

21CY681 - INTERNET PROTOCOL LAB - I

Name: Surya S Nair

Register Number: CB.EN.P2CYS22007

Date: 28th September 2022

Assignment Topic: Basic Network Administration and Troubleshooting Using Windows Command Line Utilities

AIM:

To perform troubleshooting in the network using basic Windows command-line utilities

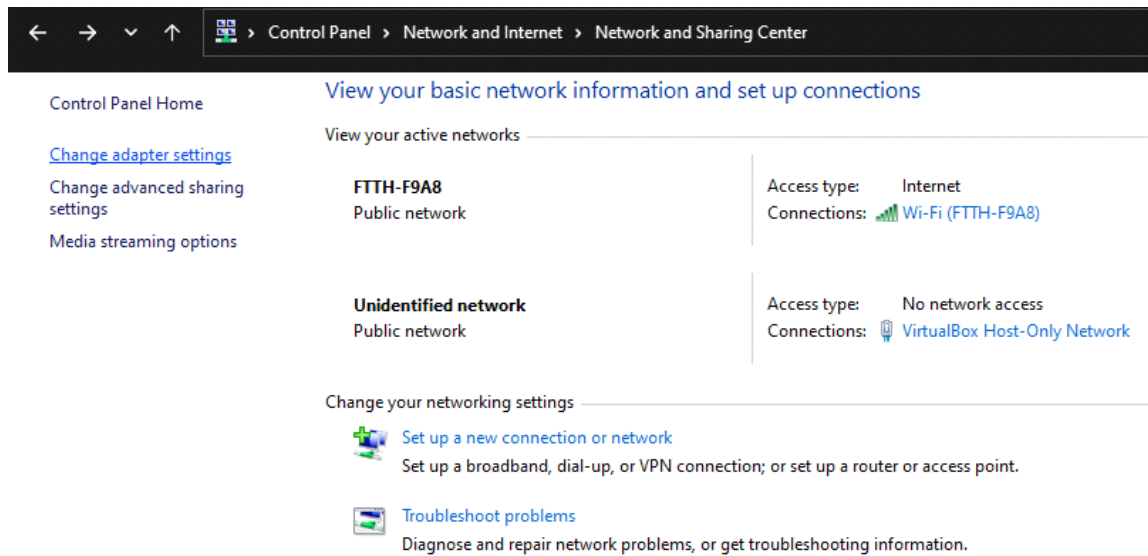
TOOLS REQUIRED:

- Windows Server 2012 and Windows 10VMs
- Administrator privileges to run the tools

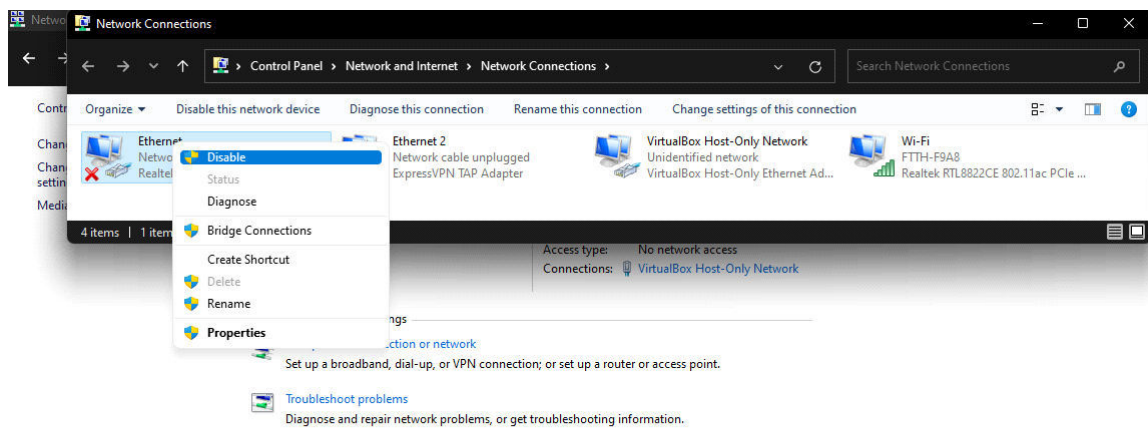
PROCEDURE:

Login to Windows 10 VM and disable the network adapter:

- Go to Control Panel then to Network and Internet then to Network and Sharing Center, and click Change adapter settings.

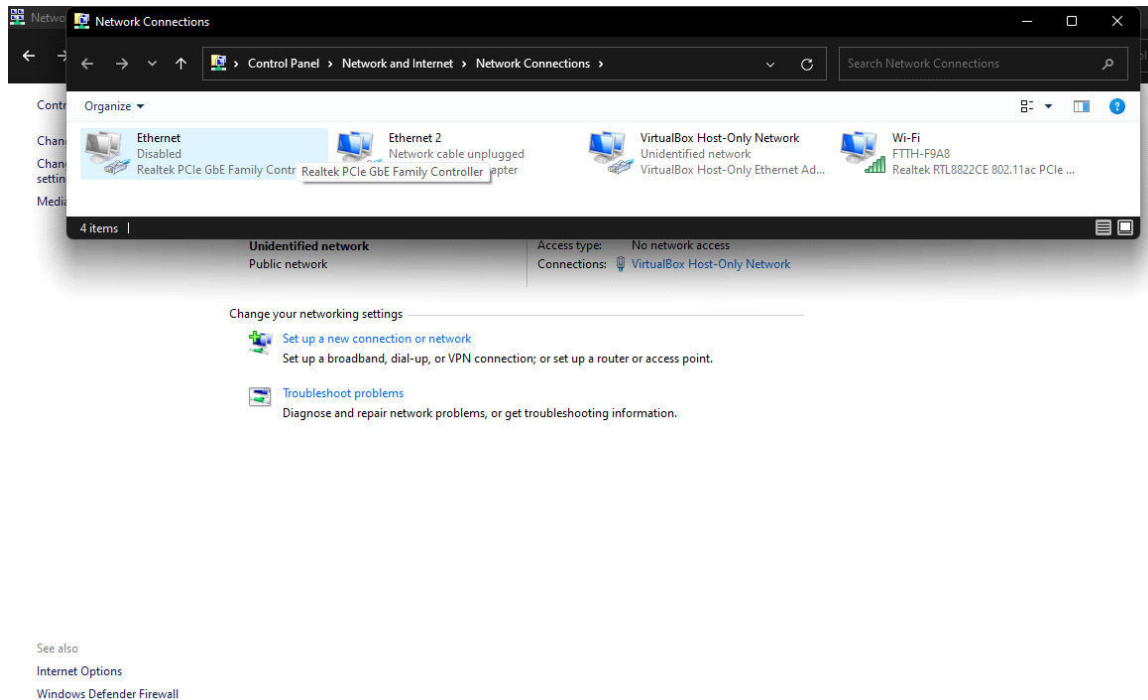


- Select and right-click the Ethernet adapter, and click Disable from the context menu.



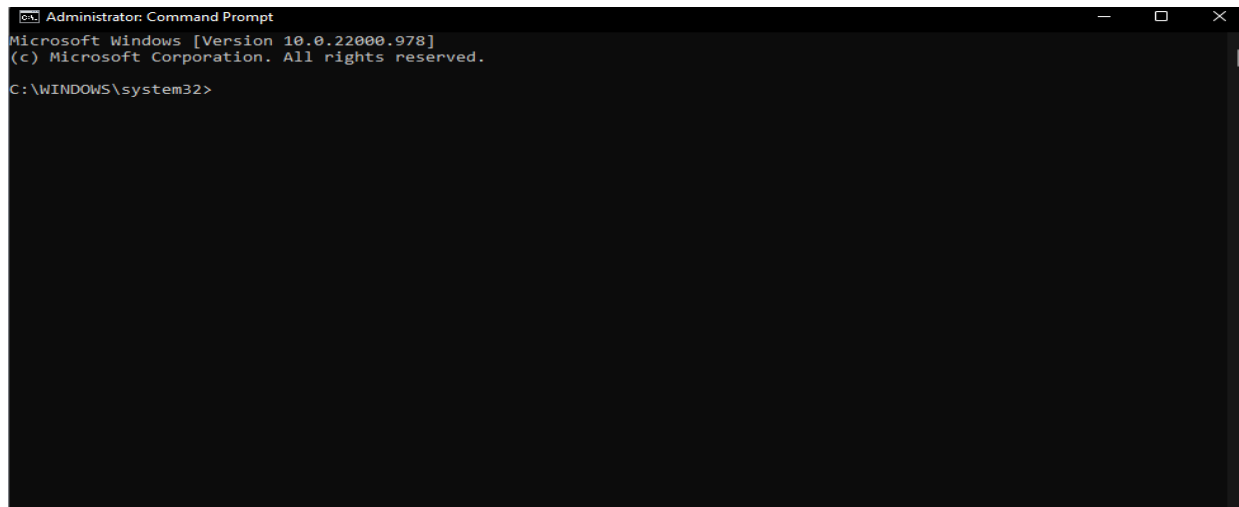
See also
[Internet Options](#)
[Windows Defender Firewall](#)

- It will disable Ethernet adapter as shown below:



TASK 1:

- **Verifying IP Configuration Settings**
1. Launch **Windows server 2012** VM, and login to the local administrator account.
 2. Open a command prompt in Admin mode by right-clicking on the **Start** icon and then click on **Command Prompt (Admin)** from the context menu.
 3. The command prompt appears on the screen

A screenshot of a Windows Command Prompt window titled "Administrator: Command Prompt". The window has a black background with white text. The text inside the window reads: "Microsoft Windows [Version 10.0.22000.978]" followed by "(c) Microsoft Corporation. All rights reserved." on the next line. The current directory is shown as "C:\WINDOWS\system32>".

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.22000.978]
(c) Microsoft Corporation. All rights reserved.
C:\WINDOWS\system32>
```

4. Type **ipconfig** in the command prompt and press **Enter** to verify the IP configuration settings of the machine.
5. The IP Configuration details of the system will be displayed.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.22000.978]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 2:

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

Ethernet adapter VirtualBox Host-Only Network:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::5890:9542:683:4d7d%11
    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::8181:96a9:19f3:33c4%10
    IPv4 Address. . . . . : 192.168.1.8
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

C:\WINDOWS\system32>
```

6.Using different ipconfig parameters to perform various network troubleshooting activities.

- a. ipconfig /all ----> Displays the full TCP/IP configurations for all adapters.

C:\ Administrator: Command Prompt

Microsoft Windows [Version 10.0.22000.978]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ipconfig /all

Windows IP Configuration

Host Name : LAPTOP-KB8USE6Q
Primary Dns Suffix :
Node Type : Unknown
IP Routing Enabled. : No
WINS Proxy Enabled. : No

Ethernet adapter Ethernet 2:

Media State : Media disconnected
Connection-specific DNS Suffix . :
Description : ExpressVPN TAP Adapter
Physical Address. : 00-FF-C9-7A-6A-90
DHCP Enabled. : Yes
Autoconfiguration Enabled : Yes

Ethernet adapter VirtualBox Host-Only Network:

Connection-specific DNS Suffix . :
Description : VirtualBox Host-Only Ethernet Adapter
Physical Address. : 0A-00-27-00-00-0B
DHCP Enabled. : No
Autoconfiguration Enabled : Yes
Link-local IPv6 Address : fe80::5890:9542:683:4d7d%11(Preferred)
IPv4 Address. : 192.168.56.1(Preferred)
Subnet Mask : 255.255.255.0
Default Gateway :
DHCPv6 IAID : 705298471
DHCPv6 Client DUID. : 00-01-00-01-28-6C-03-FD-50-81-40-30-E6-ED
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. : 82-D2-1D-FB-E3-F3

```
C:\> Administrator: Command Prompt

Physical Address. . . . . : 82-D2-1D-FB-E3-F3
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. . . . . : C2-D2-1D-FB-E3-F3
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . :
Description . . . . . : Realtek RTL8822CE 802.11ac PCIe Adapter
Physical Address. . . . . : 80-D2-1D-FB-E3-F3
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::8181:96a9:19f3:33c4%10(Preferred)
IPv4 Address. . . . . : 192.168.1.8(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 30 September 2022 18:35:47
Lease Expires . . . . . : 03 October 2022 10:52:09
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 192991773
DHCPv6 Client DUID. . . . . : 00-01-00-01-28-6C-03-FD-50-81-40-30-E6-ED
DNS Servers . . . . . : 103.199.160.80
                        8.8.8.8
NetBIOS over Tcpip. . . . . : Enabled

C:\WINDOWS\system32>
```

b. `ipconfig /renew [Adapter]` ---->Renews DHCP configuration for all adapters.

```
C:\Administrator: Command Prompt
Microsoft Windows [Version 10.0.22000.978]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ipconfig /renew[Adapter]

Error: unrecognized or incomplete command line.

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 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.

Examples:
> ipconfig          ... Show information
> ipconfig /all      ... Show detailed information
> ipconfig /renew     ... renew all adapters
> ipconfig /renew EL* ... renew any connection that has its
                        name starting with EL
> ipconfig /release *Con* ... release all matching connections,
                        eg. "Wired Ethernet Connection 1" or
                        "Wired Ethernet Connection 2"
> ipconfig /allcompartments ... Show information about all
                        compartments
> ipconfig /allcompartments /all ... Show detailed information about all
                        compartments
```

- c. `ipconfig /release [Adapter]` ---->Sends a DHCPRELEASE message to the DHCP server to release the current DHCP configuration and discard the IP

address configuration for either all adapters or for a specified adapter.

```
C:\> Administrator: Command Prompt
Microsoft Windows [Version 10.0.22000.978]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ipconfig /release [Adapter]

Windows IP Configuration

The operation failed as no adapter is in the state permissible for
this operation.

C:\WINDOWS\system32>
```

d. `ipconfig /flushdns` ----> Flushes and resets the contents of the DNS client resolver cache.

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

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\WINDOWS\system32>
```

e. `ipconfig /displaydns` ----> Displays the contents of the DNS client resolver cache, which includes both entries preloaded from the local Hosts file and any recently obtained resource records for name queries resolved by the computer.

Administrator: Command Prompt

Microsoft Windows [Version 10.0.22000.978]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ipconfig /displaydns

Windows IP Configuration

array805.prod.do.dsp.mp.microsoft.com

Record Name : array805.prod.do.dsp.mp.microsoft.com
Record Type : 1
Time To Live : 1125
Data Length : 4
Section : Answer
A (Host) Record . . . : 52.143.80.209

ocws.officeapps.live.com

Record Name : ocws.officeapps.live.com
Record Type : 5
Time To Live : 82
Data Length : 8
Section : Answer
CNAME Record : prod.ocws1.live.com.akadns.net

Record Name : prod.ocws1.live.com.akadns.net
Record Type : 5
Time To Live : 82
Data Length : 8
Section : Answer
CNAME Record : asia2.ocws1.live.com.akadns.net

Record Name : asia2.ocws1.live.com.akadns.net
Record Type : 1
Time To Live : 82
Data Length : 4
Section : Answer
A (Host) Record . . . : 52.109.56.86

```

provision.ccs.mcafee.com
-----
Record Name . . . . : provision.ccs.mcafee.com
Record Type . . . . : 5
Time To Live . . . . : 32
Data Length . . . . : 8
Section . . . . . : Answer
CNAME Record . . . . : provcs-prod-r53-ext.awscommon.mcafee.com

Record Name . . . . : provcs-prod-r53-ext.awscommon.mcafee.com
Record Type . . . . : 5
Time To Live . . . . : 32
Data Length . . . . : 8
Section . . . . . : Answer
CNAME Record . . . . : nlb-external-provcs-b4eb602d91cf3c92.elb.us-west-2.amazonaws.com

Record Name . . . . : nlb-external-provcs-b4eb602d91cf3c92.elb.us-west-2.amazonaws.com
Record Type . . . . : 1
Time To Live . . . . : 32
Data Length . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 54.186.12.176

Record Name . . . . : nlb-external-provcs-b4eb602d91cf3c92.elb.us-west-2.amazonaws.com
Record Type . . . . : 1

```

```

Administrator: Command Prompt
Record Name . . . . : nlb-external-provcs-b4eb602d91cf3c92.elb.us-west-2.amazonaws.com
Record Type . . . . : 1
Time To Live . . . . : 32
Data Length . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 44.237.149.221

Record Name . . . . : nlb-external-provcs-b4eb602d91cf3c92.elb.us-west-2.amazonaws.com
Record Type . . . . : 1
Time To Live . . . . : 32
Data Length . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 35.165.28.5

login.live.com
-----
Record Name . . . . : login.live.com
Record Type . . . . : 5
Time To Live . . . . : 144
Data Length . . . . : 8
Section . . . . . : Answer
CNAME Record . . . . : login.msa.msidentity.com

Record Name . . . . : login.msa.msidentity.com
Record Type . . . . : 5
Time To Live . . . . : 144
Data Length . . . . : 8
Section . . . . . : Answer
CNAME Record . . . . : www.tm.lg.prod.aadmsa.trafficmanager.net

Record Name . . . . : www.tm.lg.prod.aadmsa.trafficmanager.net
Record Type . . . . : 5
Time To Live . . . . : 144
Data Length . . . . : 8
Section . . . . . : Answer
CNAME Record . . . . : prda.aadg.msidentity.com

Record Name . . . . : prda.aadg.msidentity.com

```

Record Name : prda.aadg.msidentity.com
Record Type : 5
Time To Live : 144
Data Length : 8
Section : Answer
CNAME Record : www.tm.a.prd.aadg.trafficmanager.net

Record Name : www.tm.a.prd.aadg.trafficmanager.net
Record Type : 1
Time To Live : 144
Data Length : 4
Section : Answer
A (Host) Record : 40.126.17.132

Record Name : www.tm.a.prd.aadg.trafficmanager.net
Record Type : 1
Time To Live : 144
Data Length : 4
Section : Answer
A (Host) Record : 40.126.17.133

Record Name : www.tm.a.prd.aadg.trafficmanager.net
Record Type : 1
Time To Live : 144
Data Length : 4
Section : Answer

A (Host) Record . . . : 20.190.145.142

login.microsoftonline.com

Record Name : login.microsoftonline.com
Record Type : 5
Time To Live : 133
Data Length : 8
Section : Answer
CNAME Record : ak.privatelink.msidentity.com

Record Name : ak.privatelink.msidentity.com
Record Type : 5
Time To Live : 133
Data Length : 8
Section : Answer
CNAME Record : www.tm.ak.prd.aadg.trafficmanager.net

Record Name : www.tm.ak.prd.aadg.trafficmanager.net
Record Type : 1
Time To Live : 133
Data Length : 4
Section : Answer
A (Host) Record . . . : 20.190.146.33

Record Name : www.tm.ak.prd.aadg.trafficmanager.net
Record Type : 1
Time To Live : 133
Data Length : 4
Section : Answer
A (Host) Record . . . : 20.190.146.36

Record Name : www.tm.ak.prd.aadg.trafficmanager.net
Record Type : 1
Time To Live : 133
Data Length : 4
Section : Answer
A (Host) Record . . . : 20.190.146.35

```

Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . : 20.190.146.32

Record Name . . . . . : www.tm.ak.prd.aadg.trafficmanager.net
Record Type . . . . . : 1
Time To Live . . . . . : 133
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . : 40.126.18.32

Record Name . . . . . : www.tm.ak.prd.aadg.trafficmanager.net
Record Type . . . . . : 1
Time To Live . . . . . : 133
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . : 20.190.146.34

C:\WINDOWS\system32>
```

f. `ipconfig /registerdns` ---->Initiates manual dynamic registration for the DNS names and IP addresses that are configured at a computer.

```

Microsoft Windows [Version 10.0.22000.978]
(c) Microsoft Corporation. All rights reserved.

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.

C:\WINDOWS\system32>
```

g. `ipconfig /showclassid Adapter` ---->Displays the DHCP class ID for a specified adapter.

```
C:\WINDOWS\system32>ipconfig/showclassid Adapter

Windows IP Configuration

The operation failed as no adapter is in the state permissible for
this operation.

C:\WINDOWS\system32>
```

h. `ipconfig /setclassid Adapter[ClassID]` ----> Configures the DHCP class ID for a specified adapter.

```
C:\WINDOWS\system32>ipconfig/setclassid Adapter [ClassID]

Windows IP Configuration

The operation failed as no adapter is in the state permissible for
this operation.

C:\WINDOWS\system32>
```

i. `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.
```

```
Administrator: Command Prompt

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.

Examples:
> ipconfig          ... Show information
> ipconfig /all     ... Show detailed information
> ipconfig /renew   ... renew all adapters
> ipconfig /renew EL* ... renew any connection that has its
                        name starting with EL
> ipconfig /release *Con* ... release all matching connections,
                        eg. "Wired Ethernet Connection 1" or
                        "Wired Ethernet Connection 2"
> ipconfig /allcompartments ... Show information about all
                        compartments
> ipconfig /allcompartments /all ... Show detailed information about all
                        compartments

C:\WINDOWS\system32>
```

7.Type **ipconfig /all** and press **Enter**.This command will list out the System's IP configuration ,host name,Ethernet Adapter installed and its MAC Address (Physical Address) and so on, as shown in the screenshot.

C:\ Administrator: Command Prompt

Microsoft Windows [Version 10.0.22000.978]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ipconfig /all

Windows IP Configuration

Host Name : LAPTOP-KB8USE6Q
Primary Dns Suffix :
Node Type : Unknown
IP Routing Enabled. : No
WINS Proxy Enabled. : No

Ethernet adapter Ethernet 2:

Media State : Media disconnected
Connection-specific DNS Suffix . :
Description : ExpressVPN TAP Adapter
Physical Address. : 00-FF-C9-7A-6A-90
DHCP Enabled. : Yes
Autoconfiguration Enabled : Yes

Ethernet adapter VirtualBox Host-Only Network:

Connection-specific DNS Suffix . :
Description : VirtualBox Host-Only Ethernet Adapter
Physical Address. : 0A-00-27-00-00-0B
DHCP Enabled. : No
Autoconfiguration Enabled : Yes
Link-local IPv6 Address : fe80::5890:9542:683:4d7d%11(Preferred)
IPv4 Address. : 192.168.56.1(Preferred)
Subnet Mask : 255.255.255.0
Default Gateway :
DHCPv6 IAID : 705298471
DHCPv6 Client DUID. : 00-01-00-01-28-6C-03-FD-50-81-40-30-E6-ED
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. : 82-D2-1D-FB-E3-F3

```
C:\> Administrator: Command Prompt

Physical Address. . . . . : 82-D2-1D-FB-E3-F3
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. . . . . : C2-D2-1D-FB-E3-F3
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . :
Description . . . . . : Realtek RTL8822CE 802.11ac PCIe Adapter
Physical Address. . . . . : 80-D2-1D-FB-E3-F3
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::8181:96a9:19f3:33c4%10(Preferred)
IPv4 Address. . . . . : 192.168.1.8(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 30 September 2022 18:35:47
Lease Expires . . . . . : 03 October 2022 11:36:16
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 192991773
DHCPv6 Client DUID. . . . . : 00-01-00-01-28-6C-03-FD-50-81-40-30-E6-ED
DNS Servers . . . . . : 103.199.160.80
                        8.8.8.8
NetBIOS over Tcpip. . . . . : Enabled

C:\WINDOWS\system32>
```

TASK 2:

- **Checking IP level Connectivity Using Ping command**

8.Type **ping** followed by the IP address of the Windows 10 machine

```
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>
```

TASK 3:

- Tracing the route of packets using **tracert** command

9.Type **tracert** followed by the target system IP address the command prompt and press Enter.

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

Tracing route to LAPTOP-KB8USE6Q [192.168.56.1]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  LAPTOP-KB8USE6Q [192.168.56.1]

Trace complete.

C:\WINDOWS\system32>
```

tracert command is to know the number of hops between a source and a destination node in a network.**tracert** is useful for troubleshooting large networks where several paths can lead to the same point or where many intermediate components are involved.

The **tracert** diagnostic utility determines the route to a destination by sending Internet Control Message Protocol echo packets to the destination. In these packets, **tracert** uses varying IP Time-To-Live values. **Tracert** sends the first echo packet with a TTL of 1 and increments the TTL by 1 on each subsequent transmission, until the destination responds or until the maximum

TTL is reached. The ICMP «Time Exceeded» messages that intermediate routers send back show the route.

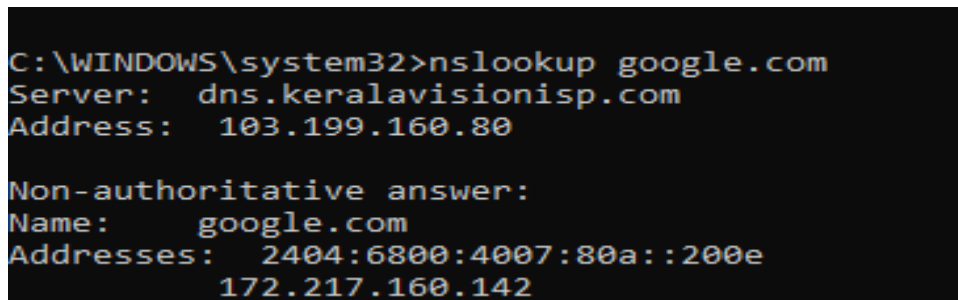
Using the -d option with the tracert command instructs tracert not to perform a DNS lookup on each IP address, so that tracert reports the IP address of the near side interface of the routers.

10. From the above screenshot, we can see that the destination was reached in the first hop itself.

TASK 4:

- **Resolving Domain names with Using nslookup command**

11. On the Windows Server 2012 machine, type **nslookup** followed by the domain name which we want to resolve (here I used google.com) in the command prompt and press Enter.



```
C:\WINDOWS\system32>nslookup google.com
Server:  dns.keralavisionisp.com
Address:  103.199.160.80

Non-authoritative answer:
Name:     google.com
Addresses: 2404:6800:4007:80a::200e
          172.217.160.142
```

12. From the above screenshot, we will see that the domain name (google.com) resolves to its corresponding IP address (172.217.160.142)

13. We can also use the nslookup command with the type parameters to get non-authoritative name server (NS) information as shown in the screenshot below:

```
C:\WINDOWS\system32>nslookup -type=A google.com
Server:  dns.keralavisionisp.com
Address: 103.199.160.80

Non-authoritative answer:
Name:    google.com
Address: 172.217.160.142
```

14.To get an authoritative NS information,we can use -type=soa parameter with nslookup.

```
C:\WINDOWS\system32>nslookup -type=soa google.com
Server:  dns.keralavisionisp.com
Address: 103.199.160.80

Non-authoritative answer:
google.com
    primary name server = ns1.google.com
    responsible mail addr = dns-admin.google.com
    serial    = 478064308
    refresh  = 900 (15 mins)
    retry    = 900 (15 mins)
    expire   = 1800 (30 mins)
    default TTL = 60 (1 min)
```

15.The address labelled as primary name server in the above screenshot is the DNS authority for the domain.

TASK 5:

- **Checking our network configuration and statistics netstat command**

16.Type the **netstat** command to check our network statics as shown below

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

Active Connections

Proto	Local Address	Foreign Address	State
TCP	10.11.133.91:54941	20.197.71.89:https	ESTABLISHED
TCP	10.11.133.91:54948	104:https	TIME_WAIT
TCP	10.11.133.91:55049	sd-in-f188:https	ESTABLISHED
TCP	10.11.133.91:55076	whatsapp-cdn-shv-02-maa2:https	ESTABLISHED
TCP	10.11.133.91:55419	151.101.40.134:https	ESTABLISHED
TCP	10.11.133.91:55420	151.101.40.134:https	ESTABLISHED
TCP	10.11.133.91:55423	151.101.192.134:https	ESTABLISHED
TCP	10.11.133.91:55427	151.101.192.134:https	ESTABLISHED
TCP	10.11.133.91:55430	151.101.192.134:https	ESTABLISHED
TCP	10.11.133.91:55432	146.75.94.49:https	ESTABLISHED
TCP	10.11.133.91:55438	151.101.52.64:https	ESTABLISHED
TCP	10.11.133.91:55441	151.101.52.64:https	ESTABLISHED
TCP	10.11.133.91:55445	151.101.52.64:https	ESTABLISHED
TCP	10.11.133.91:55446	151.101.24.134:https	ESTABLISHED
TCP	10.11.133.91:55448	65:https	ESTABLISHED
TCP	10.11.133.91:55453	104.18.101.194:https	TIME_WAIT
TCP	10.11.133.91:55454	146:https	ESTABLISHED
TCP	10.11.133.91:55455	146:https	ESTABLISHED
TCP	10.11.133.91:55457	193:https	ESTABLISHED
TCP	10.11.133.91:55463	218:https	ESTABLISHED
TCP	10.11.133.91:55465	3:https	ESTABLISHED
TCP	10.11.133.91:55466	a23-59-80-240:https	ESTABLISHED
TCP	10.11.133.91:55468	server-108-158-229-117:https	CLOSE_WAIT
TCP	10.11.133.91:55469	server-108-158-243-98:http	CLOSE_WAIT
TCP	10.11.133.91:55471	server-65-8-84-214:http	CLOSE_WAIT
TCP	10.11.133.91:55473	server-18-66-65-27:http	CLOSE_WAIT
TCP	10.11.133.91:55474	a23-49-60-103:https	CLOSE_WAIT
TCP	10.11.133.91:55504	bom07s37-in-f3:https	TIME_WAIT

```
C:\> Administrator: Command Prompt
```

TCP	10.11.133.91:55504	bom07s37-in-f3:https	TIME_WAIT
TCP	10.11.133.91:55509	maa03s41-in-f14:https	ESTABLISHED
TCP	10.11.133.91:55510	52.182.143.67:https	TIME_WAIT
TCP	10.11.133.91:55512	ec2-52-27-137-96:https	TIME_WAIT
TCP	10.11.133.91:55513	ec2-54-149-233-116:https	TIME_WAIT
TCP	10.11.133.91:55514	ec2-44-232-31-100:https	TIME_WAIT
TCP	10.11.133.91:55515	bom07s36-in-f2:https	ESTABLISHED
TCP	10.11.133.91:55516	180.149.61.152:http	TIME_WAIT
TCP	10.11.133.91:55517	bom12s20-in-f3:https	ESTABLISHED
TCP	10.11.133.91:55518	20.189.173.14:https	ESTABLISHED
TCP	10.11.133.91:55519	20.189.173.14:https	ESTABLISHED
TCP	10.11.133.91:55520	20.189.173.14:https	ESTABLISHED
TCP	10.11.133.91:55521	bom07s16-in-f14:https	ESTABLISHED
TCP	127.0.0.1:52052	LAPTOP-KB8USE6Q:52057	ESTABLISHED
TCP	127.0.0.1:52057	LAPTOP-KB8USE6Q:52052	ESTABLISHED

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

17. Use different netstat parameters to obtain important connection information

a. netstat -a ----> Displays all active TCP connections and the TCP and UDP ports on which the computer is listening.

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

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	LAPTOP-KB8USE6Q:0	LISTENING
TCP	0.0.0.0:445	LAPTOP-KB8USE6Q:0	LISTENING
TCP	0.0.0.0:5040	LAPTOP-KB8USE6Q:0	LISTENING
TCP	0.0.0.0:6646	LAPTOP-KB8USE6Q:0	LISTENING
TCP	0.0.0.0:49664	LAPTOP-KB8USE6Q:0	LISTENING
TCP	0.0.0.0:49665	LAPTOP-KB8USE6Q:0	LISTENING
TCP	0.0.0.0:49666	LAPTOP-KB8USE6Q:0	LISTENING
TCP	0.0.0.0:49667	LAPTOP-KB8USE6Q:0	LISTENING
TCP	0.0.0.0:49668	LAPTOP-KB8USE6Q:0	LISTENING
TCP	0.0.0.0:49670	LAPTOP-KB8USE6Q:0	LISTENING
TCP	127.0.0.1:2015	LAPTOP-KB8USE6Q:0	LISTENING
TCP	127.0.0.1:61832	LAPTOP-KB8USE6Q:0	LISTENING
TCP	127.0.0.1:61832	LAPTOP-KB8USE6Q:61834	ESTABLISHED
TCP	127.0.0.1:61834	LAPTOP-KB8USE6Q:61832	ESTABLISHED
TCP	192.168.1.8:139	LAPTOP-KB8USE6Q:0	LISTENING
TCP	192.168.1.8:61661	20.198.119.84:https	ESTABLISHED
TCP	192.168.1.8:61900	whatsapp-cdn-shv-02-bom1:https	ESTABLISHED
TCP	192.168.1.8:62131	si-in-f188:5228	ESTABLISHED
TCP	192.168.1.8:62132	maa03s41-in-f5:https	ESTABLISHED
TCP	192.168.1.8:62154	maa05s12-in-f3:https	TIME_WAIT
TCP	192.168.1.8:62157	a-0003:https	TIME_WAIT
TCP	192.168.1.8:62164	a-0003:https	TIME_WAIT
TCP	192.168.1.8:62168	dns:https	TIME_WAIT
TCP	192.168.1.8:62169	204.79.197.239:https	TIME_WAIT
TCP	192.168.1.8:62170	a-0003:https	TIME_WAIT
TCP	192.168.1.8:62172	a-0003:https	TIME_WAIT
TCP	192.168.1.8:62175	a-0001:https	TIME_WAIT
TCP	192.168.1.8:62180	13.107.246.58:https	FIN_WAIT_2
TCP	192.168.1.8:62182	52.231.207.240:https	FIN_WAIT_1
TCP	192.168.1.8:62183	52.231.207.240:https	TIME_WAIT
TCP	192.168.1.8:62184	maa05s21-in-f4:https	LAST_ACK
TCP	192.168.1.8:62189	whatsapp-cdn-shv-02-bom1:https	ESTABLISHED

```

TCP    0.0.0.0:5040      LAPTOP-KB8USE6Q:0    LISTENING
TCP    0.0.0.0:6646      LAPTOP-KB8USE6Q:0    LISTENING
TCP    0.0.0.0:49664     LAPTOP-KB8USE6Q:0    LISTENING
TCP    0.0.0.0:49665     LAPTOP-KB8USE6Q:0    LISTENING
TCP    0.0.0.0:49666     LAPTOP-KB8USE6Q:0    LISTENING
TCP    0.0.0.0:49667     LAPTOP-KB8USE6Q:0    LISTENING
TCP    0.0.0.0:49668     LAPTOP-KB8USE6Q:0    LISTENING
TCP    0.0.0.0:49670     LAPTOP-KB8USE6Q:0    LISTENING
TCP    127.0.0.1:2015     LAPTOP-KB8USE6Q:0    LISTENING
TCP    127.0.0.1:61832    LAPTOP-KB8USE6Q:0    LISTENING
TCP    127.0.0.1:61832    LAPTOP-KB8USE6Q:61834 ESTABLISHED
TCP    127.0.0.1:61834    LAPTOP-KB8USE6Q:61832 ESTABLISHED
TCP    192.168.1.8:139    LAPTOP-KB8USE6Q:0    LISTENING
TCP    192.168.1.8:61661  20.198.119.84:https   ESTABLISHED
TCP    192.168.1.8:61900  whatsapp-cdn-shv-02-bom1:https ESTABLISHED
TCP    192.168.1.8:62131  si-in-f188:5228       ESTABLISHED
TCP    192.168.1.8:62132  maa03s41-in-f5:https  ESTABLISHED
TCP    192.168.1.8:62154  maa05s12-in-f3:https  TIME_WAIT
TCP    192.168.1.8:62157  a-0003:https          TIME_WAIT
TCP    192.168.1.8:62164  a-0003:https          TIME_WAIT
TCP    192.168.1.8:62168  dns:https             TIME_WAIT
TCP    192.168.1.8:62169  204.79.197.239:https  TIME_WAIT
TCP    192.168.1.8:62170  a-0003:https          TIME_WAIT
TCP    192.168.1.8:62172  a-0003:https          TIME_WAIT
TCP    192.168.1.8:62175  a-0001:https          TIME_WAIT
TCP    192.168.1.8:62180  13.107.246.58:https   FIN_WAIT_2
TCP    192.168.1.8:62182  52.231.207.240:https  FIN_WAIT_1
TCP    192.168.1.8:62183  52.231.207.240:https  TIME_WAIT
TCP    192.168.1.8:62184  maa05s21-in-f4:https  LAST_ACK
TCP    192.168.1.8:62189  whatsapp-cdn-shv-02-bom1:https ESTABLISHED
TCP    192.168.1.8:62192  waw02s08-in-f195:https ESTABLISHED
TCP    192.168.56.1:139   LAPTOP-KB8USE6Q:0    LISTENING
TCP    [::]:135          LAPTOP-KB8USE6Q:0    LISTENING
TCP    [::]:445          LAPTOP-KB8USE6Q:0    LISTENING
TCP    [::]:49664        LAPTOP-KB8USE6Q:0    LISTENING
TCP    [::]:49665        LAPTOP-KB8USE6Q:0    LISTENING
TCP    [::]:49666        LAPTOP-KB8USE6Q:0    LISTENING
TCP    [::]:49667        LAPTOP-KB8USE6Q:0    LISTENING
TCP    [::]:49668        LAPTOP-KB8USE6Q:0    LISTENING
TCP    [::]:49670        LAPTOP-KB8USE6Q:0    LISTENING
TCP    [::1]:49669       LAPTOP-KB8USE6Q:0    LISTENING
UDP    0.0.0.0:123       *:*
UDP    0.0.0.0:5050      *:*
```


C:\ Administrator: Command Prompt

```
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    0.0.0.0:5355      *: *
UDP    0.0.0.0:6646      *: *
UDP    0.0.0.0:50045     142.250.193.110:443
UDP    0.0.0.0:50384      *: *
UDP    0.0.0.0:51828     142.250.205.238:443
UDP    0.0.0.0:53475     172.217.167.131:443
UDP    0.0.0.0:54696     8.8.4.4:443
UDP    0.0.0.0:55116     142.250.195.170:443
UDP    0.0.0.0:59192     142.250.205.238:443
UDP    0.0.0.0:59262     8.8.4.4:443
UDP    0.0.0.0:62006     172.217.167.131:443
UDP    0.0.0.0:62080     172.217.31.202:443
UDP    0.0.0.0:62480     142.250.193.110:443
UDP    10.11.133.91:50340  172.17.18.2:53
UDP    10.11.133.91:50774  172.17.18.2:53
UDP    10.11.133.91:51226  172.17.18.2:53
UDP    10.11.133.91:59422  172.17.18.2:53
UDP    10.11.133.91:62901  172.17.18.2:53
UDP    10.11.133.91:63194  172.17.18.2:53
UDP    127.0.0.1:1900      *: *
UDP    127.0.0.1:50779    127.0.0.1:50779
UDP    127.0.0.1:60883     *: *
UDP    127.0.0.1:61576    127.0.0.1:61576
UDP    192.168.1.8:137     *: *
UDP    192.168.1.8:138     *: *
UDP    192.168.1.8:1900    *: *
UDP    192.168.1.8:54650   103.199.160.80:53
UDP    192.168.1.8:60882  *: *
UDP    192.168.56.1:137   *: *
UDP    192.168.56.1:138   *: *
UDP    192.168.56.1:1900   *: *
UDP    192.168.56.1:60881  *: *
UDP    [::]:123            *: *
```

```

C:\> Select Administrator: Command Prompt

UDP    10.11.133.91:63194      172.17.18.2:53
UDP    127.0.0.1:1900         *: *
UDP    127.0.0.1:50779        127.0.0.1:50779
UDP    127.0.0.1:60883        *: *
UDP    127.0.0.1:61576        127.0.0.1:61576
UDP    192.168.1.8:137        *: *
UDP    192.168.1.8:138        *: *
UDP    192.168.1.8:1900        *: *
UDP    192.168.1.8:54650      103.199.160.80:53
UDP    192.168.1.8:60882        *: *
UDP    192.168.56.1:137        *: *
UDP    192.168.56.1:138        *: *
UDP    192.168.56.1:1900        *: *
UDP    192.168.56.1:60881      *: *
UDP    [::]:123                *: *
UDP    [::]:5353               *: *
UDP    [::]:5353               *: *
UDP    [::]:5353               *: *
UDP    [::]:5353               *: *
UDP    [::]:5353               *: *
UDP    [::]:5355               *: *
UDP    [::]:50384              *: *
UDP    [::1]:1900              *: *
UDP    [::1]:60880             *: *
UDP    [fe80::5890:9542:683:4d7d%11]:1900 *: *
UDP    [fe80::5890:9542:683:4d7d%11]:60878 *: *
UDP    [fe80::8181:96a9:19f3:33c4%10]:1900 *: *
UDP    [fe80::8181:96a9:19f3:33c4%10]:60879 *: *

```

b. netstat -e ---->Displays Ethernet statistics, such as the number of bytes and packets sent and received.This parameter can be combined with-s

```

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


```

	Received	Sent
Bytes	2926640544	645910153
Unicast packets	12890150	7777679
Non-unicast packets	5222	16044
Discards	0	0
Errors	0	0
Unknown protocols	0	

c.netstat -n ---->Displays active TCP connections, however, addresses and port numbers are expressed numerically and no attempt is made to determine names.

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

Active Connections

Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:61832	127.0.0.1:61834	ESTABLISHED
TCP	127.0.0.1:61834	127.0.0.1:61832	ESTABLISHED
TCP	192.168.1.8:61661	20.198.119.84:443	ESTABLISHED
TCP	192.168.1.8:61900	31.13.79.53:443	ESTABLISHED
TCP	192.168.1.8:62131	172.217.194.188:5228	ESTABLISHED
TCP	192.168.1.8:62132	142.250.195.165:443	ESTABLISHED
TCP	192.168.1.8:62197	142.250.195.206:443	ESTABLISHED
TCP	192.168.1.8:62198	142.250.195.206:443	ESTABLISHED
TCP	192.168.1.8:62201	52.140.118.28:443	TIME_WAIT
TCP	192.168.1.8:62202	52.182.143.67:443	ESTABLISHED
TCP	192.168.1.8:62203	35.166.168.175:443	TIME_WAIT
TCP	192.168.1.8:62204	44.230.112.48:443	TIME_WAIT
TCP	192.168.1.8:62205	54.188.179.92:443	TIME_WAIT
TCP	192.168.1.8:62206	52.12.84.31:443	TIME_WAIT
TCP	192.168.1.8:62207	104.208.16.0:443	ESTABLISHED
TCP	192.168.1.8:62208	18.235.133.164:443	ESTABLISHED
TCP	192.168.1.8:62209	35.83.87.190:443	ESTABLISHED
TCP	192.168.1.8:62210	35.83.87.190:443	ESTABLISHED
TCP	192.168.1.8:62211	44.230.112.48:443	TIME_WAIT
TCP	192.168.1.8:62212	142.250.182.100:443	CLOSE_WAIT

d.netstat -o ---->Displays active TCP connections and includes the process ID (PID) for each connection. You can find the application based on the PID on the Processes tab in Windows Task Manager. This parameter can be combined with -a, -n, and -p.

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

Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	127.0.0.1:61832	LAPTOP-KB8USE6Q:61834	ESTABLISHED	17848
TCP	127.0.0.1:61834	LAPTOP-KB8USE6Q:61832	ESTABLISHED	5252
TCP	192.168.1.8:61661	20.198.119.84:https	ESTABLISHED	5560
TCP	192.168.1.8:61900	whatsapp-cdn-shv-02-bom1:https	ESTABLISHED	9516
TCP	192.168.1.8:62131	si-in-f188:5228	ESTABLISHED	11856
TCP	192.168.1.8:62132	maa03s41-in-f5:https	ESTABLISHED	11856
TCP	192.168.1.8:62197	maa03s42-in-f14:https	TIME_WAIT	0
TCP	192.168.1.8:62198	maa03s42-in-f14:https	TIME_WAIT	0
TCP	192.168.1.8:62207	104.208.16.0:https	TIME_WAIT	0
TCP	192.168.1.8:62208	ec2-18-235-133-164:https	TIME_WAIT	0
TCP	192.168.1.8:62209	ec2-35-83-87-190:https	ESTABLISHED	8740
TCP	192.168.1.8:62212	maa05s21-in-f4:https	CLOSE_WAIT	11856
TCP	192.168.1.8:62213	ec2-35-163-39-37:https	TIME_WAIT	0
TCP	192.168.1.8:62216	whatsapp-cdn-shv-02-bom1:https	ESTABLISHED	9516

e.netstat -p protocol ----> Shows connections for the protocol specified by Protocol. In this case,the Protocol can be tcp, udp, tepv6, or udpv6. If this parameter is used with -s to display statistics by protocol, Protocol can be tcp, udp, icmp, ip, tcpv6, udpv6, icmpv6, or ipv6.

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

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.

```

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 Redisplay selected statistics, pausing interval seconds
        between each display. Press CTRL+C to stop redisplaying
        statistics. If omitted, netstat will print the current
        configuration information once.

```

f.netstat -s ---->Displays statistics by protocol. By default, statistics are shown for the TCP, UDP, ICMP, and IP protocols. If the IPv6 protocol for Windows XP is installed, statistics are shown for the TCP over IPv6, UDP over IPv6, ICMPv6, and IPv6 protocols. The -p parameter can be used to specify a set of protocols.

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

IPv4 Statistics

Packets Received	= 5746235
Received Header Errors	= 1727
Received Address Errors	= 420477
Datagrams Forwarded	= 0
Unknown Protocols Received	= 0
Received Packets Discarded	= 867317
Received Packets Delivered	= 5441943
Output Requests	= 3121468
Routing Discards	= 0
Discarded Output Packets	= 4828
Output Packet No Route	= 55
Reassembly Required	= 74228
Reassembly Successful	= 37109
Reassembly Failures	= 0
Datagrams Successfully Fragmented	= 0
Datagrams Failing Fragmentation	= 0
Fragments Created	= 0

IPv6 Statistics

Packets Received	= 1553563
Received Header Errors	= 0
Received Address Errors	= 1070887
Datagrams Forwarded	= 0
Unknown Protocols Received	= 0
Received Packets Discarded	= 515607
Received Packets Delivered	= 488237
Output Requests	= 23896
Routing Discards	= 0

C:\ Administrator: Command Prompt

Errors	0	0
Destination Unreachable	349	1568
Time Exceeded	56	5
Parameter Problems	0	0
Source Quenches	0	0
Redirects	0	0
Echo Replies	23	11
Echos	12	114
Timestamps	0	0
Timestamp Replies	0	0
Address Masks	0	0
Address Mask Replies	0	0
Router Solicitations	0	0
Router Advertisements	8	0

ICMPv6 Statistics

	Received	Sent
Messages	102689	1657
Errors	0	0
Destination Unreachable	0	0
Packet Too Big	0	0
Time Exceeded	0	0
Parameter Problems	0	0
Echos	0	0
Echo Replies	0	0
MLD Queries	98483	0
MLD Reports	0	0
MLD Dones	0	0
Router Solicitations	0	758
Router Advertisements	0	0
Neighbor Solicitations	43	457
Neighbor Advertisements	4163	442
Redirects	0	0
Router Renumberings	0	0

TCP Statistics for IPv4

Active Opens	= 29753
Passive Opens	= 1612
Failed Connection Attempts	= 2538
Reset Connections	= 6709
Current Connections	= 6

```

Reset Connections           = 6709
Current Connections        = 6
Segments Received          = 3844954
Segments Sent              = 2684697
Segments Retransmitted     = 48881

TCP Statistics for IPv6

Active Opens               = 80
Passive Opens              = 14
Failed Connection Attempts = 87
Reset Connections         = 28
Current Connections        = 0
Segments Received          = 4137
Segments Sent              = 4005
Segments Retransmitted     = 132

UDP Statistics for IPv4

Datagrams Received        = 2871627
No Ports                  = 57953
Receive Errors            = 6
Datagrams Sent            = 339334

UDP Statistics for IPv6

Datagrams Received        = 1219666
No Ports                  = 7699
Receive Errors            = 1
Datagrams Sent            = 11209

```

g.netstat -r ---->Displays the contents of the IP routing table. This is equivalent to the route print command.


```
C:\WINDOWS\system32>netstat -r
=====
Interface List
20...50 81 40 30 e6 ed .....Realtek PCIe GbE Family Controller
15...00 ff c9 7a 6a 90 .....ExpressVPN TAP Adapter
11...0a 00 27 00 00 0b .....VirtualBox Host-Only Ethernet Adapter
9...82 d2 1d fb e3 f3 .....Microsoft Wi-Fi Direct Virtual Adapter
18...c2 d2 1d fb e3 f3 .....Microsoft Wi-Fi Direct Virtual Adapter #2
10...80 d2 1d fb e3 f3 .....Realtek RTL8822CE 802.11ac PCIe Adapter
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        50
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        306
192.168.1.8                 255.255.255.255    On-link          192.168.1.8        306
192.168.1.255               255.255.255.255    On-link          192.168.1.8        306
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        306
255.255.255.255             255.255.255.255    On-link          127.0.0.1         331
255.255.255.255             255.255.255.255    On-link          192.168.56.1       281
255.255.255.255             255.255.255.255    On-link          192.168.1.8        306
=====
Persistent Routes:
None

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination          Gateway
1 331 ::1/128 On-link
11 281 fe80::/64 On-link
10 306 fe80::/64 On-link
11 281 fe80::5890:9542:683:4d7d/128 On-link
10 306 fe80::8181:96a9:19f3:33c4/128 On-link
1 331 ff00::/8 On-link
11 281 ff00::/8 On-link
10 306 ff00::/8 On-link
=====
Persistent Routes:
None
```

```
=====
Persistent Routes:
None

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination          Gateway
1 331 ::1/128 On-link
11 281 fe80::/64 On-link
10 306 fe80::/64 On-link
11 281 fe80::5890:9542:683:4d7d/128 On-link
10 306 fe80::8181:96a9:19f3:33c4/128 On-link
1 331 ff00::/8 On-link
11 281 ff00::/8 On-link
10 306 ff00::/8 On-link
=====
Persistent Routes:
None
```

h.netstat Interval---->Redisplays the selected information every Internal seconds. Press CTRL+C to stop the redisplay. If this parameter is omitted,

netstat prints the selected information only once.

```
C:\WINDOWS\system32>netstat interval
```

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

	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 between each display. Press CTRL+C to stop redisplaying statistics. If omitted, netstat will print the current configuration information once.

```

-y          Displays the TCP connection template for all connections.
           Cannot be combined with the other options.
interval    Redisplays selected statistics, pausing interval seconds
           between each display. Press CTRL+C to stop redisplaying
           statistics. If omitted, netstat will print the current
           configuration information once.

```

h.netstat/? ---->Displays help at the command prompt.

```

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.

```

TASK 6:

- **Displaying Address Resolution Protocol (ARP) cache using arp command**

18.The **arp -a** command displays ARP cache.The cache mapping of IP addresses with their respective MAC addresses.It has many options and if we use ARP without any option it displays the available options.

19.Type **arp -a** command and press Enter to display the ARP cache entries.

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

Interface: 10.11.133.91 --- 0xa
  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
  10.11.159.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.18            01-00-5e-00-00-12     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
  224.0.1.60            01-00-5e-00-01-3c     static
  239.192.152.143       01-00-5e-40-98-8f     static
  239.255.102.18        01-00-5e-7f-66-12     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.56.1 --- 0xb
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.18            01-00-5e-00-00-12     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
  224.0.1.60            01-00-5e-00-01-3c     static
  224.0.1.187           01-00-5e-00-01-bb     static
  224.77.77.77          01-00-5e-4d-4d-4d     static
  239.192.152.143       01-00-5e-40-98-8f     static
  239.255.102.18        01-00-5e-7f-66-12     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

C:\WINDOWS\system32>
```

20.Similarly we can use other commands for network administration and troubleshooting.

a.Gpresult ---->Starts the Operating System Group Policy Result tool.

```
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

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

Examples:

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

b. `ipconfig /flushdns` ----> Flushes the DNS resolver cache. Helpful when troubleshooting DNS name resolution problems.

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

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\WINDOWS\system32>
```

c. `nbstat -a<Machine Name>` ----> Obtains info from WINS or LMHOST (discovers who is logged on).

d. `nbtstat -A<IP>` ----> Gets info from WINS or LMHOST (discovers who is logged on).

e. `nbtstat -R` ----> Purges and reloads the remote cache name table.

```
C:\WINDOWS\system32>nbtstat -R
    Successful purge and preload of the NBT Remote Cache Name Table.

C:\WINDOWS\system32>
```

f.nbtstat -n ---->Lists local 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
        -----
        LAPTOP-KB8USE6Q<20>  UNIQUE      Registered
        LAPTOP-KB8USE6Q<00>  UNIQUE      Registered
        WORKGROUP            <00>        GROUP       Registered

Ethernet 2:
Node IpAddress: [0.0.0.0] Scope Id: []

        No names in cache

Ethernet:
Node IpAddress: [0.0.0.0] Scope Id: []

        No names in cache

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

        NetBIOS Local Name Table

        Name                Type        Status
        -----
        LAPTOP-KB8USE6Q<20>  UNIQUE      Registered
        LAPTOP-KB8USE6Q<00>  UNIQUE      Registered
        WORKGROUP            <00>        GROUP       Registered

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

        No names in cache
```



```

Ethernet:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache

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

    NetBIOS Local Name Table

    Name                Type        Status
    -----
    LAPTOP-KB8USE6Q<20>  UNIQUE      Registered
    LAPTOP-KB8USE6Q<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

C:\WINDOWS\system32>

```

g.nbtstat -r ---->Useful for detecting errors when browsing WINS or NetBIOS.

```

C:\WINDOWS\system32>nbtstat -r

    NetBIOS Names Resolution and Registration Statistics
    -----

    Resolved By Broadcast      = 0
    Resolved By Name Server    = 0

    Registered By Broadcast    = 111
    Registered By Name Server  = 179

C:\WINDOWS\system32>

```


h.netstat -ab ---->The b switch links each used port with its application.

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

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	LAPTOP-KB8USE6Q:0	LISTENING
RpcEptMapper [svchost.exe]			
TCP	0.0.0.0:445	LAPTOP-KB8USE6Q:0	LISTENING
Can not obtain ownership information			
TCP	0.0.0.0:5040	LAPTOP-KB8USE6Q:0	LISTENING
CDPSvc [svchost.exe]			
TCP	0.0.0.0:6646	LAPTOP-KB8USE6Q:0	LISTENING
[MMSSHOST.EXE]			
TCP	0.0.0.0:49664	LAPTOP-KB8USE6Q:0	LISTENING
[lsass.exe]			
TCP	0.0.0.0:49665	LAPTOP-KB8USE6Q:0	LISTENING

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	LAPTOP-KB8USE6Q:0	LISTENING
RpcEptMapper			
[svchost.exe]			
TCP	0.0.0.0:445	LAPTOP-KB8USE6Q:0	LISTENING
Can not obtain ownership information			
TCP	0.0.0.0:5040	LAPTOP-KB8USE6Q:0	LISTENING
CDPSvc			
[svchost.exe]			
TCP	0.0.0.0:6646	LAPTOP-KB8USE6Q:0	LISTENING
[MMSSHOST.EXE]			
TCP	0.0.0.0:49664	LAPTOP-KB8USE6Q:0	LISTENING
[lsass.exe]			
TCP	0.0.0.0:49665	LAPTOP-KB8USE6Q:0	LISTENING
Can not obtain ownership information			
TCP	0.0.0.0:49666	LAPTOP-KB8USE6Q:0	LISTENING
Schedule			
[svchost.exe]			
TCP	0.0.0.0:49667	LAPTOP-KB8USE6Q:0	LISTENING
EventLog			
[svchost.exe]			
TCP	0.0.0.0:49668	LAPTOP-KB8USE6Q:0	LISTENING
[spoolsv.exe]			
TCP	0.0.0.0:49670	LAPTOP-KB8USE6Q:0	LISTENING
Can not obtain ownership information			
TCP	127.0.0.1:2015	LAPTOP-KB8USE6Q:0	LISTENING
[expressvpnd.exe]			
TCP	127.0.0.1:65182	LAPTOP-KB8USE6Q:0	LISTENING
[ExpressVPNNotificationService.exe]			
TCP	127.0.0.1:65182	LAPTOP-KB8USE6Q:65188	ESTABLISHED
[ExpressVPNNotificationService.exe]			
TCP	127.0.0.1:65188	LAPTOP-KB8USE6Q:65182	ESTABLISHED
[expressvpnd.exe]			
TCP	192.168.1.8:139	LAPTOP-KB8USE6Q:0	LISTENING
Can not obtain ownership information			
TCP	192.168.1.8:65057	20.198.118.190:https	ESTABLISHED
WpnService			
[svchost.exe]			
TCP	192.168.1.8:65357	keralavisionisp-dynamic-34:https	CLOSE_WAIT
[SearchHost.exe]			
TCP	192.168.1.8:65396	maa05s16-in-f14:https	TIME_WAIT
TCP	192.168.1.8:65402	maa03s42-in-f2:https	TIME_WAIT

C:\> Administrator: Command Prompt

```
TCP    127.0.0.1:65182    LAPTOP-KB8USE6Q:0    LISTENING
[ExpressVPNNotificationService.exe]
TCP    127.0.0.1:65182    LAPTOP-KB8USE6Q:65188  ESTABLISHED
[ExpressVPNNotificationService.exe]
TCP    127.0.0.1:65188    LAPTOP-KB8USE6Q:65182  ESTABLISHED
[expressvpnd.exe]
TCP    192.168.1.8:139     LAPTOP-KB8USE6Q:0    LISTENING
Can not obtain ownership information
TCP    192.168.1.8:65057    20.198.118.190:https  ESTABLISHED
WpnService
[svchost.exe]
TCP    192.168.1.8:65357    keralavisionisp-dynamic-34:https  CLOSE_WAIT
[SearchHost.exe]
TCP    192.168.1.8:65396    maa05s16-in-f14:https  TIME_WAIT
TCP    192.168.1.8:65402    maa03s42-in-f2:https  TIME_WAIT
TCP    192.168.1.8:65403    maa03s42-in-f2:https  TIME_WAIT
TCP    192.168.1.8:65407    200:https            LAST_ACK
[chrome.exe]
TCP    192.168.1.8:65413    sd-in-f188:5228       ESTABLISHED
[chrome.exe]
TCP    192.168.56.1:139     LAPTOP-KB8USE6Q:0    LISTENING
Can not obtain ownership information
TCP    [::]:135             LAPTOP-KB8USE6Q:0    LISTENING
RpcEptMapper
[svchost.exe]
TCP    [::]:445             LAPTOP-KB8USE6Q:0    LISTENING
Can not obtain ownership information
TCP    [::]:49664           LAPTOP-KB8USE6Q:0    LISTENING
[lsass.exe]
TCP    [::]:49665           LAPTOP-KB8USE6Q:0    LISTENING
Can not obtain ownership information
TCP    [::]:49666           LAPTOP-KB8USE6Q:0    LISTENING
Schedule
[svchost.exe]
TCP    [::]:49667           LAPTOP-KB8USE6Q:0    LISTENING
EventLog
[svchost.exe]
TCP    [::]:49668           LAPTOP-KB8USE6Q:0    LISTENING
[spoolsv.exe]
TCP    [::]:49670           LAPTOP-KB8USE6Q:0    LISTENING
Can not obtain ownership information
TCP    [::1]:49669          LAPTOP-KB8USE6Q:0    LISTENING
[jhi service.exe]
```

Administrator: Command Prompt

```
[lsass.exe]
TCP    [::]:49665          LAPTOP-KB8USE6Q:0    LISTENING
Can not obtain ownership information
TCP    [::]:49666          LAPTOP-KB8USE6Q:0    LISTENING
Schedule
[svchost.exe]
TCP    [::]:49667          LAPTOP-KB8USE6Q:0    LISTENING
EventLog
[svchost.exe]
TCP    [::]:49668          LAPTOP-KB8USE6Q:0    LISTENING
[spoolsv.exe]
TCP    [::]:49670          LAPTOP-KB8USE6Q:0    LISTENING
Can not obtain ownership information
TCP    [::1]:49669         LAPTOP-KB8USE6Q:0    LISTENING
[jhi_service.exe]
UDP    0.0.0.0:123         *:*
W32Time
[svchost.exe]
UDP    0.0.0.0:5050        *:*
CDPSvc
[svchost.exe]
UDP    0.0.0.0:5353        *:*
[msedge.exe]
UDP    0.0.0.0:5353        *:*
[chrome.exe]
UDP    0.0.0.0:5353        *:*
Dnscache
[svchost.exe]
UDP    0.0.0.0:5353        *:*
[msedge.exe]
UDP    0.0.0.0:5353        *:*
[chrome.exe]
UDP    0.0.0.0:5353        *:*
[msedge.exe]
UDP    0.0.0.0:5353        *:*
[chrome.exe]
UDP    0.0.0.0:5353        *:*
[msedge.exe]
UDP    0.0.0.0:5353        *:*
[chrome.exe]
UDP    0.0.0.0:5355        *:*
Dnscache
[svchost.exe]
```

Administrator: Command Prompt

```
Dnscache
[svchost.exe]
UDP 0.0.0.0:6646 *: *
[MMSSHOST.EXE]
UDP 0.0.0.0:50569 172.217.160.138:443
[chrome.exe]
UDP 0.0.0.0:56719 142.250.196.46:443
[chrome.exe]
UDP 0.0.0.0:56786 142.250.77.142:443
[chrome.exe]
UDP 0.0.0.0:57967 142.250.195.193:443
[chrome.exe]
UDP 0.0.0.0:58236 142.250.183.238:443
[chrome.exe]
UDP 0.0.0.0:60082 172.217.163.163:443
[chrome.exe]
UDP 0.0.0.0:60815 142.250.196.3:443
[chrome.exe]
UDP 0.0.0.0:60930 *: *
Dnscache
[svchost.exe]
UDP 0.0.0.0:62223 142.250.193.138:443
[chrome.exe]
UDP 0.0.0.0:63355 103.168.200.79:443
[chrome.exe]
UDP 10.11.133.91:50340 172.17.18.2:53
[expressvpn.exe]
UDP 10.11.133.91:50774 172.17.18.2:53
[expressvpn.exe]
UDP 10.11.133.91:51226 172.17.18.2:53
[expressvpn.exe]
UDP 10.11.133.91:59422 172.17.18.2:53
[expressvpn.exe]
UDP 10.11.133.91:62901 172.17.18.2:53
[expressvpn.exe]
UDP 10.11.133.91:63194 172.17.18.2:53
[expressvpn.exe]
UDP 127.0.0.1:1900 *: *
SSDPSRV
[svchost.exe]
UDP 127.0.0.1:50764 *: *
SSDPSRV
[svchost.exe]
```

```
C:\> Administrator: Command Prompt

[chrome.exe]
UDP [::]:5353 *:*
Dnscache
[svchost.exe]
UDP [::]:5353 *:*
[msedge.exe]
UDP [::]:5353 *:*
[msedge.exe]
UDP [::]:5355 *:*
Dnscache
[svchost.exe]
UDP [::]:60930 *:*
Dnscache
[svchost.exe]
UDP [::1]:1900 *:*
SSDPSRV
[svchost.exe]
UDP [::1]:50761 *:*
SSDPSRV
[svchost.exe]
UDP [fe80::5890:9542:683:4d7d%11]:1900 *:*
SSDPSRV
[svchost.exe]
UDP [fe80::5890:9542:683:4d7d%11]:50759 *:*
SSDPSRV
[svchost.exe]
UDP [fe80::8181:96a9:19f3:33c4%10]:1900 *:*
SSDPSRV
[svchost.exe]
UDP [fe80::8181:96a9:19f3:33c4%10]:50760 *:*
SSDPSRV
[svchost.exe]

C:\WINDOWS\system32>
```

i.netstat -an ---->Shows 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	127.0.0.1:2015	0.0.0.0:0	LISTENING
TCP	127.0.0.1:61832	0.0.0.0:0	LISTENING
TCP	127.0.0.1:61832	127.0.0.1:61834	ESTABLISHED
TCP	127.0.0.1:61834	127.0.0.1:61832	ESTABLISHED
TCP	192.168.1.8:139	0.0.0.0:0	LISTENING
TCP	192.168.1.8:61661	20.198.119.84:443	ESTABLISHED
TCP	192.168.1.8:61900	31.13.79.53:443	ESTABLISHED
TCP	192.168.1.8:62131	172.217.194.188:5228	ESTABLISHED
TCP	192.168.1.8:62276	142.250.182.100:443	ESTABLISHED
TCP	192.168.1.8:62296	184.24.152.127:443	CLOSE_WAIT
TCP	192.168.1.8:62332	216.239.36.117:443	ESTABLISHED
TCP	192.168.1.8:62333	142.250.195.165:443	ESTABLISHED
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	:::49670	:::0	LISTENING
TCP	:::1:49669	:::0	LISTENING
UDP	0.0.0.0:123	*:*	
UDP	0.0.0.0:5050	*:*	
UDP	0.0.0.0:5353	*:*	

```

UDP    0.0.0.0:54150      142.250.183.238:443
UDP    0.0.0.0:54861      142.250.195.106:443
UDP    0.0.0.0:55027      8.8.4.4:443
UDP    0.0.0.0:63810      *: *
UDP    0.0.0.0:63987      142.250.195.106:443
UDP    0.0.0.0:64161      142.250.77.170:443
UDP    0.0.0.0:64830      142.250.183.238:443
UDP    0.0.0.0:65027      142.250.183.238:443
UDP    10.11.133.91:50340  172.17.18.2:53
UDP    10.11.133.91:50774  172.17.18.2:53
UDP    10.11.133.91:51226  172.17.18.2:53
UDP    10.11.133.91:59422  172.17.18.2:53
UDP    10.11.133.91:62901  172.17.18.2:53
UDP    10.11.133.91:63194  172.17.18.2:53
UDP    127.0.0.1:1900      *: *
UDP    127.0.0.1:50779     127.0.0.1:50779
UDP    127.0.0.1:60883     *: *
UDP    127.0.0.1:61576     127.0.0.1:61576
UDP    192.168.1.8:137     *: *
UDP    192.168.1.8:138     *: *
UDP    192.168.1.8:1900    *: *
UDP    192.168.1.8:54650    103.199.160.80:53
UDP    192.168.1.8:60882    *: *
UDP    192.168.56.1:137    *: *
UDP    192.168.56.1:138    *: *
UDP    192.168.56.1:1900    *: *
UDP    192.168.56.1:60881    *: *
UDP    [::]:123             *: *
UDP    [::]:5353            *: *
UDP    [::]:5353            *: *
UDP    [::]:5353            *: *
UDP    [::]:5353            *: *
UDP    [::]:5353            *: *
UDP    [::]:5355            *: *
UDP    [::]:49945           *: *
UDP    [::]:63810           *: *
UDP    [::1]:1900           *: *
UDP    [::1]:60880           *: *
UDP    [fe80::5890:9542:683:4d7d%11]:1900  *: *
UDP    [fe80::5890:9542:683:4d7d%11]:60878  *: *
UDP    [fe80::8181:96a9:19f3:33c4%10]:1900  *: *
UDP    [fe80::8181:96a9:19f3:33c4%10]:60879  *: *

```

j.netstat -an | find "15868" ---->Locates only lines with the number 15868 and redisplay every one second.


```
C:\> Administrator: Command Prompt
Microsoft Windows [Version 10.0.22000.978]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>netstat -an l | find "15868"

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

-y          Displays the TCP connection template for all connections.
           Cannot be combined with the other options.
interval    Redisplays selected statistics, pausing interval seconds
           between each display. Press CTRL+C to stop redisplaying
           statistics. If omitted, netstat will print the current
           configuration information once.

C:\WINDOWS\system32>
```

k.netstat -an | find "LISTENING" ---->Shows open ports with LISTENING status.

```

C:\WINDOWS\system32>netstat -an | 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    127.0.0.1:2015       0.0.0.0:0          LISTENING
TCP    127.0.0.1:65182      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    [::]:49670          [::]:0             LISTENING
TCP    [::1]:49669         [::]:0             LISTENING

C:\WINDOWS\system32>

```

l.net use ---->Retrieves a list of network connections.

```

C:\WINDOWS\system32>net use
New connections will be remembered.

There are no entries in the list.

C:\WINDOWS\system32>

```

m.net user ---->Shows user account for the computer.

```

C:\WINDOWS\system32>net user

User accounts for \\LAPTOP-KB8USE6Q

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

C:\WINDOWS\system32>

```

n.net user/domain ---->Displays user accounts for the domain.

```

C:\WINDOWS\system32>net user/domain
The syntax of this command is:

NET
[ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
  HELPMMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
  STATISTICS | STOP | TIME | USE | USER | VIEW ]

C:\WINDOWS\system32>

```

o.net user/domain<UserName> ---->Shows account details for specific user

p.net view/domain: <DomainName> | more ---->Shows user accounts from specific domain.

q.net view/cache ---->Shows workstation names.

```

STATISTICS | STOP | TIME | USE | USER | VIEW ]

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>

```

r.ping-a <IP> ---->Resolves IP to Hostnames.

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

Pinging LAPTOP-KB8USE6Q [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>
```

s.ping-t<IP> ---->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
```

t.Pathping ---->Displays the route and ping information when performing queries such as -n and -h options representing hostnames and maximum hops respectively.

```

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>

```

u.set U ---->Shows which user is logged on.

```

C:\WINDOWS\system32>set U
USERDOMAIN=LAPTOP-KB8USE6Q
USERDOMAIN_ROAMINGPROFILE=LAPTOP-KB8USE6Q
USERNAME=user
USERPROFILE=C:\Users\user

C:\WINDOWS\system32>

```

v.set L ---->Shows the logon server .

```

C:\WINDOWS\system32>set L
LOCALAPPDATA=C:\Users\user\AppData\Local
LOGONSERVER=\\LAPTOP-KB8USE6Q

C:\WINDOWS\system32>

```

w.telnet <IP> <port> ---->Confirms whether the port is open.

RESULT:

Studied and performed basic network administration and troubleshooting using Windows command line utilities.