

## COMPUTER NETWORKS

### ASSIGNMENT 1

#### Question 1:

a)

Attached below is the screenshot of the Ubuntu terminal in which 'ifconfig' command has been used.

On using the 'ifconfig' command for the first time, it shows all the currently active network interfaces. In the screenshot below, 2 interfaces, namely 'ens33' and 'lo' are active.

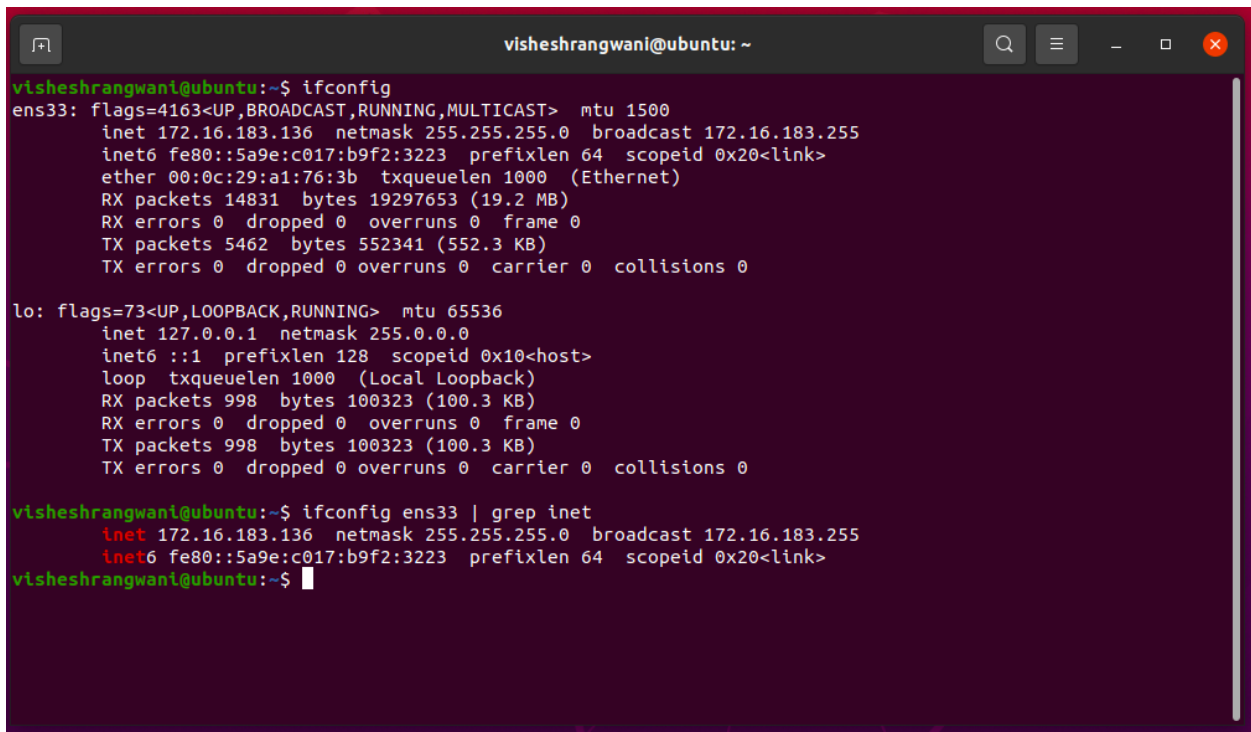
The screenshot shows 'inet' and 'inet6' which are respectively IP addresses in IPv4 and IPv6 format respectively.

For 'ens33' interface, the IP address is:

IPv4 format: 172.16.183.136

IPv6 format: fe80::5a9e:c017:b9f2:3223

These are also displayed by using grep for 'ens33' in the ifconfig command.



```
visheshrangwani@ubuntu:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.16.183.136 netmask 255.255.255.0 broadcast 172.16.183.255
    inet6 fe80::5a9e:c017:b9f2:3223 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:a1:76:3b txqueuelen 1000 (Ethernet)
    RX packets 14831 bytes 19297653 (19.2 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 5462 bytes 552341 (552.3 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

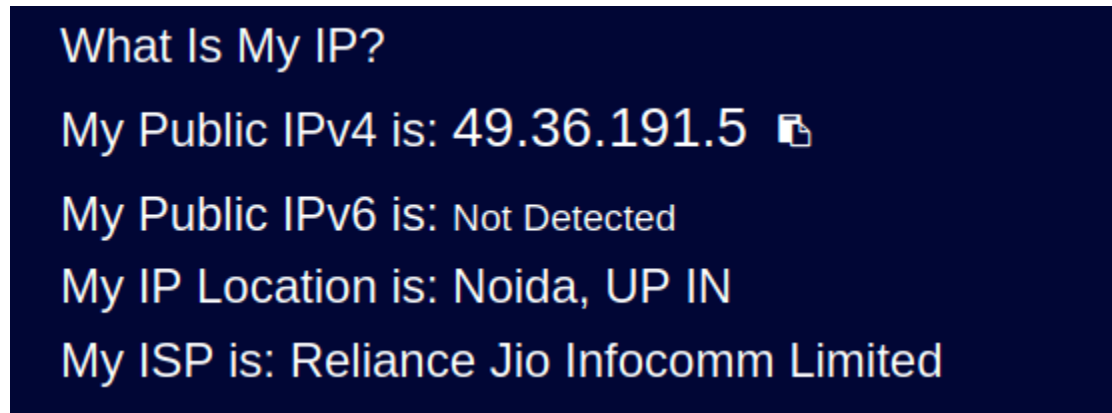
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 998 bytes 100323 (100.3 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 998 bytes 100323 (100.3 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

visheshrangwani@ubuntu:~$ ifconfig ens33 | grep inet
    inet 172.16.183.136 netmask 255.255.255.0 broadcast 172.16.183.255
    inet6 fe80::5a9e:c017:b9f2:3223 prefixlen 64 scopeid 0x20<link>
visheshrangwani@ubuntu:~$
```

**b)**

The screenshot below shows the result of IP address shown on the web page <https://www.whatismyip.com> . The IP shown on the web page is different from the IP we see by running the ifconfig command.

The IP shown by the website is: 49.36.191.5



The reason for the website showing a different IP is that 'ifconfig' command shows the private IP address of the machine. It shows the IP address of my machine in the local area network created by the modem for communicating within the LAN. However the IP on the website is the IP provided by the ISP for communicating on the internet. Unlike private IP address from 'ifconfig', the IP shown on whatismyip.com is a public address used for communicating on Wide Area Network over the Internet. The 'ifconfig' IP being private to my machine in the LAN cannot be perceived on the internet on the website. The IP, displayed on the web is common for all devices that are trying to access internet within the same network as it is provided by the ISP.

## **Question 2:**

**a)**

Nslookup command is used to get the IP address of a website from DNS server.

To find the IP address of google.com, the command: nslookup google.com shows a non-authoritative answer (as shown in the screenshot).

In order to get authoritative result, we need to get the details of the authoritative name server. To get that, we use the option -type=soa.

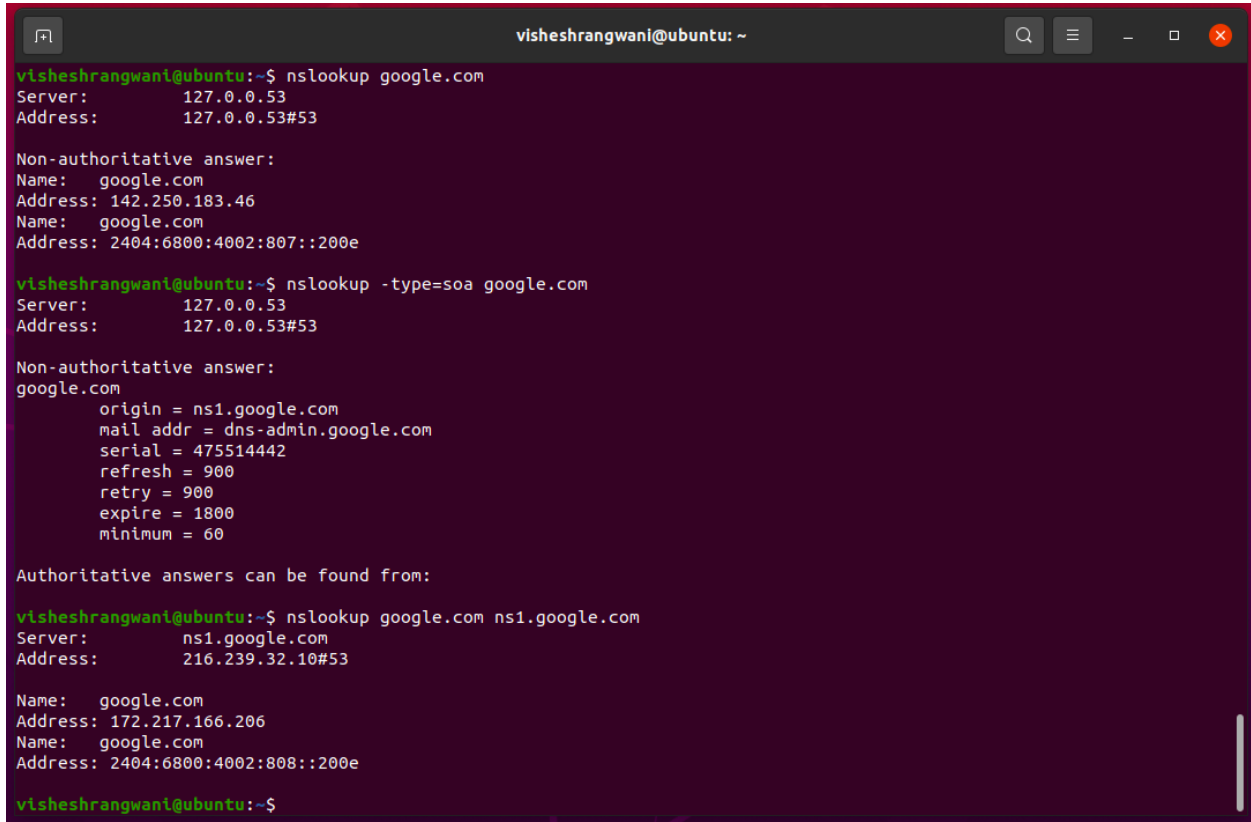
Command: nslookup -type=soa google.com

SOA stands for Start of Authority and this options returns the administrative details of the DNS server.

We can use this administrative details, i.e. the origin (in the details of the DNS server) and mention the server as well in nslookup query along with 'google.com' for getting the authoritative answer.

Command: nslookup google.com ns1.google.com

The steps mentioned above are shown to be performed in the screenshot below.



```
visheshrangwani@ubuntu: ~  
visheshrangwani@ubuntu:~$ nslookup google.com  
Server:      127.0.0.53  
Address:     127.0.0.53#53  
  
Non-authoritative answer:  
Name:   google.com  
Address: 142.250.183.46  
Name:   google.com  
Address: 2404:6800:4002:807::200e  
  
visheshrangwani@ubuntu:~$ nslookup -type=soa google.com  
Server:      127.0.0.53  
Address:     127.0.0.53#53  
  
Non-authoritative answer:  
google.com  
      origin = ns1.google.com  
      mail addr = dns-admin.google.com  
      serial = 475514442  
      refresh = 900  
      retry = 900  
      expire = 1800  
      minimum = 60  
  
Authoritative answers can be found from:  
  
visheshrangwani@ubuntu:~$ nslookup google.com ns1.google.com  
Server:      ns1.google.com  
Address:     216.239.32.10#53  
  
Name:   google.com  
Address: 172.217.166.206  
Name:   google.com  
Address: 2404:6800:4002:808::200e  
  
visheshrangwani@ubuntu:~$
```

**b)**

In order to find out Time to Live for any website on local DNS, we can use the command:

nslookup -debug [www.amazon.in](http://www.amazon.in)

This would give the Time to Live (TTL) for [www.amazon.in](http://www.amazon.in) on the local DNS.

Screenshot:

```
visheshrangwani@ubuntu:~$ nslookup -debug www.amazon.in
Server:      127.0.0.53
Address:     127.0.0.53#53

-----
QUESTIONS:
  www.amazon.in, type = A, class = IN
ANSWERS:
-> www.amazon.in
   canonical name = tp.c95e7e602-frontier.amazon.in.
   ttl = 5
-> tp.c95e7e602-frontier.amazon.in
   canonical name = www-amazon-in.customer.fastly.net.
   ttl = 4
-> www-amazon-in.customer.fastly.net
   internet address = 162.219.225.220
   ttl = 4
AUTHORITY RECORDS:
ADDITIONAL RECORDS:
-----
Non-authoritative answer:
www.amazon.in canonical name = tp.c95e7e602-frontier.amazon.in.
tp.c95e7e602-frontier.amazon.in canonical name = www-amazon-in.customer.fastly.net.
Name:   www-amazon-in.customer.fastly.net
Address: 162.219.225.220
-----
QUESTIONS:
  www-amazon-in.customer.fastly.net, type = AAAA, class = IN
ANSWERS:
-> www-amazon-in.customer.fastly.net
   has AAAA address 2606:2cc0:3::476
   ttl = 5
-> www-amazon-in.customer.fastly.net
   has AAAA address 2606:2cc0::476
   ttl = 5
-> www-amazon-in.customer.fastly.net
   has AAAA address 2606:2cc0:1::476
   ttl = 5
-> www-amazon-in.customer.fastly.net
   has AAAA address 2606:2cc0:2::476
   ttl = 5
AUTHORITY RECORDS:
ADDITIONAL RECORDS:
-----
Name:   www-amazon-in.customer.fastly.net
Address: 2606:2cc0:3::476
Name:   www-amazon-in.customer.fastly.net
Address: 2606:2cc0::476
Name:   www-amazon-in.customer.fastly.net
Address: 2606:2cc0:1::476
Name:   www-amazon-in.customer.fastly.net
Address: 2606:2cc0:2::476
```

There are 2 types of records for [www.amazon.com](http://www.amazon.com) on the local.

One is type=A. This means that the IP stored for this is an IPv4 address. The ttl shown for such records is 5 seconds for 1st record, 4 seconds for 2nd record and 4 seconds for 3rd record. The different records represents the different levels in DNS hierarchy, i.e. root servers, top level domain servers and authoritative servers. The records would expire in 5, 4 and 4 seconds respectively and will have to be refreshed in the servers.

Second type is type=AAAA, which means that it stores IPv6 type of records. Each record belongs to a particular hierarchy in DNS server and has a ttl of 5 seconds. This means that each of the records in the DNS servers would expire in 5 seconds.

As for the unit of time which is not written in terminal, but is claimed by me to be seconds. The reason for this is that on running the same command several times repeated almost instantaneously, the ttl values change very frequently from 5->3->1->5 and somewhat this pattern is observed if a run the command in very short intervals.

### Question 3:

a)

The screenshot is attached below.

```
visheshrangwani@ubuntu:~$ traceroute google.in
traceroute to google.in (142.250.192.100), 64 hops max
 1  172.16.183.2  0.320ms  0.296ms  0.366ms
 2  192.168.29.1  3.656ms  1.746ms  2.706ms
 3  10.13.24.1  9.117ms  21.700ms  9.505ms
 4  172.16.26.1  8.034ms  9.881ms  9.786ms
 5  192.168.128.140  6.405ms  9.773ms  192.168.128.138  9.463ms
 6  172.27.248.53  9.707ms  8.319ms  11.446ms
 7  172.27.248.35  9.560ms  11.424ms  192.168.44.22  6.269ms
 8  192.168.44.22  7.867ms  192.168.44.24  7.458ms  192.168.44.23  7.764ms
 9  192.168.44.29  8.483ms  7.739ms  172.26.14.75  10.017ms
10  172.16.18.0  8.502ms  7.116ms  172.26.14.73  7.803ms
11  72.14.195.22  8.009ms  7.981ms  *
12  142.250.47.144  9.581ms  8.093ms  *
13  * * *
14  216.239.57.32  9.479ms  8.051ms  108.170.251.107  8.423ms
15  108.170.251.107  7.992ms  8.458ms  142.250.230.116  36.708ms
16  72.14.232.138  27.412ms  27.802ms  216.239.50.22  31.086ms
17  72.14.237.139  34.255ms  32.358ms  142.250.192.100  34.275ms
visheshrangwani@ubuntu:~$
```

As in screenshot attached, there are 17 hosts in total that can be seen. Ignoring the ones with a '\*\*\*', there are 16 hosts to be considered.

Traceroute command sends 3 packet to each host. Their corresponding Round trip time ( $\approx 2 \times \text{latencies}$ ) are written in 3rd, 4th and 5th columns respectively.

The following are the details of each host:

1. IP address: 172.16.183.2  
Average Latency =  $(0.320 + 0.296 + 0.366) / 3 = 0.3273333333$  ms
2. IP address: 192.168.29.1

- Average Latency =  $(3.656+1.746+2.706)/3 = 2.702666667$  ms
3. IP address: 10.13.24.1  
Average Latency =  $(9.117+21.7+9.505)/3 = 13.44066667$  ms
  4. IP address: 172.16.26.1  
Average Latency =  $(8.034+9.881+9.786)/3 = 9.233666667$  ms
  5. IP address: 192.168.128.140  
Average Latency =  $(6.405+9.773+9.463)/3 = 8.547$  ms
  6. IP address: 172.27.248.53  
Average Latency =  $(9.707+8.319+11.446)/3 = 9.824$  ms
  7. IP address: 172.27.248.35  
Average Latency =  $(9.56+11.424+6.269)/3 = 9.084333333$  ms
  8. IP address: 192.168.44.22  
Average Latency =  $(7.867+7.458+7.764)/3 = 7.696333333$  ms
  9. IP address: 192.168.44.29  
Average Latency =  $(8.483+7.739+10.017)/3 = 8.746333333$  ms
  10. IP address: 172.16.18.0  
Average Latency =  $(8.502+7.116+7.803)/3 = 7.807$  ms
  11. IP address: 72.14.195.22  
Average Latency =  $(8.009+7.981)/2 = 7.995$  ms
  12. IP address: 142.250.47.144  
Average Latency =  $(9.581+8.093)/2 = 8.837$  ms
  13. IP address: \* \* \*
  14. IP address: 216.239.57.32  
Average Latency =  $(9.479+8.051+8.423)/3 = 8.651$  ms
  15. IP address: 108.170.251.107  
Average Latency =  $(7.992+8.458+36.708)/3 = 17.71933333$  ms
  16. IP address: 72.14.232.138  
Average Latency =  $(27.412+27.802+31.086)/3 = 28.76666667$  ms
  17. IP address: 72.14.237.139  
Average Latency =  $(34.255+32.358+34.27)/3 = 33.62766667$  ms

Since the traceroute shows the time for data packet to be sent to the server and back to the client, it is the Round Trip Time. In the above computations, we have found out the average Round Trip Time for 3 packets for each of the 17 hops. To get a measurement of latency, we can divide the Round Trip Time by 2.

**b)**

100 ping messages to google.in were sent using the command:  
ping -c 100 google.in

```
visheshrangwani@ubuntu:~$ ping -c 100 google.in
PING google.in (142.250.192.228) 56(84) bytes of data.
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=1 ttl=128 time=10.3 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=2 ttl=128 time=12.7 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=3 ttl=128 time=82.1 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=4 ttl=128 time=190 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=5 ttl=128 time=71.6 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=6 ttl=128 time=11.8 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=7 ttl=128 time=16.6 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=8 ttl=128 time=15.0 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=9 ttl=128 time=13.0 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=10 ttl=128 time=7.23 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=11 ttl=128 time=21.6 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=12 ttl=128 time=19.0 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=13 ttl=128 time=13.2 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=14 ttl=128 time=17.7 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=15 ttl=128 time=26.5 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=16 ttl=128 time=11.5 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=17 ttl=128 time=10.7 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=18 ttl=128 time=17.8 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=19 ttl=128 time=14.3 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=20 ttl=128 time=18.0 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=21 ttl=128 time=12.2 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=22 ttl=128 time=13.1 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=23 ttl=128 time=17.5 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=24 ttl=128 time=13.5 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=25 ttl=128 time=15.6 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=26 ttl=128 time=14.2 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=27 ttl=128 time=16.2 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=28 ttl=128 time=8.22 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=29 ttl=128 time=18.0 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=30 ttl=128 time=20.5 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=31 ttl=128 time=15.6 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=32 ttl=128 time=19.7 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=33 ttl=128 time=16.4 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=34 ttl=128 time=6.79 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=35 ttl=128 time=15.6 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=36 ttl=128 time=14.8 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=37 ttl=128 time=19.6 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=38 ttl=128 time=24.0 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=39 ttl=128 time=31.5 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=40 ttl=128 time=11.7 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=41 ttl=128 time=12.9 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=42 ttl=128 time=17.6 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=43 ttl=128 time=19.8 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=44 ttl=128 time=12.7 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=45 ttl=128 time=14.7 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=46 ttl=128 time=9.67 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=47 ttl=128 time=13.3 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=48 ttl=128 time=12.9 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=49 ttl=128 time=8.21 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=50 ttl=128 time=7.90 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=51 ttl=128 time=17.4 ms
```



```

64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=52 ttl=128 time=14.1 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=53 ttl=128 time=14.1 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=54 ttl=128 time=10.6 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=55 ttl=128 time=28.5 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=56 ttl=128 time=52.2 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=57 ttl=128 time=18.0 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=58 ttl=128 time=9.04 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=59 ttl=128 time=19.7 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=60 ttl=128 time=17.4 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=61 ttl=128 time=7.07 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=62 ttl=128 time=13.9 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=63 ttl=128 time=18.9 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=64 ttl=128 time=13.3 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=65 ttl=128 time=9.21 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=66 ttl=128 time=26.0 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=67 ttl=128 time=45.4 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=68 ttl=128 time=9.72 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=69 ttl=128 time=14.9 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=70 ttl=128 time=8.01 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=71 ttl=128 time=19.4 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=72 ttl=128 time=11.9 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=73 ttl=128 time=7.49 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=74 ttl=128 time=16.6 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=75 ttl=128 time=17.3 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=76 ttl=128 time=21.1 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=77 ttl=128 time=14.0 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=78 ttl=128 time=19.3 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=79 ttl=128 time=13.3 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=80 ttl=128 time=21.6 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=81 ttl=128 time=13.1 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=82 ttl=128 time=14.0 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=83 ttl=128 time=12.1 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=84 ttl=128 time=17.8 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=85 ttl=128 time=26.5 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=86 ttl=128 time=13.3 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=87 ttl=128 time=14.6 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=88 ttl=128 time=17.2 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=89 ttl=128 time=13.9 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=90 ttl=128 time=14.2 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=91 ttl=128 time=17.1 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=92 ttl=128 time=18.3 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=93 ttl=128 time=20.3 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=94 ttl=128 time=17.7 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=95 ttl=128 time=14.9 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=96 ttl=128 time=16.4 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=97 ttl=128 time=19.4 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=98 ttl=128 time=6.17 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=99 ttl=128 time=36.4 ms
64 bytes from del11s13-in-f4.1e100.net (142.250.192.228): icmp_seq=100 ttl=128 time=17.4 ms

--- google.in ping statistics ---
100 packets transmitted, 100 received, 0% packet loss, time 99711ms
rtt min/avg/max/mdev = 6.166/19.250/190.122/20.382 ms

```

Ping command shows the Round Trip Time i.e. time to send echo message and receive reply. As shown and highlighted in the last line, the average Round Trip Time of 100 pings is 19.250ms. Correspondingly, the average latency would be  $RTT/2 = 19.250/2 = 9.625$  ms

c)

100 ping messages to columbia.edu were sent using the command:  
ping -c 100 columbia.edu



```
visheshrangwani@ubuntu:~$ ping -c 100 columbia.edu
PING columbia.edu (128.59.105.24) 56(84) bytes of data.
64 bytes from columbia.edu (128.59.105.24): icmp_seq=1 ttl=128 time=410 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=2 ttl=128 time=371 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=3 ttl=128 time=403 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=4 ttl=128 time=329 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=5 ttl=128 time=339 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=6 ttl=128 time=358 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=7 ttl=128 time=291 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=8 ttl=128 time=407 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=9 ttl=128 time=331 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=10 ttl=128 time=357 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=11 ttl=128 time=391 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=12 ttl=128 time=286 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=13 ttl=128 time=328 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=14 ttl=128 time=376 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=15 ttl=128 time=467 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=16 ttl=128 time=389 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=17 ttl=128 time=270 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=18 ttl=128 time=274 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=19 ttl=128 time=360 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=20 ttl=128 time=381 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=21 ttl=128 time=358 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=22 ttl=128 time=269 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=23 ttl=128 time=271 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=24 ttl=128 time=363 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=25 ttl=128 time=410 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=26 ttl=128 time=405 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=27 ttl=128 time=576 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=28 ttl=128 time=362 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=29 ttl=128 time=466 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=30 ttl=128 time=390 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=31 ttl=128 time=315 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=32 ttl=128 time=350 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=33 ttl=128 time=333 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=34 ttl=128 time=384 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=35 ttl=128 time=385 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=36 ttl=128 time=387 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=37 ttl=128 time=451 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=38 ttl=128 time=322 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=39 ttl=128 time=350 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=40 ttl=128 time=460 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=41 ttl=128 time=282 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=42 ttl=128 time=417 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=43 ttl=128 time=379 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=44 ttl=128 time=344 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=45 ttl=128 time=355 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=46 ttl=128 time=371 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=47 ttl=128 time=333 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=48 ttl=128 time=469 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=49 ttl=128 time=380 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=50 ttl=128 time=279 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=51 ttl=128 time=440 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=52 ttl=128 time=279 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=53 ttl=128 time=381 ms
```

```

64 bytes from columbia.edu (128.59.105.24): icmp_seq=52 ttl=128 time=279 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=53 ttl=128 time=381 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=54 ttl=128 time=410 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=55 ttl=128 time=442 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=56 ttl=128 time=391 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=57 ttl=128 time=379 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=58 ttl=128 time=736 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=59 ttl=128 time=294 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=60 ttl=128 time=341 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=61 ttl=128 time=408 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=62 ttl=128 time=402 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=63 ttl=128 time=367 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=64 ttl=128 time=326 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=65 ttl=128 time=296 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=66 ttl=128 time=420 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=67 ttl=128 time=299 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=68 ttl=128 time=376 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=69 ttl=128 time=365 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=70 ttl=128 time=290 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=71 ttl=128 time=422 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=72 ttl=128 time=429 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=73 ttl=128 time=362 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=74 ttl=128 time=344 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=75 ttl=128 time=369 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=76 ttl=128 time=304 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=77 ttl=128 time=1110 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=78 ttl=128 time=371 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=79 ttl=128 time=370 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=80 ttl=128 time=453 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=81 ttl=128 time=1313 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=82 ttl=128 time=559 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=83 ttl=128 time=380 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=84 ttl=128 time=371 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=85 ttl=128 time=370 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=86 ttl=128 time=404 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=87 ttl=128 time=311 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=88 ttl=128 time=372 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=89 ttl=128 time=295 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=90 ttl=128 time=335 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=91 ttl=128 time=274 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=92 ttl=128 time=272 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=93 ttl=128 time=279 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=94 ttl=128 time=369 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=95 ttl=128 time=277 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=96 ttl=128 time=347 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=97 ttl=128 time=520 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=98 ttl=128 time=396 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=99 ttl=128 time=320 ms
64 bytes from columbia.edu (128.59.105.24): icmp_seq=100 ttl=128 time=334 ms

--- columbia.edu ping statistics ---
100 packets transmitted, 100 received, 0% packet loss, time 101638ms
rtt min/avg/max/mdev = 268.865/386.091/1312.914/138.093 ms, pipe 2
visheshrangwani@ubuntu:~$

```

As shown and highlighted in the last line, the average Round Trip Time of 100 pings is 386.091ms. Correspondingly, the average latency would be  $RTT/2 = 386.091/2 = 193.0455\text{ms}$

**d)**

The sum of all the latencies (precisely, RTTs) of the intermediate hosts, as found by the traceroute command is coming out to be 183.006ms. The latency would be  $183.006/2=91.503\text{ms}$

This is considerably higher than the average latency of the ping command.

The reason for this considerable difference is in the concept of how the 2 commands differ in their functionality.

The 'ping' command sends ICMP (Internet Control Message Protocol) echo message to the destination host (In this case: google.in). The source then sends back the reply and Round Trip Time (or overall latency) is noted when the client sending 'ping' message receives back the reply.

On the other hand, 'traceroute' command sends three UDP datagrams for varying TTL (Time to Live), starting from a low TTL to gradually increasing TTLs. Whenever a packet reaches a router (intermediate host) corresponding to its TTL value or expires in between, the node returns the packet ICMP Time Exceeded Message (TEM) to the source, which is noted as RTT for that particular intermediate host. In a similar way, by gradually increasing the TTL, we can trace all the nodes in between and we get the RTT for all the routers in the path of reaching the required destination.

Since in 'traceroute' we get all the RTTs for all the routers (by summing up average latencies) in the path as opposed to the RTT in 'ping' which is the time for echo message to reach the destination and reply reaching the source back, we see a considerable difference in the latencies shown by average delay in 'ping' and sum of all intermediate delays in 'traceroute'.

**e)**

The maximum latency (RTT) among intermediate hosts is for the IP address: 72.14.237.139 And its value is 33.62766667 ms. Corresponding precise latency: 16.813833335 ms This value is comparable but not matching to that of average RTT of 19.250 ms (latency: 9.625 ms) found using 'ping' command.

This is due to the fact that maximum average latency of intermediate hosts roughly represents the intermediate host that received UDP datagram the latest. This means that it was farther in network from our machine and closer to the web host. In case of 'ping', the ICMP message is directed towards the host itself, so the 2 tend to be comparable.

However, these values still are not matching despite looking for the same host because of the fact that the route taken by 'ping's' ICMP echo message may be very different from that specified in the traceroute command. This happens because, the network (internet) dynamics changes very frequently (due to load balancing, queueing, etc) and based on different parameters, the routers select the path for sending a packet over the network.

f)

Traceroute done using the command: traceroute columbia.edu

```
vi@sheshrangwani@ubuntu:~$ traceroute columbia.edu
traceroute to columbia.edu (128.59.105.24), 64 hops max
 1  172.16.183.2  1.815ms  0.350ms  0.400ms
 2  192.168.29.1  6.078ms  5.541ms  5.077ms
 3  10.13.24.1  5.925ms  7.569ms  8.348ms
 4  172.16.18.1  9.769ms  9.411ms  9.244ms
 5  192.168.128.140  7.359ms  192.168.128.138  10.086ms  192.168.128.140  5.771ms
 6  172.27.248.53  8.318ms  15.183ms  7.604ms
 7  172.27.248.35  8.674ms  9.626ms  192.168.44.22  6.314ms
 8  192.168.44.22  7.225ms  7.023ms  192.168.44.25  6.423ms
 9  192.168.44.23  7.325ms  9.870ms  172.26.14.73  8.398ms
10  172.26.14.75  11.373ms  8.924ms  9.101ms
11  172.16.18.33  7.156ms  7.253ms  172.26.29.107  57.326ms
12  172.16.5.85  54.308ms  60.557ms  54.935ms
13  172.16.5.85  55.329ms  61.110ms  103.198.140.64  77.907ms
14  * * 154.54.3.69 371.558ms
15  * * 154.54.3.69 339.468ms
16  154.54.3.69 306.665ms 306.326ms 154.54.45.161 307.532ms
17  154.54.27.117 309.300ms 305.687ms 154.54.44.85 305.972ms
18  154.54.30.161 407.774ms 409.298ms 154.54.28.129 286.164ms
19  154.54.28.129 293.080ms 287.707ms 154.54.24.221 286.647ms
20  154.54.28.129 288.489ms 291.044ms 154.54.24.221 316.800ms
21  154.54.24.221 407.004ms * 154.54.40.109 286.792ms
22  154.54.24.221 307.904ms 286.055ms 154.54.40.109 277.223ms
23  154.54.40.109 321.270ms 308.022ms 154.54.84.214 316.756ms
24  154.54.84.214 356.911ms 325.671ms 38.122.8.210 390.672ms
25  38.122.8.210 305.992ms 308.166ms 128.59.255.5 308.009ms
26  128.59.255.21 292.150ms 321.998ms 128.59.105.24 407.620ms
vi@sheshrangwani@ubuntu:~$
```

No of hops in traceroute of google.in: 17

No of hops in traceroute of columbia.edu: 26

From the values of RTTs (latency\*2) of columbia.edu, we can clearly see that these values are much larger as compared to latency values of google.in. This can distinctly be seen especially in hop no 11 to 26, which are greater than the maximum latency(and RTT) for any google.in intermediate host.

The reason for this can be attributed to the fact that 'columbia.edu' servers would not be located locally in India but in Columbia University in US. However, in case of 'google.in' servers, as is clear from the Top Level Domain '.in', would be fetching data locally from google servers in India.

Servers for 'columbia.edu' being physically far from the machine means that information will have to travel longer distances in the network and hence will have to encounter numerous intermediate hosts. Hence, more no of hops and higher latencies.



#### Question 4:

In order to fail the ping command for the IP: 127.0.0.1, it is known that the given IP is of local host (taught in tutorial). To fail it, we can close the connection to the interface of localhost. Localhost is shown in ifconfig as 'lo' with given IP. So in order to deactivate the localhost, the command: `sudo ifconfig lo down`

Is used and after doing ifconfig, we are unable to see the 'lo' interface. After that we ping messages to 127.0.0.1 and no messages are transferred and hence 100% packet lost.

Screenshots attached:

Before deactivating 'lo':

```
visheshrangwani@ubuntu:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 172.16.183.136  netmask 255.255.255.0  broadcast 172.16.183.255
    inet6 fe80::5a9e:c017:b9f2:3223  prefixlen 64  scopeid 0x20<link>
    ether 00:0c:29:a1:76:3b  txqueuelen 1000  (Ethernet)
    RX packets 36131  bytes 51501605 (51.5 MB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 14450  bytes 1051946 (1.0 MB)
    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 605  bytes 54596 (54.5 KB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 605  bytes 54596 (54.5 KB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

visheshrangwani@ubuntu:~$ ping -c 10 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=1.85 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.038 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.037 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.062 ms
64 bytes from 127.0.0.1: icmp_seq=5 ttl=64 time=0.049 ms
64 bytes from 127.0.0.1: icmp_seq=6 ttl=64 time=0.038 ms
64 bytes from 127.0.0.1: icmp_seq=7 ttl=64 time=0.040 ms
64 bytes from 127.0.0.1: icmp_seq=8 ttl=64 time=0.039 ms
64 bytes from 127.0.0.1: icmp_seq=9 ttl=64 time=0.051 ms
64 bytes from 127.0.0.1: icmp_seq=10 ttl=64 time=0.037 ms

--- 127.0.0.1 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 918ms
rtt min/avg/max/mdev = 0.037/0.223/1.845/0.540 ms
```

After deactivating 'lo' interface:

```

visheshrangwani@ubuntu:~$ sudo ifconfig lo down
visheshrangwani@ubuntu:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 172.16.183.136  netmask 255.255.255.0  broadcast 172.16.183.255
    inet6 fe80::5a9e:c017:b9f2:3223  prefixlen 64  scopeid 0x20<link>
    ether 00:0c:29:a1:76:3b  txqueuelen 1000  (Ethernet)
    RX packets 36134  bytes 51501845 (51.5 MB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 14453  bytes 1052186 (1.0 MB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

visheshrangwani@ubuntu:~$ ping -c 10 127.0.0.1
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 9201ms

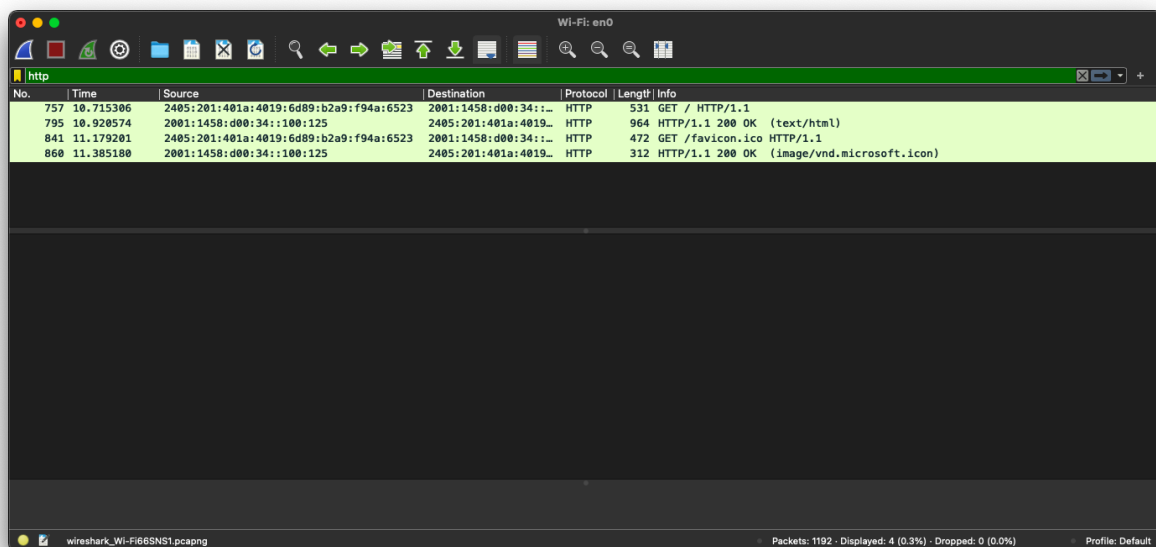
visheshrangwani@ubuntu:~$

```

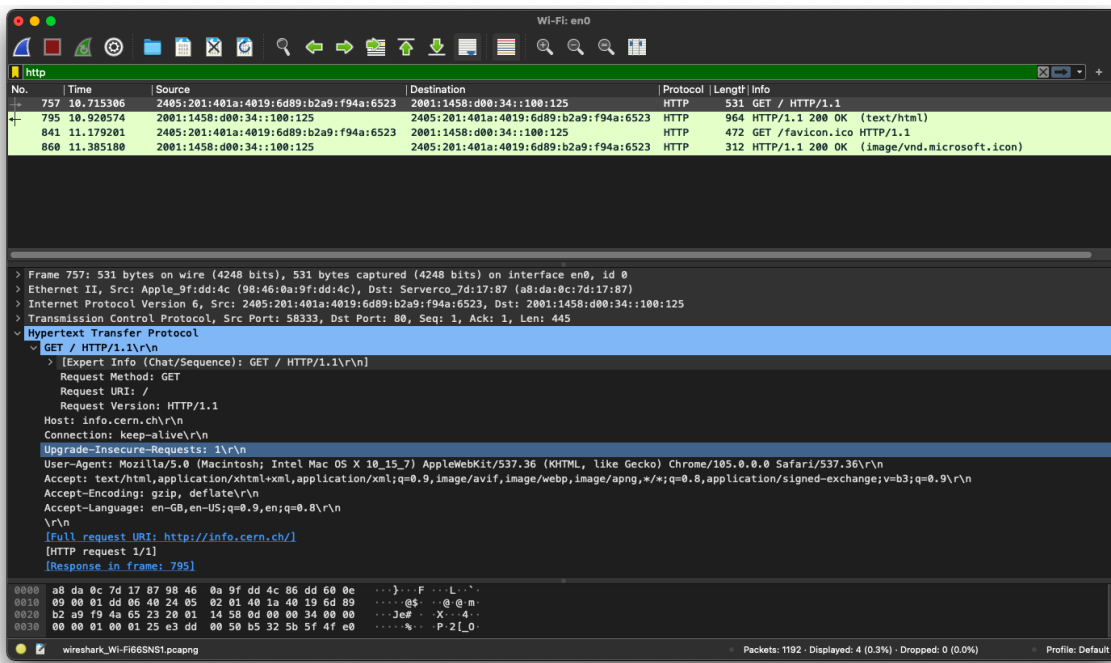
### Question 5:

Wireshark software for MacOS (that's why different IP in screenshots of wireshark) was used to capture the communication between my local machine and web server.

The screenshot for the same is attached below. The packet no. 757 is the request message from local machine to the web server while the packet no. 795 is the response message from the webserver to my local machine



- **HTTP Request packet (Packet No 757):**



- The packet no 757 is a 'Request' packet from my local machine to the webserver, requesting the web server for information.
- HTTP Request Type used is: HTTP GET Request  
The request being sent from the local machine to webserver is HTTP GET Request to request the server for the webpage contents.
- User Agent (as shown in wireshark, screenshot attached): Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_15\_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36  
The User Agent string mentioned above belongs to Chrome browser running on MAC OS. [Credits](#).  
This determines the communicating agent, i.e. browser who is communicating with the web server to fetch information.
- HTTP Request Packet's URL:  
Request URI: /  
This URI '/' shows the relative path from the webserver for the requested website.  
[Full request URI: <http://info.cern.ch/>]  
This URI shows the full Request URI as shown in Wireshark.
- Name and Version of web server:  
[Full request URI: <http://info.cern.ch/>]  
This web server is being requested to fetch information using HTTP.  
As shown in Wireshark:  
Host: info.cern.ch\r\n

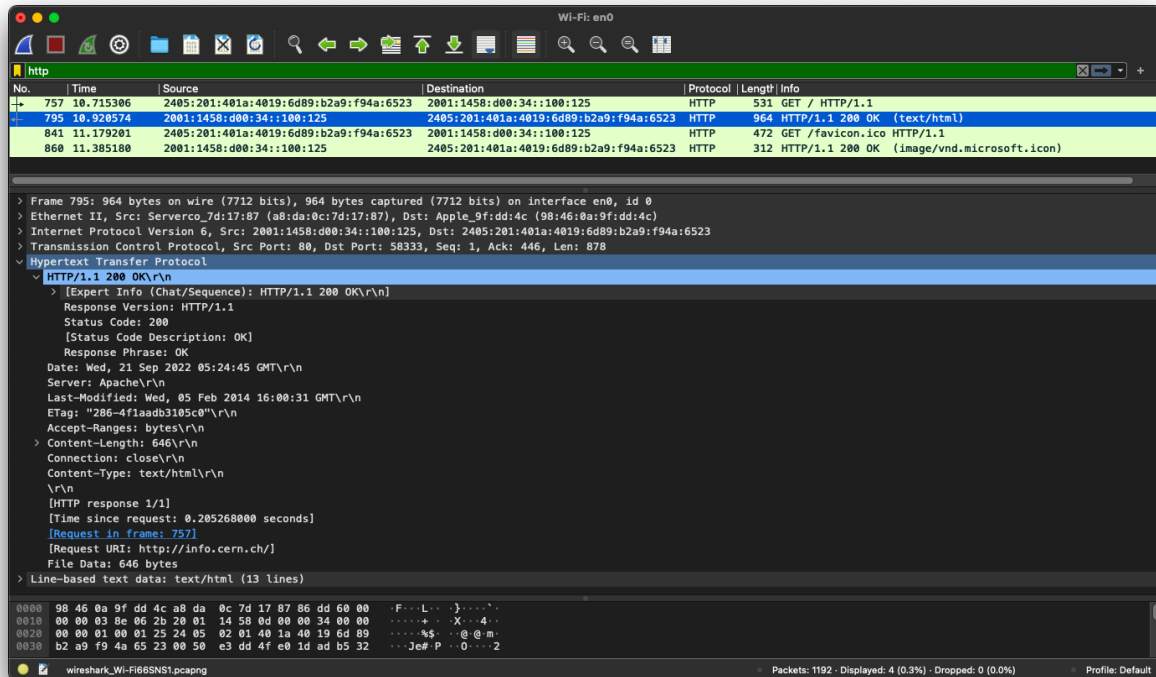


Request Version: HTTP/1.1

[GET / HTTP/1.1\r\n]

HTTP/1.1 is the version of HTTP being used for this request.

- HTTP Response Packet (Packet No 795):

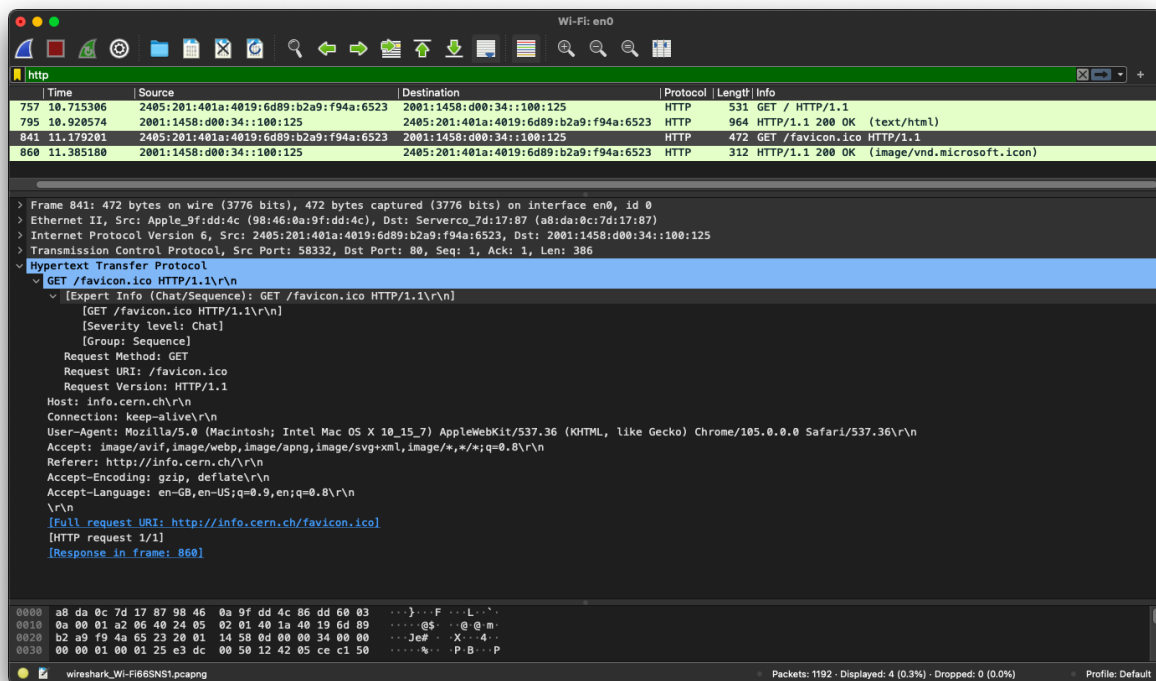


- The packet no 795 is the one for sending Response packets from the web server to the web browser on local machine for response to packet 757.
- HTTP Response Code:  
HTTP/1.1 200 OK\r\n  
Status Code: 200  
[Status Code Description: OK]  
As shown in wireshark, the HTTP Response code is '200', indicating that the request has succeeded.  
Response has been successfully delivered to the local machine and there were no errors to be reported.
- HTTP response description:  
Response Version: HTTP/1.1  
Status Code: 200  
[Status Code Description: OK]  
Response Phrase: OK  
The Status Code 200 indicates that the Request has succeeded.

The HTML response for the requested web page is sent successfully from the server to the local machine via HTTP/1.1 (HTTP version 1.1). The HTML data can be seen on Wireshark under the topic: 'Line Based Text Data'. This gets displayed on the client web browser.

- Wireshark shows that Server for this Response packet is: Apache.  
Version of web server: Not mentioned in Wireshark

- HTTP Request Packet (Packet No 841):



- The packet no 841 is a 'Request' packet from local machine to the webserver, requesting the web server 'favicon.ico' image.
- HTTP Request Type used is: HTTP GET Request  
The request being sent from the local machine to webserver is HTTP GET request to request the server for the webpage contents, specifically 'favicon.ico' image.
- User-Agent (as shown in wireshark, screenshot attached): Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_15\_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36  
As is the case for previous request packet, 757, here also the User Agent string mentioned above belongs to Chrome browser running on MacOS.

[Credits.](#)

This determines the communicating agent, i.e. browser who is communicating with the web server to fetch information.

- HTTP request packet's URL:

Request URI: /favicon.ico

This is the relative path of the file from the main web page being requested.

[Full request URI: <http://info.cern.ch/favicon.ico>]

This specifies the entire URI being requested by this packet.

- Name and Version of web server:

[Full request URI: <http://info.cern.ch/favicon.ico>]

This web server is being requested to fetch information using HTTP.

As shown in Wireshark:

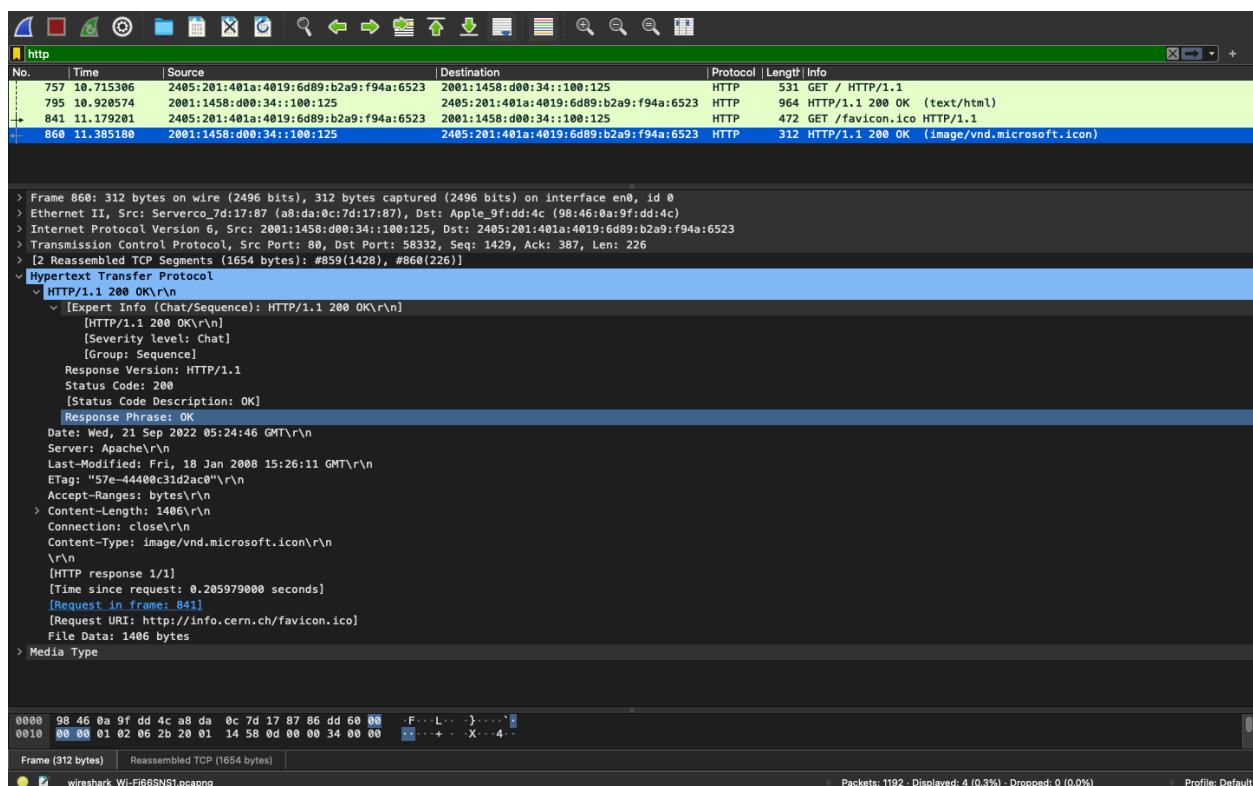
Host: info.cern.ch\r\n

Request Version: HTTP/1.1

[GET /favicon.ico HTTP/1.1\r\n]

HTTP/1.1 is the version of HTTP being used for this request.

- HTTP Response Packet (Packet No 860):



- The packet no 860 is the one for sending Response packets from the web server to the web browser on local machine for the response to packet 741.

- HTTP Response Code:  
HTTP/1.1 200 OK\r\n  
Status Code: 200  
[Status Code Description: OK]  
As shown in Wireshark, the HTTP Response code is '200', indicating that the request has succeeded.  
Response has been successfully delivered to the local machine and there were no errors to be reported.
- HTTP response description:  
Response Version: HTTP/1.1  
Status Code: 200  
[Status Code Description: OK]  
Response Phrase: OK  
The Status Code 200 indicates that the Request has succeeded.  
The HTML response for the requested web page is sent successfully from the server to the local machine via HTTP/1.1 (HTTP version 1.1). The image that has been transferred can be seen on Wireshark under the topic: 'Media Type'. This gets displayed on the client web browser. Wireshark also mentions content type and media type as:  
Content-Type: image/vnd.microsoft.icon\r\n\r\n  
Media type: image/vnd.microsoft.icon (1406 bytes)
- Wireshark shows that Server for this Response packet is: Apache  
Server: Apache\r\n\r\n  
Version of web server: Not mentioned in Wireshark
- There are 2 objects being downloaded, as can be seen on Wireshark, there are 2 response packets that are received on the client machine.  
Also, both of them were downloaded over 2 different TCP connections. This fact can be demonstrated by the fact that in the 2 screenshots of the response packets, the Dest Port for packet no 795 is 58333 and Dest Port for packet no 860 is 58332. Also, it is known that a TCP connection is uniquely identified by 2 Host addresses and 2 port nos. But port nos are not same for 2 responses. So these are 2 different TCP connections for downloading the HTML code and Media: favicon.ico.
- Since there are 2 TCP connections, this suggests that it is a non persistent HTTP connection.  
This is somewhat contradictory to the fact that the requests are fetched over HTTP version 1.1, which is by default a persistent connection. However, it can be explained as persistent connection is a default parameter for HTTP 1.1 but it can be changed to non-persistent mode. So, this can be a possibility.  
However, by observation, it can be conceptually claimed that it is a non-persistent connection.

## Question 6:

a)

Netstat command is used to view details about network connections, such as the protocol being used, program using it, its state, etc on our machine.

To view all connections we can use the command: netstat

In order to view all the TCP connections, we can add the option --tcp

Command: netstat --tcp

Alternatively: netstat -t

```
visheshrangwani@ubuntu:~$ netstat --tcp
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp      0      0 ubuntu:36352            ec2-54-149-83-187:https ESTABLISHED
tcp      0      0 ubuntu:42384            del11s14-in-f4.1e:https ESTABLISHED
tcp      0      0 ubuntu:58988            bom07s36-in-f3.1e1:http ESTABLISHED
tcp      0      0 ubuntu:41984            bom07s20-in-f3.1e:https TIME_WAIT
tcp      0      0 ubuntu:40104            del12s05-in-f14.1:https ESTABLISHED
tcp      0      0 ubuntu:49646            bom12s06-in-f22.1:https TIME_WAIT
tcp      0      0 ubuntu:48628            bom07s35-in-f2.1e:https TIME_WAIT
tcp      0      0 ubuntu:58976            bom07s36-in-f3.1e1:http ESTABLISHED
tcp      0      0 ubuntu:57096            del12s01-in-f14.1:https TIME_WAIT
tcp      0      0 ubuntu:41698            bom12s17-in-f10.1:https TIME_WAIT
tcp      0      0 ubuntu:41048            bom12s19-in-f10.1:https TIME_WAIT
tcp      0      0 ubuntu:60604            bom07s28-in-f3.1e:https TIME_WAIT
tcp      0      0 ubuntu:42210            bom12s06-in-f1.1e:https TIME_WAIT
tcp      0      0 ubuntu:37920            123.208.120.34:https ESTABLISHED
tcp      0      0 ubuntu:34970            del12s11-in-f6.1e:https TIME_WAIT
tcp      0      0 ubuntu:44752            bom07s36-in-f3.1e:https ESTABLISHED
tcp      0      0 ubuntu:60536            bom12s14-in-f13.1:https TIME_WAIT
tcp      0      0 ubuntu:59006            bom07s36-in-f3.1e1:http ESTABLISHED
tcp      0      0 ubuntu:58998            bom07s36-in-f3.1e1:http ESTABLISHED
visheshrangwani@ubuntu:~$ netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp      0      0 ubuntu:36352            ec2-54-149-83-187:https ESTABLISHED
tcp      0      0 ubuntu:42384            del11s14-in-f4.1e:https ESTABLISHED
tcp      0      0 ubuntu:58988            bom07s36-in-f3.1e1:http ESTABLISHED
tcp      0      0 ubuntu:41984            bom07s20-in-f3.1e:https TIME_WAIT
tcp      0      0 ubuntu:40104            del12s05-in-f14.1:https ESTABLISHED
tcp      0      0 ubuntu:49646            bom12s06-in-f22.1:https TIME_WAIT
tcp      0      0 ubuntu:48628            bom07s35-in-f2.1e:https TIME_WAIT
tcp      0      0 ubuntu:58976            bom07s36-in-f3.1e1:http ESTABLISHED
tcp      0      0 ubuntu:57096            del12s01-in-f14.1:https TIME_WAIT
tcp      0      0 ubuntu:41698            bom12s17-in-f10.1:https TIME_WAIT
tcp      0      0 ubuntu:41048            bom12s19-in-f10.1:https TIME_WAIT
tcp      0      0 ubuntu:60604            bom07s28-in-f3.1e:https TIME_WAIT
tcp      0      0 ubuntu:42210            bom12s06-in-f1.1e:https TIME_WAIT
tcp      0      0 ubuntu:37920            123.208.120.34:https ESTABLISHED
tcp      0      0 ubuntu:34970            del12s11-in-f6.1e:https TIME_WAIT
tcp      0      0 ubuntu:44752            bom07s36-in-f3.1e:https ESTABLISHED
tcp      0      0 ubuntu:60536            bom12s14-in-f13.1:https TIME_WAIT
tcp      0      0 ubuntu:59006            bom07s36-in-f3.1e1:http ESTABLISHED
tcp      0      0 ubuntu:58998            bom07s36-in-f3.1e1:http ESTABLISHED
```

This will show all the TCP connections but will not show the corresponding PIDs. In order to get that, we add the option of `--program`.

Command: `netstat --tcp --program`

Alternatively: `netstat -tp`

```
visheshrangwani@ubuntu:~$ netstat --tcp --program
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 ubuntu:36352            ec2-54-149-83-187:https ESTABLISHED 2121/firefox
tcp        0      0 ubuntu:42384            del11s14-in-f4.1e:https ESTABLISHED 2121/firefox
tcp        0      0 ubuntu:58988            bom07s36-in-f3.1e1:http ESTABLISHED 2121/firefox
tcp        0      0 ubuntu:47100            bom07s28-in-f14.1:https TIME_WAIT   -
tcp        0      0 ubuntu:40104            del12s05-in-f14.1:https ESTABLISHED 2121/firefox
tcp        0      0 ubuntu:58976            bom07s36-in-f3.1e1:http ESTABLISHED 2121/firefox
tcp        0      0 ubuntu:41698            bom12s17-in-f10.1:https TIME_WAIT   -
tcp        0      0 ubuntu:37920            123.208.120.34.bc:https ESTABLISHED 2121/firefox
tcp        0      0 ubuntu:34970            del12s11-in-f6.1e:https TIME_WAIT   -
tcp        0      0 ubuntu:44752            bom07s36-in-f3.1e:https ESTABLISHED 2121/firefox
tcp        0      0 ubuntu:47106            bom07s28-in-f14.1:https ESTABLISHED 2121/firefox
tcp        0      0 ubuntu:59006            bom07s36-in-f3.1e1:http ESTABLISHED 2121/firefox
tcp        0      0 ubuntu:58998            bom07s36-in-f3.1e1:http ESTABLISHED 2121/firefox

visheshrangwani@ubuntu:~$ netstat -tp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 ubuntu:36352            ec2-54-149-83-187:https ESTABLISHED 2121/firefox
tcp        0      0 ubuntu:42384            del11s14-in-f4.1e:https ESTABLISHED 2121/firefox
tcp        0      0 ubuntu:58988            bom07s36-in-f3.1e1:http ESTABLISHED 2121/firefox
tcp        0      0 ubuntu:47100            bom07s28-in-f14.1:https TIME_WAIT   -
tcp        0      0 ubuntu:40104            del12s05-in-f14.1:https ESTABLISHED 2121/firefox
tcp        0      0 ubuntu:58976            bom07s36-in-f3.1e1:http ESTABLISHED 2121/firefox
tcp        0      0 ubuntu:37920            123.208.120.34.bc:https ESTABLISHED 2121/firefox
tcp        0      0 ubuntu:44752            bom07s36-in-f3.1e:https ESTABLISHED 2121/firefox
tcp        0      0 ubuntu:47106            bom07s28-in-f14.1:https ESTABLISHED 2121/firefox
tcp        0      0 ubuntu:59006            bom07s36-in-f3.1e1:http ESTABLISHED 2121/firefox
tcp        0      0 ubuntu:58998            bom07s36-in-f3.1e1:http ESTABLISHED 2121/firefox

visheshrangwani@ubuntu:~$
```

To get a list of all TCP connections which are in LISTENING state, we can add the option `--listening` as well.

Command: `netstat --tcp --program --listening`

Alternatively: `netstat -tpl`

```

visheshrangwani@ubuntu:~$ netstat --tcp --program --listening
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)

```

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	localhost:ipp	0.0.0.0:*	LISTEN	-
tcp	0	0	localhost:domain	0.0.0.0:*	LISTEN	-
tcp6	0	0	ip6-localhost:ipp	:::*	LISTEN	-

```

visheshrangwani@ubuntu:~$ netstat -tplt
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)

```

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	localhost:ipp	0.0.0.0:*	LISTEN	-
tcp	0	0	localhost:domain	0.0.0.0:*	LISTEN	-
tcp6	0	0	ip6-localhost:ipp	:::*	LISTEN	-

```

visheshrangwani@ubuntu:~$ █

```

To get all the TCP connections with PIDs,  
 Command: netstat --tcp --program --all  
 Alternatively: netstat -atp



```
visheshrangwani@ubuntu:~$ netstat --tcp --program --all
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN      -
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN      -
tcp        0      0 ubuntu:36352            ec2-54-149-83-187:https ESTABLISHED 2121/firefox
tcp        0      0 ubuntu:42384            del11s14-in-f4.1e:https ESTABLISHED 2121/firefox
tcp        0      0 ubuntu:58988            bom07s36-in-f3.1e1:http TIME_WAIT   -
tcp        0      0 ubuntu:40104            del12s05-in-f14.1:https ESTABLISHED 2121/firefox
tcp        0      0 ubuntu:34398            server-108-158-24:https ESTABLISHED 2121/firefox
tcp        0      0 ubuntu:33488            191.144.160.34.bc:https ESTABLISHED 2121/firefox
tcp        0      0 ubuntu:44750            del12s01-in-f14.1:https ESTABLISHED 2121/firefox
tcp        0      0 ubuntu:58976            bom07s36-in-f3.1e1:http TIME_WAIT   -
tcp        0      0 ubuntu:34272            36.75.98.34.bc.go:https ESTABLISHED 2121/firefox
tcp        0      0 ubuntu:36840            bom07s35-in-f2.1e:https ESTABLISHED 2121/firefox
tcp        0      0 ubuntu:37920            123.208.120.34.bc:https ESTABLISHED 2121/firefox
tcp        0      0 ubuntu:44752            bom07s36-in-f3.1e:https ESTABLISHED 2121/firefox
tcp        0      0 ubuntu:47106            bom07s28-in-f14.1:https ESTABLISHED 2121/firefox
tcp        0      0 ubuntu:59006            bom07s36-in-f3.1e1:http TIME_WAIT   -
tcp        0      0 ubuntu:58998            bom07s36-in-f3.1e1:http TIME_WAIT   -
tcp6       0      0 ip6-localhost:ipp      [::]:*                 LISTEN      -
visheshrangwani@ubuntu:~$ netstat -atp
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN      -
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN      -
tcp        0      0 ubuntu:36352            ec2-54-149-83-187:https ESTABLISHED 2121/firefox
tcp        0      0 ubuntu:42384            del11s14-in-f4.1e:https ESTABLISHED 2121/firefox
tcp        0      0 ubuntu:58988            bom07s36-in-f3.1e1:http TIME_WAIT   -
tcp        0      0 ubuntu:40104            del12s05-in-f14.1:https ESTABLISHED 2121/firefox
tcp        0      0 ubuntu:34398            server-108-158-24:https ESTABLISHED 2121/firefox
tcp        0      0 ubuntu:33488            191.144.160.34.bc:https ESTABLISHED 2121/firefox
tcp        0      0 ubuntu:44750            del12s01-in-f14.1:https ESTABLISHED 2121/firefox
tcp        0      0 ubuntu:58976            bom07s36-in-f3.1e1:http TIME_WAIT   -
tcp        0      0 ubuntu:34272            36.75.98.34.bc.go:https ESTABLISHED 2121/firefox
tcp        0      0 ubuntu:36840            bom07s35-in-f2.1e:https ESTABLISHED 2121/firefox
tcp        0      0 ubuntu:37920            123.208.120.34.bc:https ESTABLISHED 2121/firefox
tcp        0      0 ubuntu:44752            bom07s36-in-f3.1e:https ESTABLISHED 2121/firefox
tcp        0      0 ubuntu:47106            bom07s28-in-f14.1:https ESTABLISHED 2121/firefox
tcp        0      0 ubuntu:59006            bom07s36-in-f3.1e1:http TIME_WAIT   -
tcp        0      0 ubuntu:58998            bom07s36-in-f3.1e1:http TIME_WAIT   -
tcp6       0      0 ip6-localhost:ipp      [::]:*                 LISTEN      -
visheshrangwani@ubuntu:~$
```

b)

We can get all tcp connections by using the command: `netstat -at http://info.cern.ch`

Screenshot:

```
visheshrangwani@ubuntu:~$ netstat -at http://info.cern.ch
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp        0      0 ubuntu:57438            ec2-54-69-181-45.:https ESTABLISHED
tcp6       0      0 ip6-localhost:ipp      [::]:*                 LISTEN
visheshrangwani@ubuntu:~$
```

The localhost:domain connection is in LISTENING state.  
The localhost:ipp connection is in LISTENING state.  
The ubuntu:57438 connection is in ESTABLISHED state with Foreign address:  
ec2-54-69-181-45.:https.  
The ip6-localhost:ipp connection is in LISTENING state.

## **References:**

Lecture slides

Tutorial slides

<https://www.lifewire.com/netstat-command-2618098>

<https://www.geeksforgeeks.org/difference-between-ping-and-traceroute/>

<https://serverfault.com/questions/109926/why-does-traceroute-take-much-longer-than-ping>

<https://cs.stanford.edu/people/eroberts/courses/soco/projects/1999-00/internet/tcp.html>

<https://www.meridianoutpost.com/resources/articles/command-line/nslookup.php#AuthoritativeResponse>

<https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-software-releases-121-mainline/12778-ping-traceroute.html#delay>

<https://www.ionos.com/digitalguide/server/configuration/understanding-and-configuring-dns-ttl/>