:0                LISTENING
 [vmware-authd.exe]
  TCP    0.0.0.0:913            shebu:0                LISTENING
 [vmware-authd.exe]
  TCP    0.0.0.0:5040           shebu:0                LISTENING
```

14. **nbtstat –an** : Displays the NetBIOS name table of a remote computer . “-n” Displays the NetBIOS name table of the local computer. The status of **registered** indicates that the name is registered either by broadcast or with a WINS server.

```
C:\Windows\System32>nbtstat -n

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

    No names in cache

VMware Network Adapter VMnet1:
Node IpAddress: [169.254.200.239] Scope Id: []

               NetBIOS Local Name Table

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

15. **nbtstat -an 1 | find “LISTENTING”**

Note – no o/p was shown

16**. net use** – This command list of all the shared resources currently in use under the user account that's currently logged in.

```
C:\Windows\System32>net use
New connections will be remembered.

There are no entries in the list.
```

There is no shared resource in this computer .

17. **net user** – This command return the list of all the uer in the computer.

```
C:\Windows\System32>net user

User accounts for \\SHEBU

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
shebu                    WDAGUtilityAccount
The command completed successfully.
```

18. **net domain –**

NOTE – syntax error

19. **Net user /domain <username>** - This command displays details of a particular user in the computer

```
C:\Windows\System32>net user shebu
User name                    shebu
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            03-10-2021 18:56:58
Password expires             Never
Password changeable          03-10-2021 18:56:58
Password required            No
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   01-10-2022 12:30:50

Logon hours allowed          All

Local Group Memberships      *Administrators        *ORA_DBA
Global Group memberships     *None
The command completed successfully.
```

20. **net group / domain**

21. **net view**

22. **net view /domain**

23. **net view /domain:<domain_name> | more**

24. **net view /cache**

```
C:\Windows\System32>net view /cache
System error 6118 has occurred.

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

NOTE – Not the right o/p

25. **ping –a <ip>** - This command is used to send ping requests to a specific domain/ip

```
C:\Windows\System32>ping -a google.com

Pinging google.com [2404:6800:4009:81f::200e] with 32 bytes of data:
Reply from 2404:6800:4009:81f::200e: time=68ms
Reply from 2404:6800:4009:81f::200e: time=72ms
Reply from 2404:6800:4009:81f::200e: time=82ms

Ping statistics for 2404:6800:4009:81f::200e:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 68ms, Maximum = 82ms, Average = 74ms
```

26. **ping –t <ip>** - This command is used to ping the host until until stopped

```
C:\Windows\System32>ping -t google.com

Pinging google.com [2404:6800:4009:81f::200e] with 32 bytes of data:
Reply from 2404:6800:4009:81f::200e: time=63ms
Reply from 2404:6800:4009:81f::200e: time=76ms
Reply from 2404:6800:4009:81f::200e: time=67ms
Reply from 2404:6800:4009:81f::200e: time=85ms
Reply from 2404:6800:4009:81f::200e: time=70ms
Reply from 2404:6800:4009:81f::200e: time=77ms
Reply from 2404:6800:4009:81f::200e: time=88ms
Reply from 2404:6800:4009:81f::200e: time=71ms
```

27. **pathping** – It is a command that combines the functionality of ping and tracert

```
C:\Windows\System32>pathping google.com

Tracing route to google.com [2404:6800:4007:824::200e]
over a maximum of 30 hops:
  0  shebu [2409:4072:6e0d:dbc:5098:3e93:9c41:b351]
  1  2409:4072:6e0d:dbc::3a
  2     *        *        *
Computing statistics for 25 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                          shebu [2409:4072:6e0d:dbc:5098:3e93:9c41:b351]
                                 0/ 100 =  0%   |
  1    5ms     0/ 100 =  0%     0/ 100 =  0%  2409:4072:6e0d:dbc::3a

Trace complete.
```

28. **set U** – This command is used to display environmental variables for a specific user

```
C:\Windows\System32>set U
USERDOMAIN=SHEBU
USERDOMAIN_ROAMINGPROFILE=SHEBU
USERNAME=shebu
USERPROFILE=C:\Users\shebu
```

29. **set L** - The set l command displays everything from the set command that starts with L

```
C:\Windows\System32>set L
LOCALAPPDATA=C:\Users\shebu\AppData\Local
LOGONSERVER=\\SHEBU
```

30. **telnet <ip> <port>** - It is used to connect to remote computer usin telnet program.

NOTE- Cant connect without ip and port

Result :

Learnt various command line utilities available in windows to perform network troubleshooting.