Assignment-1
Using command-line utilities for network debugging

Q1)

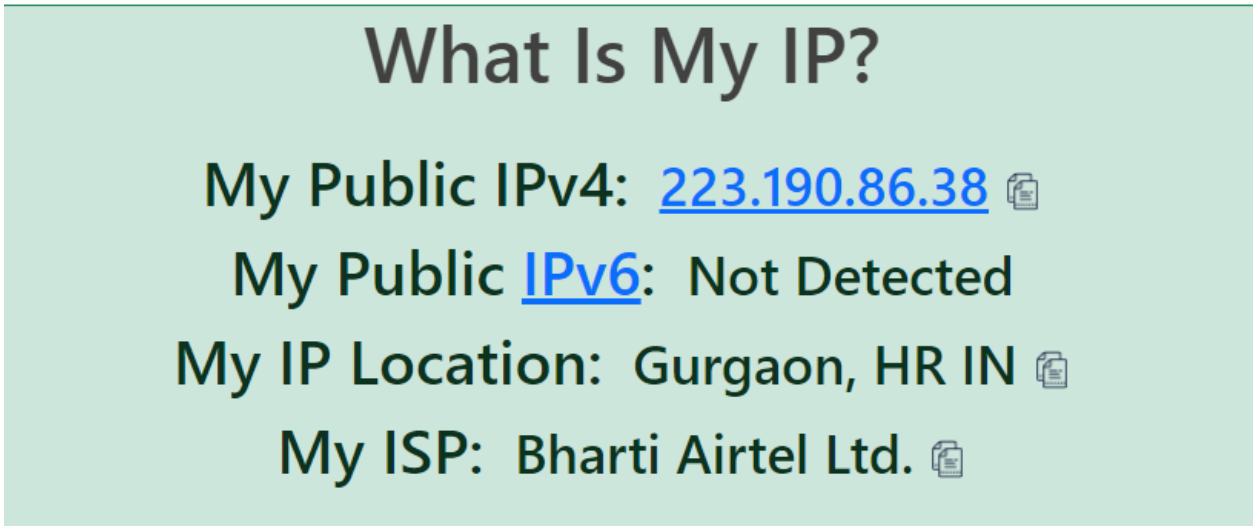
a)

```
gargdhawal05@Dhawal:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.24.232.90  netmask 255.255.240.0  broadcast 172.24.239.255
        inet6 fe80::215:5dff:febc:e162  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:bc:e1:62  txqueuelen 1000  (Ethernet)
        RX packets 5  bytes 310 (310.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 15  bytes 1082 (1.0 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 4  bytes 591 (591.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 591 (591.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- Inet corresponds to a private IPv4 address (172.24.232.90).
- Inet6 corresponds to a private IPv6 address (fe80::215:5dff:febc:e162).
- Ether corresponds to MAC address i.e (00:15:5d:bc:e1:62).

b)



- The public IPv4 address is 223.190.86.38.
- The IP address shown on `https://www.whatismyip.com` is different from the one obtained via `ifconfig` because the former is public IP assigned by ISP and is unique on the wider internet, while the latter is local IP unique within the private network and is used for internal communication.

Q2)

```
gargdhawal05@Dhawal:~$ sudo  ifconfig eth0 192.168.23.21
[sudo] password for gargdhawal05:
gargdhawal05@Dhawal:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.23.21  netmask 255.255.255.0  broadcast 192.168.23.255
        inet6 fe80::215:5dff:febc:e162  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:bc:e1:62  txqueuelen 1000  (Ethernet)
        RX packets 361  bytes 295838 (295.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 128  bytes 48289 (48.2 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 16  bytes 1815 (1.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16  bytes 1815 (1.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

gargdhawal05@Dhawal:~$ sudo ifconfig eth0 172.24.232.90
gargdhawal05@Dhawal:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.24.232.90  netmask 255.255.0.0  broadcast 172.24.255.255
        inet6 fe80::215:5dff:febc:e162  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:bc:e1:62  txqueuelen 1000  (Ethernet)
        RX packets 396  bytes 301800 (301.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 128  bytes 48289 (48.2 KB)
```

- Original IP address: 172.24.232.90
- IP address change using command: sudo ifconfig <interface> <new ip_address>
- New IP address: 192.168.23.21
- IP address is again reverted to original IP address

Q3)

a)

```
gargdhawal05@Dhawal:~$ nc -l -p 1230
hi
i am dhawal garg
```

Server is set up using the command: nc -l -p <port number>

```
gargdhawal05@Dhawal:~$ nc localhost 1230
hi
i am dhawal garg
```

Client is set up using the command: nc <localhost> <port address>

b)

```
gargdhawal05@Dhawal:~$ netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:52186         localhost:1230          ESTABLISHED
tcp        0      0 localhost:1230          localhost:52186         ESTABLISHED
```

The TCP connection is successfully established and active, allowing for communication between the two endpoints (`localhost:52186` and `localhost:1230`).

Q4)

a)

Step 1: We first get the authoritative name server of the host “google.in” using the following command: nslookup -query=soa google.com (Here type=’soa’).

```
gargdhawal05@Dhawal:~$ nslookup -query=soa google.com
Server:         10.255.255.254
Address:        10.255.255.254#53

Non-authoritative answer:
google.com
        origin = ns1.google.com
        mail addr = dns-admin.google.com
        serial = 666268564
        refresh = 900
        retry = 900
        expire = 1800
        minimum = 60

Authoritative answers can be found from:
google.com      nameserver = ns2.google.com.
google.com      nameserver = ns3.google.com.
google.com      nameserver = ns4.google.com.
google.com      nameserver = ns1.google.com.
ns1.google.com  internet address = 216.239.32.10
ns1.google.com  has AAAA address 2001:4860:4802:32::a
ns4.google.com  internet address = 216.239.38.10
ns4.google.com  has AAAA address 2001:4860:4802:38::a
ns3.google.com  internet address = 216.239.36.10
ns3.google.com  has AAAA address 2001:4860:4802:36::a
ns2.google.com  internet address = 216.239.34.10
ns2.google.com  has AAAA address 2001:4860:4802:34::a
```

I obtained 4 authoritative names:

- ns1.google.com
- ns2.google.com
- ns3.google.com
- ns4.google.com

Step 2: Now we will use these authoritative names to get authoritative responses from the host server using the following command: nslookup google.in <authoritative name>.
The address of each authoritative response represents its IP address.

```
gargdhawal05@Dhawal:~$ nslookup google.in ns1.google.com
Server:         ns1.google.com
Address:        216.239.32.10#53

Name:   google.in
Address: 142.250.194.100
Name:   google.in
Address: 2404:6800:4002:821::2004

gargdhawal05@Dhawal:~$ nslookup google.in ns2.google.com
Server:         ns2.google.com
Address:        216.239.34.10#53

Name:   google.in
Address: 142.250.194.100
Name:   google.in
Address: 2404:6800:4002:821::2004

gargdhawal05@Dhawal:~$ nslookup google.in ns3.google.com
Server:         ns3.google.com
Address:        216.239.36.10#53

Name:   google.in
Address: 142.250.194.100
Name:   google.in
Address: 2404:6800:4002:821::2004

gargdhawal05@Dhawal:~$ nslookup google.in ns4.google.com
Server:         ns4.google.com
Address:        216.239.38.10#53

Name:   google.in
Address: 142.250.194.100
Name:   google.in
Address: 2404:6800:4002:821::2004
```

b)

```
gargdhawal05@Dhawal:~$ nslookup -debug google.in
Server:         10.255.255.254
Address:        10.255.255.254#53

------------
    QUESTIONS:
        google.in, type = A, class = IN
    ANSWERS:
    ->  google.in
        internet address = 172.217.167.36
        ttl = 233
    AUTHORITY RECORDS:
    ADDITIONAL RECORDS:
------------
Non-authoritative answer:
Name:   google.in
Address: 172.217.167.36
------------
    QUESTIONS:
        google.in, type = AAAA, class = IN
    ANSWERS:
    ->  google.in
        has AAAA address 2404:6800:4002:825::2004
        ttl = 233
    AUTHORITY RECORDS:
    ADDITIONAL RECORDS:
------------
Name:   google.in
Address: 2404:6800:4002:825::2004
```

Time to Live(TTL) value for caching DNS records is 233 seconds for “google.in”. After 233 seconds this entry would expire.

Q5)

a)

Number of intermediate hosts:10

Intermediate Host number	Average Latency	IP address
1	2.017ms	172.24.224.1
2	2.932ms	192.168.1.1
3	7.505ms	223.182.79.255
4	20.476ms	122.187.30.9
5	15.498ms	116.119.109.8
6	12.990ms	142.250.168.34
7	----------	Unknown
8	11.347ms	142.251.54.94 142.251.54.92 64.233.174.70
9	15.484ms	142.251.52.209 142.251.255.54
10	10.477ms	216.239.50.23 196.194.250.142

```
gargdhawal05@Dhawal:~$ traceroute google.in
traceroute to google.in (142.250.194.196), 30 hops max, 60 byte packets
 1  172.24.224.1 (172.24.224.1)  2.335 ms  2.197 ms  1.520 ms
 2  192.168.1.1 (192.168.1.1)  3.316 ms  2.999 ms  2.481 ms
 3  223.182.79.255 (223.182.79.255)  7.285 ms  7.250 ms  7.980 ms
 4  9.30.187.122.in-addr.arpa (122.187.30.9)  14.136 ms 5.30.187.122.in-addr.arpa (122.187.
30.5)  33.822 ms 9.30.187.122.in-addr.arpa (122.187.30.9)  13.470 ms
 5  116.119.109.8 (116.119.109.8)  15.954 ms  10.660 ms  19.880 ms
 6  142.250.168.34 (142.250.168.34)  12.806 ms  15.629 ms  10.534 ms
 7  * * *
 8  142.251.54.94 (142.251.54.94)  12.349 ms 142.251.54.92 (142.251.54.92)  12.392 ms 64.23
3.174.70 (64.233.174.70)  9.299 ms
 9  142.251.52.209 (142.251.52.209)  10.509 ms 142.251.255.54 (142.251.255.54)  25.597 ms 1
42.251.52.209 (142.251.52.209)  10.347 ms
10  216.239.50.23 (216.239.50.23)  10.477 ms 196.194.250.142.in-addr.arpa (1gargdhawal05@Dh
```

b)

Average Latency: 9.078 ms

```
gargdhawal05@Dhawal:~$ ping -c 50 google.in
PING google.in (172.217.167.36) 56(84) bytes of data.
64 bytes from del03s16-in-f4.1e100.net (172.217.167.36): icmp_seq=1 ttl=59 time=13.5 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=2 ttl=59 time=7.71 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=3 ttl=59 time=9.07 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=4 ttl=59 time=8.91 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=5 ttl=59 time=9.19 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=6 ttl=59 time=9.51 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=7 ttl=59 time=9.73 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=8 ttl=59 time=7.39 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=9 ttl=59 time=8.17 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=10 ttl=59 time=7.81 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=11 ttl=59 time=8.33 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=12 ttl=59 time=8.70 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=13 ttl=59 time=8.46 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=14 ttl=59 time=7.81 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=15 ttl=59 time=8.01 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=16 ttl=59 time=8.10 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=17 ttl=59 time=7.85 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=18 ttl=59 time=8.51 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=19 ttl=59 time=9.08 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=20 ttl=59 time=9.00 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=21 ttl=59 time=8.40 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=22 ttl=59 time=8.12 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=23 ttl=59 time=8.74 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=24 ttl=59 time=8.25 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=25 ttl=59 time=8.53 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=26 ttl=59 time=8.50 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=27 ttl=59 time=7.95 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=28 ttl=59 time=9.09 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=29 ttl=59 time=7.51 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=30 ttl=59 time=8.78 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=31 ttl=59 time=9.48 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=32 ttl=59 time=8.67 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=33 ttl=59 time=8.52 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=34 ttl=59 time=8.16 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=35 ttl=59 time=8.42 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=36 ttl=59 time=7.84 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=37 ttl=59 time=9.70 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=38 ttl=59 time=7.08 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=39 ttl=59 time=8.36 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=40 ttl=59 time=8.48 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=41 ttl=59 time=7.71 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=42 ttl=59 time=10.6 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=43 ttl=59 time=7.95 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=44 ttl=59 time=8.51 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=45 ttl=59 time=11.1 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=46 ttl=59 time=8.85 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=47 ttl=59 time=8.33 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=48 ttl=59 time=9.88 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=49 ttl=59 time=9.01 ms
64 bytes from 36.167.217.172.in-addr.arpa (172.217.167.36): icmp_seq=50 ttl=59 time=28.6 ms

--- google.in ping statistics ---
50 packets transmitted, 50 received, 0% packet loss, time 49084ms
rtt min/avg/max/mdev = 7.077/9.078/28.570/2.968 ms
```

c)

- The total ping latency of all intermediate hosts is: 2.017 + 2.932 + 7.505 + 20.476 + 15.498 + 12.990 + 11.347 + 15.484 + 10.477 = 97.726 ms.
- The average latency of all intermediate hosts in a) part : 97.726 ms / 9 = 10.863 ms.
- The average latency obtained in b) part: 9.078 ms
- The latencies obtained in both the parts are close to each other which suggests that the latency of the intermediate hosts is a significant contributor to the overall latency of the connection.
- This makes sense, as the latency of each hop can affect the overall latency of the connection.

d)

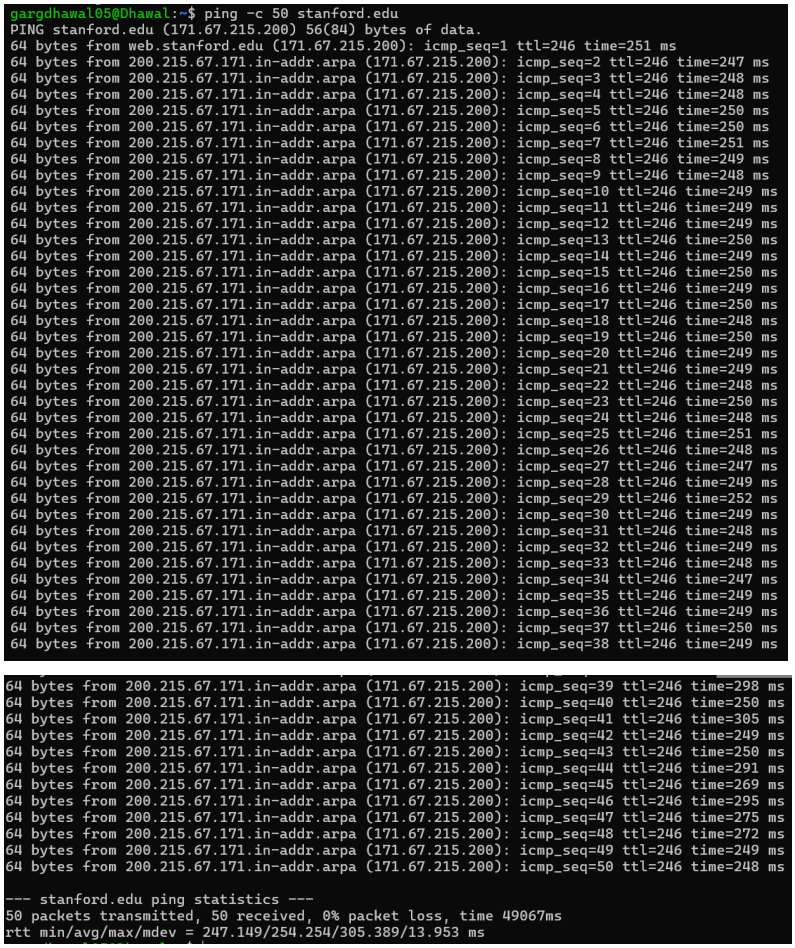
- The maximum average latency amongst the intermediate hosts is 20.476 ms, which is significantly higher than the average latency of 9.078 ms obtained in part (b).
- Maximum latency represents the worst-case scenario, where a particular intermediate host is experiencing a higher latency.
- On the other hand, the average latency obtained in part (b) is a representation of the overall latency of the connection, which is averaged out over multiple packets and multiple hops.
- The maximum latency represents the "bottleneck" in the connection, where the latency is highest, whereas the average latency represents the overall "average" performance of the connection.

e)

Multiple entries in traceroute command in a single hop represents multiple packets(mostly three) sent by the traceroute to each hop for a more accurate estimate of the response time(latency).

f)

Average latency: 254.254 ms



g)

```
gargdhawal05@Dhawal:~$ traceroute stanford.edu
traceroute to stanford.edu (171.67.215.200), 30 hops max, 60 byte packets
 1  172.24.224.1 (172.24.224.1)  0.540 ms  1.398 ms  0.585 ms
 2  192.168.1.1 (192.168.1.1)  2.310 ms  2.323 ms  2.147 ms
 3  223.182.79.255 (223.182.79.255)  7.088 ms  7.078 ms  7.866 ms
 4  9.30.187.122.in-addr.arpa (122.187.30.9)  7.225 ms  7.219 ms  7.210 ms
 5  116.119.44.134 (116.119.44.134)  240.266 ms 116.119.44.132 (116.119.44.132)  248.220 ms 116.119.44.134 (116.119.44.134)  249.574 ms
 6  * * *
 7  * * port-channel8.core2.lax1.he.net (184.104.197.109)  264.140 ms
 8  * port-channel12.core3.sjc2.he.net (184.104.195.50)  263.831 ms *
 9  * * *
10  stanford-university.e0-62.core2.pao1.he.net (184.105.177.238)  249.805 ms  265.227 ms  288.595 ms
11  campus-east-rtr-vl1018.SUNet (171.64.255.228)  244.924 ms campus-east-rtr-vl1118.SUNet (171.66.255.228)  255.224 ms  244.859 ms
12  * * *
13  200.215.67.171.in-addr.arpa (171.67.215.200)  255.348 ms  251.877 ms  241.662 ms
```

The number of hops for stanford.edu is 13 which is greater than the number of hops for google.edu (10).

h) The difference between the latency of ‘google.in’ and ‘stanford.edu’ is due to geographical distance and network infrastructure. Servers for Google located in India are geographically closer to my location as compared to Stanford’s server associated with the US causing high latency due to the longer distance data must travel.

Q6)
Step 1: Shutdown the loopback interface (lo interface) using the : sudo ifconfig lo down
Step 2: Use the ping command to send 100 packets to 127.0.0.1
Since the interface which is used to communicate (loopback) is turned down no packets would be transferred resulting in 100% packet loss.

```
gargdhawal05@Dhawal:~$ sudo ifconfig lo down
[sudo] password for gargdhawal05:
Sorry, try again.
[sudo] password for gargdhawal05:
gargdhawal05@Dhawal:~$ ping -c 100 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.

--- 127.0.0.1 ping statistics ---
100 packets transmitted, 0 received, 100% packet loss, time 102933ms
```