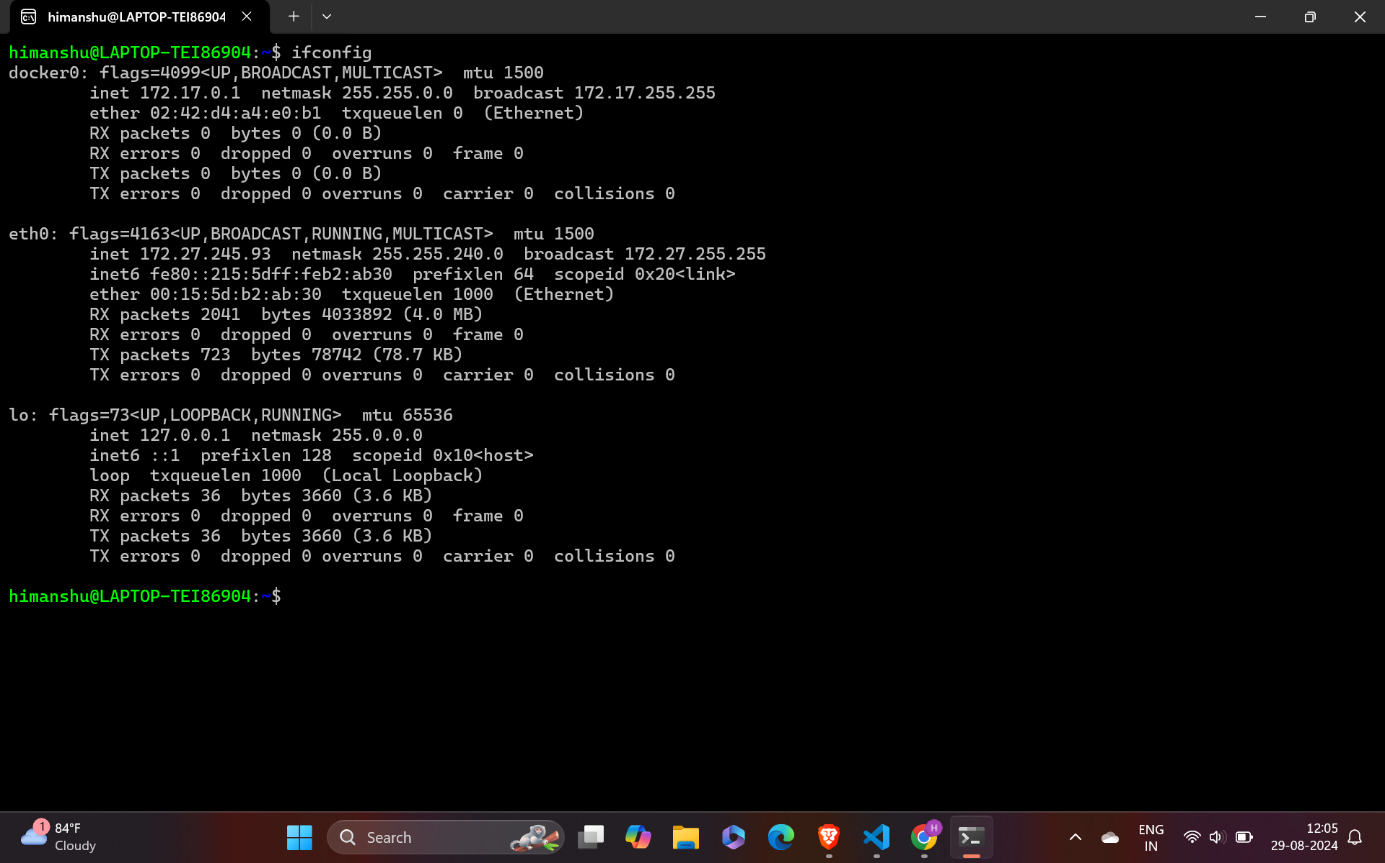
CN Assignment 1

Himanshu Kumar 2022215

Question 1

1. ifconfig image is given below.



Here ip address is 172.27.245.93

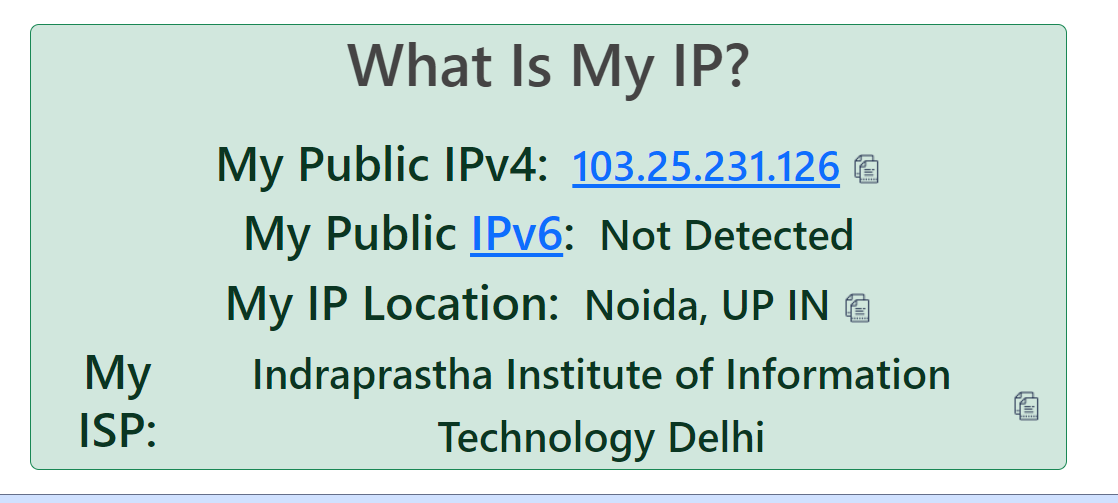
1. It shows ip address is 103.25.231.126 which is different shown from command ifconfig(it show ip address is 172.27.245.93). it means they both are different.

Reason :

Local IP Address ( 172.27.245.93 from ifconfig): This is my private IP address within my local network. This IP is assigned to my device by local router via DHCP and is only visible within my local network.

Public IP Address ( 103.25.231.126 from whatismyip.com): This is my public IP address, which is assigned to your network by my Internet Service Provider (ISP). It is the IP address that is visible to the outside world when you access websites and services on the internet.

The difference occurs because my router uses a technology called Network Address Translation (NAT) to translate the private IP address of my device to the public IP address assigned by ISP. This process allows multiple devices on local network to share a single public IP address.



Question 2

ifconfig -a : it gives this

Primary Network Interface: eth0 -- this is main ip address

Docker Virtual Interface: docker0

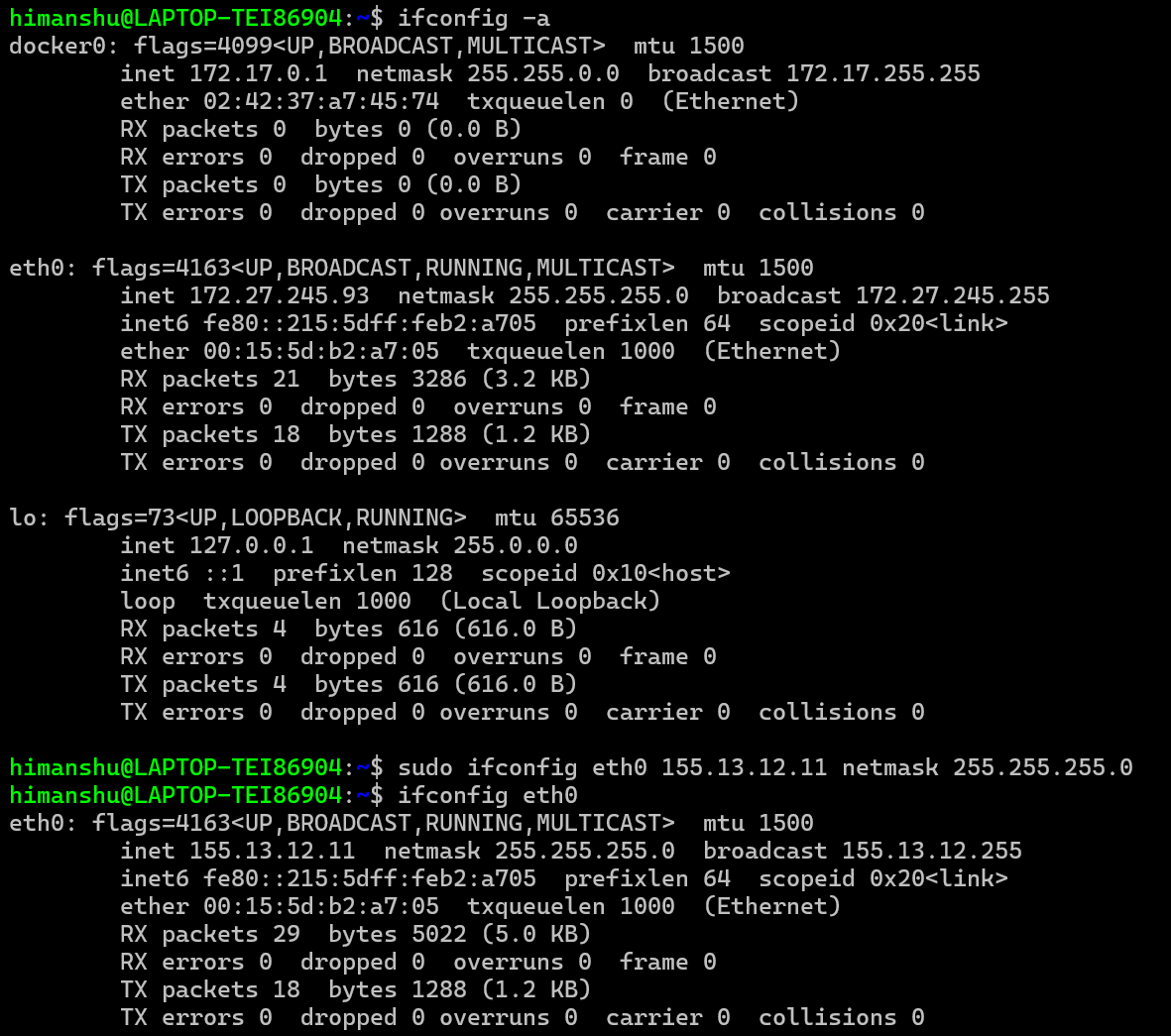
Loopback Interface: lo

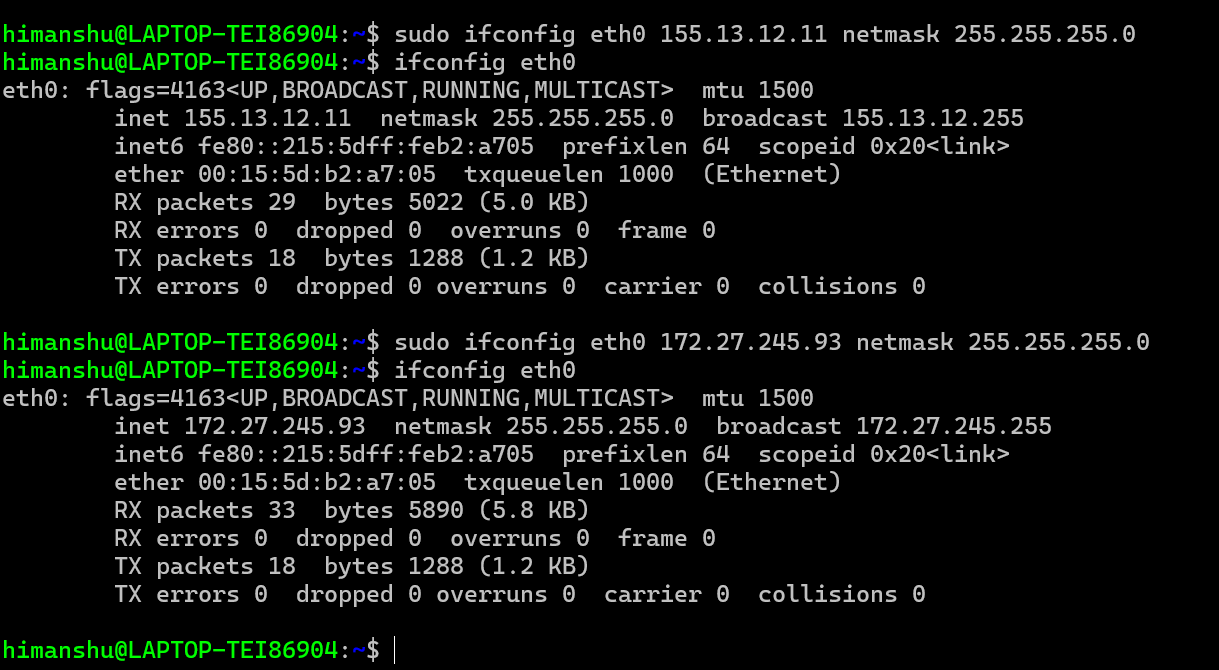
sudo ifconfig eth0 155.13.12.11 netmask 255.255.255.0 : it changes ip to 155.13.12.11

ifconfig eth0 : here check changes

sudo ifconfig eth0 172.27.245.93 netmask 255.255.255.0: again, change to original ip address

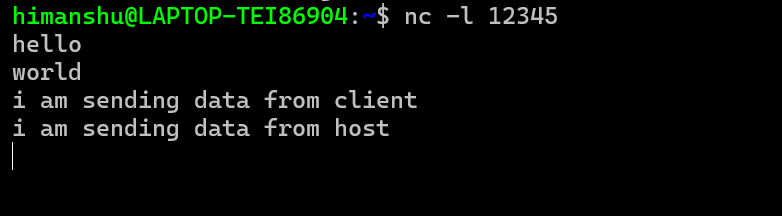
ifconfig eth0 : again, check the ip address

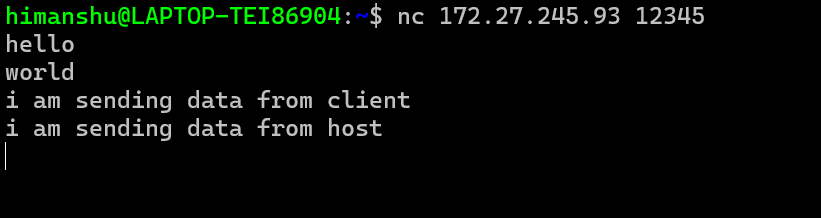




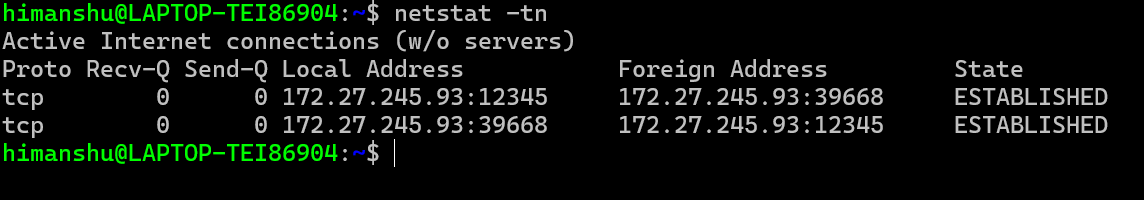
Question 3

1. We type nc -l 12345 in host server . then we find nc server\_ip 12345 in clint server . now we are able to send message from host to clint and vice-versa.





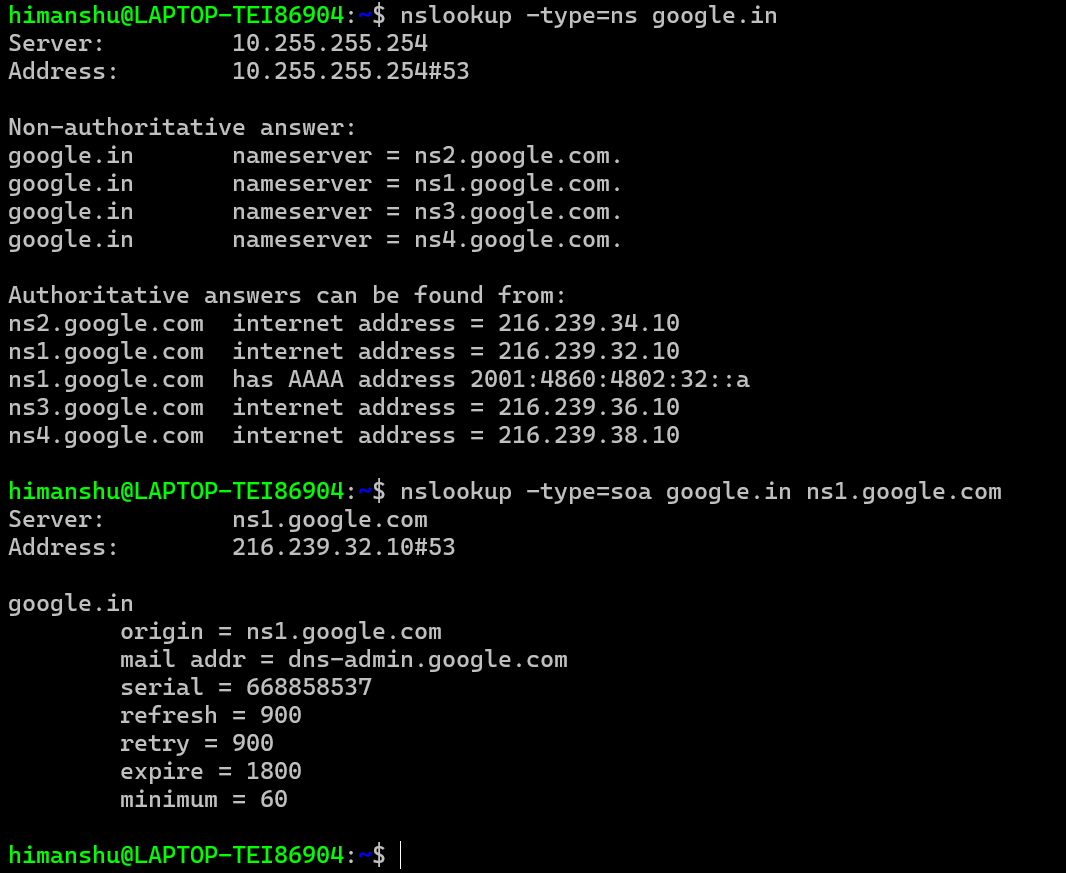
1. We can use this command netstat -tn . it will give all state of the TCP connection .





Question 4

a) The nslookup command with the -type=soa option queries the DNS to find the authoritative server for the google.in domain. The authoritative DNS server is responsible for the domain's DNS records, ensuring the response is accurate and up-to-date.

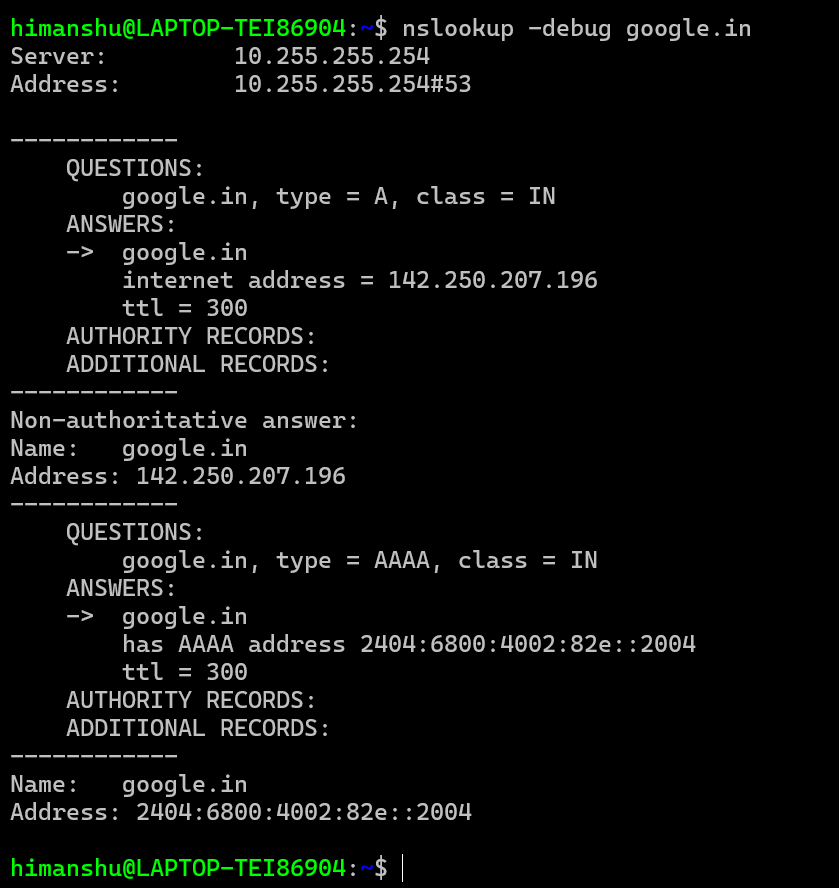


To get an authoritative result for google.in, we need to specify that we want an authoritative answer by querying the authoritative DNS servers directly.

The -type=soa option tells nslookup to query for the Start of Authority (SOA) record, which provides information about the authoritative DNS server for the domain.

The output will show the primary name server (the authoritative server) for the domain, among other details.

b ) The TTL value of 300 seconds indicates that the DNS entry for google.in will be stored in the local DNS cache for 300 seconds. After this time, the DNS server will remove the cached entry and will have to query the authoritative DNS server again for the IP address if requested.



For IPv4 (A record): google.in

Internet address = 142.250.207.196

TTL = 300 seconds

----------------------------------------------------------------

For IPv6 (AAAA record): google.in

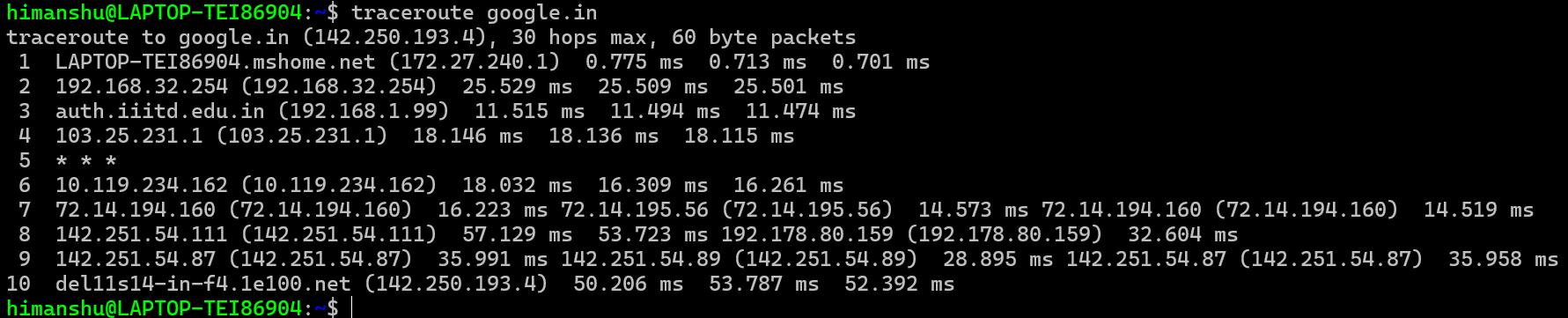
Has AAAA address = 2404:6800:4002:82e::2004

TTL = 300 seconds

-----------------------------------------------------------------

Question 5

1. There are 8 intermediate host(except the last host server).



s.no. I.p address average latency

1 172.27.240.1 (0.775 + 0.713 + 0.701) / 3 = 0.73 ms

2 192.168.32.254 (25.529 + 25.509 + 25.501) / 3 = 25.51 ms

3 192.168.1.99 (11.515 + 11.494 + 11.474) / 3 = 11.49 ms

4 103.25.231.1 (18.146 + 18.136 + 18.115) / 3 = 18.13 ms

5 10.119.234.162 (18.032 + 16.309 + 16.261) / 3 = 16.87 ms

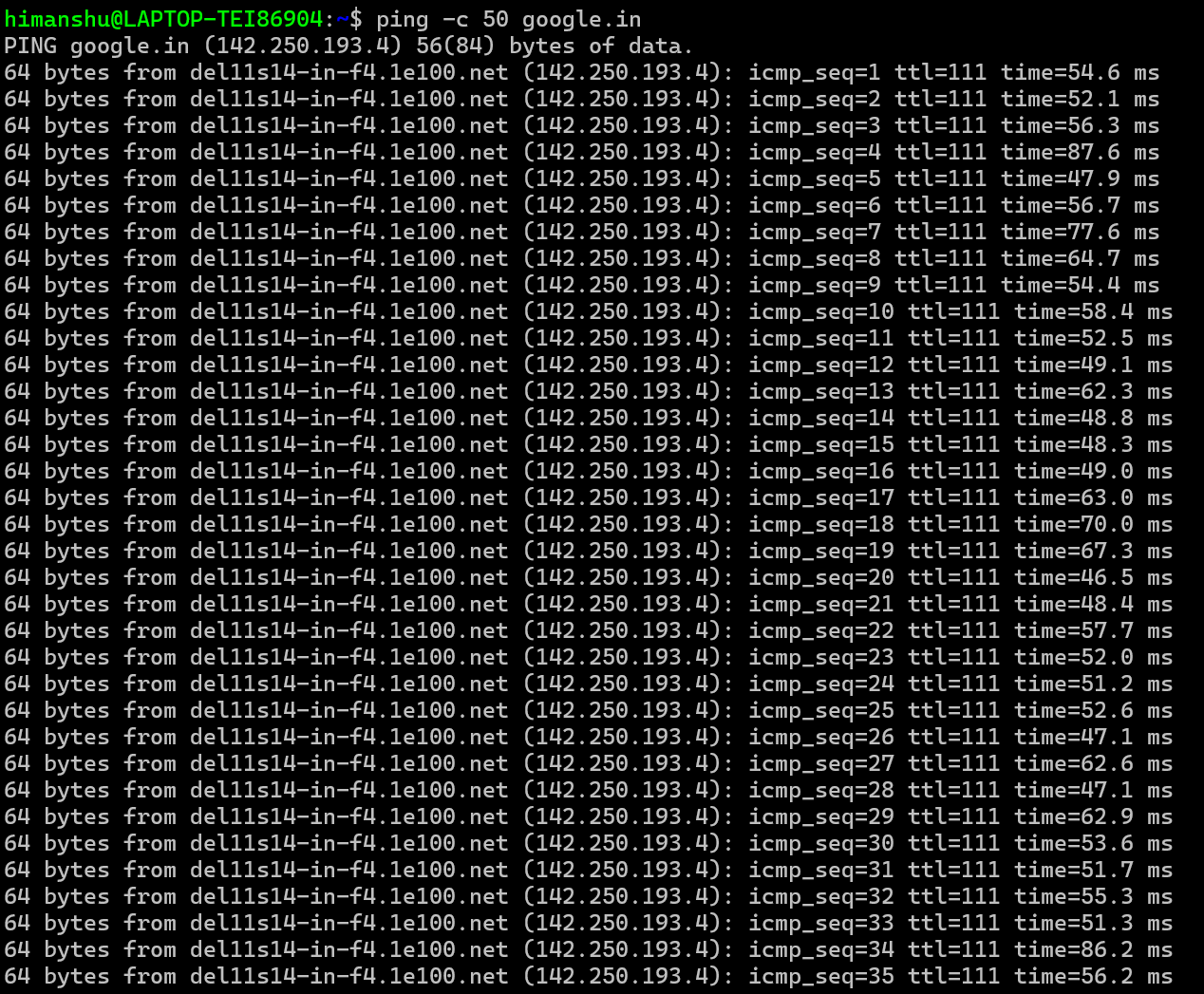
6 72.14.194.160 (16.223 + 14.573 + 14.519) / 3 = 15.11 ms

7 142.251.54.111 (57.129 + 53.723 + 32.604) / 3 = 47.15 ms

8 142.251.54.87 (35.991 + 28.895 + 35.958) / 3 = 33.61 ms

1. Here average latency is 56.786 ms. Image is given below.

we send 50 packet using command ping -c 50 google.in





1. Total Latency of a= 0.73 + 25.51 + 11.49 + 18.13 + 16.87 + 15.11 + 47.15 + 33.61 = 168.6 ms

Avg. latency of b = 56.786 ms

Total latency of a is much higher than average latency of b.

Reason:

Traceroute Latencies: The latencies measured in traceroute are the round-trip times for packets between my machine and each intermediate router. These include the delays at each hop along the route.

Ping Latencies: The average latency measured by ping is typically the round-trip time between my machine and the final destination (in this case, google.in), which can include the sum of delays across all intermediate hops but is usually averaged over a larger set of packets.

1. maximum ping latency of all the host in a is 57.129 ms .

Avg. latency of b = 56.786 ms.

It is almost equal.

Small Difference: The difference between the two values is only 0.343 ms. This small difference is within the range of normal network variability, such as slight fluctuations in network traffic, routing paths, or timing of the measurements.

Practical Consideration: In networking, such a minor difference is often considered negligible, as it doesn't significantly impact the overall network performance or user experience. Therefore, for practical purposes, these two values can be treated as equal.

e) When using the traceroute command, we may see multiple entries for a single hop. Here’s what these entries represent:

Multiple Entries for a Single Hop

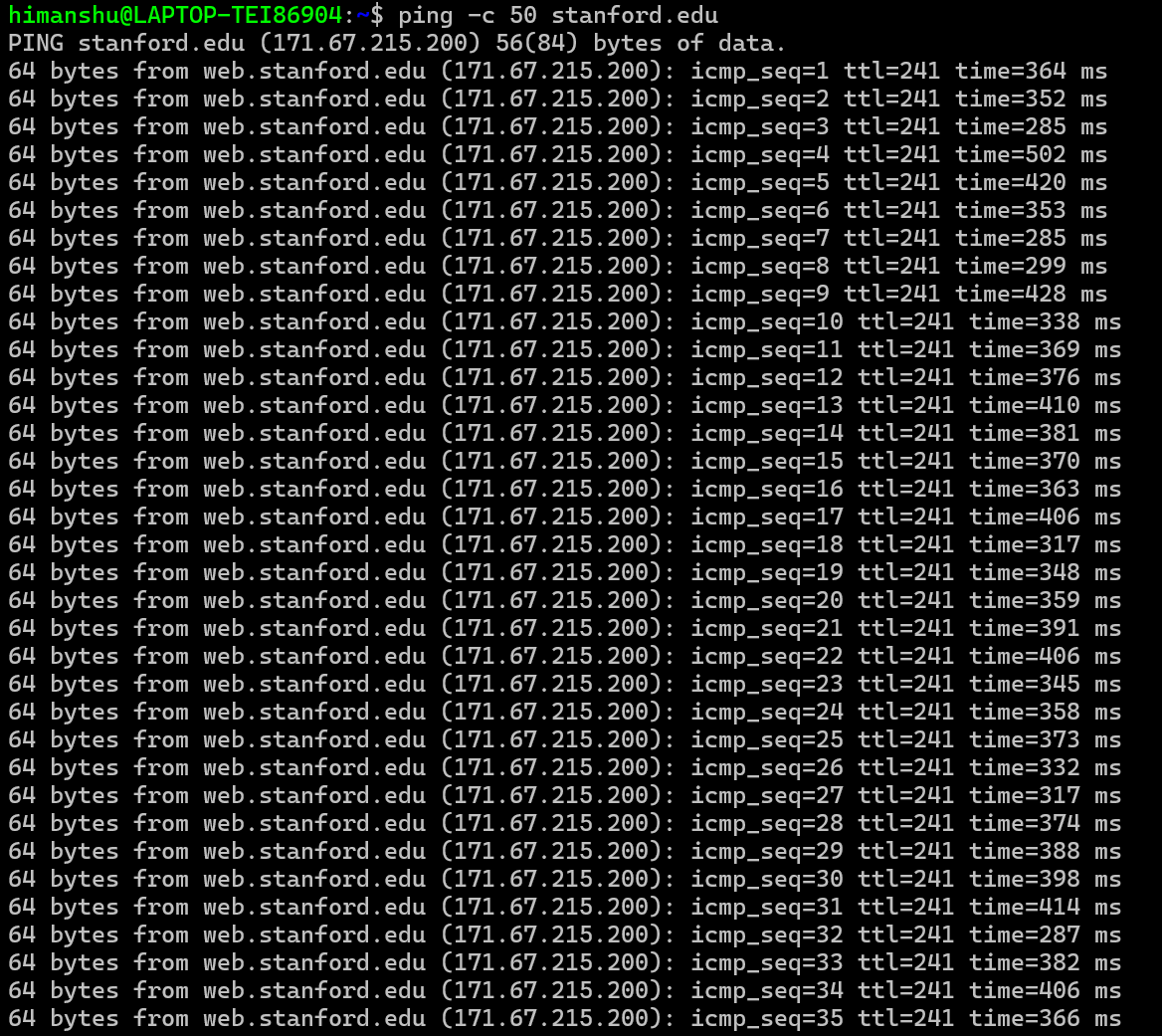
Purpose:

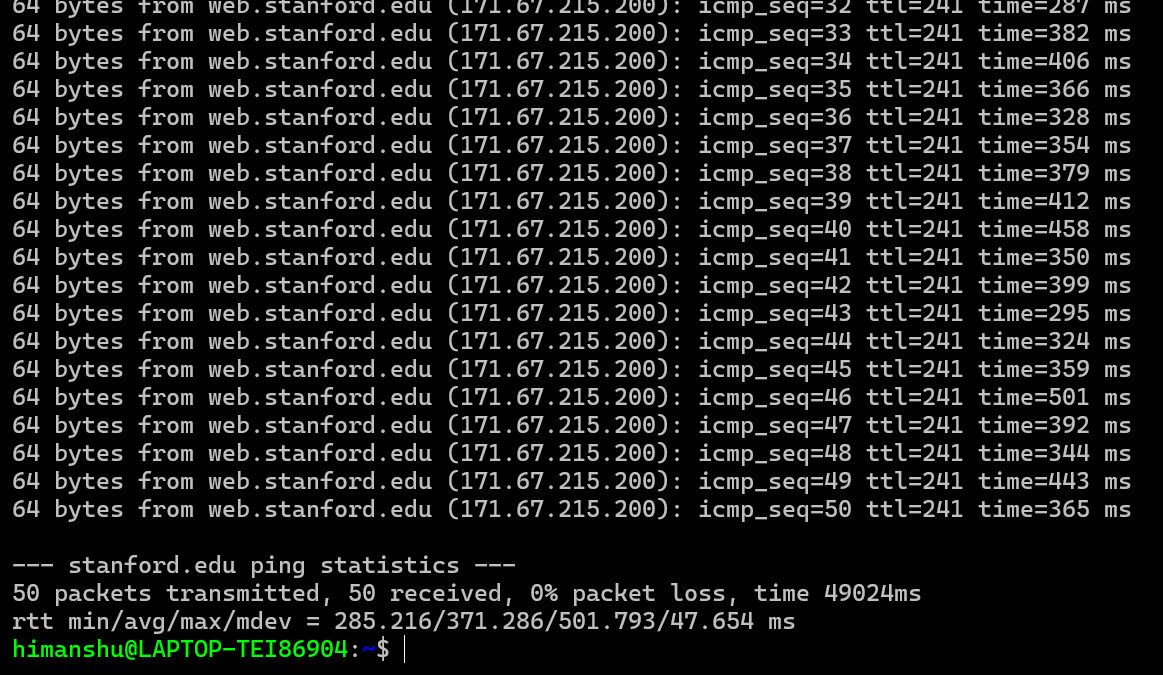
Traceroute works by sending a series of packets with increasing Time-To-Live (TTL) values. Each hop along the route decrements the TTL, and when TTL reaches zero, the router returns a "Time Exceeded" message. This process helps identify the path taken by packets.

Entries in Output:

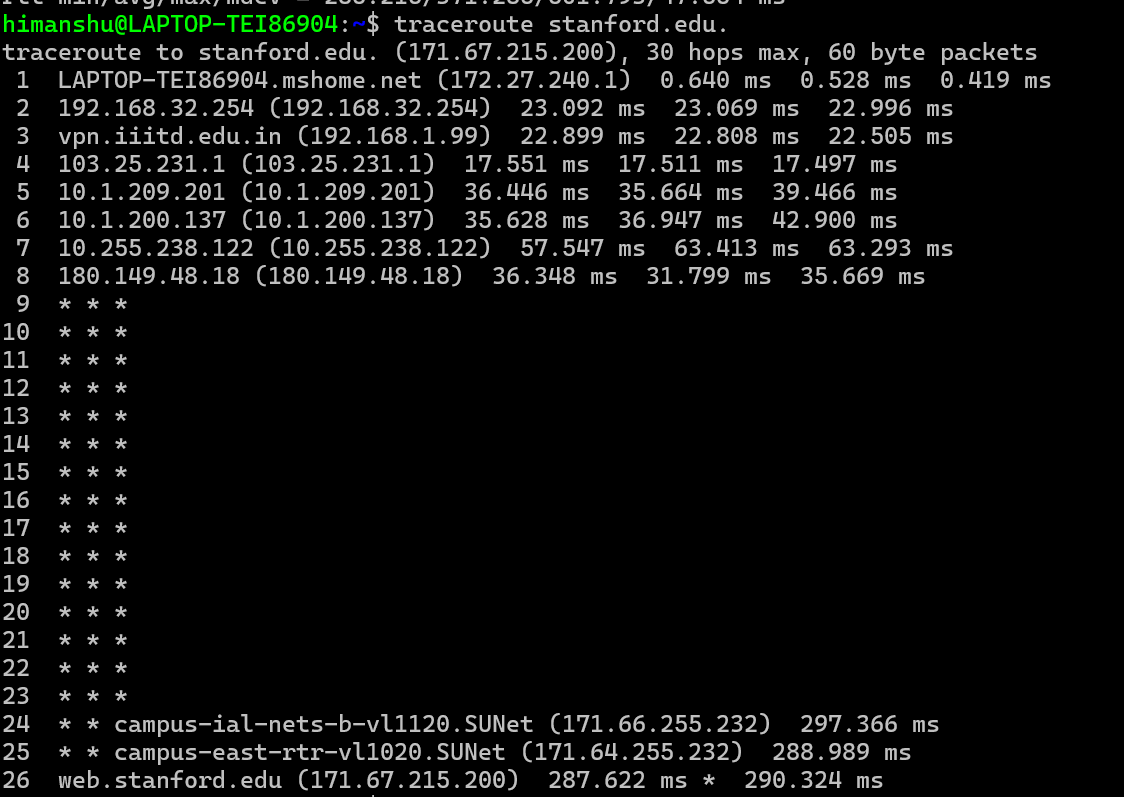
Multiple Response Times: Each line of output for a hop typically shows the round-trip times (RTTs) for three different packets sent to that hop. This is done to provide a more accurate representation of latency and to observe variations in response times.

f) here average latency is 371.286 ms

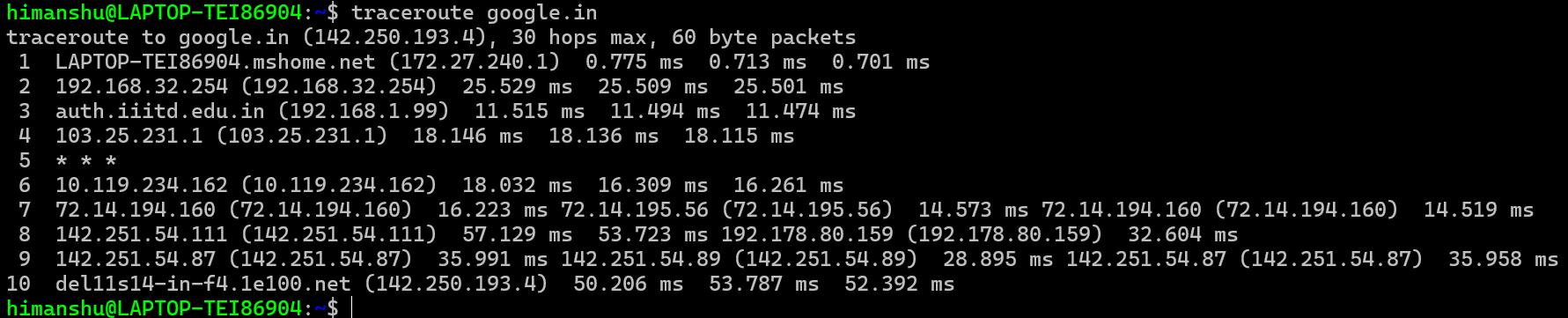




g) traceroute Stanford.edu give 26 hop (it means data pass from 26 different router or intermediate device) including host .



traceroute google.in give 10 hop (it means data pass from 26 different router or intermediate device) including host.



The difference in the number of hops can be due to :

1. Network Paths: Different routes or paths are taken by packets to reach different destinations.
2. Routing Policies: Network policies and routing configurations may vary between networks, resulting in different numbers of hops.
3. May be google server much closer to me than Stanford server.

h) The latency difference between google.in and stanford.edu can be attributed to several factors:

1. Geographic Distance : Latency often increases with physical distance between my machine and the destination. If stanford.edu is geographically closer to me than google.in, you might expect lower latency for stanford.edu. Conversely, a greater distance can result in higher latency.
2. Network Path Complexity

Number of Hops: As observed, the number of hops can affect latency. More hops typically introduce more potential points of delay. If google.in has more hops than stanford.edu, the additional routers and network segments could contribute to higher latency.

1. Routing and Network Congestion

Network Path: Different destinations might have different network paths with varying levels of congestion. If the path to google.in encounters more congestion or delays, it would result in higher latency.

Network Load: The load on intermediate routers and links can impact latency. A more congested network can cause higher latency.

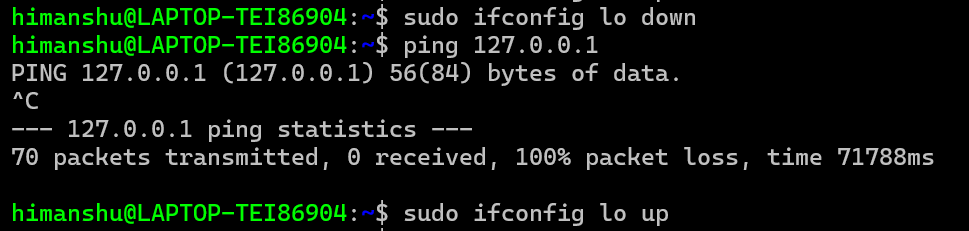
1. Network Infrastructure

Different Networks: google.in and stanford.edu might be served by different ISPs or network infrastructures with varying performance characteristics. For instance, Google's infrastructure might be optimized for lower latency due to its extensive network and data center locations, while Stanford's network might have different performance characteristics.

Question 6

We are using three commands :

1. sudo ifconfig lo down
2. ping 127.0.0.1
3. sudo ifconfig lo up



We are doing this by :

1. Disabling the Loopback Interface: The loopback interface (lo on Linux or lo0 on macOS) is responsible for handling packets addressed to 127.0.0.1. By disabling this interface, packets to 127.0.0.1 are dropped, resulting in 100% packet loss.
2. Ping Command: When you ping 127.0.0.1, you are sending packets to the local machine. With the loopback interface down, the packets cannot be transmitted or received, leading to packet loss.
3. Re-enabling: After testing, bringing the loopback interface back up restores normal functionality, allowing pings to 127.0.0.1 to succeed again.