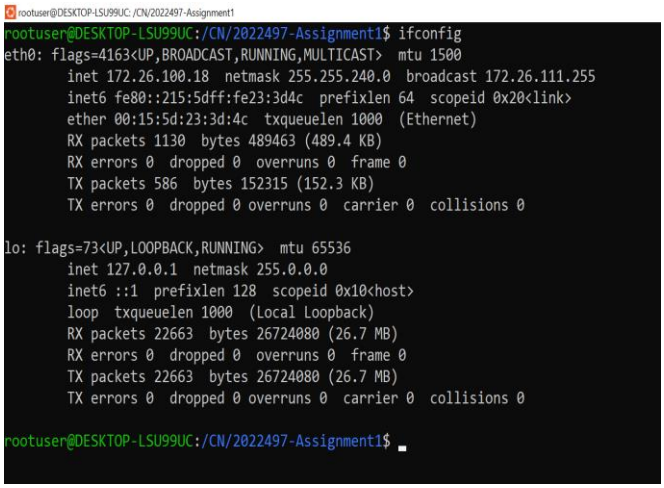
Question 1)

a) IP Address -> IPV4 – 172.26.100.18

IPV6 - fe80::215::5dff:fe23:3d4




b) On the whatsimyip.com My Public IPv4: 27.123.242.77

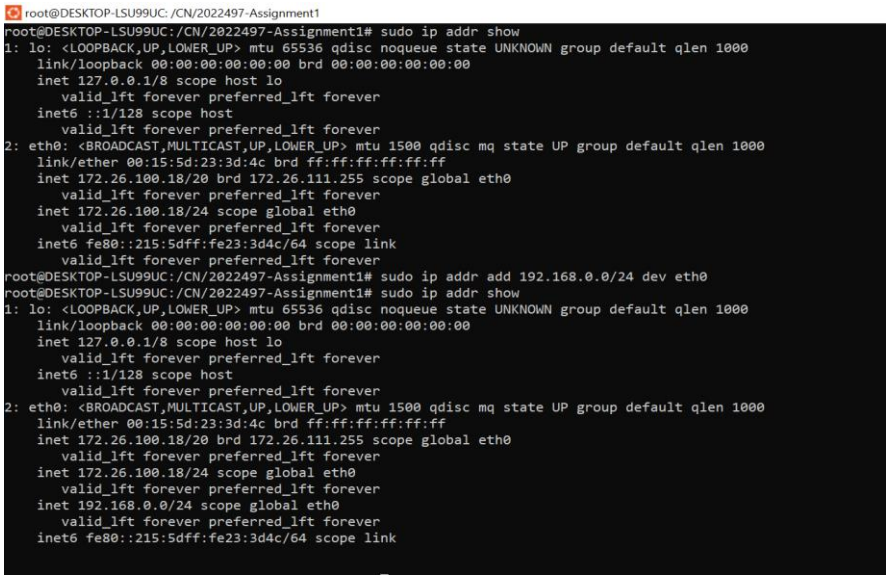
My Public IPv6: Not Detected

IP Address are different because IP Address to my system is private and it is used for communication with LAN(Local Area Network) such as home or office network and the IP Address assign on whatismyip.com is assigned by Internet to Router or Gateway by service Provider(ISP).

IPV6 is NOT Detected could mean My ISP does not support IPV6 or my network configuration does not include IPV6.

Question-2)

**Adding Custom IP Address**



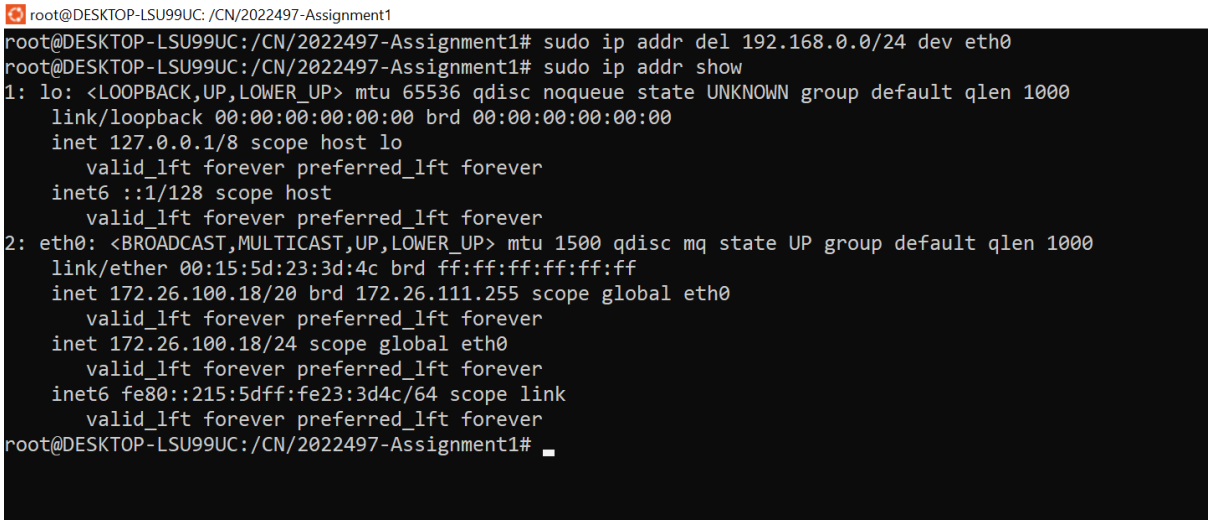

Code on Terminal->

sudo ip addr show

sudo ip addr add 192.168.0.0/24 dev eth0

sudo ip addr show

**Revert IP Address changes**

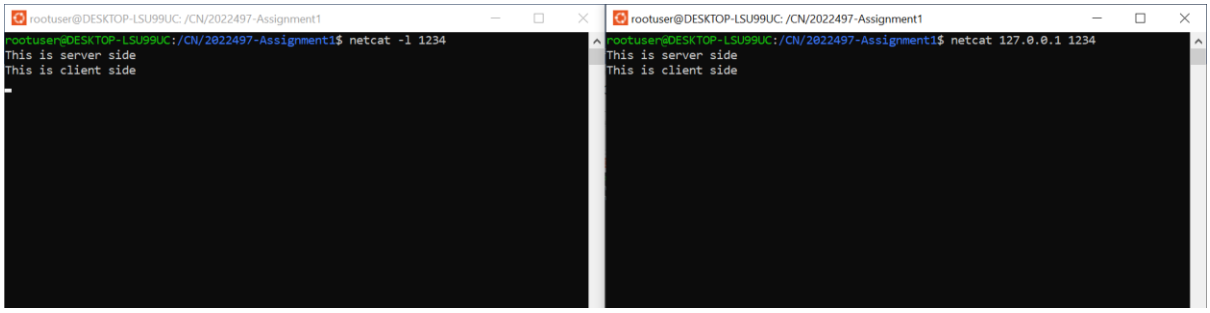



Code on Terminal->

sudo ip addr del 192.168.0.0/24 dev eth0

sudo ip addr show

Question-3)

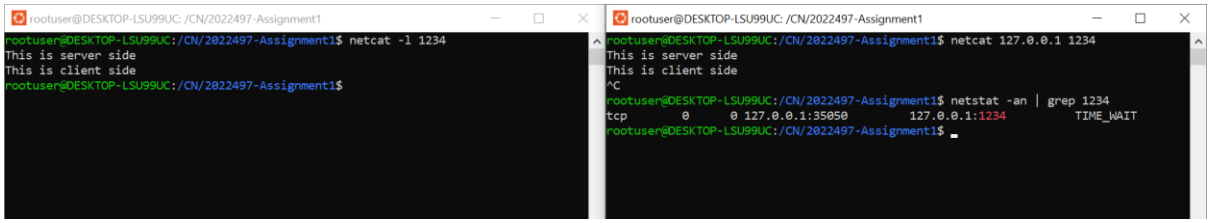



At Server Side

netcat -l 1234

At Client Side

netcat 127.0.0.1 1234

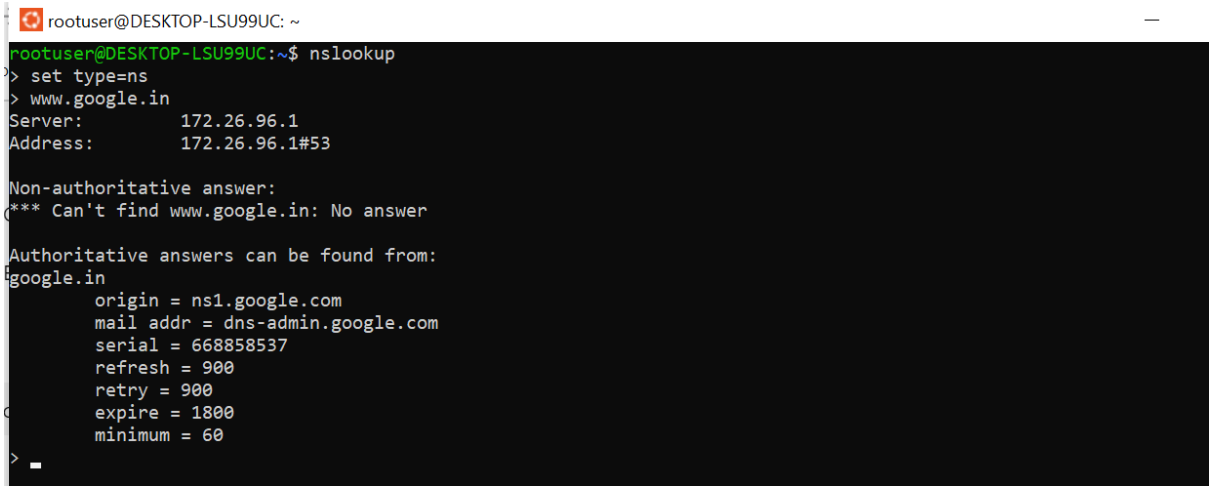



At Client Side

netstat -an | grep 1234

Question-4)

a)



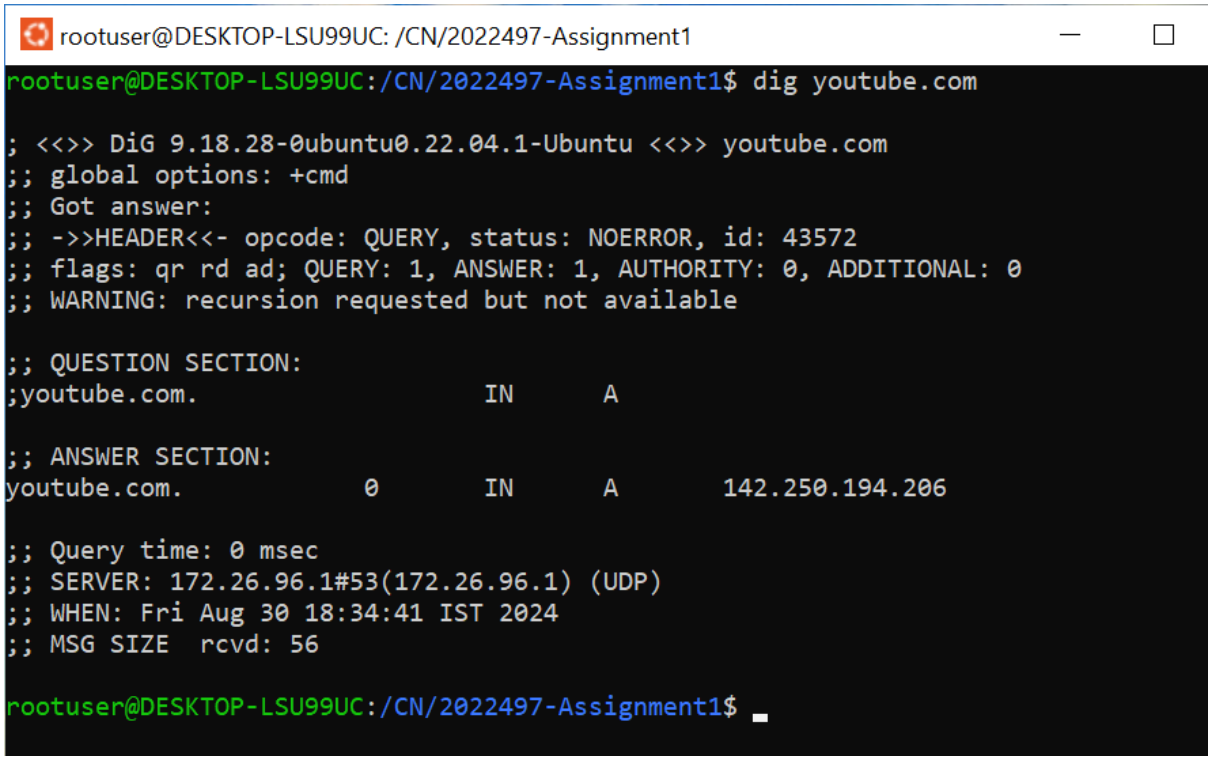

command->

nslookup

set type=ns

www.google.in

b)

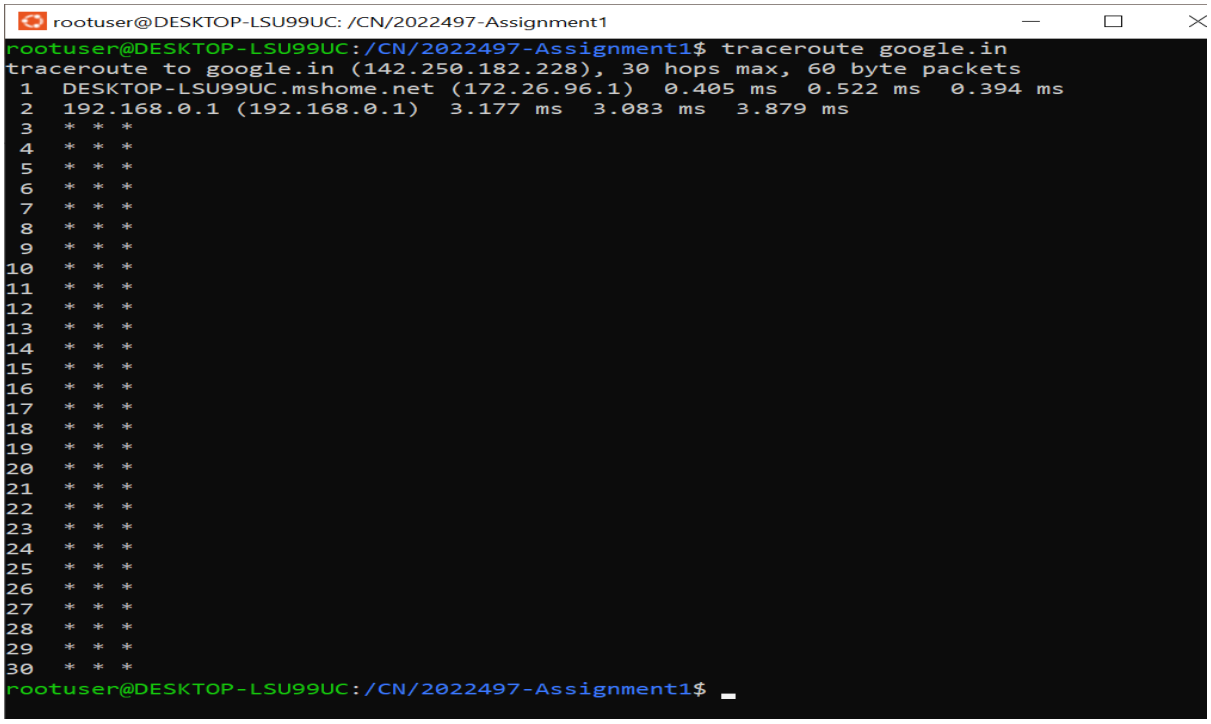



time to live for youtube.com is  0 second.

Since the time to live(TTL) is 0 the record is not meant to be cached and it considered as expired immediately.

Question-5)

a)




There are 2 intermediate hosts.

IP addresses

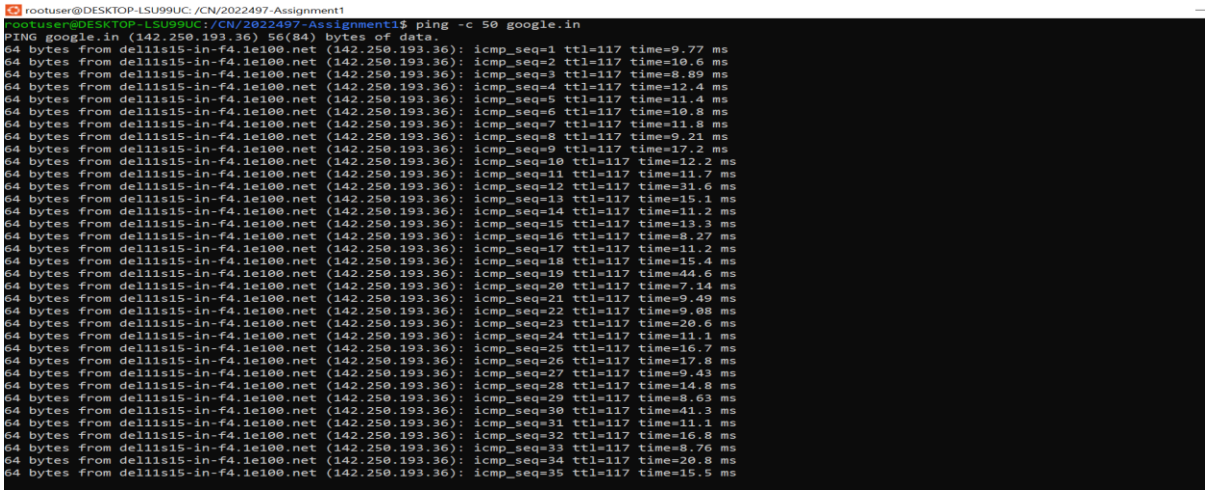
host1-> 172.26.96.1 0.405 ms 0.522 ms 0.394 ms

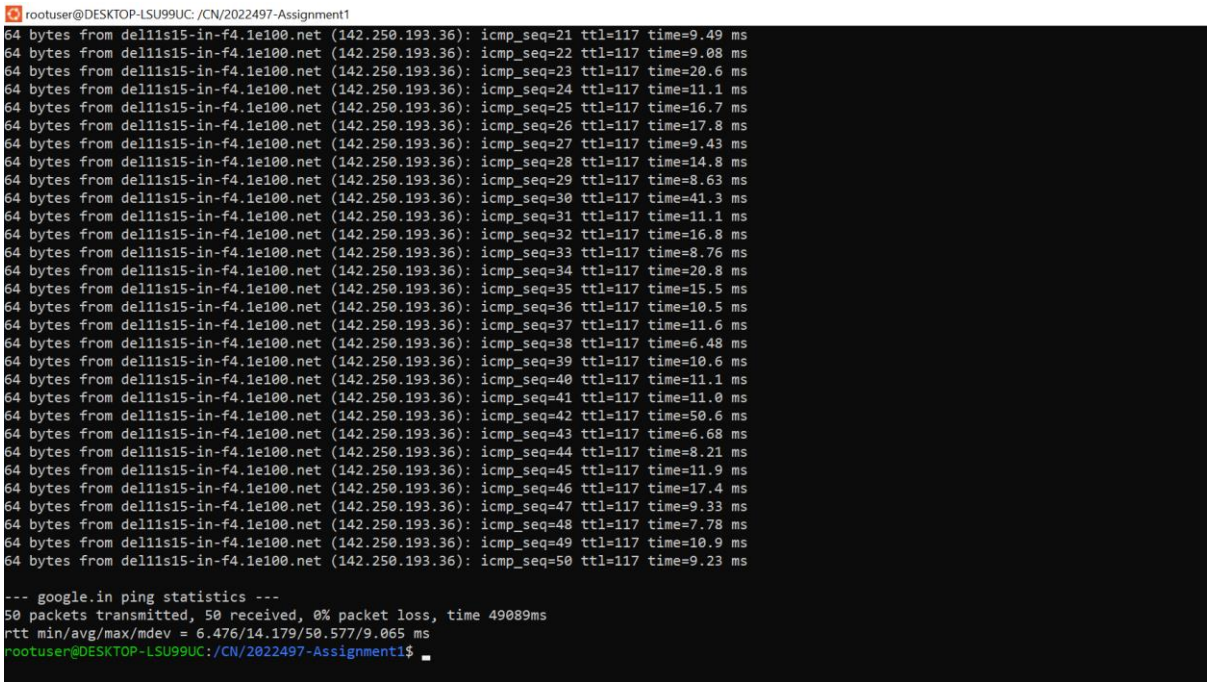
host2-> 192.168.0.1 3.177 ms 3.083 ms 3.879 ms

Average latency of host1 = 0.405+0.522+3.94/3 = 0.440 ms

Average latency of host1 = 3.177+3.083+3.879/3 = 3.376 ms

b) command-> ping -c 50 google.in






Average latency -> 14.179ms

c) a) Average total latency of traceroute command -> 3.816 ms

b) Average latency of ping command -> 14.179 ms

There are not matching.

Latency of ping is higher than ping command because of the following reason.

1)Many intermediate hops did not receive a response(“***”) meaning their latency is not added in the overall traceroute latency sum .

2)Ping command measures the round-trip time from client(my computer) to destination(google.in) and back,covering the entire path,including all intermediate hops,

Whereas traceroute only measures the time to each hop independently and does not get a response from every hop.

d) a)Max latency of traceroute command -> 3.879 ms

b) Max latency of ping command -> 50.577 ms

There are not matching.

Latency of ping is higher than ping command because of the following reason.

1)Many intermediate hops did not receive a response(“***”) meaning their latency is not added in the overall traceroute latency sum in traceroute command.

2)Ping command measures the round-trip time from client(my computer) to destination(google.in) and back,covering the entire path,including all intermediate hops,

Whereas traceroute only measures the time to each hop independenly and does not get a response from every hop.

e) There is no multiple entry for any single hop in traceroute google.in (ignoring “***”).

If multiple entries were present for a single hop, it would following indicate:

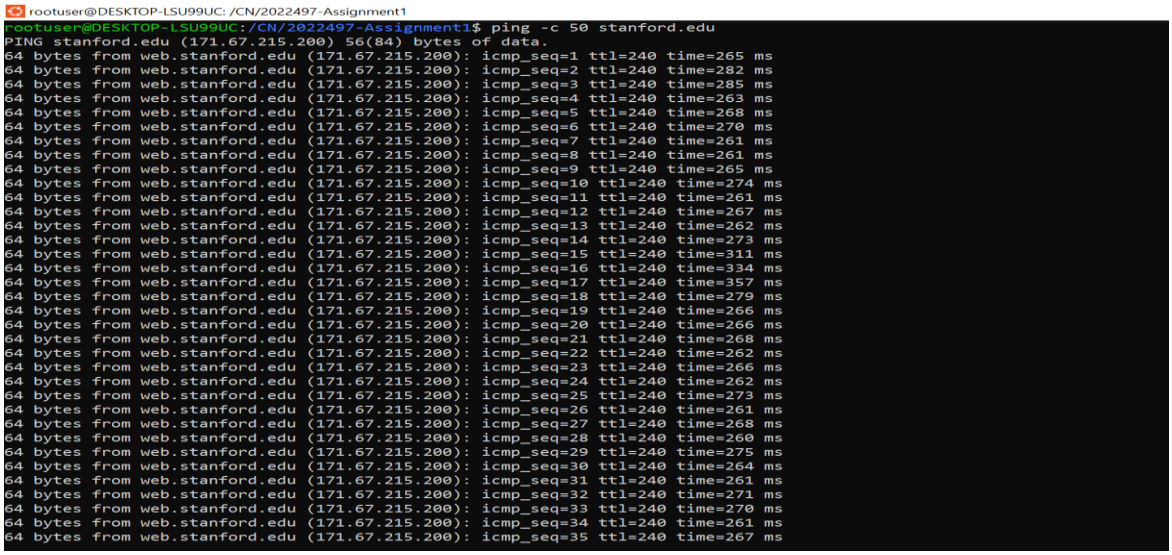
1)Load Balancing: Traffic is distributed across multiple paths.

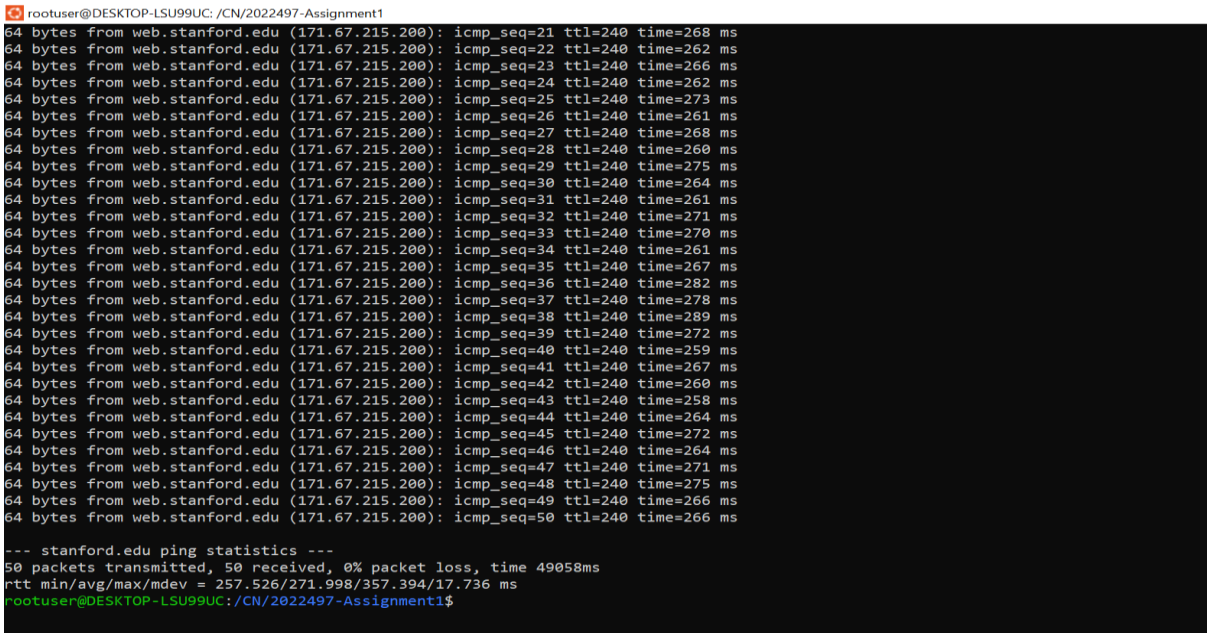
2)Different Interfaces: Device at that hop has multiple network interfaces.

3)Multiple Routers: Responses from closely located routers.

4)Network Changes: Dynamic updates in network routing.

f) command-> ping -c 50 stanford.edu

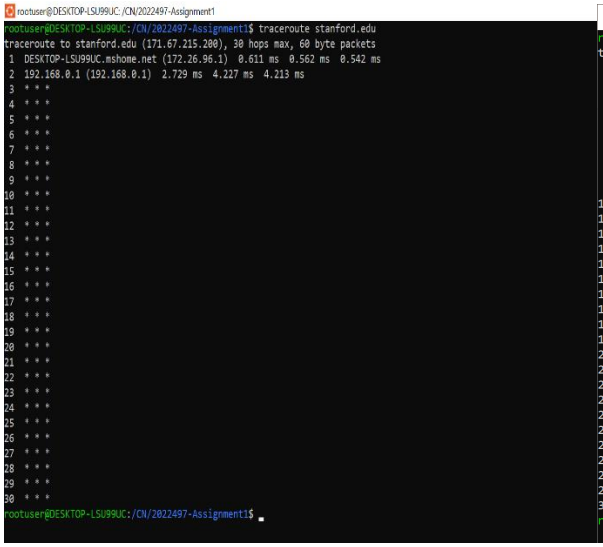




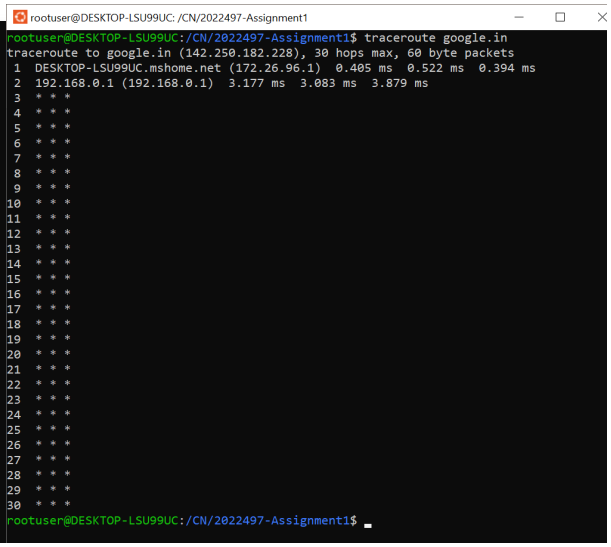

Average latency-> 271.998 ms

g)

traceroute  stanford.edu




traceroute google.in




Both have same number of hops It suggest the number of intermediate devices in the route are similar for both direction.

h)

ping -c 50 google.in

rrt min/avg/max/mdev = 6.476 / 14.179 / 50.577 / 9.065 ms

ping -c 50 stanford.edu

rrt min/avg/max/mdev = 257.526 / 271.998 / 357.394 / 17.736 ms

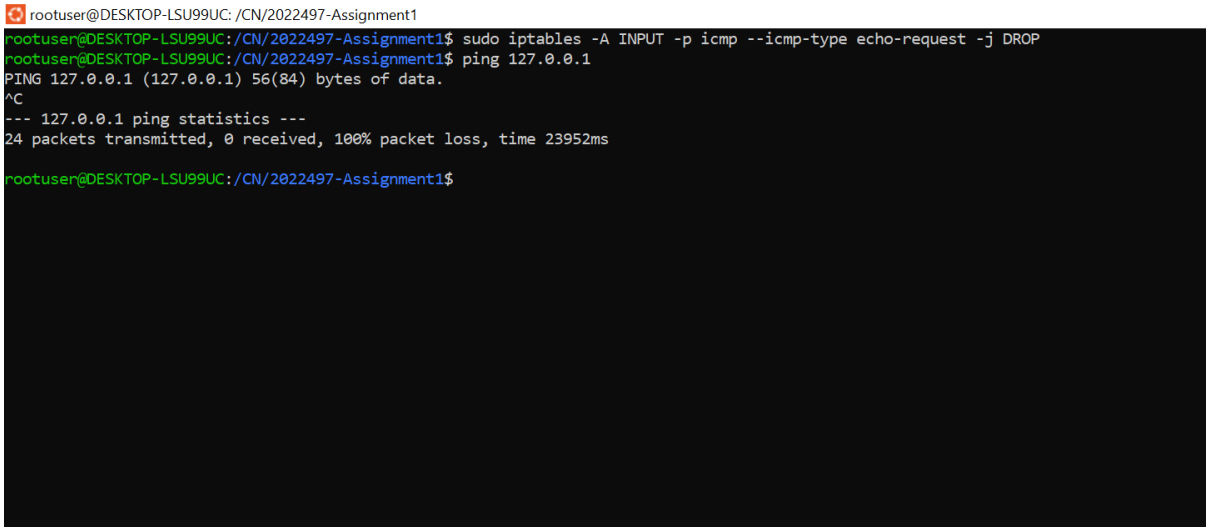
Differences due to the following reason->

1)Geographic location: google.in servers are more nearly than standford.edu in which are located outside the India causing the latency of stanford.edu > google.in

2)Network Infrastructure: Google has a globally distributed infrastructure and extensive use of CDN network causing the fastest network and lower latency.

3)Optimization : Google's infrastructure is highly optimized for speed, which helps them keeps the latency low . whereas Stanford being a academic institution may not have the same level of optimization.

Question-6)




To block ICMP Requests->

sudo iptables -A INPUT -p icmp --icmp-type echo-request -j DROP

-A INPUT: Adds rule to the incoming packets

-p icmp: Specifies ICMP protocol

--icmp-type echo-request : target echo requests packets that is used by ping.

-j DROP: Drops the packet make the ping command fails.

ping 127.0.0.1

To restore ICMP Requests->

sudo iptables -D INPUT -p icmp –icmp-type echo-request -j DROP

To achieve 100% packets loss we can do this by blocking ICMP(Internet Control Message Protocol) requests which ping uses to send and receive packets. ‘ping’ command relies on ICMP echo requests and replies. After blocking with ICMP Requests, machine will never replies, and ‘ping’ command fails completely.