Practical – 4

Submitted by: Om Gupta

Roll. No.: 214027

Explore and Write short note on the following network tools:

a) ipconfig:

- *ipconfig* is a command-line utility in Windows used to display the configuration of network interfaces on a local computer.
- It provides information about the computer's IP address, subnet mask, default gateway, and more.
- To find the IP address, subnet mask, class, host ID, and other details, simply open a command prompt and type ipconfig.

```
C:\Users\aaumg>ipconfig

Windows IP Configuration


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 WiFi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2406:b400:52:cbd5:2a12:2093:89f9:20a3
   Temporary IPv6 Address. . . . . . : 2406:b400:52:cbd5:4993:8ec9:e34b:e40
   Link-local IPv6 Address . . . . . : fe80::c7:234a:c899:28c9%8
   IPv4 Address. . . . . . . . . . . : 192.168.0.162
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::522b:73ff:fe95:dea0%8
                                       192.168.0.1
```

b) b. ping:

- `ping` is a network utility used to test the reachability of a host on an Internet Protocol (IP) network.
- It sends ICMP (Internet Control Message Protocol) echo request packets to a target host and waits for replies.
- You can use `ping` to check if you can connect to other systems on your network by pinging their IP addresses.

```
C:\Users\aaumg>ping 142.250.192.209

Pinging 142.250.192.209 with 32 bytes of data:
Reply from 142.250.192.209: bytes=32 time=5ms TTL=118
Reply from 142.250.192.209: bytes=32 time=6ms TTL=118
Reply from 142.250.192.209: bytes=32 time=7ms TTL=118
Reply from 142.250.192.209: bytes=32 time=6ms TTL=118

Ping statistics for 142.250.192.209:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 7ms, Average = 6ms
```

c) c. telnet:

- `telnet` is a network protocol and command used to establish a remote connection to a device over a network.
- It can be used for various purposes, including remote administration and troubleshooting.
- You can use `telnet` to connect to remote servers and network devices, but it's less secure than SSH.

d) d. ssh:

- `ssh` (Secure Shell) is a network protocol and command used to securely access and manage remote systems over a network.
- It provides encrypted communication, making it a more secure alternative to telnet for remote access.
- To use SSH, you need an SSH client and a remote system with SSH server software installed.

e) e. tracert/traceroute:

- `tracert` (Windows) or `traceroute` (Unix/Linux) is a network diagnostic tool used to trace the route that packets take from your computer to a target host.
- It helps you identify the network hops and latency along the path to a destination.
- To use `tracert` or `traceroute`, simply enter the command followed by the target host's IP or domain name.

With the help of ping, check if you are connected to other systems of your network and find the route to connect to that system using tracert.

```
C:\Users\aaumg>ping 192.168.0.197

Pinging 192.168.0.197 with 32 bytes of data:
Reply from 192.168.0.197: bytes=32 time=220ms TTL=64
Reply from 192.168.0.197: bytes=32 time=3ms TTL=64
Reply from 192.168.0.197: bytes=32 time=113ms TTL=64
Reply from 192.168.0.197: bytes=32 time=202ms TTL=64

Ping statistics for 192.168.0.197:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 220ms, Average = 134ms

C:\Users\aaumg>tracert 192.168.0.197

Tracing route to 192.168.0.197 over a maximum of 30 hops

  1    77 ms     4 ms    14 ms  192.168.0.197

Trace complete.
```

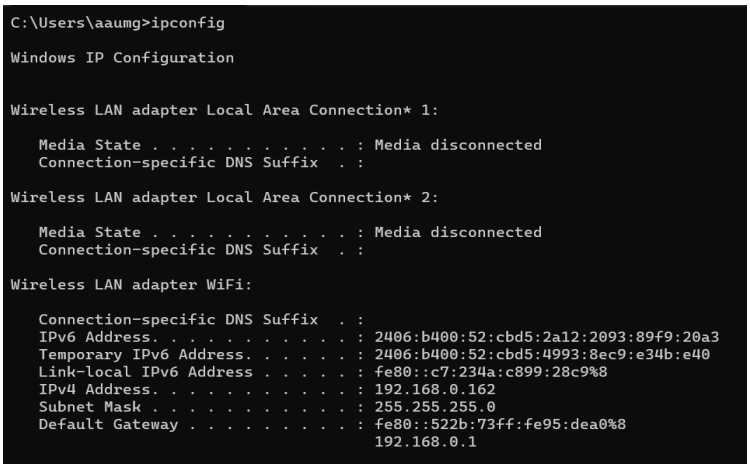
Explore netstat command and list all the processes which are using ports for TCP protocol.

```
C:\Users\aaumg>netstat -ano | find "TCP"
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1224
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       6456
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING       1676
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       560
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       884
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       2792
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       2944
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       3504
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING       424
  TCP    127.0.0.1:43227        0.0.0.0:0              LISTENING       9092
  TCP    192.168.0.162:139      0.0.0.0:0              LISTENING       4
  TCP    192.168.0.162:49423    20.198.119.84:443      ESTABLISHED     4136
  TCP    192.168.0.162:63162    20.198.119.84:443      ESTABLISHED     10116
  TCP    192.168.0.162:63195    20.212.88.117:443      ESTABLISHED     10116
  TCP    192.168.0.162:63197    192.168.0.160:8009     ESTABLISHED     10116
  TCP    192.168.0.162:65384    3.109.6.190:443        TIME_WAIT       0
  TCP    [::]:135               [::]:0                 LISTENING       1224
  TCP    [::]:445               [::]:0                 LISTENING       4
  TCP    [::]:7680              [::]:0                 LISTENING       1676
  TCP    [::]:49664             [::]:0                 LISTENING       560
  TCP    [::]:49665             [::]:0                 LISTENING       884
  TCP    [::]:49666             [::]:0                 LISTENING       2792
  TCP    [::]:49667             [::]:0                 LISTENING       2944
  TCP    [::]:49668             [::]:0                 LISTENING       3504
  TCP    [::]:49670             [::]:0                 LISTENING       424
  TCP    [::1]:42050            [::]:0                 LISTENING       6752
  TCP    [::1]:49669            [::]:0                 LISTENING       4440
  TCP    [2406:b400:52:cbd5:4993:8ec9:e34b:e40]:63893  [2600:140f:5::17d9:6eca]:443  CLOSE_WAIT      5992
  TCP    [2406:b400:52:cbd5:4993:8ec9:e34b:e40]:65376  [2a03:2880:f22f:1c7:face:b00c:0:7260]:5222  TIME_WAIT       0
  TCP    [2406:b400:52:cbd5:4993:8ec9:e34b:e40]:65377  [2a03:2880:f244:c2:face:b00c:0:167]:443  ESTABLISHED     6716
  TCP    [2406:b400:52:cbd5:4993:8ec9:e34b:e40]:65378  [2a03:2880:f244:c2:face:b00c:0:167]:443  ESTABLISHED     6716
  TCP    [2406:b400:52:cbd5:4993:8ec9:e34b:e40]:65379  [2a03:2880:f244:c2:face:b00c:0:167]:443  ESTABLISHED     6716
  TCP    [2406:b400:52:cbd5:4993:8ec9:e34b:e40]:65380  [2a03:2880:f244:1c3:face:b00c:0:167]:443  ESTABLISHED     6716
  TCP    [2406:b400:52:cbd5:4993:8ec9:e34b:e40]:65381  [2406:b400:50:5:face:b00c:3333:7020]:443  ESTABLISHED     6716
  TCP    [2406:b400:52:cbd5:4993:8ec9:e34b:e40]:65382  [2a03:2880:f22f:c5:face:b00c:0:167]:443  ESTABLISHED     6716
  TCP    [2406:b400:52:cbd5:4993:8ec9:e34b:e40]:65383  [2a03:2880:f22f:1c6:face:b00c:0:167]:443  ESTABLISHED     6716
```

Display your systems IP Address, Subnet mask using ipconfig, and find out the following:

IP Address: 192.168.0.162

Subnet Mask: 255.255.255.0



a) **class of this IP address**

Class C

b) **Host id**

192.168.0.162

c) **Maximum no. of subnets**

$2^0 = 1$

(Since, the subnet mask is the default one of Class C and there are no borrowed bits, no subnetting happening actually.)

d) **Subnet address of your host**

192.168.0.0