

Name: Manan Aggarwal
Roll Number: 2022273

Q1. a)

```
manan@DESKTOP-S69HDK5:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1280
    inet 172.21.66.114 netmask 255.255.240.0 broadcast 172.21.79.255
    inet6 fe80::215:5dff:fe81:c36b prefixlen 64 scopeid 0x20<link>
    ether 00:15:5d:81:c3:6b txqueuelen 1000 (Ethernet)
    RX packets 138 bytes 297393 (297.3 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 105 bytes 9136 (9.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0


lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 48 bytes 3469 (3.4 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 48 bytes 3469 (3.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

IP address for network interface eth0 is 172.21.66.114


IP address for network interface lo is 127.0.0.1 which is also the loopback interface and not actually connected to the internet


b)

What Is My IP?

My Public IPv4: [103.25.231.126](#) 

My Public [IPv6](#): Not Detected

My IP Location: Noida, UP IN 

My ISP: Indraprastha Institute of Information Technology Delhi 

The IP assigned for network interface eth0 is different from the IP address obtained from <https://www.whatismyip.com> since the IP assigned for eth0 is the local ip address and the IP address obtained from the website is the global IP address

Q2.

The command utilized to change the IP address was

```
sudo ifconfig eth0 172.21.66.115
```

```
manan@DESKTOP-S69HDK5:~$ sudo ifconfig eth0 172.21.66.115
manan@DESKTOP-S69HDK5:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1280
    inet 172.21.66.115 netmask 255.255.0.0 broadcast 172.21.255.255
    inet6 fe80::215:5dff:fe81:c36b prefixlen 64 scopeid 0x20<link>
    ether 00:15:5d:81:c3:6b txqueuelen 1000 (Ethernet)
    RX packets 196 bytes 311728 (311.7 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 119 bytes 10432 (10.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

In the above screenshot we can see that the IP address has been changed from 172.21.66.114 to 172.21.66.115

This change can be reverted back by using the command

```
sudo ifconfig eth0 172.21.66.114
```

```
manan@DESKTOP-S69HDK5:~$ sudo ifconfig eth0 172.21.66.114
manan@DESKTOP-S69HDK5:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1280
    inet 172.21.66.114 netmask 255.255.0.0 broadcast 172.21.255.255
    inet6 fe80::215:5dff:fe81:c36b prefixlen 64 scopeid 0x20<link>
    ether 00:15:5d:81:c3:6b txqueuelen 1000 (Ethernet)
    RX packets 208 bytes 313895 (313.8 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 120 bytes 10502 (10.5 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Q3. a)

Using the command to open a netcat server on port 8888

```
netcat -l 8888
```

```
manan@DESKTOP-S69HDK5:~$ netcat -l 8888
hi
```

Connecting to localhost port 8888 using

```
netcat localhost 8888
```

```
manan@DESKTOP-S69HDK5:~$ netcat localhost 8888
hi
```

b)

Using the command to find all network connections using port 8888

```
netstat | grep 8888
```

```
manan@DESKTOP-S69HDK5:~$ netstat | grep 8888
tcp        0      0 localhost:58680    localhost:8888    ESTABLISHED
tcp        0      0 localhost:8888     localhost:58680   ESTABLISHED
```

The state of the TCP connection is ESTABLISHED

Q4. a)

First we find the authoritative nameserver using nslookup using

```
nslookup -type=soa google.in
```

This gives the state of authority name server for google.in

```
Authoritative answers can be found from:
google.in
    origin = ns1.google.com
    mail addr = dns-admin.google.com
    serial = 664720666
    refresh = 900
    retry = 900
    expire = 1800
    minimum = 60
```

Now we query ns1.google.com for the authoritative nameserver for google.in

```
nslookup google.in ns1.google.com
```

```
manan@DESKTOP-S69HDK5:~$ nslookup google.in ns1.google.com
Server:      ns1.google.com
Address:     216.239.32.10#53

Name:   google.in
Address: 142.250.195.4
Name:   google.in
Address: 2404:6800:4002:826::2004
```

Which give the authoritative answer from ns1.google.com as 142.250.195.4

b)

```
nslookup -debug google.in
```

```
manan@DESKTOP-S69HDK5:~$ nslookup -debug google.com
Server:      10.255.255.254
Address:     10.255.255.254#53

-----
QUESTIONS:
    google.com, type = A, class = IN
ANSWERS:
-> google.com
    internet address = 216.58.221.46
    ttl = 205
AUTHORITY RECORDS:
ADDITIONAL RECORDS:
-----
Non-authoritative answer:
Name:   google.com
Address: 216.58.221.46
```

This gives us the time to live (ttl) as 205 seconds.

This implies that the entry would expire after 205 seconds and would again need to be fetched from the authoritative nameserver

Q5

- a) A total of 8 intermediate (excluding the destination hop) hosts can be seen

IP Address	Average Latency
172.21.64.1	1.055 ms
192.168.32.254	86.601 ms
192.168.1.99	4.473 ms
103.25.231.1	5.503 ms
10.119.234.162	22.370 ms
72.14.194.160	8.954 ms
142.251.226.85	353.443 ms
142.251.52.211	390.615 ms

```
manan@DESKTOP-S69HDK5:~$ traceroute google.in
traceroute to google.in (142.250.195.4), 64 hops max
 1  172.21.64.1  0.452ms  0.335ms  0.268ms
 2  192.168.32.254  52.814ms  108.780ms  98.208ms
 3  192.168.1.99  5.054ms  4.162ms  4.203ms
 4  103.25.231.1  5.002ms  4.401ms  7.106ms
 5  * * *
 6  10.119.234.162  35.065ms  7.020ms  25.026ms
 7  72.14.194.160  9.453ms  10.449ms  6.961ms
 8  142.251.226.85  706.720ms  31.071ms  322.538ms
 9  142.251.52.211  31.421ms  41.259ms  1099.164ms
10  142.250.195.4  341.058ms  90.018ms  33.225ms
```

- b) The average latency when pinging google.in with 50 messages is 331.702 ms

```
ping google.in -c 50
```

```
--- google.in ping statistics ---
50 packets transmitted, 50 received, 0% packet loss, time 49348ms
rtt min/avg/max/mdev = 28.026/331.702/1112.461/359.723 ms, pipe 2
```

- c) The sum of average latencies from (a) is 873.014 ms which is far apart from the 331.702 ms latency obtained from (b)

This is due to the fact that traceroute pings every intermediate host to get their latencies while ping just pings the last host [\[source\]](#)

This can also be observed that for the last host 142.251.52.211 the average latency is 390.615 ms while the latency from ping was 331.702 ms which are really close

- d) The maximum ping latency in (a) is 1099.164 ms and for (b) is 1112.461 ms which are really close, this shows that hop 9 (where the max ping latency occurred) might have significantly contributed to the latency this can be due to a possible latency spike or bottleneck at Hop 9
- e) The multiple entries (3 in this case) for each hop while using the traceroute command gives the latency of pinging these IPs which helps to better measure the latency for a particular hop
- f) The average latency for pinging stanford.edu is 568.998 ms

`ping stanford.edu -c 50`

```
--- stanford.edu ping statistics ---
50 packets transmitted, 50 received, 0% packet loss, time 49392ms
rtt min/avg/max/mdev = 289.952/568.998/1094.376/260.573 ms, pipe 2
```

- g) Since we can ignore "***" the number of intermediate hops would be 9 (excluding the destination hop) which is 1 more hop than obtained in (a)

`traceroute stanford.edu`

```
manan@DESKTOP-S69HDK5:~$ traceroute stanford.edu
traceroute to stanford.edu (171.67.215.200), 64 hops max
 1  172.21.64.1  0.379ms  0.277ms  0.192ms
 2  192.168.32.254  5.687ms  10.564ms  31.953ms
 3  192.168.1.99  3.812ms  4.457ms  3.787ms
 4  103.25.231.1  4.933ms  4.126ms  3.483ms
 5  10.1.209.201  30.339ms  40.040ms  30.260ms
 6  10.1.200.137  29.953ms  28.764ms  28.548ms
 7  10.255.238.254  50.713ms  61.695ms  50.451ms
 8  180.149.48.18  29.230ms  29.391ms  29.625ms
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  171.66.255.232  288.430ms  287.986ms  293.007ms
26  * * *
27  171.67.215.200  290.505ms  290.092ms  289.369ms
```

- h) There is a significant latency difference between stanford.edu and google.in having 568.998 ms and 331.702 ms on average respectively, this can be because of the servers begin in geographically different parts of the world, where the google.in's server is closer.

Q6.

The ping command can be made to fail for 127.0.0.1 by deactivating the loopback interface "lo"

`sudo ifconfig lo down`

Command used for pinging

`ping 127.0.0.1 -c 10`

```
manan@DESKTOP-S69HDK5:~$ ping 127.0.0.1 -c 10
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.

--- 127.0.0.1 ping statistics ---
10 packets transmitted, 0 received, 100% packet loss, time 9375ms
```