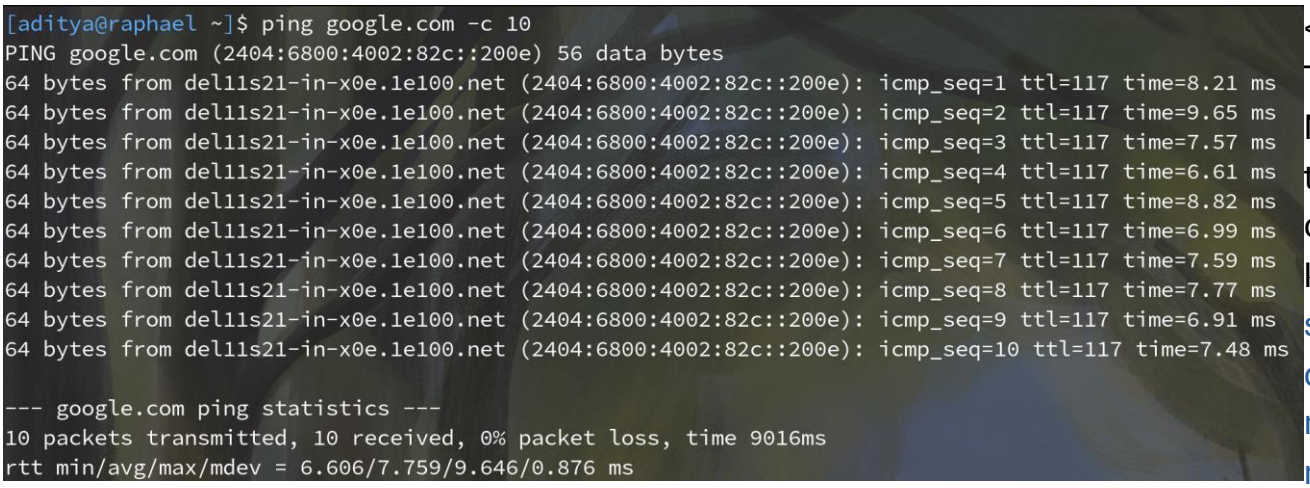
Assignment 1

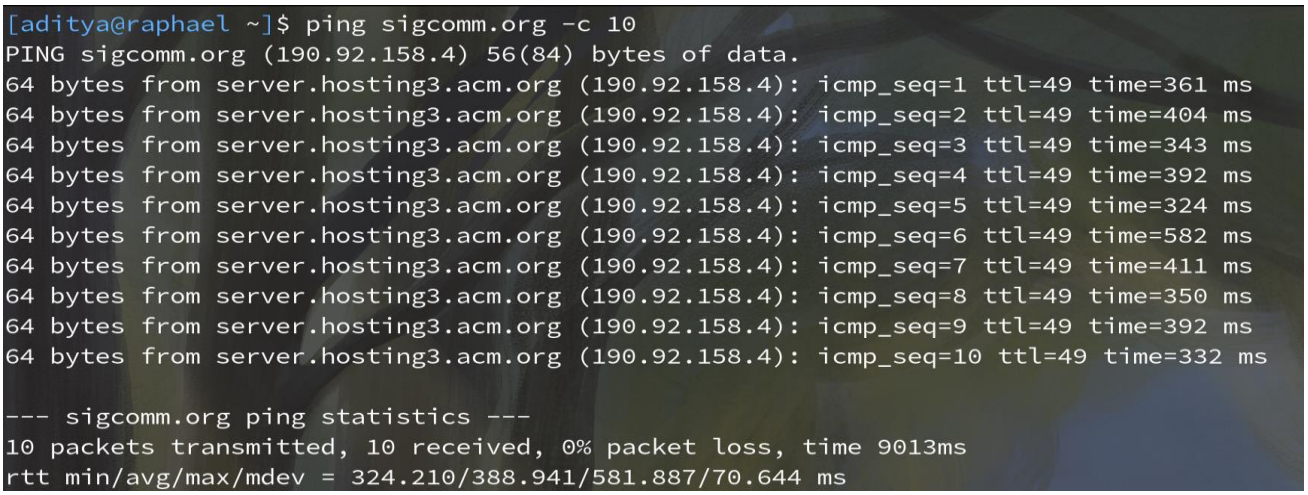
Network Measurement Tools

1. Ping

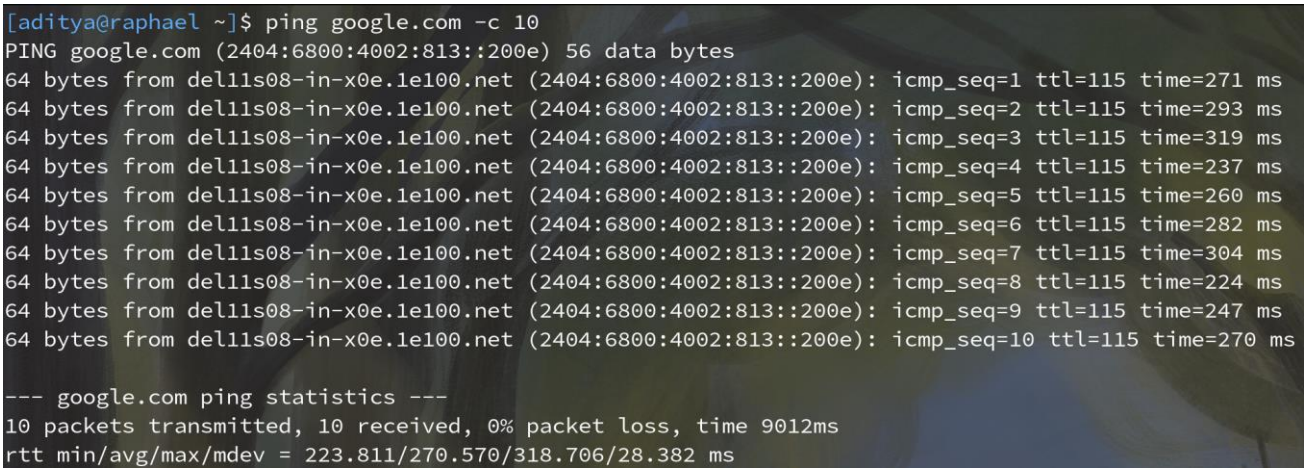
<IITD Network, google.com>



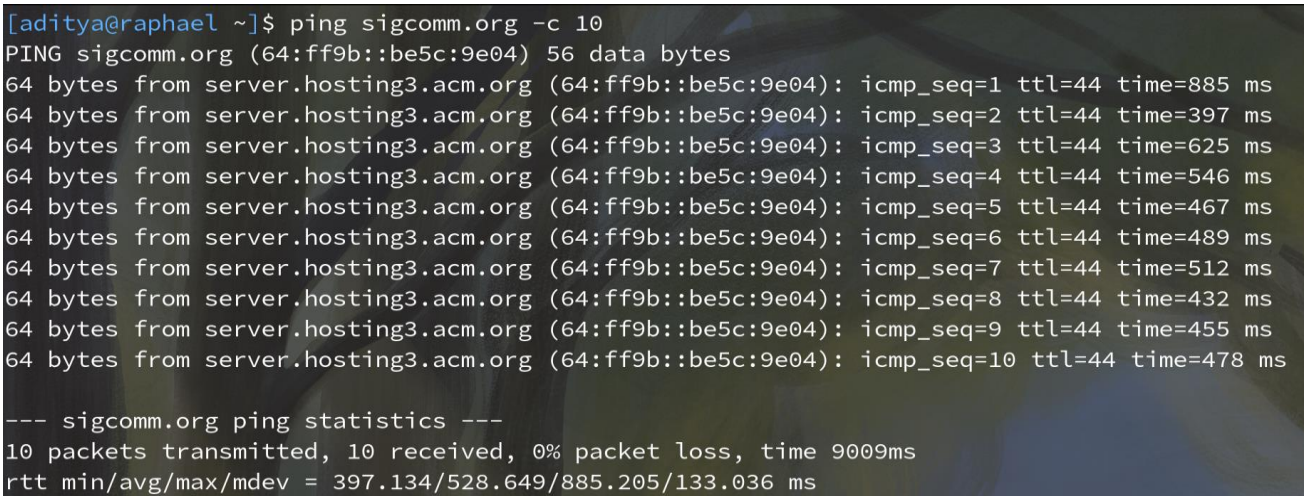
<IITD Network, sigcomm.org>



<Cellular Network, google.com>



<Cellular Network, sigcomm.org>



A. Average ping latencies for google.com is lower than sigcomm.org over both the networks. One of the major reasons is that Google peers directly to nearly all transit providers in the world, which reduces the distance between my computer and from where the request is being processed. Sigcomm doesn't have such global presence.

For both websites, IITD network has lower ping latencies than my cellular network. The reason is that, for both the websites, packets must travel through a greater number of hops when using cellular network. Also, the response delays across nodes are higher for the cellular network.

B. The ping tool uses the Internet Control Message Protocol (ICMP). It sends an ICMP echo request packet to the target host, and if the host is reachable, it replies with an ICMP echo reply packet. It then measures the time it takes for the echo request to travel to the target and for the echo reply to return, calculating the round-trip time.

An ICMP packet (used by ping) has a theoretical upper limit of 65527 bytes (adding the 8-byte ICMP header makes a total of 65535 bytes), in comparison to 56 bytes (total of 64 bytes) in a standard ping call. I am not able to ping these websites on this theoretical maximum packet size. The google.com website truncates responses for any packet size above 68 bytes (76 bytes total) and stops responding for anything above 1452 bytes while the sigcomm.org website for a maximum packet size of 35512 bytes and above responds with the phrase "message too long". The reasons are the following:

a. Google implements a strict limit size on ICMP packet sizes to enhance their security and manage network traffic efficiently. Truncation limits the impact of attacks like large packet attacks and reduce unnecessary network traffic that could congest their infrastructure.

b. Sigcomm allows larger packet sizes but still enforces a limit to protect against oversized packets, which could cause issues on the server or network. The looser restrictions (as compared to Google) may also be linked to Sigcomm trying to facilitate networking experiments as they are one of the top networking conferences in the world.

C. To ping google.com using IPv6, I used the ping6 command and used their IPv6 domain ipv6.google.com. The results:

<IITD network, google.com>

```
[aditya@raphael ~]$ ping google.com -c 5
PING google.com (2404:6800:4002:82c::200e) 56 data bytes
64 bytes from del11s21-in-x0e.1e100.net (2404:6800:4002:82c::200e): icmp_seq=1 ttl=117 time=6.61 ms
64 bytes from del11s21-in-x0e.1e100.net (2404:6800:4002:82c::200e): icmp_seq=2 ttl=117 time=7.68 ms
64 bytes from del11s21-in-x0e.1e100.net (2404:6800:4002:82c::200e): icmp_seq=3 ttl=117 time=7.14 ms
64 bytes from del11s21-in-x0e.1e100.net (2404:6800:4002:82c::200e): icmp_seq=4 ttl=117 time=7.53 ms
64 bytes from del11s21-in-x0e.1e100.net (2404:6800:4002:82c::200e): icmp_seq=5 ttl=117 time=7.81 ms

--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 6.611/7.352/7.808/0.432 ms
```

```
[aditya@raphael ~]$ ping6 ipv6.google.com -c 5
PING ipv6.google.com (2404:6800:4002:81d::200e) 56 data bytes
64 bytes from del11s18-in-x0e.1e100.net (2404:6800:4002:81d::200e): icmp_seq=1 ttl=118 time=8.50 ms
64 bytes from del11s18-in-x0e.1e100.net (2404:6800:4002:81d::200e): icmp_seq=2 ttl=118 time=5.31 ms
64 bytes from del11s18-in-x0e.1e100.net (2404:6800:4002:81d::200e): icmp_seq=3 ttl=118 time=6.96 ms
64 bytes from del11s18-in-x0e.1e100.net (2404:6800:4002:81d::200e): icmp_seq=4 ttl=118 time=6.94 ms
64 bytes from del11s18-in-x0e.1e100.net (2404:6800:4002:81d::200e): icmp_seq=5 ttl=118 time=6.81 ms

--- ipv6.google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 5.307/6.902/8.498/1.010 ms
```

```
[aditya@raphael ~]$ ping google.com -c 5
PING google.com (2404:6800:4002:81d::200e) 56 data bytes
64 bytes from del11s18-in-x0e.1e100.net (2404:6800:4002:81d::200e): icmp_seq=1 ttl=115 time=45.3 ms
64 bytes from del11s18-in-x0e.1e100.net (2404:6800:4002:81d::200e): icmp_seq=2 ttl=115 time=44.6 ms
64 bytes from del11s18-in-x0e.1e100.net (2404:6800:4002:81d::200e): icmp_seq=3 ttl=115 time=41.9 ms
64 bytes from del11s18-in-x0e.1e100.net (2404:6800:4002:81d::200e): icmp_seq=4 ttl=115 time=65.4 ms
64 bytes from del11s18-in-x0e.1e100.net (2404:6800:4002:81d::200e): icmp_seq=5 ttl=115 time=67.2 ms

--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 41.928/52.870/67.177/11.027 ms
```

Standard (ipv4) ping

IPv6 ping

It also worked for the cellular network.

<Cellular network, google.com>

Standard (ipv4) ping

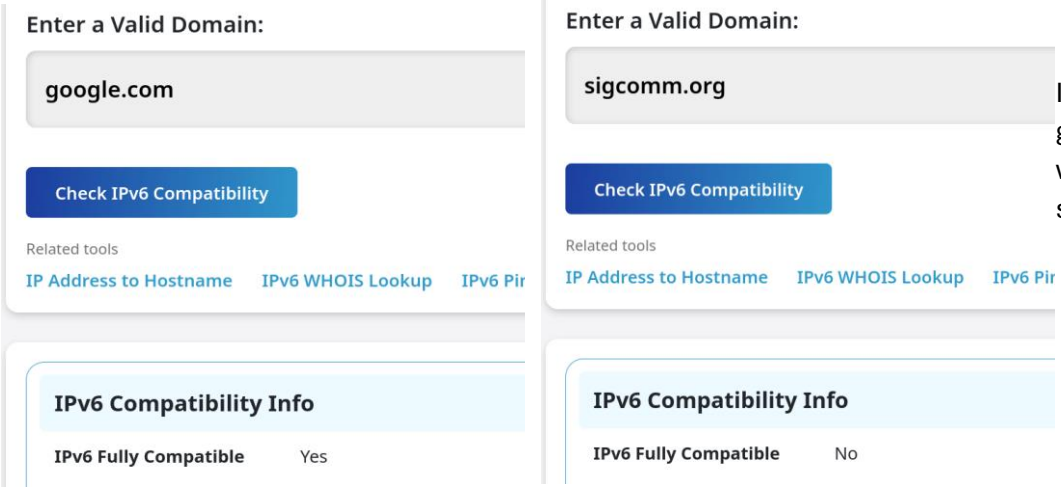
```
[aditya@raphael ~]$ ping6 ipv6.google.com -c 5
PING ipv6.google.com (2404:6800:4002:80b::200e) 56 data bytes
64 bytes from del03s16-in-x0e.1e100.net (2404:6800:4002:80b::200e): icmp_seq=1 ttl=116 time=45.9 ms
64 bytes from del03s16-in-x0e.1e100.net (2404:6800:4002:80b::200e): icmp_seq=2 ttl=116 time=54.6 ms
64 bytes from del03s16-in-x0e.1e100.net (2404:6800:4002:80b::200e): icmp_seq=3 ttl=116 time=51.4 ms
64 bytes from del03s16-in-x0e.1e100.net (2404:6800:4002:80b::200e): icmp_seq=4 ttl=116 time=80.4 ms
64 bytes from del03s16-in-x0e.1e100.net (2404:6800:4002:80b::200e): icmp_seq=5 ttl=116 time=47.3 ms

--- ipv6.google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 45.893/55.929/80.392/12.609 ms
```

IPv6 ping

```
[aditya@raphael ~]$ ping6 ip6v.sigcomm.org -c 5
ping6: ip6v.sigcomm.org: Name or service not known
```

But this doesn't work for sigcomm.org. For both the networks, it responds with the same message.

The reason being that sigcomm.org domain doesn't have support for ipv6 yet. This can be checked on DNSChecker's website.



It can be observed that google.com is compatible with ipv6 while sigcomm.org is not.

2. Traceroute

<IITD Network, google.com>

<IITD Network, sigcomm.org>

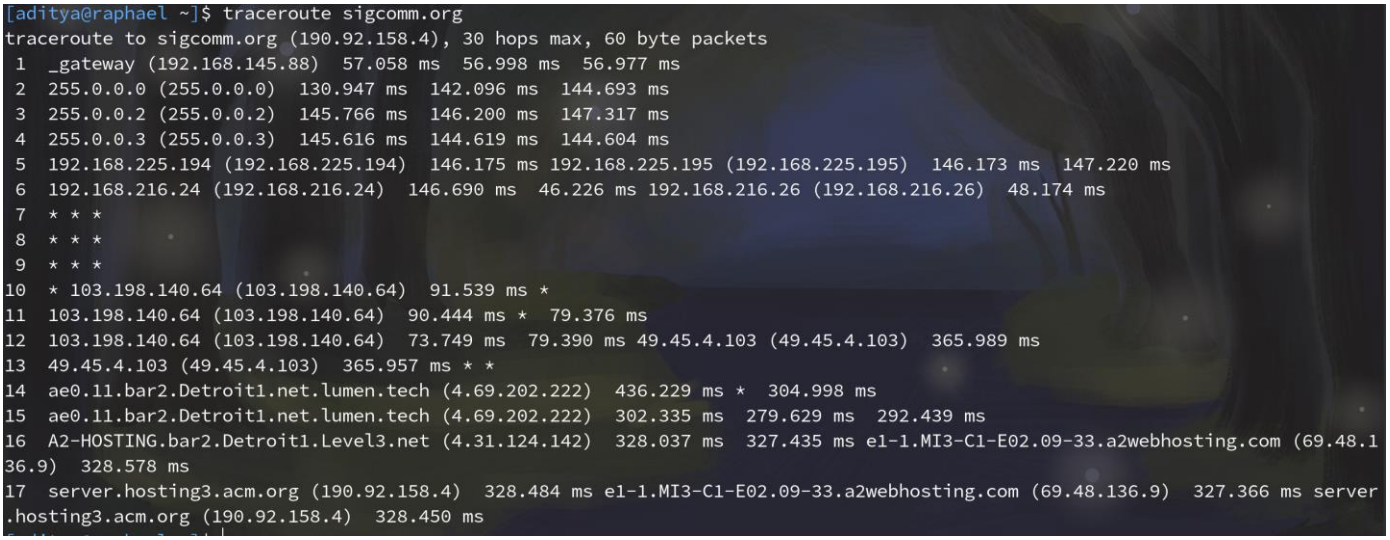
```
[aditya@raphael ~]$ traceroute google.com
traceroute to google.com (142.250.206.142), 30 hops max, 60 byte packets
 1  10.184.0.13 (10.184.0.13)  3.164 ms  3.344 ms  4.513 ms
 2  10.255.107.3 (10.255.107.3)  5.689 ms  6.054 ms  4.818 ms
 3  10.119.233.65 (10.119.233.65)  7.143 ms  6.685 ms  6.776 ms
 4  * * *
 5  10.119.234.162 (10.119.234.162)  10.211 ms  10.179 ms  10.160 ms
 6  72.14.194.160 (72.14.194.160)  11.168 ms  7.321 ms 72.14.195.56 (72.14.195.56)  3.677 ms
 7  142.251.54.111 (142.251.54.111)  6.185 ms 192.178.80.159 (192.178.80.159)  5.562 ms  5.545 ms
 8  142.251.76.197 (142.251.76.197)  5.474 ms  5.456 ms  5.437 ms
 9  del11s21-in-f14.1e100.net (142.250.206.142)  5.387 ms  5.368 ms  5.350 ms
```

```
[aditya@raphael ~]$ traceroute sigcomm.org
traceroute to sigcomm.org (190.92.158.4), 30 hops max, 60 byte packets
 1  10.184.0.13 (10.184.0.13)  86.629 ms  87.223 ms  106.017 ms
 2  10.255.107.3 (10.255.107.3)  109.025 ms  153.721 ms  155.024 ms
 3  10.119.233.65 (10.119.233.65)  234.666 ms  194.906 ms  223.407 ms
 4  * * *
 5  10.119.234.162 (10.119.234.162)  241.434 ms  264.440 ms  257.734 ms
 6  136.232.148.177 (136.232.148.177)  269.742 ms  13.432 ms  18.002 ms
 7  * * *
 8  * * *
 9  * * *
10  49.45.4.103 (49.45.4.103)  306.155 ms  306.134 ms  294.533 ms
11  4.7.26.61 (4.7.26.61)  288.206 ms  288.876 ms  288.778 ms
12  ae0.11.bar2.detroit1.net.lumen.tech (4.69.202.222)  288.773 ms  288.747 ms a2-hosting.bar2.detroit1.level3.net (4.31.124.1
42)  382.495 ms
13  e1-1.mi3-c1-e02.09-33.a2webhosting.com (69.48.136.9)  382.386 ms  382.362 ms a2-hosting.bar2.detroit1.level3.net (4.31.124
.142)  382.353 ms
14  e1-1.mi3-c1-e02.09-33.a2webhosting.com (69.48.136.9)  380.276 ms  380.180 ms  380.529 ms
15  server.hosting3.acm.org (190.92.158.4)  380.644 ms  388.120 ms  388.014 ms
```

<Cellular Network, google.com>

<Cellular Network, sigcomm.org>

```
[aditya@raphael ~]$ traceroute google.com
traceroute to google.com (142.250.206.142), 30 hops max, 60 byte packets
 1  _gateway (192.168.145.88)  4.727 ms  7.481 ms  7.464 ms
 2  255.0.0.0 (255.0.0.0)  142.528 ms  142.553 ms  142.538 ms
 3  255.0.0.2 (255.0.0.2)  143.582 ms  143.568 ms  144.523 ms
 4  255.0.0.3 (255.0.0.3)  143.621 ms  145.859 ms  144.304 ms
 5  192.168.225.195 (192.168.225.195)  145.754 ms 192.168.225.194 (192.168.225.194)  144.325 ms 192.168.225.195 (192.168.225.1
95)  145.724 ms
 6  192.168.216.30 (192.168.216.30)  145.783 ms  53.004 ms 192.168.216.24 (192.168.216.24)  36.949 ms
 7  * * *
 8  * * *
 9  * * *
10  72.14.195.34 (72.14.195.34)  53.657 ms 74.125.48.196 (74.125.48.196)  54.434 ms 142.250.161.100 (142.250.161.100)  53.648
ms
11  * * *
12  142.251.76.199 (142.251.76.199)  35.550 ms 142.251.52.212 (142.251.52.212)  39.912 ms 142.251.76.199 (142.251.76.199)  55.
201 ms
13  192.178.83.224 (192.178.83.224)  54.483 ms 142.251.76.197 (142.251.76.197)  54.951 ms 216.239.54.92 (216.239.54.92)  50.18
4 ms
14  del11s21-in-f14.1e100.net (142.250.206.142)  44.763 ms  44.682 ms  35.101 ms
```


[aditya@raphael ~]$ traceroute sigcomm.org
traceroute to sigcomm.org (190.92.158.4), 30 hops max, 60 byte packets
1 _gateway (192.168.145.88) 57.058 ms 56.998 ms 56.977 ms
2 255.0.0.0 (255.0.0.0) 130.947 ms 142.096 ms 144.693 ms
3 255.0.0.2 (255.0.0.2) 145.766 ms 146.200 ms 147.317 ms
4 255.0.0.3 (255.0.0.3) 145.616 ms 144.619 ms 144.604 ms
5 192.168.225.194 (192.168.225.194) 146.175 ms 192.168.225.195 (192.168.225.195) 146.173 ms 147.220 ms
6 192.168.216.24 (192.168.216.24) 146.690 ms 46.226 ms 192.168.216.26 (192.168.216.26) 48.174 ms
7 * * *
8 * * *
9 * * *
10 * 103.198.140.64 (103.198.140.64) 91.539 ms *
11 103.198.140.64 (103.198.140.64) 90.444 ms * 79.376 ms
12 103.198.140.64 (103.198.140.64) 73.749 ms 79.390 ms 49.45.4.103 (49.45.4.103) 365.989 ms
13 49.45.4.103 (49.45.4.103) 365.957 ms * *
14 ae0.11.bar2.Detroit1.net.lumen.tech (4.69.202.222) 436.229 ms * 304.998 ms
15 ae0.11.bar2.Detroit1.net.lumen.tech (4.69.202.222) 302.335 ms 279.629 ms 292.439 ms
16 A2-HOSTING.bar2.Detroit1.Level3.net (4.31.124.142) 328.037 ms 327.435 ms e1-1.MI3-C1-E02.09-33.a2webhosting.com (69.48.136.9) 328.578 ms
17 server.hosting3.acm.org (190.92.158.4) 328.484 ms e1-1.MI3-C1-E02.09-33.a2webhosting.com (69.48.136.9) 327.366 ms server.hosting3.acm.org (190.92.158.4) 328.450 ms

A.

I. 9 hops
(10.0.0.0 - 10.255.255.255): IANA Special use addresses
(72.14.192.0 - 72.14.255.255): Google Direct Allocation addresses
(192.178.0.0 - 192.179.255.255): Google (AS15169)
(142.250.0.0 - 142.251.255.255): Google (AS15169)

II. 15 hops
(10.0.0.0 - 10.255.255.255): IANA Special use addresses
(36.232.0.0 - 136.233.255.255): Reliance JIO (AS55836)
(49.32.0.0 - 49.47.255.255): Reliance JIO (AS64049)
(4.0.0.0 - 4.127.255.255): LVLT-ORG Direct Allocation addresses
(69.48.136.0 - 69.48.139.255): A2HOS (AS55293)
(190.92.128.0 - 190.92.159.255): INTERNET-BLK-A2HOS (AS55293)

III. 14 hops
(192.168.0.0 - 192.168.255.255): IANA Special use addresses
(240.0.0.0 - 255.255.255.255): IANA Special use addresses
(72.14.192.0 - 72.14.255.255): Google Direct Allocation addresses
(142.250.0.0 - 142.251.255.255): Google (AS15169)
(192.178.0.0 - 192.179.255.255): Google (AS15169)
(216.239.32.0 - 216.239.63.255): Google Direct Allocation addresses

IV. 17 hops
(192.168.0.0 - 192.168.255.255): IANA Special use addresses
(240.0.0.0 - 255.255.255.255): IANA Special use addresses
(103.198.140.0 - 103.198.140.255): RJIPL-SG (AS64049)
(49.32.0.0 - 49.47.255.255): Reliance JIO (AS64049)
(4.0.0.0 - 4.127.255.255): LVLT-ORG Direct Allocation addresses
(69.48.136.0 - 69.48.139.255): A2HOS (AS55293)
(190.92.128.0 - 190.92.159.255): INTERNET-BLK-A2HOS (AS55293)

B. Yes, I observed "*" in my output. A * indicates a timeout or a hop where the response was not received. This might occur due to firewalls, network security settings, or routing issues.

C. Yes, I observed multiple IP addresses on the same hop. These indicate that the traffic is being routed through multiple channels due to load balancing mechanisms.

D. I observed a 2-tiered architecture in both of Google's traceroutes as the packets are transferred from IANA special use IPs to Google's servers. Sigcomm has a 3-tiered architecture where packets travel from special use IPs to intermediate servers (Reliance Jio in this case) and then to Sigcomm's servers. If in some case, we do not observe a clear tiered architecture, it could be due to a direct peering relationship between ISPs, a highly optimized route with minimal hops.

E. For Google, the geolocations of the IP addresses are close to each other and hence the RTTs are very fast and hence they make sense. But for Sigcomm, the RTTs for IPs which are closer to each other as per geolocations are larger in some cases than IPs far away. So, IP geolocations don't really make sense.

Network Data Collection and Header analysis

A.

1. Network Layer Protocols:
   - Internet Protocol Version 6 (IPv6): 99.6% packets
   - Internet Protocol Version 4 (IPv4): 0.4% packets
2. Transport Layer Protocols:
   - User Datagram Protocol (UDP):
     - 99.1% packets (IPv6)
     - 0.1% packets (IPv4)
   - Transmission Control Protocol (TCP):
     - 0.4% packets (IPv6)
     - 0.3% packets (IPv7)
   - Internet Control Message Protocol (ICMPv6): 0.1%
3. Application Layer Protocols:
   - Session Traversal Utilities for NAT (STUN): 0.2% packets
   - Real-time Transport Control Protocol (RTCP): 2.1% packets
   - Data (unspecified): 96.7% packets
   - Transport Layer Security: 0.2% packets
   - Domain Name System: 0.1%

B. During the analysis, it was observed that there is no direct connection between the two hosts.

Host A: 192:168:145:69 (IPv4), 2001:df4:e000:3fd1::25c3 (IPv6)

Host B: 192:168:247:70 (IPv4), 2001:df4:e000:3fd1::2adf (IPv6)

Intermediate IPs: 34.107.221.82, 34.107.243.93, 52.123.164.68

There is no direct connection due to NAT traversal, where both participants are behind NAT and cannot establish a direct peer-to-peer connection. Additionally, Microsoft may route traffic through their servers to ensure secure communication and optimize performance.

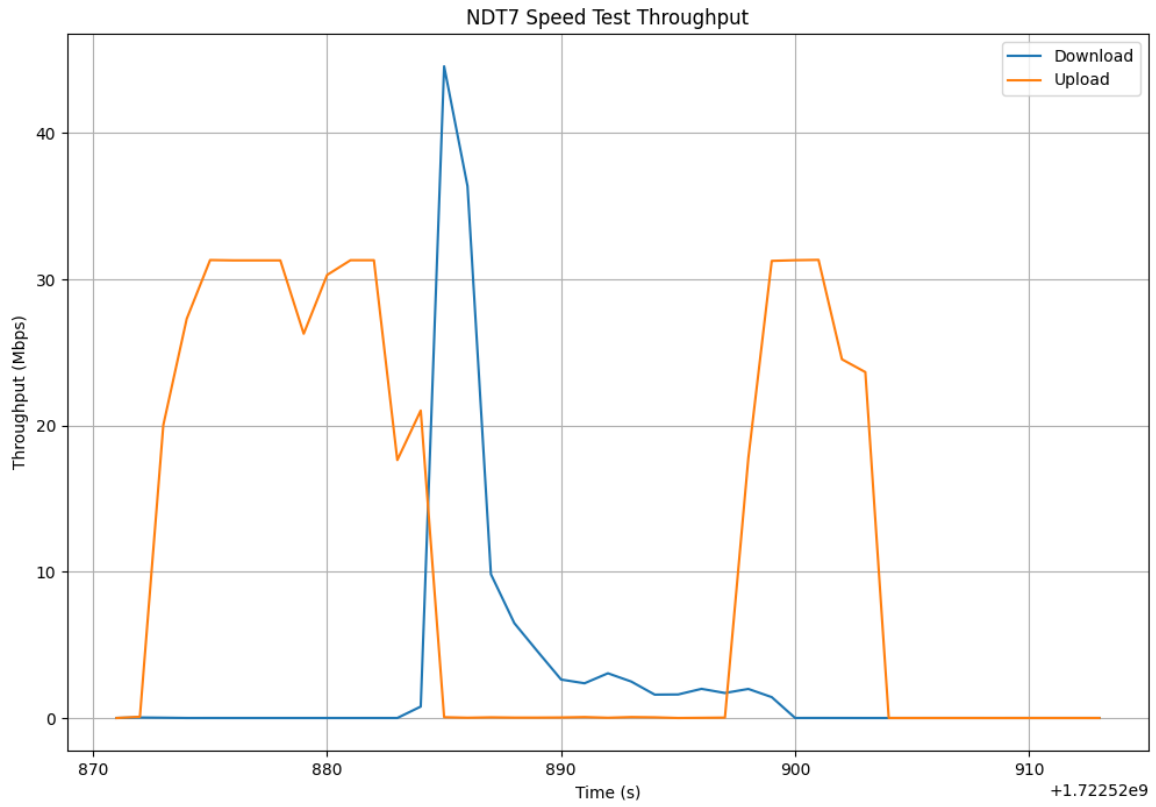
C.

Network traffic analysis

We first read the pcap file and extract all the packets. Then we analyse all packets to determine which port have the highest volume of traffic, assuming these are used by the speed test. Then we check for packets using TCP and if their ports match the port we found earlier. These packets should be the ones corresponding to NDT7 speed test.

Speed Test traffic: 88.45%

Plot of throughputs:



Average Download Speeds: 2.94 MBps

Average Upload Speeds: 11.69 MBps

TOOLS

- Whois (for ASN)
- Keycdn (for geolocation)
- DNS checker (for ipv6)
- Ifconfig (for local network configurations)