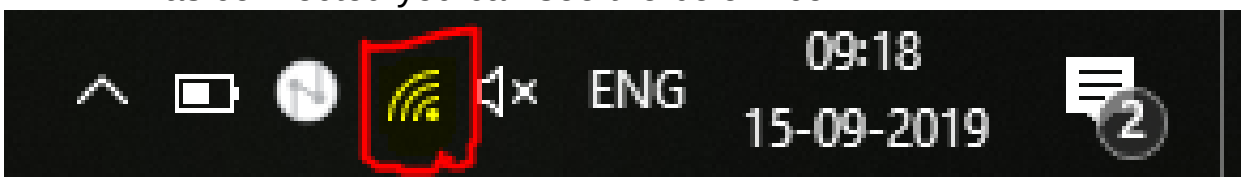
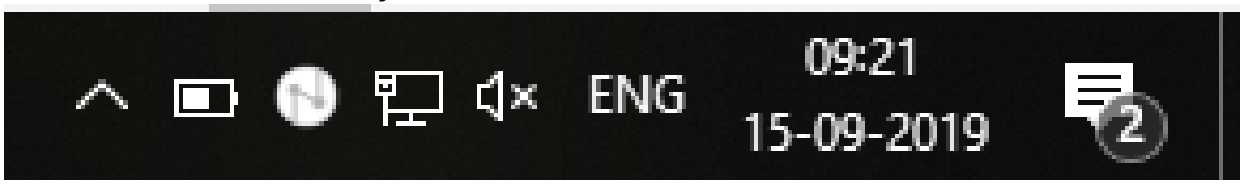
TROUBLESHOOTING STEPS:

1) CHECK THE CONNECTIVITY

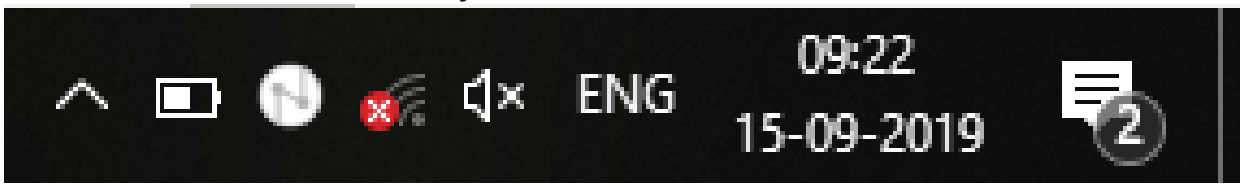
If WI-FI was connected you can see the below icon



If LAN was connected you can see the below icon



If WI-FI was not connected you can see the below icon



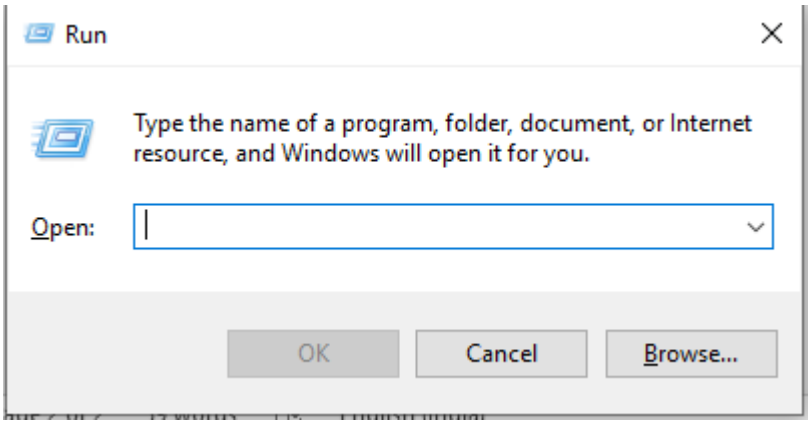
If LAN was not connected you can see the below icon

If there is no connectivity even you connected the cable to port. Then there is a problem either with the cable or with the port.

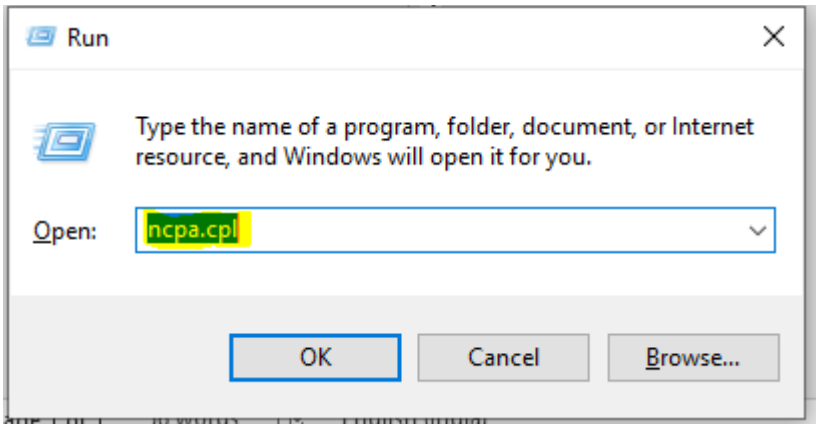
Just check with other cable and check the connectivity even it was not connected then you can confirm there may be port issue.

2) ***ENABLE THE NETWORK***

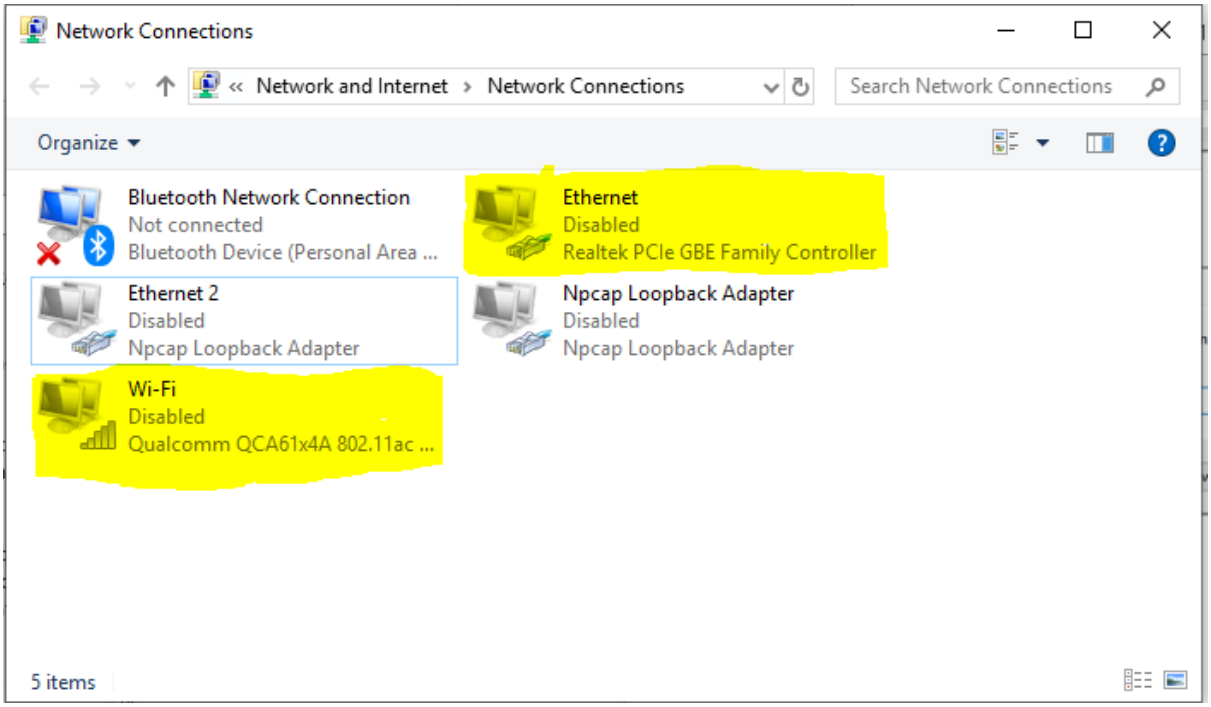
Press start button type run and press enter



Type **ncpa.cpl** and press **OK**

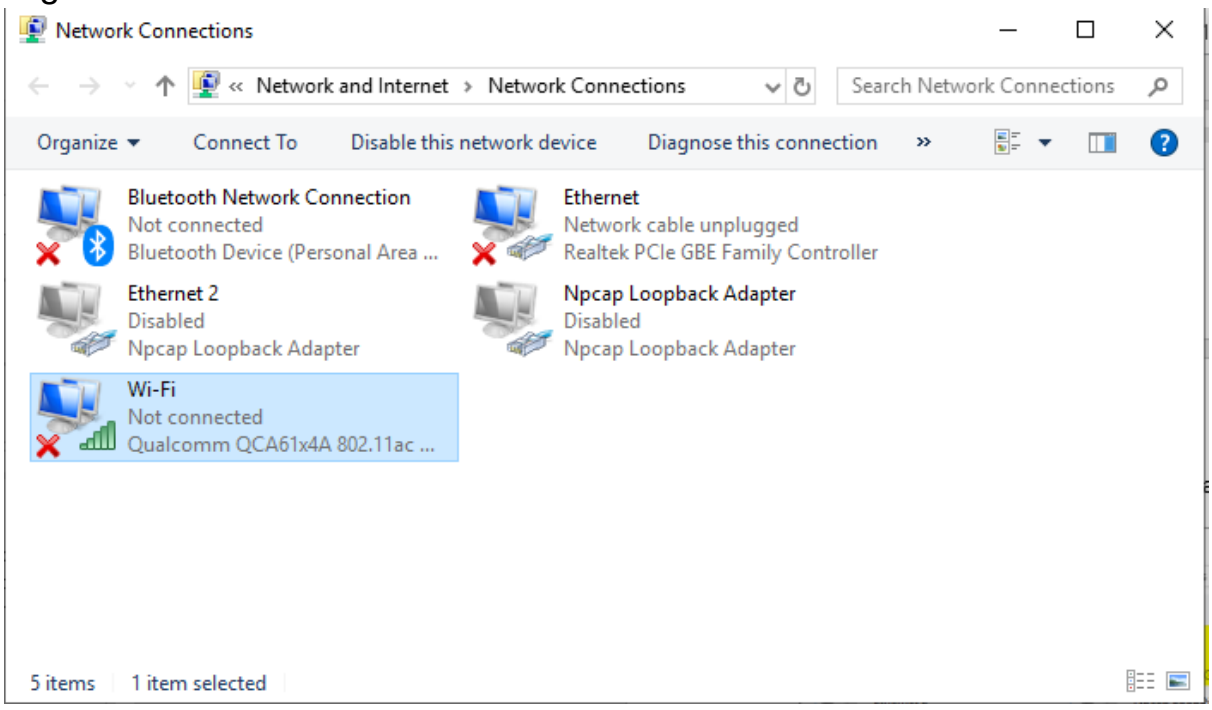


Check whether the Ethernet and WI-FI was in Disable state or Enable State

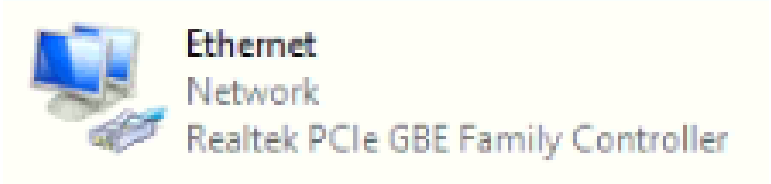


In case the port is in Disable state just Enable it.

Right click on it and select Enable



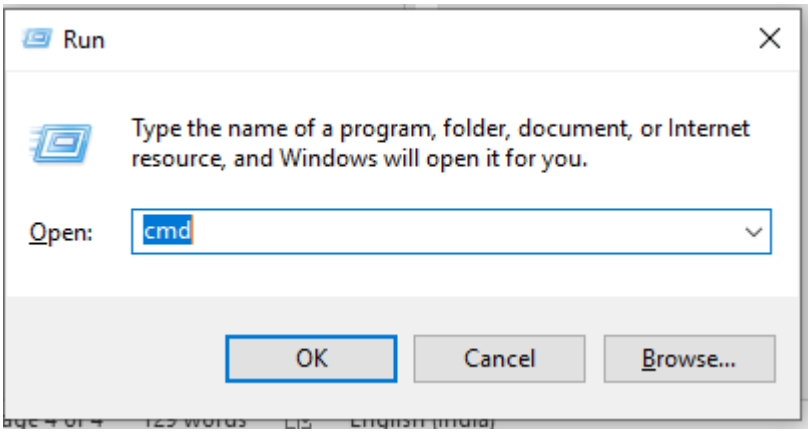
If the connectivity was there then you can see like below image



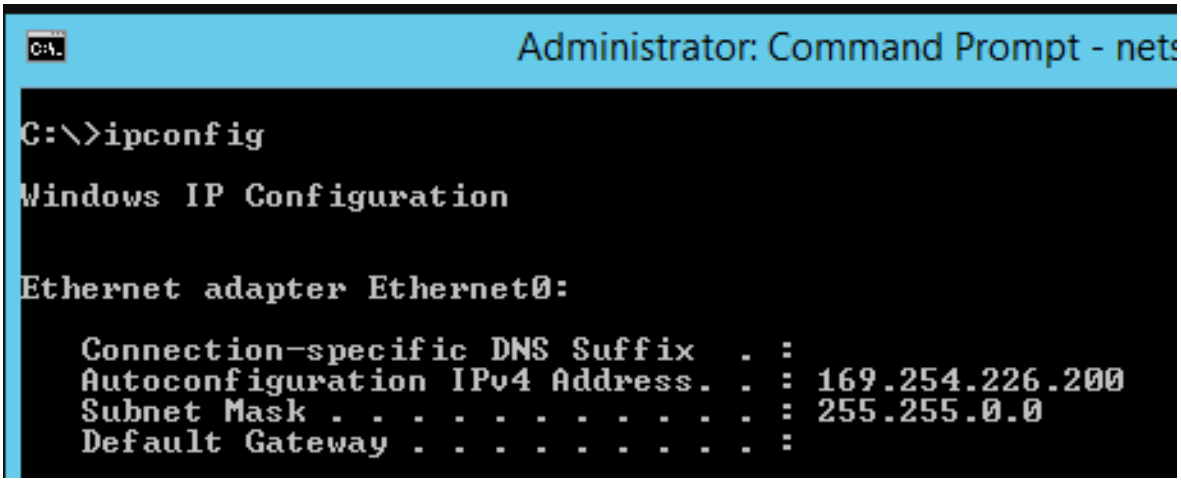
3) ***IP ADDRESS***

Now you have to check whether you are getting the IP address are not.

Go to RUN and type **“CMD”**



Type ipconfig



If you find that 169.254.X.X network address then you are not getting IP Address.

This IP Address is called **APIPA (Automatic Private IP Address)** Its range is 169.254.1.1 to 169.254.254.254 so what ever IP you are getting in this range is APIPA.

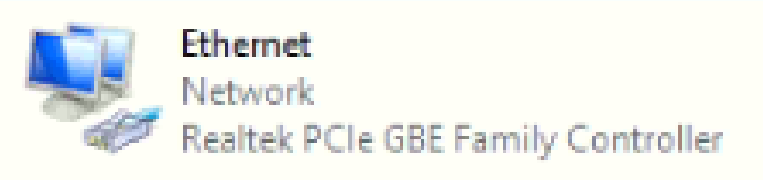
This will happen due to connectivity issue or DHCP (Dynamic Host Configuration Protocol) is not releasing the IP Address so you have to check the connectivity or follow the below steps.

i. Click on Start and click Run.
ii. Inside Run, type ipconfig /release to release the IP address.
iii. Then after the IP address is released, type ipconfig /renew

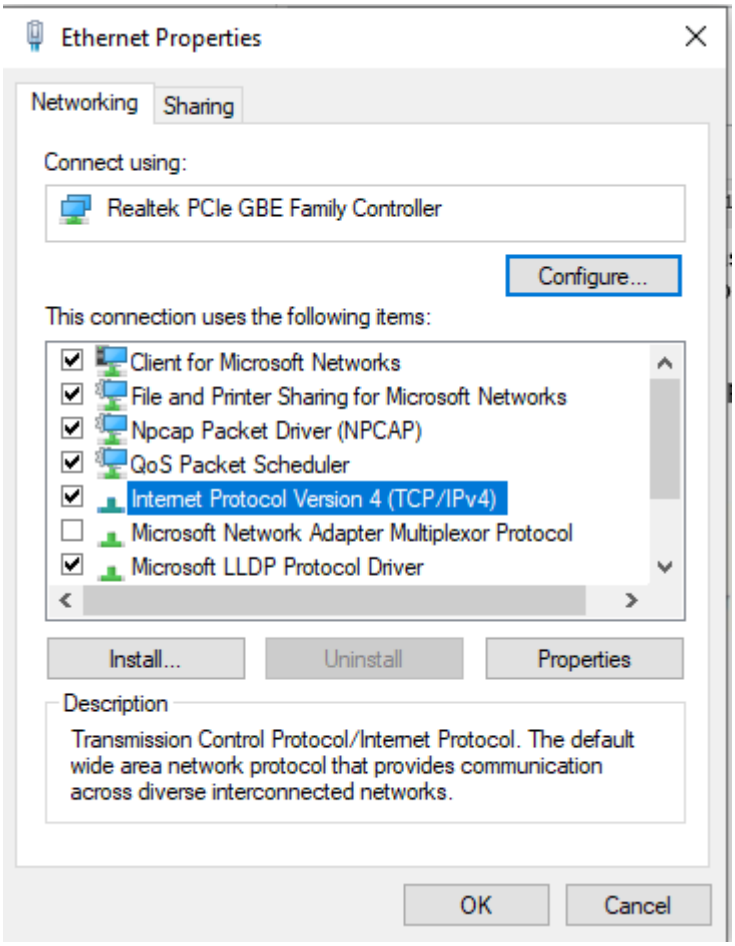
4) REMOVE THE STATIC IP

If any static IP was assigned to your Desktop / Laptop just make it into Dynamic.

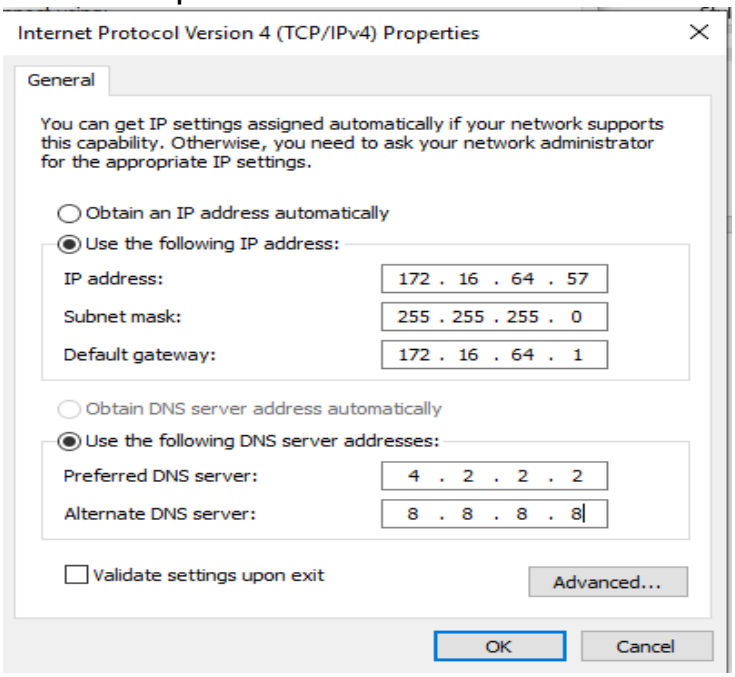
Steps to check the static IP Address



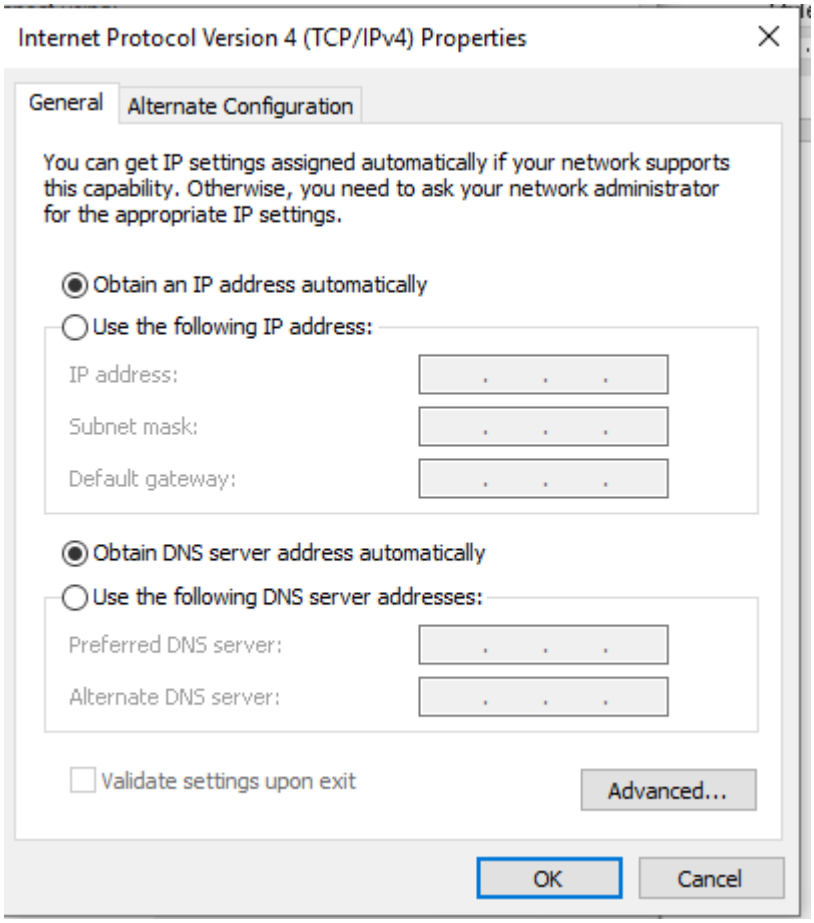
Right Click on Ethernet select Properties
Here Select Internet Protocol Version 4 (TCP/IP4) and click on properties.



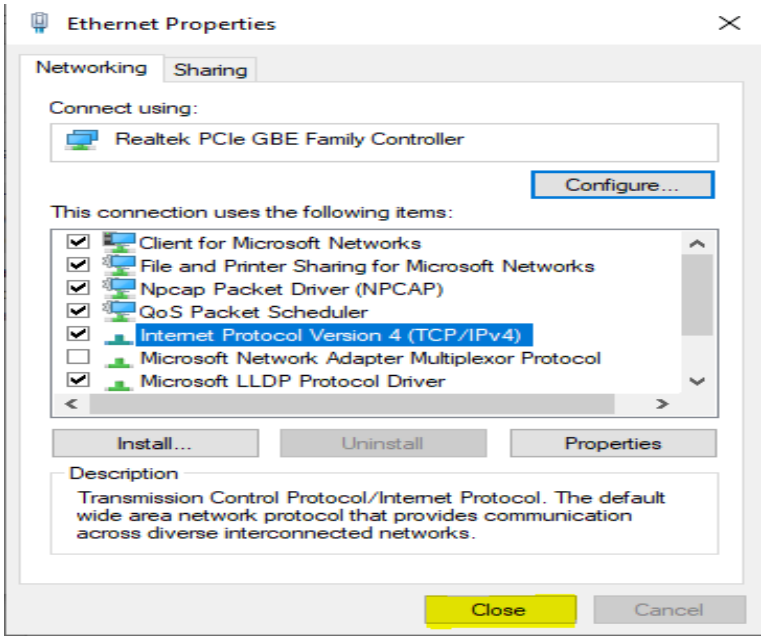
Select Properties



If you find any IP Address which was mention like above image then select “**Obtain an IP address automatically”** and **“Obtain an DNS server address automatically”**



Press **“OK”**



Click on **Close.**

5) ***VALID IP ADDRESS***

Inside the campus we will get 172.16.X.X network IP Address. So, check whether you are getting valid IP address or not.

```
C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::689f:3c3c:f8aa:61fa%3
   IPv4 Address. . . . . . . . . . . : 172.16.
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Default Gateway . . . . . . . . . : 172.16.  .1
```

In case you are getting 192.168.X.X network then it may be someone connected modem in the network.

While getting 192.168.X.X network IP Address sometimes you can access internet and sometimes you are unable to access the internet.

So, please make sure which IP Address you are getting.

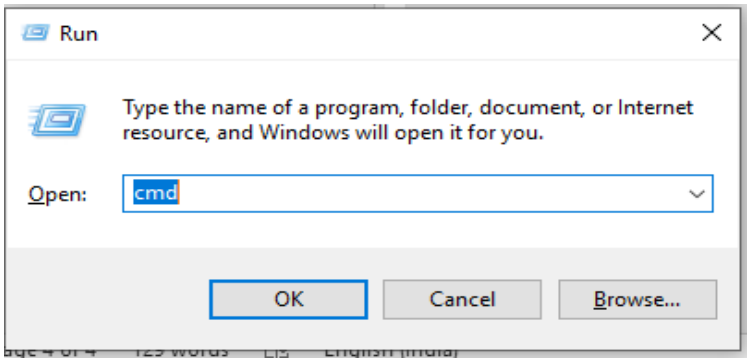
For getting detail of all IP's type "**ipconfig /all"**

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

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-PEO2R5D
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   Physical Address. . . . . . . . . : D8-9E-F3-1A-11-AE
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::689f:3c3c:f8aa:61fa%3(Preferred)
   IPv4 Address. . . . . . . . . . . : 172.16.  (Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Default Gateway . . . . . . . . . : 172.16.  .1
   DHCPv6 IAID . . . . . . . . . . . : 64528115
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-33-4C-7E-D8-9E-F3-1A-11-AE
   DNS Servers . . . . . . . . . . . : 4.2.2.2
                                       172.16.0.30
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

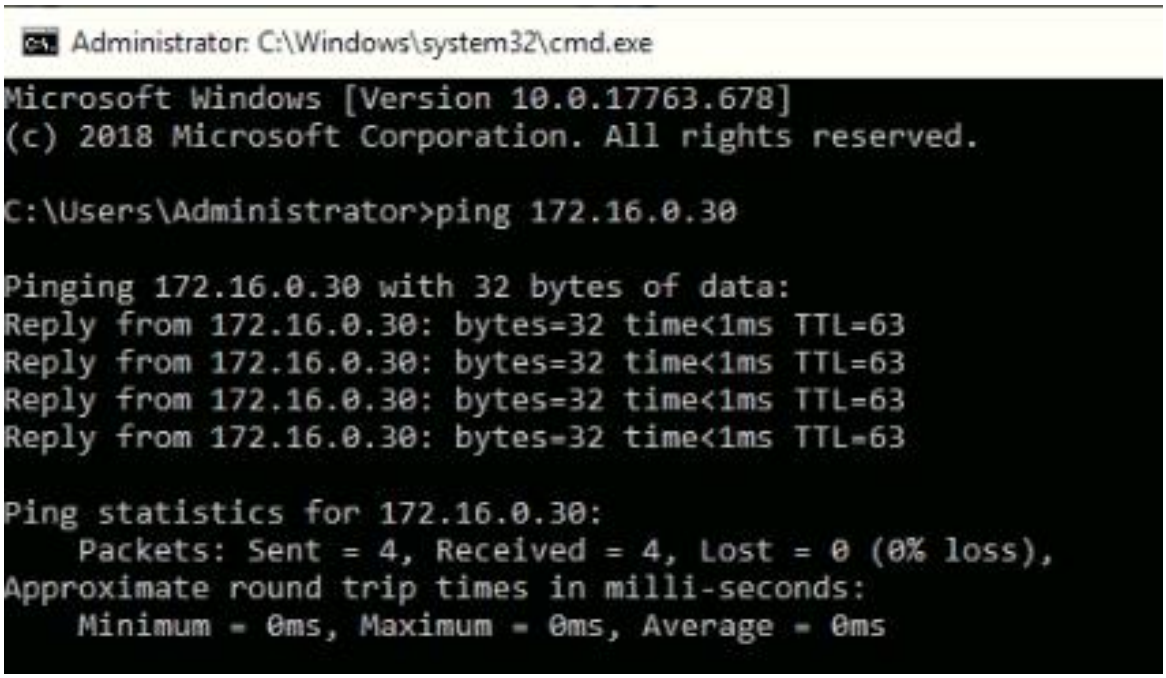
6) ***CONNECTIVITY TEST FROM SOPHOS FIREWALL (TROUBLESHOOTING).***

First check whether the firewall is able to communicate

Go to RUN and type **“CMD”**

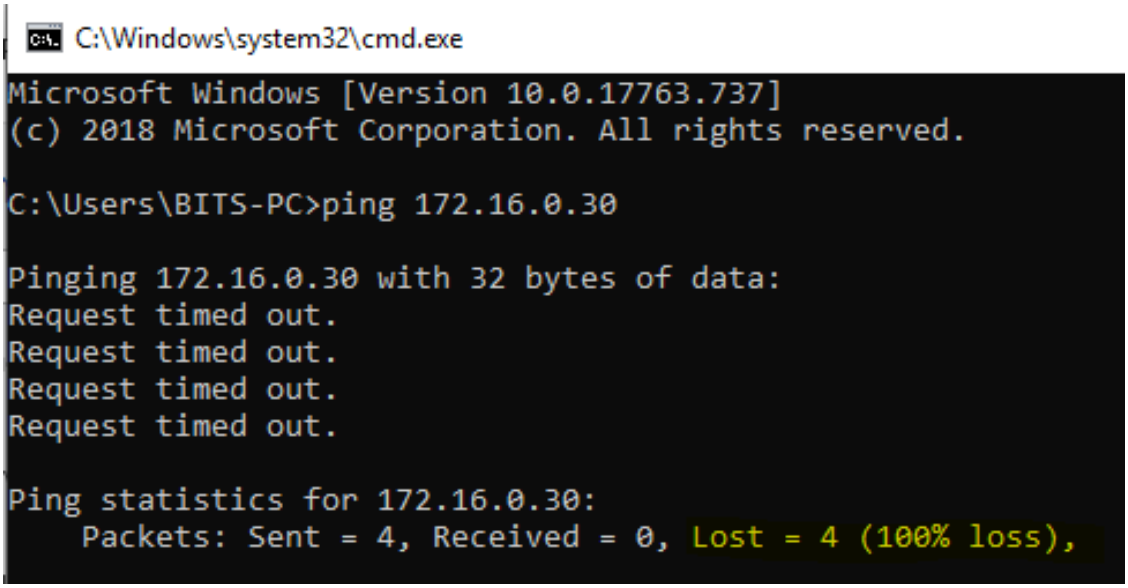


Type “**ping 172.16.0.30”**

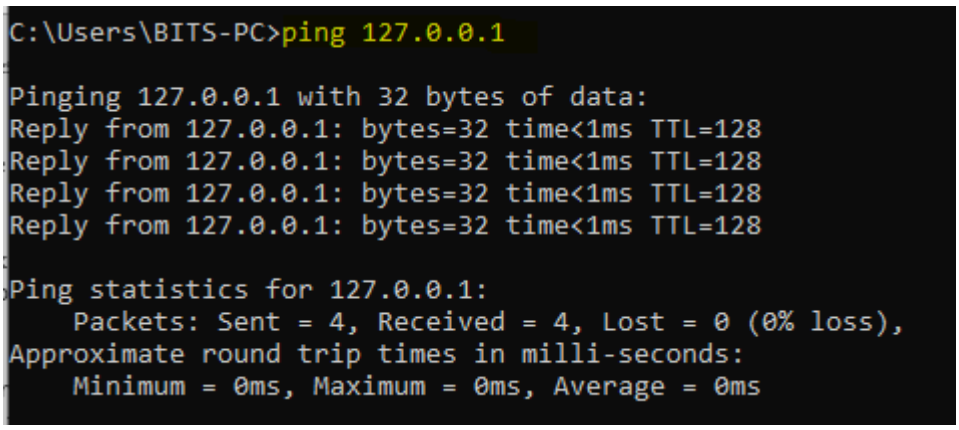


If you are getting reply from the firewall then there is no issue from the firewall.

If any issue was there from firewall or you are not connected to the firewall properly the packet will be lost.



If you are unable to communicate the firewall then you can't access the internet.
Then check your LAN adapter whether it is working properly are there is some issue to check it type "**ping 127.0.0.1**". It is Loopback address even you didn't have the network connectivity you will get the reply.

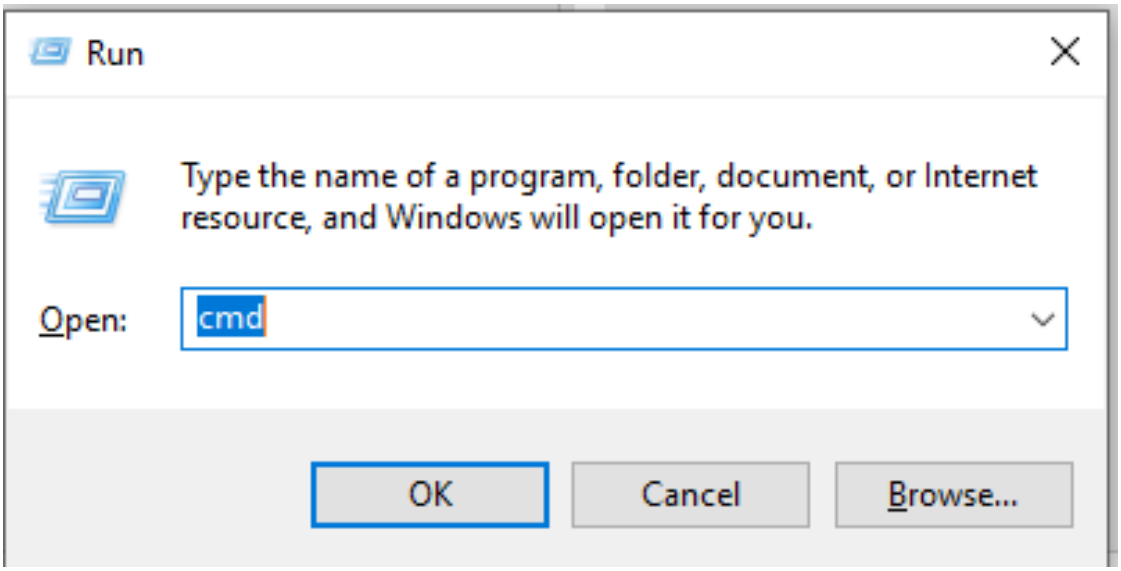


7) PACKET LOSS TEST (CONTINUOUS PING)

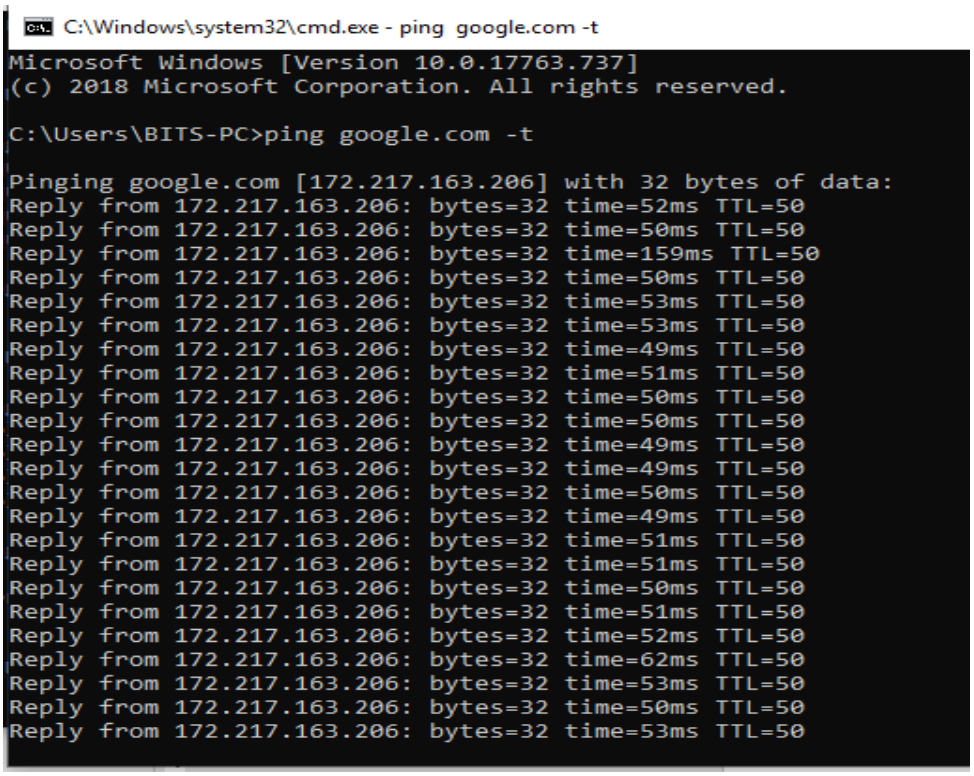
To test the packet loss, we have to ping continuously to particular website or particular IP.

Here I'm showing the google.com

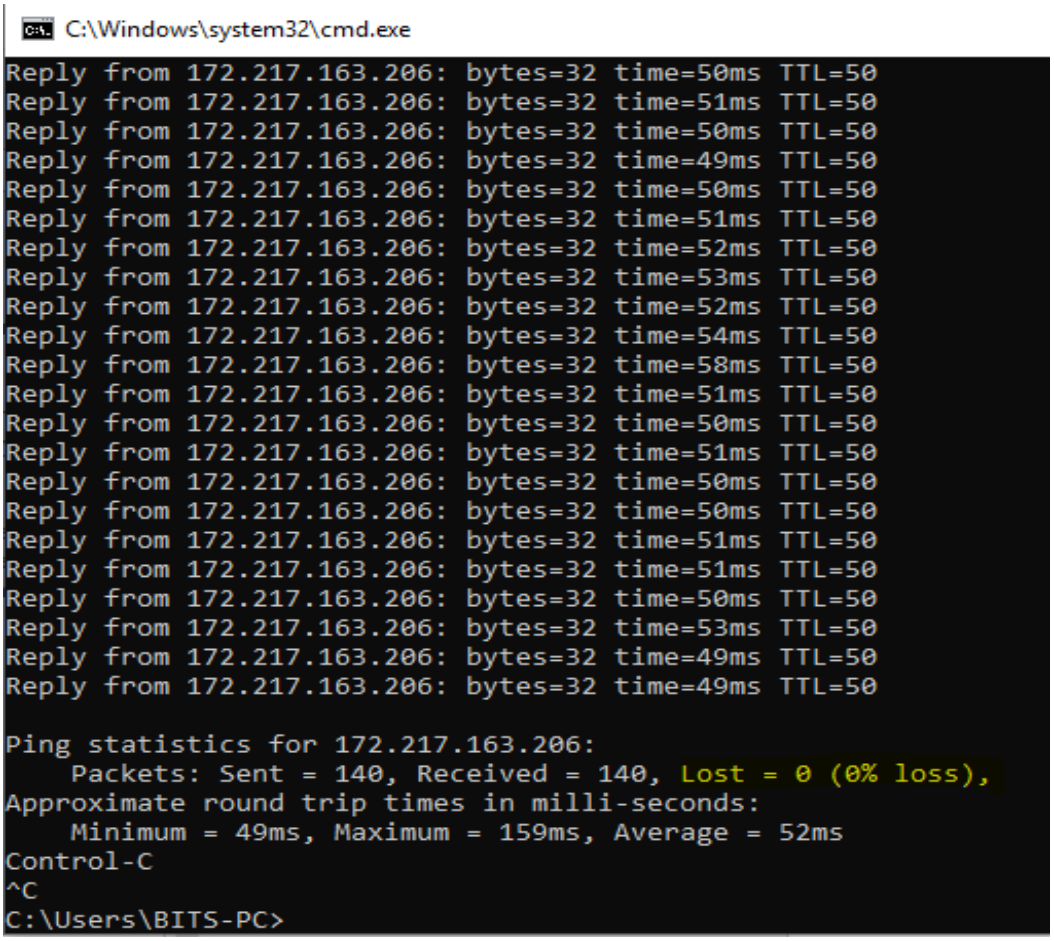
Go to RUN and type **"CMD"**



Type **ping google.com -t**



Until pressing **CTRL+C** it will ping continuously.

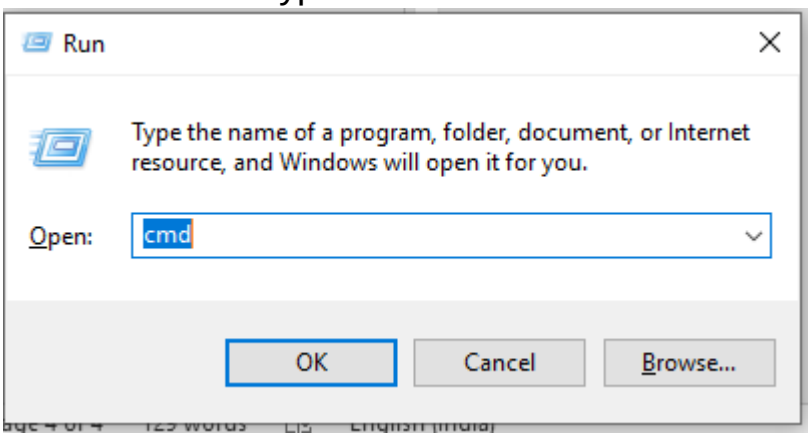


Here there is no loss in the packets or connectivity.

8) ***TRACE ROUTE THE PATH***

The connectivity was good and able to ping the SOPHOS firewall but still not getting internet then check whether you are allowed from the firewall.

Go to RUN and type **“CMD”**



Type **“tracert google.com”**

```
C:\Users\Administrator>tracert google.com

Tracing route to google.com [172.217.166.46]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  172.16.2.4
  2    <1 ms    <1 ms    <1 ms  172.16.0.30
  3    10 ms     4 ms     3 ms  136.232.34.53
  4    15 ms     4 ms     4 ms  115.113.207.165.static-hyderabad.vsnl.net.in [115.113.207.165]
  5    14 ms    15 ms    15 ms  172.17.31.109
  6    14 ms    14 ms     *     172.16.168.33
  7    15 ms    14 ms    17 ms  216.239.42.242
  8    17 ms    31 ms    20 ms  121.240.1.50
  9    16 ms    16 ms    18 ms  74.125.242.155
 10    17 ms    33 ms    55 ms  108.170.248.209
 11    29 ms    29 ms    63 ms  108.170.235.51
 12    30 ms    19 ms    50 ms  bom07s18-in-f14.1e100.net [172.217.166.46]
```

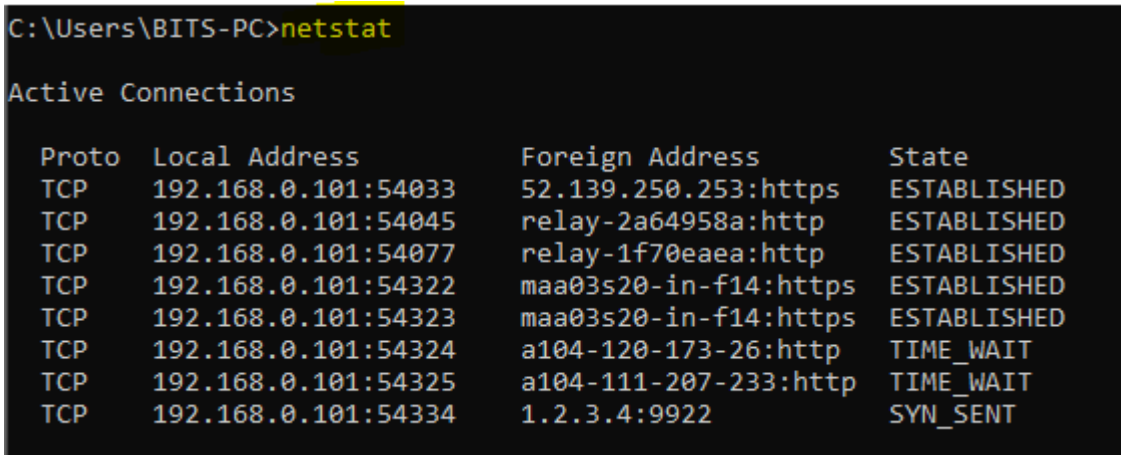
If any site was not allowed in the firewall then it will drop at the firewall.

```
C:\Users\Administrator>tracert google.com

Tracing route to google.com [172.217.166.46]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  172.16.2.4
  2    <1 ms    <1 ms    <1 ms  172.16.0.30
  3    10 ms     4 ms     3 ms  136.232.34.53
  4    15 ms     4 ms     4 ms  115.113.207.165.static-hyderabad.vsnl.net.in [115.113.207.165]
  5    14 ms    15 ms    15 ms  172.17.31.109
  6    14 ms    14 ms     *     172.16.168.33
  7    15 ms    14 ms    17 ms  216.239.42.242
  8    17 ms    31 ms    20 ms  121.240.1.50
  9    16 ms    16 ms    18 ms  74.125.242.155
 10    17 ms    33 ms    55 ms  108.170.248.209
 11    29 ms    29 ms    63 ms  108.170.235.51
 12    30 ms    19 ms    50 ms  bom07s18-in-f14.1e100.net [172.217.166.46]
```

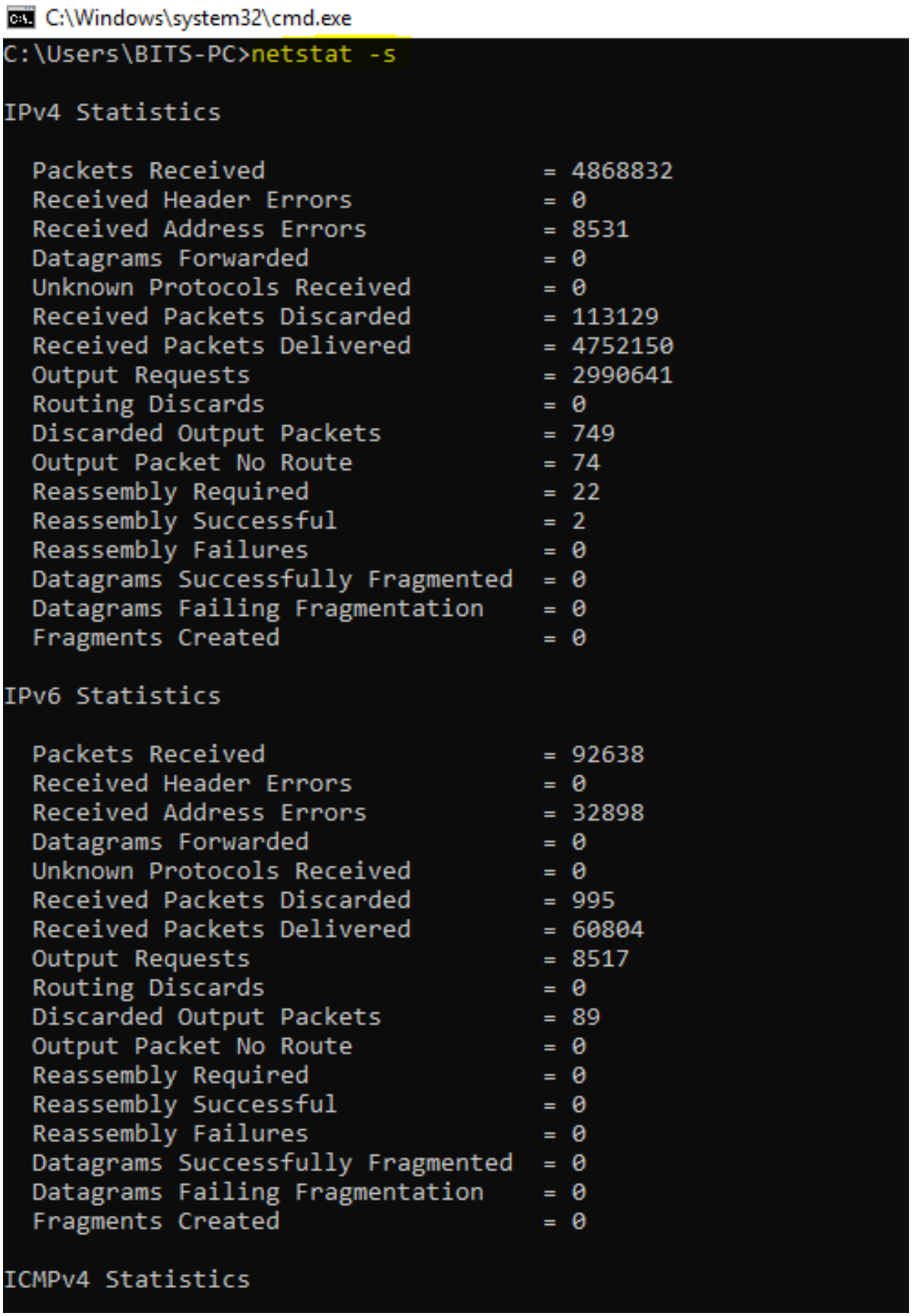
9) ***NETSTAT***

Netstat (Network Statistics) displays network connections (both incoming and outgoing), routing tables, and a number of network interface statistics

It is used to check traffic on the network as a performance measurement.

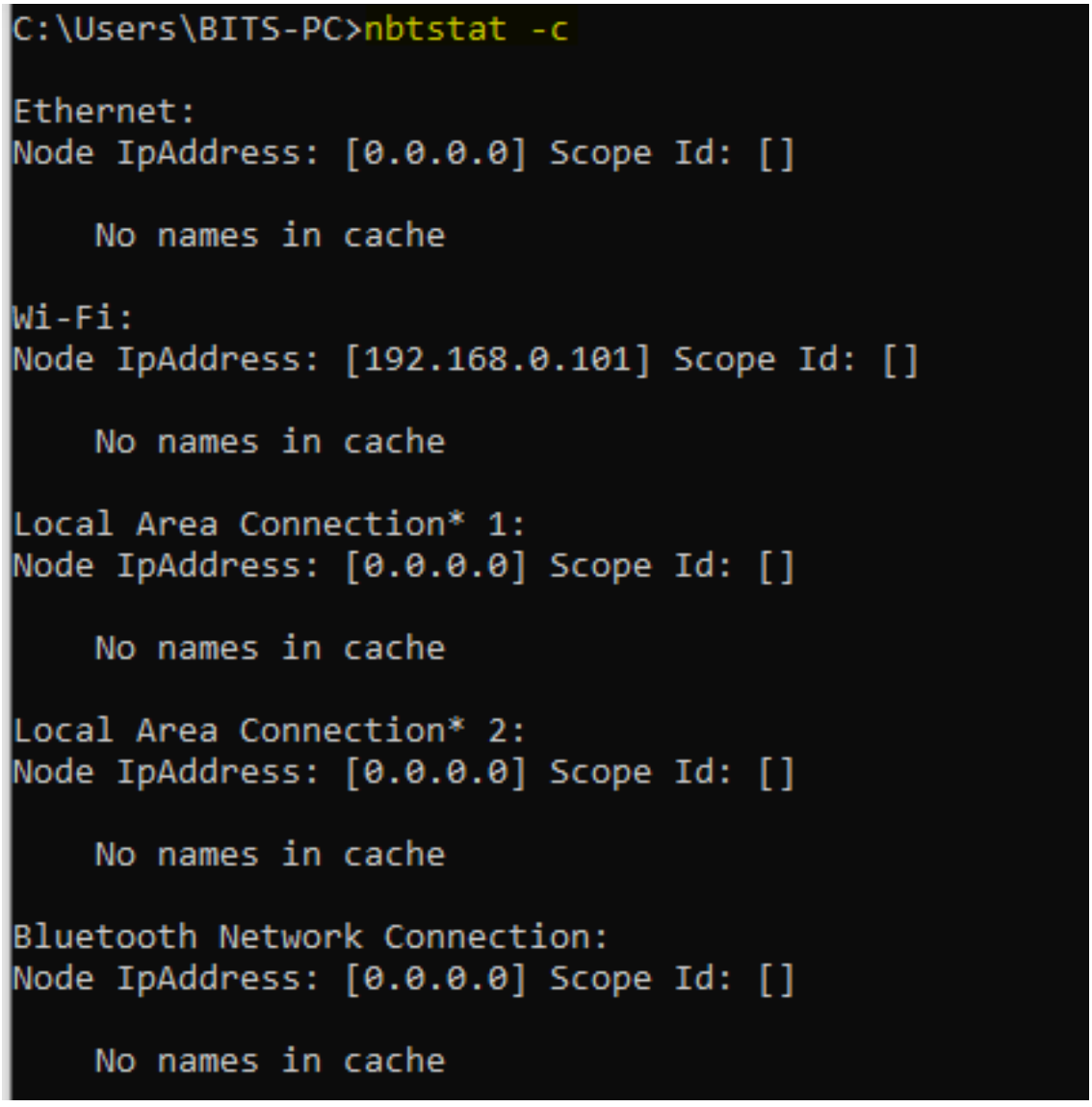


Netstat –s provides statistics about incoming and outgoing traffic.


C:\Windows\system32\cmd.exe
C:\Users\BITS-PC>netstat -s
IPv4 Statistics
Packets Received = 4868832
Received Header Errors = 0
Received Address Errors = 8531
Datagrams Forwarded = 0
Unknown Protocols Received = 0
Received Packets Discarded = 113129
Received Packets Delivered = 4752150
Output Requests = 2990641
Routing Discards = 0
Discarded Output Packets = 749
Output Packet No Route = 74
Reassembly Required = 22
Reassembly Successful = 2
Reassembly Failures = 0
Datagrams Successfully Fragmented = 0
Datagrams Failing Fragmentation = 0
Fragments Created = 0
IPv6 Statistics
Packets Received = 92638
Received Header Errors = 0
Received Address Errors = 32898
Datagrams Forwarded = 0
Unknown Protocols Received = 0
Received Packets Discarded = 995
Received Packets Delivered = 60804
Output Requests = 8517
Routing Discards = 0
Discarded Output Packets = 89
Output Packet No Route = 0
Reassembly Required = 0
Reassembly Successful = 0
Reassembly Failures = 0
Datagrams Successfully Fragmented = 0
Datagrams Failing Fragmentation = 0
Fragments Created = 0
ICMPv4 Statistics

10) NBTSTAT

Nbtstat (NetBios over TCP/IP) enables you to check information about NetBios names. It helps us view the NetBios name cache (nbtstat -c) which shows the NetBios names and the corresponding IP address that has been resolved (nbtstat -r) by a particular host as well as the names that have been registered by the local system (nbtstat –n).



```
C:\Users\BITS-PC>nbtstat -n

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

    No names in cache

Wi-Fi:
Node IpAddress: [192.168.0.101] Scope Id: []

                NetBIOS Local Name Table

       Name               Type         Status
    ---------------------------------------------
    DESKTOP-OU2E6K6<00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered
    DESKTOP-OU2E6K6<20>  UNIQUE      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

Bluetooth Network Connection:
```

11) NSLOOKUP

NSLookup provides a command-line utility for diagnosing DNS problems. In its most basic usage, NSLookup returns the IP address with the matching host name.

```
C:\Users\Administrator>nslookup google.com
Server:  b.resolvers.Level3.net
Address:  4.2.2.2

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4009:80c::200e
          172.217.26.238
```

DONT's

MODEMS ARE NOT ALLOWED IN THE HOSTELS*