

Computer Networks (CSE-232) Report

Programming Assignment -1

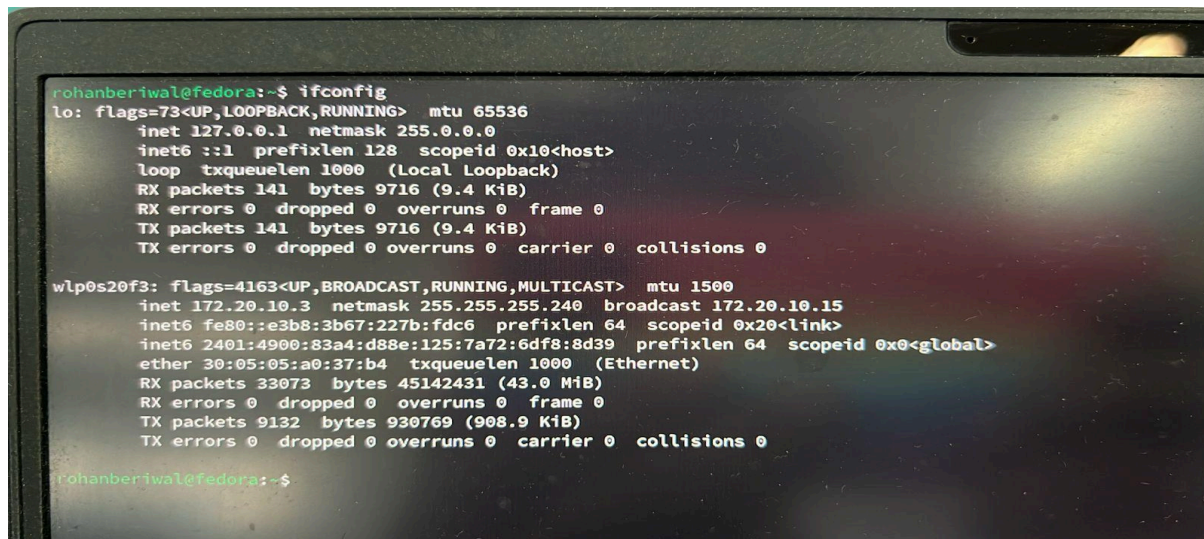
(Using command-line utilities for network debugging)

Name : Rohan Beriwal

Roll No : 2022413

Question 1.)

A)



```
rohanberiwal@fedora:~$ ifconfig
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 141 bytes 9716 (9.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 141 bytes 9716 (9.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

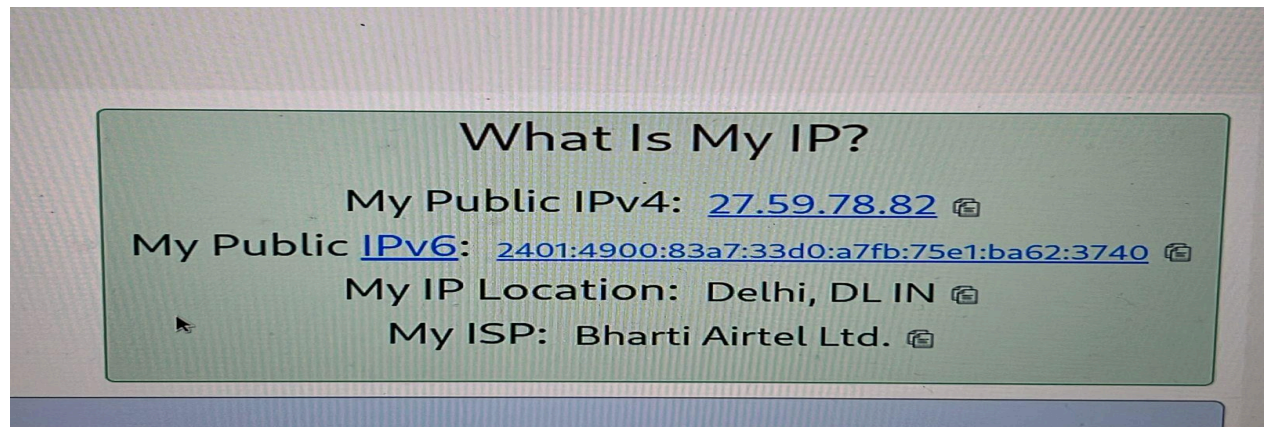
wlp0s20f3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.20.10.3 netmask 255.255.255.240 broadcast 172.20.10.15
    inet6 fe80::e3b8:3b67:227b:fdc6 prefixlen 64 scopeid 0x20<link>
    inet6 2401:4900:83a4:d88e:125:7a72:6df8:8d39 prefixlen 64 scopeid 0x0<global>
    ether 30:05:05:a0:37:b4 txqueuelen 1000 (Ethernet)
    RX packets 33073 bytes 45142431 (43.0 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 9132 bytes 930769 (908.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

rohanberiwal@fedora:~$
```

Description :

ifconfig command : This command is used in Unix-like operating systems . This is used to display the network configurations of the machines . I used the Linux shell and used the **ifconfig** command to get the network output of my machines .The ip address of the machine is 172.20.10.3 as it is connected to a wireless interface (Wi-Fi) .

B)



No, the IP for the machine that was found using the **ifconfig** command on the machine and the IP on the website <https://www.whatismyip.com> are not the same.

Reason of Different IP :

The IP on the machine found using the **ifconfig** command shows the IP is a private IP that is present in the local network and this IP is assigned using **Dynamic Host Configuration Protocol server (DHCP)** while the IP present on the website is a IP assigned by the ISP(Internet service provider) and this is used to communicate over the Internet.

Question 2)

Changing IP to New IP :

```
rohanberiwal@alienware14:/mnt/c/Users/rohan$ sudo ifconfig eth0 192.168.1.100
[sudo] password for rohanberiwal:
rohanberiwal@alienware14:/mnt/c/Users/rohan$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1358
    inet 192.168.1.100 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::215:5dff:febe:47e6 prefixlen 64 scopeid 0x20<link>
    ether 00:15:5d:be:47:e6 txqueuelen 1000 (Ethernet)
    RX packets 306 bytes 530385 (530.3 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 179 bytes 17664 (17.6 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 18 bytes 2030 (2.0 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 18 bytes 2030 (2.0 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

rohanberiwal@alienware14:/mnt/c/Users/rohan$
```


Description :

This screen Shot shows the IP address of the machine getting changed . I first used the **Ifconfig command** to get the Ip address of the machine and saved that IP address . I use the port eth0 to find the inet (172.19.187.101 in this case) which is the IP of the machine . Now to change the IP of the to some other desired address I used

sudo ifconfig eth0 <New_ip address> , I used a random IP address of 192.168.1.100 , I filled the password for the machine as my privilege was changed from the regular user to **“superuser do”(sudo / ~ root)** . Then , using the **ifconfig command** we can print the IP address that got changed .

Reverting the IP address back to Original :

```
rohanberiwala@alienware14:~$ sudo ifconfig eth0 172.19.187.101
rohanberiwala@alienware14:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1358
    inet 172.19.187.101  netmask 255.255.0.0  broadcast 172.19.255.255
    inet6 fe80::215:5dff:febe:47e6  prefixlen 64  scopeid 0x20<link>
    ether 00:15:5d:be:47:e6  txqueuelen 1000  (Ethernet)
    RX packets 370  bytes 543393 (543.3 KB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 180  bytes 17734 (17.7 KB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

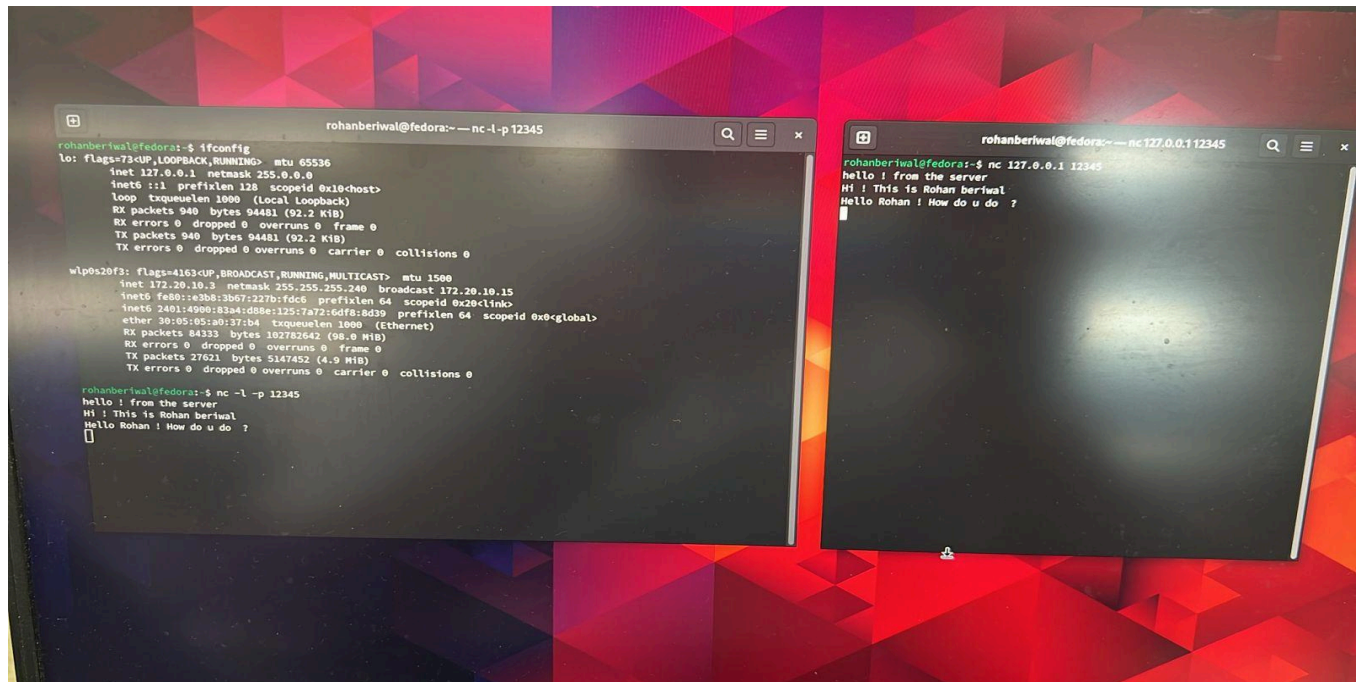
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1000  (Local Loopback)
    RX packets 42  bytes 4286 (4.2 KB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 42  bytes 4286 (4.2 KB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```

Description :

After changing the IP address from 172.19.187.101 to 192.168.1.100 I used the same **sudo ifconfig eth0 172.19.187.101** here the IP address is the same IP that we had before .

Question3.)

A)



Description:

To Generate a connection between two machines we have to use the IP address to connect two machines for the TCP connections . I opened two different terminal windows . The left side being terminal 1 and right being terminal 2 now using Terminal 1 I found the IP address of the machine using the **ifconfig command** . Now i tried to establish a connection between terminal using the **nc -l -p 12345** .

The **nc** here stands for the **netcat** that is a tool for generating a connection between the two machines / two VMs or two terminals .

The **-l flag** is used to set the netcat in the listening mode .

The **-p** is the flag that denotes the port number .

I have set a random port number of 12345 .

Now in the terminal 2 :

Now in the second terminal we use the **nc IP address (Client) Port No** command and after this we can generate the TCP connection between the two machines .

B)

```

rohanberawal@fedora:~$ ifconfig
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 1177 bytes 117829 (115.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1177 bytes 117829 (115.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlp0s20f3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.20.10.3 netmask 255.255.255.240 broadcast 172.20.10.15
    inet6 fe80::e3b8:3b67:227b:fdc6 prefixlen 64 scopeid 0x20<link>
    inet6 2401:4900:83a4:d88e:125:7a72:6df8:8d39 prefixlen 64 scopeid 0x0<global>
    ether 30:05:05:a0:37:b4 txqueuelen 1000 (Ethernet)
    RX packets 92919 bytes 111006555 (105.8 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 32510 bytes 6076116 (5.7 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

rohanberawal@fedora:~$ nc -l -p 12345
Hi rohan this side
Hello rohan I am server2
Hello server 2 I am server1
netstat -tn

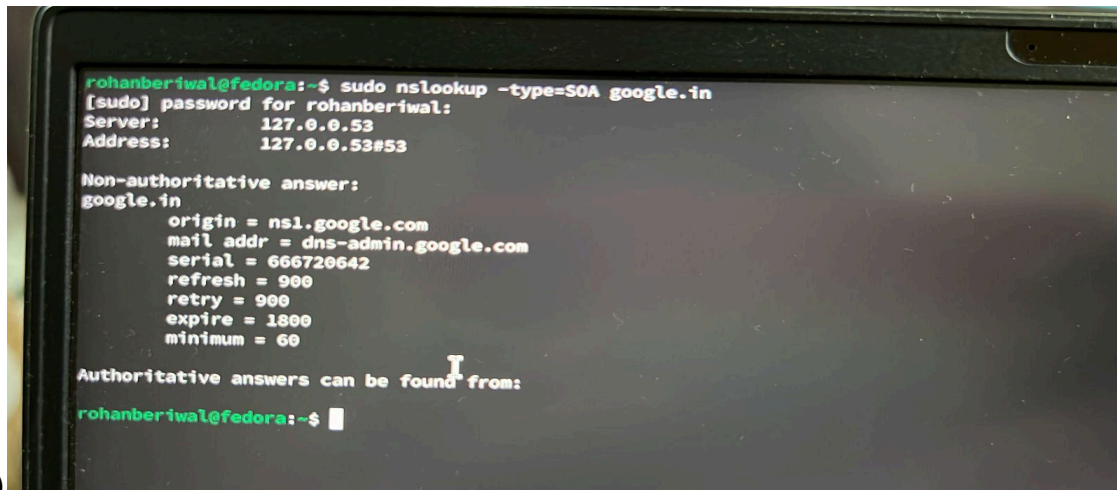
rohanberawal@fedora:~$ netstat -tn
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:12345          0.0.0.0:0               LISTENING
tcp        0      0 172.20.10.3:55198      54.71.156.207:443      ESTABLISHED
tcp        0      0 172.20.10.3:55198      172.20.10.3:12345      ESTABLISHED
tcp6       0      0 2401:4900:83a4:d88e:125:7a72:6df8:8d39:443 2401:4900:83a4:d88e:125:7a72:6df8:8d39:443 ESTABLISHED
tcp6       0      0 2401:4900:83a4:d88e:125:7a72:6df8:8d39:443 2401:4900:83a4:d88e:125:7a72:6df8:8d39:443 ESTABLISHED
tcp6       0      0 2401:4900:83a4:d88e:125:7a72:6df8:8d39:443 2401:4900:83a4:d88e:125:7a72:6df8:8d39:443 ESTABLISHED
tcp6       0      0 2401:4900:83a4:d88e:125:7a72:6df8:8d39:443 2401:4900:83a4:d88e:125:7a72:6df8:8d39:443 ESTABLISHED
tcp6       0      0 2401:4900:83a4:d88e:125:7a72:6df8:8d39:443 2401:4900:83a4:d88e:125:7a72:6df8:8d39:443 ESTABLISHED

```

The status of the TCP client is “**ESTABLISHED**”. That can be found using the **netcat -tn** . In this we use the -t to specify the default mode of the TCP and n for preventing the DNS resolution . The DNS resolution is used to convert the Human readable domain names into the IP addresses .

In the above ss we can see the local client and the foreign client is established .

Question 4.)

A terminal window on a Fedora system. The user 'rohanberiwal' runs the command 'sudo nslookup -type=SOA google.in'. The terminal shows the password prompt, the server address '127.0.0.53', and a non-authoritative answer for 'google.in' with SOA details: origin = ns1.google.com, mail addr = dns-admin.google.com, serial = 666720642, refresh = 900, retry = 900, expire = 1800, minimum = 60. It also indicates that authoritative answers can be found from the same server.

```
rohanberiwal@fedora:~$ sudo nslookup -type=SOA google.in
[sudo] password for rohanberiwal:
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
google.in
  origin = ns1.google.com
  mail addr = dns-admin.google.com
  serial = 666720642
  refresh = 900
  retry = 900
  expire = 1800
  minimum = 60

Authoritative answers can be found from:
rohanberiwal@fedora:~$
```

A)

Description :

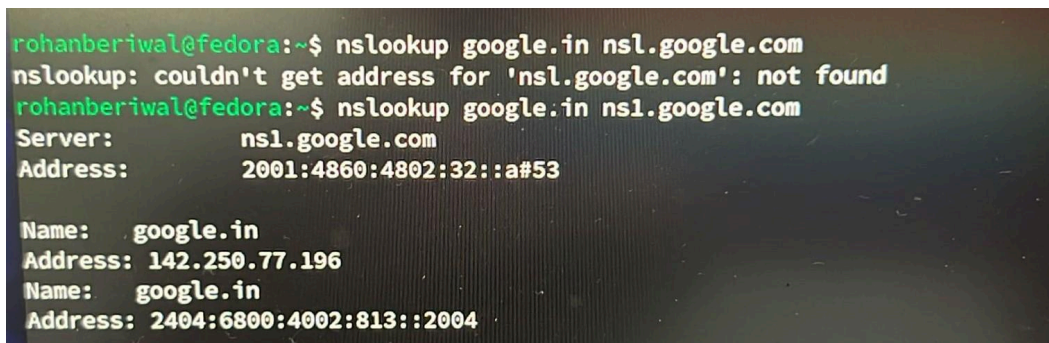
NOTE : I have used sudo in this because in the regular privilege the output was not satisfactory . The authoritative answer was blank before and after the sudo privilege .

In this I use the command **sudo nslookup -type = SOA google.in** to get an authoritative result for the website google.in . The nslookup command is used for the querying on the dns to obtain the IP address and information about the given website .

-type = SOA is used to set the query search on the dns to State of Authority(SOA) and get the authoritative result for the website that is getting entered .

Now since the origin of the website is ns1.google.com we can use that to find the output of the authoritative results .

Continued ...

A terminal window showing the user 'rohanberiwal' running 'nslookup google.in ns1.google.com'. The first command fails with 'nslookup: couldn't get address for 'ns1.google.com': not found'. The second command, 'nslookup google.in ns1.google.com', succeeds, showing the server as 'ns1.google.com' with address '2001:4860:4802:32::a#53'. It then displays the authoritative DNS records for 'google.in', including an A record with IP '142.250.77.196' and an AAAA record with IP '2404:6800:4002:813::2004'.

```
rohanberiwal@fedora:~$ nslookup google.in ns1.google.com
nslookup: couldn't get address for 'ns1.google.com': not found
rohanberiwal@fedora:~$ nslookup google.in ns1.google.com
Server:      ns1.google.com
Address:     2001:4860:4802:32::a#53

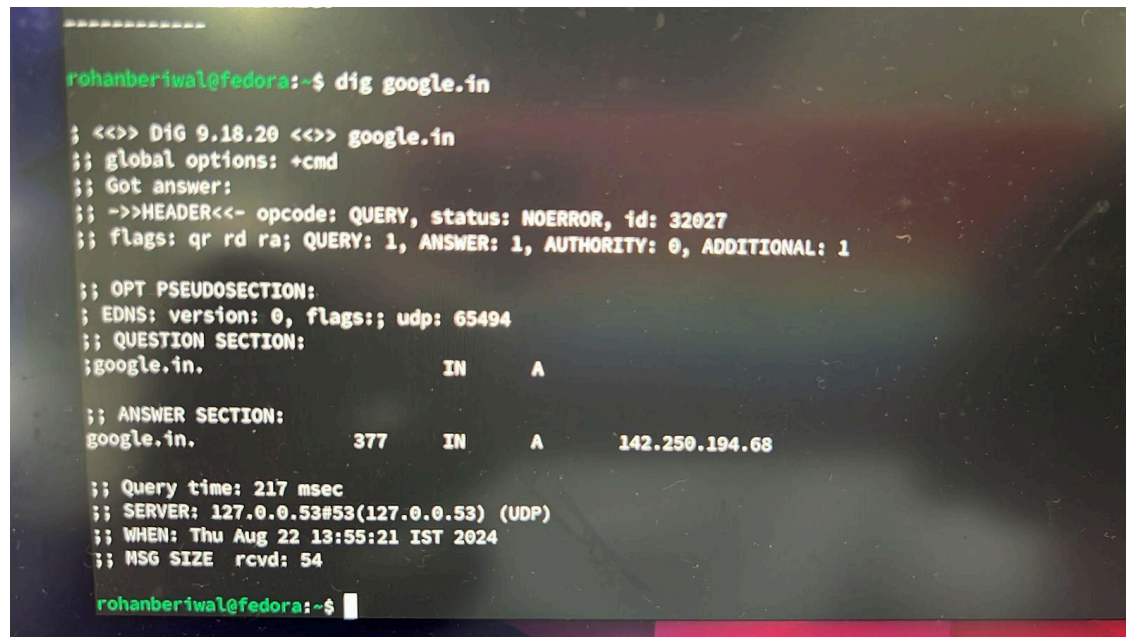
Name:   google.in
Address: 142.250.77.196
Name:   google.in
Address: 2404:6800:4002:813::2004
```

Now after getting the dns query output from the command nslookup google.com. We use the query command of :

nslookup <website domain> <authoritative result>

After using this we can see the output for the authoritative result for the website of google.in .

B)



```
rohanberiwala@fedora:~$ dig google.in

;<>> DiG 9.18.20 <>> google.in
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 32027
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.in.                IN      A

;; ANSWER SECTION:
google.in.                 377     IN      A      142.250.194.68

;; Query time: 217 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Thu Aug 22 13:55:21 IST 2024
;; MSG SIZE rcvd: 54

rohanberiwala@fedora:~$
```

Description :

The dig command is used to query the DNS server and find the information about the domain with the specified names . The typical syntax for the dig is :

dig < website domain>

In the answer section we get the TTL (time to live) value for a website in our case it is google.in .

In our case for the google.in the TTL is 377 so we can infer that the query will be cached or saved for 377 seconds and after 377 second the query will become obsolete .

Question 5)

A)

```
rohanberiwal@alienware14: /mnt/c/Users/rohan$ traceroute google.in
traceroute to google.in (142.250.194.100), 64 hops max
 1  172.19.176.1  0.345ms  0.266ms  0.138ms
 2  172.20.10.1  1.952ms  1.833ms  1.780ms
 3  106.208.189.225  18.904ms  20.453ms  40.092ms
 4  117.96.31.66  19.750ms  17.868ms  14.887ms
 5  182.71.124.173  20.167ms  19.655ms  22.098ms
 6  116.119.109.8  18.346ms  25.869ms  33.282ms
 7  142.250.168.34  18.587ms  20.220ms  19.805ms
 8  * * *
 9  142.251.76.202  64.459ms  23.878ms  24.348ms
10  142.251.52.223  19.885ms  24.936ms  20.453ms
11  142.250.194.100  19.918ms  26.000ms  29.392ms
rohanberiwal@alienware14: /mnt/c/Users/rohan$ |
```

Description :

The Number of intermediate nodes that I can see are 10.

IP address of each intermediate node / intermediate host

Host 1 : IP(172.19.176.1)-> Tavg = 0.2496667 ms

Host2 : IP(172.20.10.1)-> Tavg = 1.855 ms

Host3 : IP(106.208.189.225) -> Tavg = 26.483 ms

Host4 : IP(117.96.31.66) -> Tavg = 17.5016 ms

Host 5: IP(182.71.124.173) -> Tavg = 20.64 ms

Host 6 : IP(116.119.109.8) -> Tavg = 25.832 ms

Host 7 : IP(142.250.168.34) -> Tavg = 19.537 ms

Host 8 : IP(142.251.76.202) -> Tavg = 56.3435 ms

Host 9 : IP(142.251.52.223) -> Tavg = 21.578 ms

Host10 : IP(142.250.194.100) -> Tavg = 25.10333 ms

B)

```

rohanberima@delienuare14: /mnt/c/Users/rohan$ ping -c 50 google.in
PING google.in (142.250.193.36) 56(84) bytes of data:
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=1 ttl=57 time=46.3 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=2 ttl=57 time=42.2 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=3 ttl=57 time=33.9 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=4 ttl=57 time=31.8 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=5 ttl=57 time=31.5 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=6 ttl=57 time=26.0 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=7 ttl=57 time=29.4 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=8 ttl=57 time=26.4 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=9 ttl=57 time=40.8 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=10 ttl=57 time=40.1 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=11 ttl=57 time=30.1 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=12 ttl=57 time=32.5 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=13 ttl=57 time=22.2 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=14 ttl=57 time=60.8 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=15 ttl=57 time=34.6 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=16 ttl=57 time=44.9 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=17 ttl=57 time=38.3 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=18 ttl=57 time=49.2 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=19 ttl=57 time=19.2 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=20 ttl=57 time=32.5 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=21 ttl=57 time=25.6 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=22 ttl=57 time=39.6 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=23 ttl=57 time=46.5 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=24 ttl=57 time=36.3 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=25 ttl=57 time=19.3 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=26 ttl=57 time=53.0 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=27 ttl=57 time=19.9 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=28 ttl=57 time=33.2 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=29 ttl=57 time=37.9 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=30 ttl=57 time=39.9 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=31 ttl=57 time=32.3 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=32 ttl=57 time=30.3 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=33 ttl=57 time=29.8 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=34 ttl=57 time=33.0 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=35 ttl=57 time=27.9 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=36 ttl=57 time=24.3 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=37 ttl=57 time=18.9 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=38 ttl=57 time=42.3 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=39 ttl=57 time=23.8 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=40 ttl=57 time=42.9 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=41 ttl=57 time=128 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=42 ttl=57 time=86.6 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=43 ttl=57 time=85.7 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=44 ttl=57 time=25.4 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=45 ttl=57 time=57.0 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=46 ttl=57 time=38.3 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=47 ttl=57 time=226 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=48 ttl=57 time=29.6 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=49 ttl=57 time=48.8 ms
64 bytes from deli115-in-f4.1e100.net (142.250.193.36): icmp_seq=50 ttl=57 time=40.9 ms

--- google.in ping statistics ---
50 packets transmitted, 50 received, 0% packet loss, time 49083ms
rtt min/avg/max/mdev = 18.348/42.736/226.088/32.160 ms
rohanberima@delienuare14: /mnt/c/Users/rohan$

```

Description : From this above ping command we can infer the following :

Round trip time statistics -

- 1.) Total time : 49083 ms
- 2.) Min round trip : 18.348 ms
- 3.) Average Latency : 42.736 ms
- 4.) Max round trip time : 226.088 ms
- 5.) Mean deviation : 32.160 ms

Single route time statistics :

- 1.) Total time = $49083/2 = 24541.5$ ms
- 2.) Min round trip : $18.348/2 = 9.174$ ms
- 3.) Average Latency : $42.736 = 21.368$ ms
- 4.) Max round trip time : $226.088/2 = 113.044$ ms

C)

Time_Average = Sum(all the t avg latencies in (a)) / number of intermed node

$$T_{avg} = (0.2496667 + 1.855 + 26.483 + 17.5016 + 20.64 + 25.832 + 19.537 + 56.3435 + 21.578 + 25.10333) / 10$$

$$T_{avg_latency} = 21.5123 \text{ ms}$$

Average latency in (B) : 42.736 ms

The average latency in part B is double of the time latency in part A . The reason for the two not matching is because the **ping command** returns the round trip time(RTT) of the packet .This means the average latency is the latency of the packet sent from the source to the destination and then back to the source . While the **traceroute command** measures the time from the source to the destination server /machine .

D)

From the Part (a) we can infer the maximum latency of Host 9 having an IP address of (142.251.76.202) that is 64.459 ms .

From part B we can infer the max latency as 226.088 ms.

The max latency from part A and part B does not matches as the due to the difference in their functions :

Ping command : This is used to measure the total RTT(Round trip time) from the source to the destination and then back . The ping includes the latency between all the intermediate routers / hops and the destination .

Traceroute command : This command measures the latency between each of the intermediate hop and print the latency individually . Since it does not measure the RTT (round trip time) it is generally lower than the ping output .

E)

For each of the single hop , there are typically 3 (default) entries as the traceroute command sends 3 or multiple packets to find network latency for each hop . The average of the several multiple packets sent gives a broader idea about the network traffic , performance . If we send a single packet the latency might be very high as the packet at a particular time may face congestion . Sending multiple packet gives the average estimate of the network latency within a single hop and the time to transmit the packet from one network device to another network device .

F)

```
rohanberwal@kali:~$ ping -c 50 stanford.edu
PING stanford.edu (171.67.215.200) 56(84) bytes of data:
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=1 ttl=244 time=289 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=2 ttl=244 time=409 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=3 ttl=244 time=334 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=4 ttl=244 time=355 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=5 ttl=244 time=376 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=6 ttl=244 time=397 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=7 ttl=244 time=410 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=8 ttl=244 time=444 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=9 ttl=244 time=368 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=10 ttl=244 time=206 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=11 ttl=244 time=306 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=12 ttl=244 time=431 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=13 ttl=244 time=453 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=14 ttl=244 time=291 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=15 ttl=244 time=499 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=16 ttl=244 time=418 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=17 ttl=244 time=306 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=18 ttl=244 time=361 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=19 ttl=244 time=486 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=20 ttl=244 time=407 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=21 ttl=244 time=428 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=22 ttl=244 time=349 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=23 ttl=244 time=472 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=24 ttl=244 time=394 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=25 ttl=244 time=314 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=26 ttl=244 time=501 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=27 ttl=244 time=395 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=28 ttl=244 time=382 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=29 ttl=244 time=404 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=30 ttl=244 time=325 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=31 ttl=244 time=450 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=32 ttl=244 time=371 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=33 ttl=244 time=393 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=34 ttl=244 time=315 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=35 ttl=244 time=438 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=36 ttl=244 time=358 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=37 ttl=244 time=382 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=38 ttl=244 time=505 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=39 ttl=244 time=425 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=40 ttl=244 time=551 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=41 ttl=244 time=320 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=42 ttl=244 time=595 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=43 ttl=244 time=414 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=44 ttl=244 time=438 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=45 ttl=244 time=665 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=46 ttl=244 time=483 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=47 ttl=244 time=315 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=48 ttl=244 time=424 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=49 ttl=244 time=310 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=50 ttl=244 time=366 ms

stanford.edu ping statistics:
50 packets transmitted, 50 received, 0% packet loss, time 49295ms
rtt min/avg/max/mdev = 286.309/403.912/665.244/82.747 ms
rohanberwal@kali:~$
```

Description:

From the above we can infer the following -

- 1.) RTT minimum = 286.309 ms
- 2.) RTT average time = 403.912 ms
- 3.) max time = 665.244 ms
- 4.) mdev (mean deviation) = 82.747 ms

Single route statistics

- 1.) Minimum time (single route) = $286.309/2 = 143.154$ ms
- 2.) Average latency (single route) = $403.912/2 = 201.956$ ms
- 3.) max time (single route) = $665.244/2 = 332.612$ ms

G)

```
rohanberiwal@alienware14: /mnt/c/Users/rohan$ traceroute stanford.edu
traceroute to stanford.edu (171.67.215.200), 64 hops max
 1  172.19.176.1  0.617ms  0.188ms  0.187ms
 2  172.20.10.1  4.660ms  2.506ms  2.336ms
 3  106.208.189.225  61.339ms  23.639ms  17.396ms
 4  117.96.31.66  22.171ms  18.917ms  18.744ms
 5  182.71.124.173  54.275ms  18.500ms  16.593ms
 6  116.119.57.43  277.847ms  345.091ms  409.502ms
 7  * * *
 8  * 184.104.197.109  377.819ms *
 9  * * *
10  * * *
11  184.105.177.238  377.869ms  306.605ms  288.277ms
12  171.64.255.228  430.184ms  312.039ms  283.227ms
13  * * *
14  171.67.215.200  325.801ms  511.661ms  307.186ms
rohanberiwal@alienware14: /mnt/c/Users/rohan$ traceroute google.in
traceroute to google.in (142.250.194.100), 64 hops max
 1  172.19.176.1  0.418ms  0.390ms  0.463ms
 2  172.20.10.1  3.534ms  2.191ms  2.046ms
 3  106.208.189.225  15.441ms  14.872ms  32.511ms
 4  117.96.31.64  22.147ms  16.886ms  20.033ms
 5  182.71.124.169  22.246ms  43.702ms  17.471ms
 6  116.119.109.8  23.777ms  19.185ms  16.267ms
 7  72.14.222.116  21.744ms  19.772ms  27.150ms
 8  * * *
 9  142.251.49.120  74.742ms  19.554ms  25.662ms
10  142.250.194.100  18.781ms  20.133ms  18.580ms
rohanberiwal@alienware14: /mnt/c/Users/rohan$
```

Considering the above code of the **traceroute google.in** and **traceroute stanford.edu**

We can infer the following :

Total number of Hops in stanford.edu = 14

Total number of Hops in google.in = 10

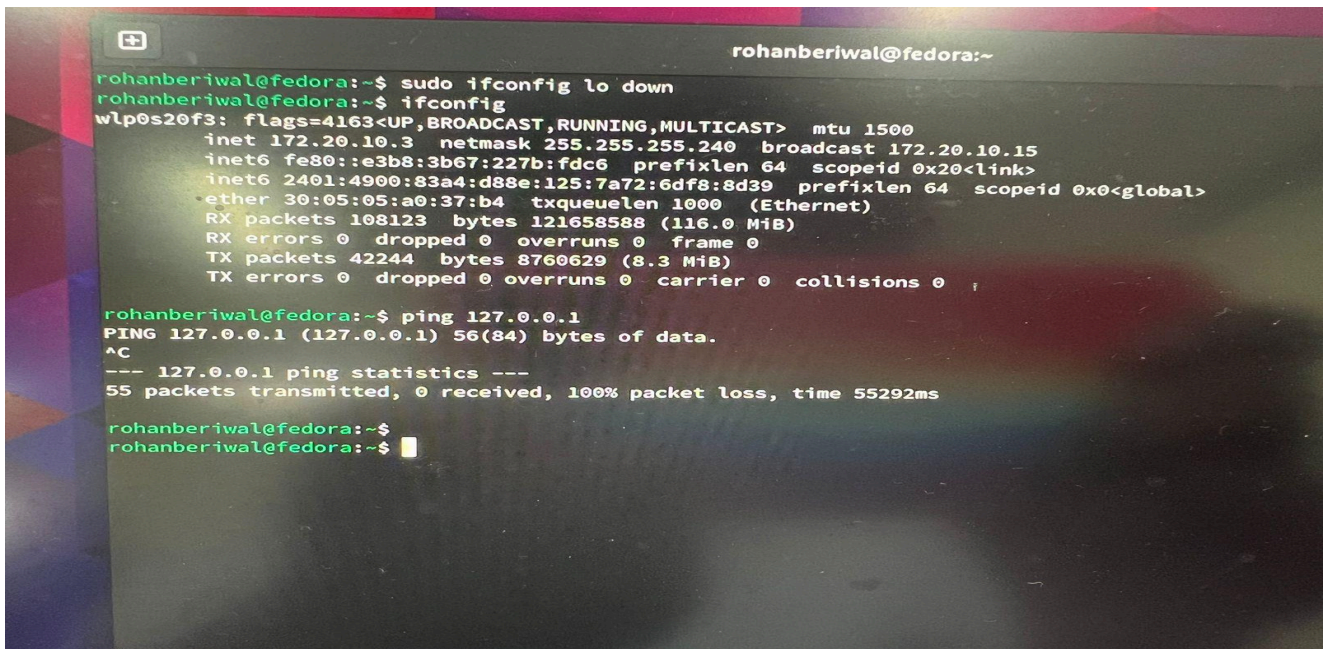
H) Considering the above code for the traceroute command for the stanford.edu and google.in :

The average latency time in stanford.edu is greater than the average time in google.in due to several factor like:

- 1.) **Geographics** of the destination server . google.in is in India while stanford.edu is situated in California USA . The distance while making a ping command increases the latency .
- 2.) **Network path and networking algorithm** : While making a ping call the network path is a major factor . The path size increases / decreases the number of the forward pass while doing a seek operation in the routing table . A server situated outside a local or at a distant position is bound to make more search operations in the routing table than a destination server present within a local network . The type of the networking algorithm and routing policies is a major factor that determines the latency of the time .

- 3.) **Network traffic** : Network traffic determines the amount of the time taken by the router to connect to the destination server . Consider two routers R1,R2 and a packet P1 . If there is a lot of traffic between R1 and R2 then the time taken for the packet to reach R2 to the destination will increase .
- 4.) **Signal Issue** : Between the two routers there may be bad weather conditions and other climatic factors that could lead to the delay in the packet transmission between the routers , increasing the overall latency of the process .

Question 6)



```
rohanberawal@fedora:~$ sudo ifconfig lo down
rohanberawal@fedora:~$ ifconfig
wlp0s20f3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.20.10.3 netmask 255.255.255.240 broadcast 172.20.10.15
    inet6 fe80::e3b8:3b67:227b:fdc6 prefixlen 64 scopeid 0x20<link>
    inet6 2401:4900:83a4:d88e:125:7a72:6df8:8d39 prefixlen 64 scopeid 0x0<global>
    ether 30:05:05:a0:37:b4 txqueuelen 1000 (Ethernet)
    RX packets 108123 bytes 121658588 (116.0 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 42244 bytes 8760629 (8.3 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

rohanberawal@fedora:~$ ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
^C
--- 127.0.0.1 ping statistics ---
55 packets transmitted, 0 received, 100% packet loss, time 55292ms

rohanberawal@fedora:~$
rohanberawal@fedora:~$
```

Description :

To make the ping command fail for the mentioned IP I followed 4 Major step :

Step1 : <sudo ifconfig lo down>

This is the command to disable the loopback interface . The loopback is a special interface with the IP of <127.0.0.1> that helps the user to communicate with itself . If we put a port down then the port will be disabled .

Step2 : <ifconfig>

This command will show all the network ports available on the machine . Since we have put down / disabled the lo port that port will not be visible in the output section .

Step3 : **<ping <ip address of Lo port> /(given port)>**

When we ping this port the machine will stop and not respond . Since this port helps the machine to make the connection with itself , the machine will not respond for a while until we press control +c .

Step4 : **<Control + c>**

When we process this command we can see the number of the client packet sent through the lo port as the mentioned ip is the ip of the lo port . 0 received as we disabled the Lo port in the step 2 and finally 100% packet loss as none of the transmitted packet is received .