

# Computer Network Assignment 1

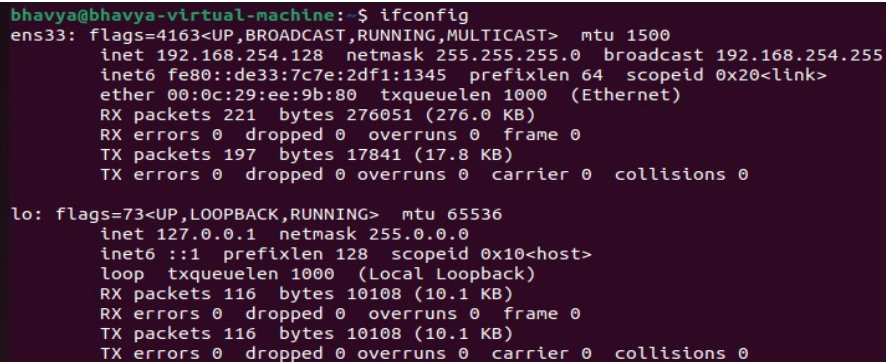
Bhavya Narnoli

## 1

[1 + 1] a) Learn to use the `ifconfig` command, and figure out the IP address of your network interface. Put a screenshot.

b) Go to the webpage <https://www.whatismyip.com> and find out what IP is shown for your machine. Are they identical or different? Why?

**1) Private IP Address:** The address next to `inet( 192.168.254.128)` which is below, is a private IP address assigned by the router within the local network. Each device within the same network is assigned a unique private IP address. This IP address is used only to communicate internally within the network.



```
bhavya@bhavya-virtual-machine:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.254.128  netmask 255.255.255.0  broadcast 192.168.254.255
    inet6 fe80::de33:7c7e:2df1:1345  prefixlen 64  scopeid 0x20<link>
    ether 00:0c:29:ee:9b:80  txqueuelen 1000  (Ethernet)
    RX packets 221  bytes 276051 (276.0 KB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 197  bytes 17841 (17.8 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 116  bytes 10108 (10.1 KB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 116  bytes 10108 (10.1 KB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figure 1: Private IP Address (beside inet)

**2) Public IP Address/Host Name:** This is the public IP address on the network edge determined by the ISP, and hence it's different from the private IP address ( not same as above) .

```
inet 192.168.254.128 netmask 255.255.255.0 broadcast 192.168.254.255
```

Figure 2: Another Private IP Address

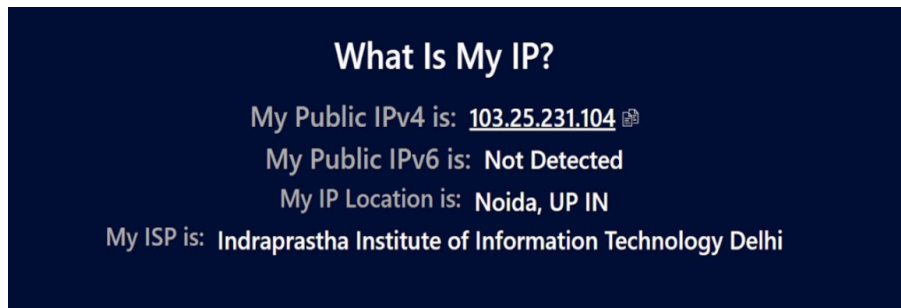


Figure 3: Public IP Address

Q2)

nslookup ([2+1] + [1+1]) a) Get an authoritative result for “google.in” using nslookup. Put a screenshot. Explain how you did it.

.

2)a) DNS Lookup for ”google.in”: To get authoritative DNS information for ”google.in” using nslookup, use the command `nslookup -type=ns google.in`.

```
bhavya@bhavya-virtual-machine:~$ nslookup -type=ns google.in
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
google.in    nameserver = ns2.google.com.
google.in    nameserver = ns1.google.com.
google.in    nameserver = ns4.google.com.
google.in    nameserver = ns3.google.com.

Authoritative answers can be found from:
ns2.google.com internet address = 216.239.34.10
ns2.google.com has AAAA address 2001:4860:4802:34::a
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
```

The NS (Name Server) record is used to delegate the authority for a particular subdomain to a set of DNS servers. Authoritative domains are responsible for maintaining and providing information about that domain to other DNS servers and clients.

## Time to Live

2)b) Find out time to live for any website on the local DNS. Put a screenshot. Explain in words (with unit) that after how much time this entry would expire from the local DNS server

```
PS C:\Users\Chief Engineer (C)> nslookup -debug google.in
-----
Got answer:
HEADER:
    opcode = QUERY, id = 1, rcode = NOERROR
    header flags:  response, auth. answer, want recursion, recursion avail.
    questions = 1,  answers = 1,  authority records = 0,  additional = 0

    QUESTIONS:
        7.1.168.192.in-addr.arpa, type = PTR, class = IN
    ANSWERS:
    -> 7.1.168.192.in-addr.arpa
        name = adc.iiitd.edu.in
        ttl = 1200 (20 mins)

-----

Got answer:
HEADER:
    opcode = QUERY, id = 6, rcode = NOERROR
    header flags:  response, want recursion, recursion avail.
    questions = 1,  answers = 1,  authority records = 0,  additional = 0

    QUESTIONS:
        google.in, type = A, class = IN
    ANSWERS:
    -> google.in
        internet address = 142.250.193.228
        ttl = 300 (5 mins)

-----

Non-authoritative answer:
-----
Got answer:
HEADER:
    opcode = QUERY, id = 7, rcode = NOERROR
    header flags:  response, want recursion, recursion avail.
    questions = 1,  answers = 1,  authority records = 0,  additional = 0

    QUESTIONS:
        google.in, type = AAAA, class = IN
    ANSWERS:
    -> google.in
        AAAA IPv6 address = 2404:6800:4002:81d::2004
        ttl = 300 (5 mins)

-----
```

**Time to Live (TTL):** Time to live (TTL) refers to the amount of time or "hops" that a packet is set to exist inside a network before being discarded by a router.

After the specified TTL duration, the records will expire from the cache, and DNS servers will need to query the authoritative DNS servers again to get updated information.

For "google.in," the "A" and "AAAA" records have TTLs of 300 seconds (5 minutes), meaning they will expire from the local DNS cache after 5 minutes.

3)a) Run the command, `tracert google.in`. How many intermediate hosts do you see? What are the IP addresses? Compute the average latency to each intermediate host. Put a screenshot. [1+2+1] Note that some of the intermediate hosts might not be visible; their IP addresses will come as “\*\*\*”, ignore those hosts for this assignment.

```
(base) PS C:\Users\Chief Engineer (C)> tracert google.in

Tracing route to google.in [142.250.193.4]
over a maximum of 30 hops:

  0  2 ms   1 ms   1 ms  192.168.100.1
  1  3 ms   3 ms  12 ms  120.57.80.1
  2  6 ms   4 ms  10 ms  triband-del-59.180.247.174.bol.net.in [59.180.247.174]
  3 13 ms   7 ms   4 ms  10.79.10.206
  4  5 ms   3 ms   6 ms  117.232.129.18
  5 24 ms  13 ms   7 ms  117.216.207.103
  6  4 ms   6 ms   4 ms  142.250.172.220
  7  4 ms   7 ms   4 ms  72.14.234.223
  8  5 ms   3 ms   4 ms  142.251.54.87
  9  3 ms   6 ms   3 ms  del11s14-in-f4.1e100.net [142.250.193.4]

Trace complete.
```

**Run `tracert google.in`**

There are 10 intermediate host of whose IP is visible

IP Address	Addition of latency/6	Intermediate host latence
192.168.100.1	4/6	0.66ms
120.57.80.1	18/6	3ms
59.180.247.174	20/6	3.33ms
10.79.10.206	24/6	4ms
117.232.129.18	14/6	2.33 ms
117.216.207.103	44/6	7.33 ms
142.250.172.220	14/6	2.33 ms
72.14.234.223	15/6	2.5ms
142.251.54.87	12/6	2ms
142.250.193.4	12/6	2ms

b) Send 50 ping messages to `google.in`, Determine the average latency. Put a screenshot. [1]

```

bhavya@bhavya-virtual-machine:~$ ping -c 50 google.in
PING google.in (142.250.193.4) 56(84) bytes of data:
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=1 ttl=128 time=7.08 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=2 ttl=128 time=5.56 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=3 ttl=128 time=4.96 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=4 ttl=128 time=10.0 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=5 ttl=128 time=5.24 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=6 ttl=128 time=18.5 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=7 ttl=128 time=6.98 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=8 ttl=128 time=5.10 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=9 ttl=128 time=6.37 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=10 ttl=128 time=5.04 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=11 ttl=128 time=4.99 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=12 ttl=128 time=6.04 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=13 ttl=128 time=5.10 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=14 ttl=128 time=6.31 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=15 ttl=128 time=7.08 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=16 ttl=128 time=5.65 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=17 ttl=128 time=5.67 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=18 ttl=128 time=12.0 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=19 ttl=128 time=4.65 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=20 ttl=128 time=5.61 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=21 ttl=128 time=5.93 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=22 ttl=128 time=5.80 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=23 ttl=128 time=5.33 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=24 ttl=128 time=5.60 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=25 ttl=128 time=5.35 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=26 ttl=128 time=6.74 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=27 ttl=128 time=6.29 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=28 ttl=128 time=11.2 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=29 ttl=128 time=6.13 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=30 ttl=128 time=6.17 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=31 ttl=128 time=5.22 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=32 ttl=128 time=7.59 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=33 ttl=128 time=5.36 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=34 ttl=128 time=6.13 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=35 ttl=128 time=6.64 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=36 ttl=128 time=5.29 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=37 ttl=128 time=6.79 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=38 ttl=128 time=6.32 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=39 ttl=128 time=5.62 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=40 ttl=128 time=4.65 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=41 ttl=128 time=4.41 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=42 ttl=128 time=4.76 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=44 ttl=128 time=7.38 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=45 ttl=128 time=7.06 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=46 ttl=128 time=36.0 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=47 ttl=128 time=4.74 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=48 ttl=128 time=5.37 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=49 ttl=128 time=5.33 ms
64 bytes from del11s14-in-f4.1e100.net (142.250.193.4): icmp_seq=50 ttl=128 time=5.74 ms

--- google.in ping statistics ---
50 packets transmitted, 49 received, 2% packet loss, time 49106ms
rtt min/avg/max/ndev = 4.407/6.996/35.960/4.766 ms
bhavya@bhavya-virtual-machine:~$

```

3)b ) Used command `ping -c 50 google.in`. As shown in screenshot average latency time is half of average rtt =  $6.996/2$  ms = 3.498 ms

**3)c) Add up the ping latency of all the intermediate hosts obtained in (a) and compare with (b). Are they matching, explain?[1+1]**

**Comparison**

- From a) The total latency time in a) from intermediate host is 29.465ms and the average latency time from b) is 3.498 ms.  
They don't match and aren't even comparable because of the following reason  
The "average ping latency time" refers to the average RTT(round trip time)/2 across multiple ping requests sent to the destination where there is no waiting /latency time anywhere in between.

The "ping" command is used to measure the round-trip time (RTT) between your computer and a destination server by sending an ICMP echo request and receiving echo reply packets which is the average value of all the requests sent to the destination and doesn't have to wait anywhere.

The "total intermediate host latency time" refers to the sum of latencies across all the intermediate hops in a single specified route with the mentioned intermediate hosts till the destination which results in a higher value because it has to wait at each intermediate host.

**d) Take the maximum of ping latency amongst the intermediate hosts (in (a)) and compare with (b). Are they matching, explain? [1+1]**

**Comparison**

- From a) maximum of intermediate host latency time is  $\max(0.66\text{ms}, 3\text{ms}, 3.33\text{ms}, 4\text{ms}, 2.33\text{ms}, 7.33\text{ms}, 2.33\text{ms}, 2.5\text{ms}, 2\text{ms}, 2\text{ms}) = 7.33\text{ms}$ , and the average latency time from b) is 3.498 ms.  
They are not matching but this is the longest delay observed among all the intermediate hosts (only one host) and hence is similar to ping and is therefore still comparable.  
The "ping" command measures the time to send ICMP echo requests b/w my computer and a destination server.



3)e) You may see multiple entries for a single hop while using traceroute command. What do these entries mean? [1]

- It sends three ICMP echo request packets to each hop along the route. This is done to get a more accurate idea of the latency between the source and each intermediate hop.

3)f) Send 50 ping messages to stanford.edu, Determine the average latency. Put a screenshot. [1]

Used command `ping -c 50 stanford.edu`

```
bhavya@bhavya-virtual-machine:~$ 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=128 time=264 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=2 ttl=128 time=266 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=3 ttl=128 time=265 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=4 ttl=128 time=266 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=5 ttl=128 time=264 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=6 ttl=128 time=266 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=7 ttl=128 time=264 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=8 ttl=128 time=264 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=9 ttl=128 time=264 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=10 ttl=128 time=265 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=11 ttl=128 time=264 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=12 ttl=128 time=265 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=13 ttl=128 time=265 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=14 ttl=128 time=266 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=15 ttl=128 time=263 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=16 ttl=128 time=265 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=17 ttl=128 time=272 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=18 ttl=128 time=265 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=19 ttl=128 time=264 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=20 ttl=128 time=267 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=21 ttl=128 time=265 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=22 ttl=128 time=267 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=23 ttl=128 time=265 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=24 ttl=128 time=263 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=25 ttl=128 time=265 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=26 ttl=128 time=264 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=27 ttl=128 time=267 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=28 ttl=128 time=267 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=29 ttl=128 time=264 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=30 ttl=128 time=265 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=31 ttl=128 time=264 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=32 ttl=128 time=746 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=33 ttl=128 time=610 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=34 ttl=128 time=268 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=35 ttl=128 time=264 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=36 ttl=128 time=265 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=37 ttl=128 time=264 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=38 ttl=128 time=264 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=39 ttl=128 time=265 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=40 ttl=128 time=264 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=41 ttl=128 time=265 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=42 ttl=128 time=264 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=43 ttl=128 time=265 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=44 ttl=128 time=265 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=45 ttl=128 time=269 ms
```

```

64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=46 ttl=128 time=265 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=47 ttl=128 time=264 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=48 ttl=128 time=265 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=49 ttl=128 time=265 ms
64 bytes from web.stanford.edu (171.67.215.200): icmp_seq=50 ttl=128 time=265 ms

--- stanford.edu ping statistics ---
50 packets transmitted, 50 received, 0% packet loss, time 52460ms
rtt min/avg/max/mdev = 262.620/281.605/746.227/82.069 ms

```

- Average latency is  $281.605\text{ms} / 2 = 140.802\text{ms}$

3)g) Run the command, `tracert stanford.edu`. Compare the number of hops between `google.in` and `stanford.edu` (between the traceroute result of `google.in` and `stanford.edu`). [1].

Used command `tracert stanford.edu`

```

(base) PS C:\Users\Chief Engineer (C)> tracert stanford.edu

Tracing route to stanford.edu [171.67.215.200]
over a maximum of 30 hops:

  0  1 ms  5 ms  1 ms  192.168.100.1
  1  12 ms 11 ms 18 ms 120.57.80.1
  2  4 ms  3 ms  3 ms triband-del-59.180.247.174.bol.net.in [59.180.247.174]
  3  10 ms 4 ms  3 ms 10.79.10.206
  4  14 ms 2 ms  2 ms 117.232.129.6
  5  10 ms 3 ms  7 ms 117.216.207.103
  6  10 ms 9 ms  6 ms nsg-corporate-105.89.186.122.airtel.in [122.186.89.105]
  7  255 ms 255 ms 254 ms 116.119.57.43
  8  250 ms * * port-channel111.core3.lax2.he.net [64.62.148.113]
  9  245 ms 256 ms 245 ms port-channel8.core2.lax1.he.net [184.104.197.109]
 10 * * * Request timed out.
 11 258 ms * 256 ms eqix-sv8.hurricaneelectric.com [198.32.176.20]
 12 264 ms 263 ms 265 ms stanford-university.100gigabitethernet5-1.core1.pao1.he.net [184.105.177.238]
 13 266 ms 265 ms 264 ms woa-west-rtr-vl2.SUNet [171.64.255.132]
 14 * * * Request timed out.
 15 264 ms 263 ms 264 ms web.stanford.edu [171.67.215.200]

Trace complete.

```

- Total 16 hops



```
(base) PS C:\Users\Chief Engineer (C)> tracert google.in

Tracing route to google.in [142.250.193.4]
over a maximum of 30 hops:

  0  1 ms  1 ms  1 ms  192.168.100.1
  1  3 ms  3 ms  12 ms  120.57.80.1
  2  6 ms  4 ms  10 ms  triband-del-59.180.247.174.bol.net.in [59.180.247.174]
  3  13 ms  7 ms  4 ms  10.79.10.206
  4  5 ms  3 ms  6 ms  117.232.129.18
  5  24 ms  13 ms  7 ms  117.216.207.103
  6  4 ms  6 ms  4 ms  142.250.172.220
  7  4 ms  7 ms  4 ms  72.14.234.223
  8  5 ms  3 ms  4 ms  142.251.54.87
  9  3 ms  6 ms  3 ms  del11s14-in-f4.1e100.net [142.250.193.4]

Trace complete.
```

Used command `tracert google.in` The ISP serving `stanford.edu` is physically located farther away from my IP network as compared to the ISP of `google.in` and that is why it takes a longer route with more intermediate routers or devices.

3)h) Can you explain the reason for the latency difference between `google.in` and `stanford.edu` (see (b) & (f))? [1]

- Average latency of `stanford.edu` is 140.802 ms and `google.in` is 3.448 ms because of more distance of the server of `stanford.edu` as compared to `google.in` and hence it has to pass through more intermediate routers when searching from `stanford.edu` as compared to `google.in`.

Q4. [2+1] Make your ping command fail for `127.0.0.1` (with 100% packet loss). Explain how you do it. Put a screenshot that it failed.

Used command

```
sudo iptables -A INPUT -p icmp --icmp-type echo-request -s 127.0.0.1 -j DROP
and then enter your password
and put command
ping -c 10 127.0.0.1
```

```

bhavya@bhavya-virtual-machine:~$ sudo iptables -A INPUT -p icmp --icmp-type echo-request -s 127.0.0.1 -j DROP
[sudo] password for bhavya:
bhavya@bhavya-virtual-machine:~$ 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 9193ms

```

**It adds a rule to the firewall configuration that drops incoming ICMP echo for effectively preventing successful pinging of 127.0.0.1**

- -A INPUT: to append a rule to the "INPUT" chain which is responsible for incoming packets targeting the local system.
- -p icmp: This specifies the protocol which here is ICMP (Internet Control Message Protocol), which is used for various network diagnostic purposes.
- --icmp-type echo-request: This specifies the type of ICMP packet. An "echo-request" packet is the type used for pinging sent to request a reply (ping response) from the destination.
- -s 127.0.0.1: This option specifies the source IP address which's 127.0.0.1, is the loopback address (localhost).
- -j DROP: Action to take when the conditions of the rule are met, it's "DROP," which means that any matching packets will be dropped (discarded) and not allowed to pass through the firewall.

Q.5 [0.5\*4 + 1] Use telnet to perform an HTTP get request on a webpage hosted at 192.168.24.12

Steps :

1. On your VM or main machine, run telnet 192.168.24.12 9900.
2. Once the connection is established, perform a GET request on /secret (Syntax : GET <access path > HTTP/1.1).
3. Now set the Host by typing Host: <host part of URL> then press enter. This tells the server the host part of the URL
4. Now close the connection
5. If the request is successful, you will receive the response on the screen. Note the value of the X-secret header and take a screenshot of the entire response.}

Used command telnet 192.168.24.12 9900 and then use  
 GET /secret HTTP/1.1  
 HOST: 192.168.24.12  
 Connection: close  
 and then double enter will give required output

```

bhavya@bhavya-virtual-machine:~$ telnet 192.168.24.12 9900
Trying 192.168.24.12...
Connected to 192.168.24.12.
Escape character is '^]'.
GET /secret HTTP/1.1
HOST: 192.168.24.12
Connection: close

HTTP/1.1 200 OK
Content-Type: text/plain
ip: 192.168.43.204
X-secret: U2FsdGVkX1/0DBRPIuFzeWCxbwIOKjC/MtyAMse+S1x6h0RdvxH17/uy13LM1b0+
Date: Tue, 22 Aug 2023 18:21:04 GMT
Connection: close
Content-Length: 8

Success
Connection closed by foreign host.

```

X-secret: U2FsdGVkX1/0DBRPIuFzeWCxbwIOKjC/MtyAMse+S1x6h0RdvxH17/uy13LM1b0+

Q6. [ 0.5\*4 + 2 + 0.5\*2 ] Use telnet to send an email to one of the other students using an SMTP server.

Steps:

1. On your VM or main machine, run telnet 192.168.24.12 smtp
2. If everything goes well you will see 220 Welcome to CSE232 Mail Server.
3. Now identify your system by sending helo cse232.com
4. If everything goes well, you will see 250 xeon01-rs-iiitd.iiitd.edu.in on the screen.
5. Now write an email by specifying the sender, recipient, subject and the body and send it to one of your friends from Section A or Section B.
  - a. Note: Both senders and receivers are identified by their roll numbers. So if you are 20018 and the recipient is 20019, then the sender address will be 20018@cse231.com and the recipient address will be 20019@cse231.com.
6. Note down the id of the message, take a screenshot and close the connection by typing quit <enter>
7. In order to confirm that your friend has received the mail, ask him to open his mailbox at 192.168.24.12/<encrypted\_key> where this key is unique to every student and is sent to them at their iiitd email.(DO NOT SHARE YOUR KEY WITH OTHERS).

```
bhavya@bhavya-virtual-machine:~$ telnet 192.168.24.12 smtp
Trying 192.168.24.12...
Connected to 192.168.24.12.
Escape character is '^]'.
220 Welcome to CSE232 Mail Server
helo cse232.com
250 xeon01-rs-iiitd.iiitd.edu.in
mail from: 21316@cse232.com
250 2.1.0 Ok
rcpt to: 21270@cse232.com
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
Subject: parisha read my message
Hello, Im bhavya and you are parisha. How are you?
.
250 2.0.0 Ok: queued as 2040F6F643AB
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

```
From 21316@cse232.com Tue Aug 22 11:45:47 2023
Return-Path: <21316@cse232.com>
X-Original-To: 21270@cse232.com
Delivered-To: 21270@cse232.com
Received: from cse232.com (unknown [192.168.43.204])
    by xeon01-rs-iiitd.iiitd.edu.in (Postfix) with SMTP id 2040F6F643AB
    for <21270@cse232.com>; Tue, 22 Aug 2023 11:44:24 +0530 (IST)
Subject: parisha read my message

Hello, Im bhavya and you are parisha. How are you?
```

Confirmation of the mail sent

Id of email sent : 2040F6F643AB. She opened her browser using 192.168.24.12/<her encrypted

## References

- private IP address vs public ip address
- Time to Live (TTL) in Networking
- Using nslookup for Authoritative Responses
- Average Latency
- Ping vs traceroute
- Block IP Address
- iptables manpage