Network Traffic Analysis - Assignment 1

OVERVIEW

This assignment involves analyzing network traffic using basic network measurement tools , getting familiar with Wireshark and conducting a detailed analysis of a network traffic trace from a speed test using the M-Lab NDT7 tool.

CONTENT

1. **Measurement Tools**
   - Ping
   - Traceroute
2. **Network Data Collection and Header Analysis**
   - Microsoft Teams Call
3. **Traffic Analysis and Network Performance**
   - Speed Test Analysis

LINKS

1. Trace file for microsoft call : col334-assign1

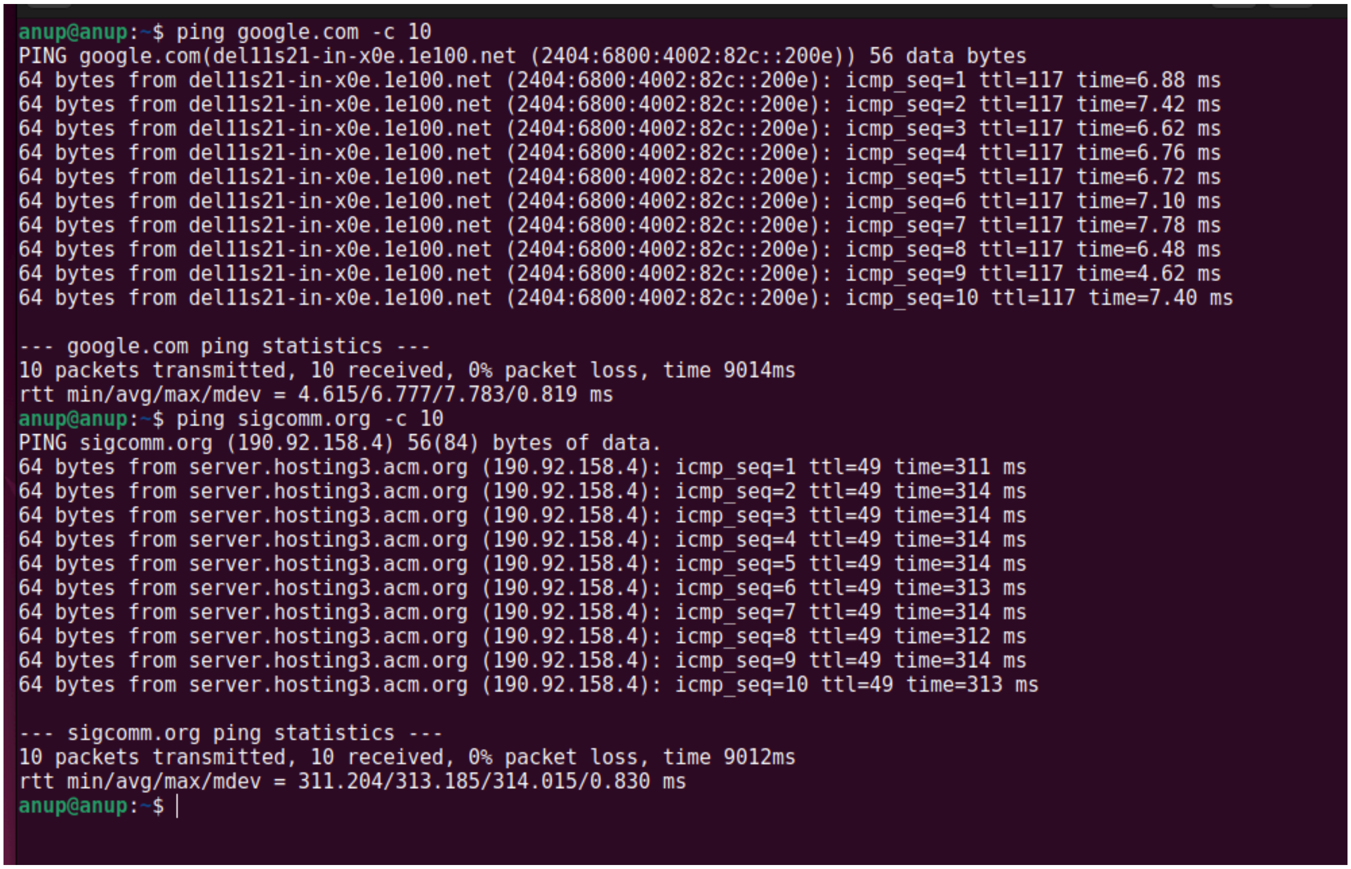
Anup Lal Nayak, 2022CS51827

Measurement Tools

Ping

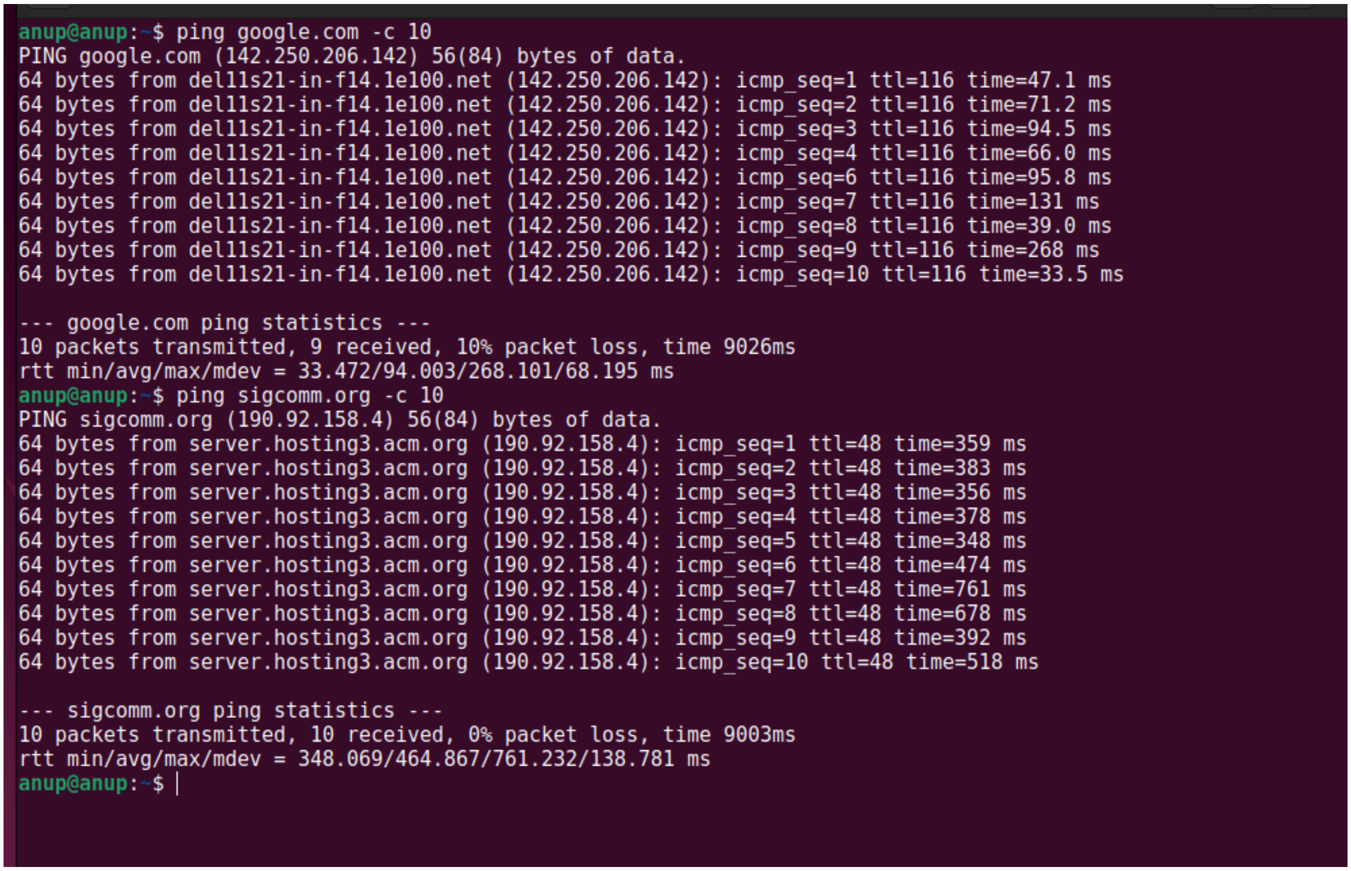
1. Execution:
   - Pings were conducted to google.com and sigcomm.org from two networks: IITD WiFi and a mobile network.
   - 10 pings were sent to each website in both networks.

IITD wifi



```
anup@anup:~$ ping google.com -c 10
PING google.com(del11s21-in-x0e.1e100.net (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=6.88 ms
64 bytes from del11s21-in-x0e.1e100.net (2404:6800:4002:82c::200e): icmp_seq=2 ttl=117 time=7.42 ms
64 bytes from del11s21-in-x0e.1e100.net (2404:6800:4002:82c::200e): icmp_seq=3 ttl=117 time=6.62 ms
64 bytes from del11s21-in-x0e.1e100.net (2404:6800:4002:82c::200e): icmp_seq=4 ttl=117 time=6.76 ms
64 bytes from del11s21-in-x0e.1e100.net (2404:6800:4002:82c::200e): icmp_seq=5 ttl=117 time=6.72 ms
64 bytes from del11s21-in-x0e.1e100.net (2404:6800:4002:82c::200e): icmp_seq=6 ttl=117 time=7.10 ms
64 bytes from del11s21-in-x0e.1e100.net (2404:6800:4002:82c::200e): icmp_seq=7 ttl=117 time=7.78 ms
64 bytes from del11s21-in-x0e.1e100.net (2404:6800:4002:82c::200e): icmp_seq=8 ttl=117 time=6.48 ms
64 bytes from del11s21-in-x0e.1e100.net (2404:6800:4002:82c::200e): icmp_seq=9 ttl=117 time=4.62 ms
64 bytes from del11s21-in-x0e.1e100.net (2404:6800:4002:82c::200e): icmp_seq=10 ttl=117 time=7.40 ms

--- google.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9014ms
rtt min/avg/max/mdev = 4.615/6.777/7.783/0.819 ms
anup@anup:~$ ping sigcomm.org -c 10
PING sigcomm.org (190.92.158.4) 56(84) bytes of data.
64 bytes from server.hosting3.acm.org (190.92.158.4): icmp_seq=1 ttl=49 time=311 ms
64 bytes from server.hosting3.acm.org (190.92.158.4): icmp_seq=2 ttl=49 time=314 ms
64 bytes from server.hosting3.acm.org (190.92.158.4): icmp_seq=3 ttl=49 time=314 ms
64 bytes from server.hosting3.acm.org (190.92.158.4): icmp_seq=4 ttl=49 time=314 ms
64 bytes from server.hosting3.acm.org (190.92.158.4): icmp_seq=5 ttl=49 time=314 ms
64 bytes from server.hosting3.acm.org (190.92.158.4): icmp_seq=6 ttl=49 time=313 ms
64 bytes from server.hosting3.acm.org (190.92.158.4): icmp_seq=7 ttl=49 time=314 ms
64 bytes from server.hosting3.acm.org (190.92.158.4): icmp_seq=8 ttl=49 time=312 ms
64 bytes from server.hosting3.acm.org (190.92.158.4): icmp_seq=9 ttl=49 time=314 ms
64 bytes from server.hosting3.acm.org (190.92.158.4): icmp_seq=10 ttl=49 time=313 ms

--- sigcomm.org ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9012ms
rtt min/avg/max/mdev = 311.204/313.185/314.015/0.830 ms
anup@anup:~$ |
```

Mobile Hotspot



```
anup@anup:~$ ping google.com -c 10
PING google.com (142.250.206.142) 56(84) bytes of data.
64 bytes from del11s21-in-f14.1e100.net (142.250.206.142): icmp_seq=1 ttl=116 time=47.1 ms
64 bytes from del11s21-in-f14.1e100.net (142.250.206.142): icmp_seq=2 ttl=116 time=71.2 ms
64 bytes from del11s21-in-f14.1e100.net (142.250.206.142): icmp_seq=3 ttl=116 time=94.5 ms
64 bytes from del11s21-in-f14.1e100.net (142.250.206.142): icmp_seq=4 ttl=116 time=66.0 ms
64 bytes from del11s21-in-f14.1e100.net (142.250.206.142): icmp_seq=6 ttl=116 time=95.8 ms
64 bytes from del11s21-in-f14.1e100.net (142.250.206.142): icmp_seq=7 ttl=116 time=131 ms
64 bytes from del11s21-in-f14.1e100.net (142.250.206.142): icmp_seq=8 ttl=116 time=39.0 ms
64 bytes from del11s21-in-f14.1e100.net (142.250.206.142): icmp_seq=9 ttl=116 time=268 ms
64 bytes from del11s21-in-f14.1e100.net (142.250.206.142): icmp_seq=10 ttl=116 time=33.5 ms

--- google.com ping statistics ---
10 packets transmitted, 9 received, 10% packet loss, time 9026ms
rtt min/avg/max/mdev = 33.472/94.003/268.101/68.195 ms
anup@anup:~$ ping sigcomm.org -c 10
PING sigcomm.org (190.92.158.4) 56(84) bytes of data.
64 bytes from server.hosting3.acm.org (190.92.158.4): icmp_seq=1 ttl=48 time=359 ms
64 bytes from server.hosting3.acm.org (190.92.158.4): icmp_seq=2 ttl=48 time=383 ms
64 bytes from server.hosting3.acm.org (190.92.158.4): icmp_seq=3 ttl=48 time=356 ms
64 bytes from server.hosting3.acm.org (190.92.158.4): icmp_seq=4 ttl=48 time=378 ms
64 bytes from server.hosting3.acm.org (190.92.158.4): icmp_seq=5 ttl=48 time=348 ms
64 bytes from server.hosting3.acm.org (190.92.158.4): icmp_seq=6 ttl=48 time=474 ms
64 bytes from server.hosting3.acm.org (190.92.158.4): icmp_seq=7 ttl=48 time=761 ms
64 bytes from server.hosting3.acm.org (190.92.158.4): icmp_seq=8 ttl=48 time=678 ms
64 bytes from server.hosting3.acm.org (190.92.158.4): icmp_seq=9 ttl=48 time=392 ms
64 bytes from server.hosting3.acm.org (190.92.158.4): icmp_seq=10 ttl=48 time=518 ms

--- sigcomm.org ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9003ms
rtt min/avg/max/mdev = 348.069/464.867/761.232/138.781 ms
anup@anup:~$ |
```

A. Latency Analysis

Average Latencies:

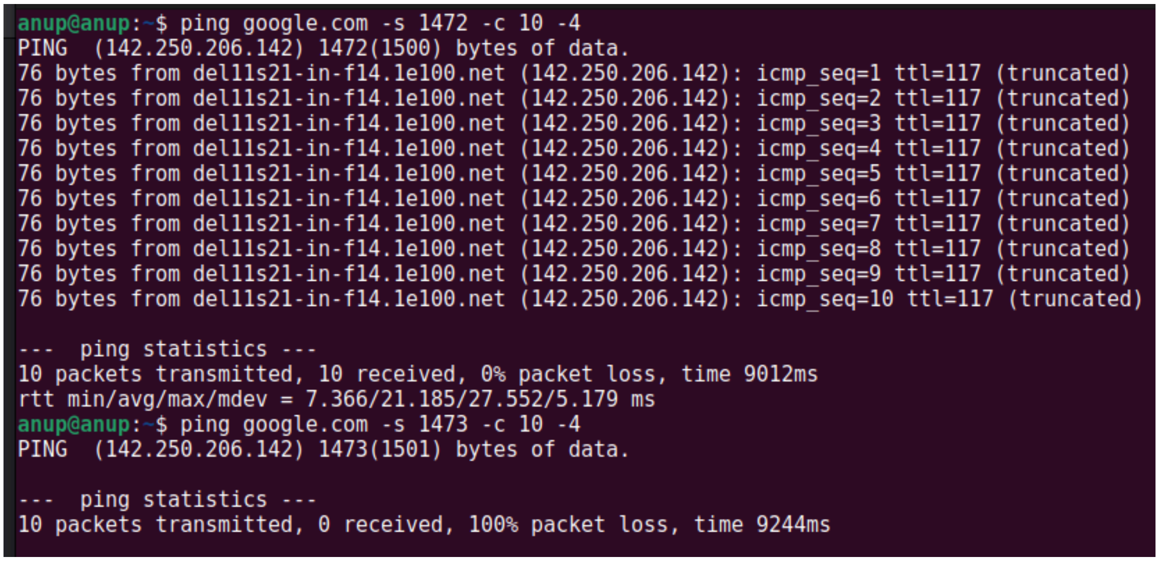
- IITD Network:
    - google.com: 6.78 ms
    - sigcomm.org: 313.18 ms
- Mobile Network:
    - google.com: 94.02 ms
    - sigcomm.org: 761.23 ms

Reasons for Differences:

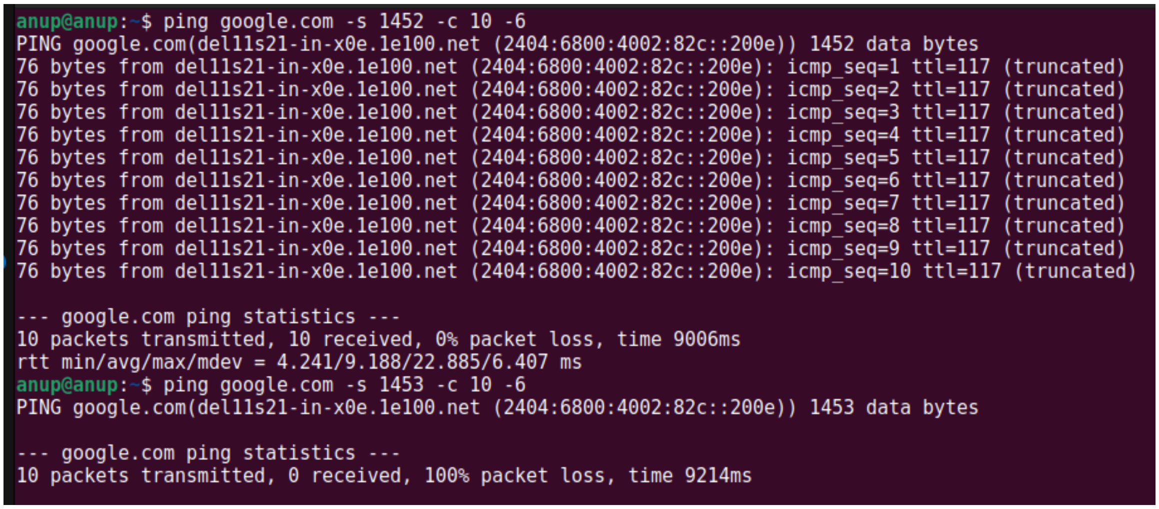
- Differences in average latency could be due to factors such as the geographical distance to the server, network congestion, and the quality of the mobile network.
- Comparison between networks shows higher latency in mobile networks, likely due to higher packet travel times and more routing hops.
- IITD performs faster than mobile data showing better network speed and from traceroute results we can clearly see that IITD wifi chooses a smaller path and hence is much faster.

B. Protocol Analysis

- The ping tool uses the Internet Control Message Protocol (ICMP).
- The theoretical upper limit of the packet size for ping is 65,535 bytes.
- The theoretical upper limit of the packet size for ICMP is 1472 bytes for ipv4 and 1452 for ipv6.
- I was successfully able to ping the websites with theoretical upper limit as these upper limits take into consideration the header overhead and hence MTU is not crossed.



```
anup@anup:~$ ping google.com -s 1472 -c 10 -4
PING  (142.250.206.142) 1472(1500) bytes of data.
76 bytes from del11s21-in-f14.1e100.net (142.250.206.142): icmp_seq=1 ttl=117 (truncated)
76 bytes from del11s21-in-f14.1e100.net (142.250.206.142): icmp_seq=2 ttl=117 (truncated)
76 bytes from del11s21-in-f14.1e100.net (142.250.206.142): icmp_seq=3 ttl=117 (truncated)
76 bytes from del11s21-in-f14.1e100.net (142.250.206.142): icmp_seq=4 ttl=117 (truncated)
76 bytes from del11s21-in-f14.1e100.net (142.250.206.142): icmp_seq=5 ttl=117 (truncated)
76 bytes from del11s21-in-f14.1e100.net (142.250.206.142): icmp_seq=6 ttl=117 (truncated)
76 bytes from del11s21-in-f14.1e100.net (142.250.206.142): icmp_seq=7 ttl=117 (truncated)
76 bytes from del11s21-in-f14.1e100.net (142.250.206.142): icmp_seq=8 ttl=117 (truncated)
76 bytes from del11s21-in-f14.1e100.net (142.250.206.142): icmp_seq=9 ttl=117 (truncated)
76 bytes from del11s21-in-f14.1e100.net (142.250.206.142): icmp_seq=10 ttl=117 (truncated)

---  ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9012ms
rtt min/avg/max/mdev = 7.366/21.185/27.552/5.179 ms
anup@anup:~$ ping google.com -s 1473 -c 10 -4
PING  (142.250.206.142) 1473(1501) bytes of data.

---  ping statistics ---
10 packets transmitted, 0 received, 100% packet loss, time 9244ms
```

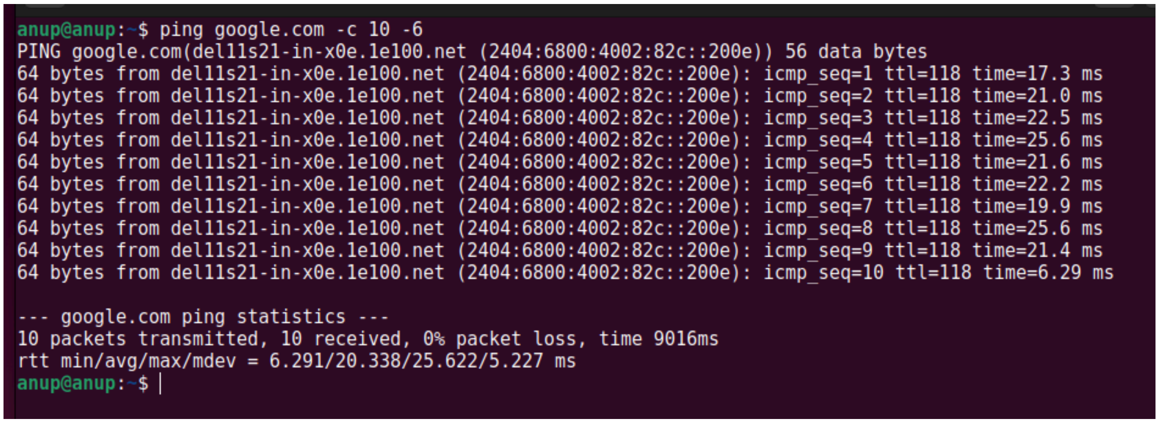


```
anup@anup:~$ ping google.com -s 1452 -c 10 -6
PING google.com(del11s21-in-x0e.1e100.net (2404:6800:4002:82c::200e)) 1452 data bytes
76 bytes from del11s21-in-x0e.1e100.net (2404:6800:4002:82c::200e): icmp_seq=1 ttl=117 (truncated)
76 bytes from del11s21-in-x0e.1e100.net (2404:6800:4002:82c::200e): icmp_seq=2 ttl=117 (truncated)
76 bytes from del11s21-in-x0e.1e100.net (2404:6800:4002:82c::200e): icmp_seq=3 ttl=117 (truncated)
76 bytes from del11s21-in-x0e.1e100.net (2404:6800:4002:82c::200e): icmp_seq=4 ttl=117 (truncated)
76 bytes from del11s21-in-x0e.1e100.net (2404:6800:4002:82c::200e): icmp_seq=5 ttl=117 (truncated)
76 bytes from del11s21-in-x0e.1e100.net (2404:6800:4002:82c::200e): icmp_seq=6 ttl=117 (truncated)
76 bytes from del11s21-in-x0e.1e100.net (2404:6800:4002:82c::200e): icmp_seq=7 ttl=117 (truncated)
76 bytes from del11s21-in-x0e.1e100.net (2404:6800:4002:82c::200e): icmp_seq=8 ttl=117 (truncated)
76 bytes from del11s21-in-x0e.1e100.net (2404:6800:4002:82c::200e): icmp_seq=9 ttl=117 (truncated)
76 bytes from del11s21-in-x0e.1e100.net (2404:6800:4002:82c::200e): icmp_seq=10 ttl=117 (truncated)

--- google.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9006ms
rtt min/avg/max/mdev = 4.241/9.188/22.885/6.407 ms
anup@anup:~$ ping google.com -s 1453 -c 10 -6
PING google.com(del11s21-in-x0e.1e100.net (2404:6800:4002:82c::200e)) 1453 data bytes

--- google.com ping statistics ---
10 packets transmitted, 0 received, 100% packet loss, time 9214ms
```

C. IPv6 Ping

- Forced IPv6 ping was attempted using the -6 option in the ping command.
- Screenshots showing success/failure are attached.

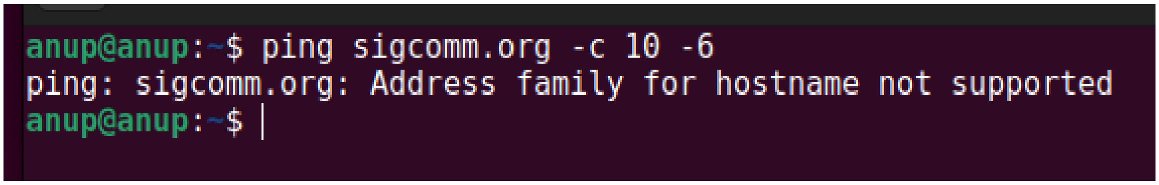
google.com



```
anup@anup:~$ ping google.com -c 10 -6
PING google.com(del11s21-in-x0e.1e100.net (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=118 time=17.3 ms
64 bytes from del11s21-in-x0e.1e100.net (2404:6800:4002:82c::200e): icmp_seq=2 ttl=118 time=21.0 ms
64 bytes from del11s21-in-x0e.1e100.net (2404:6800:4002:82c::200e): icmp_seq=3 ttl=118 time=22.5 ms
64 bytes from del11s21-in-x0e.1e100.net (2404:6800:4002:82c::200e): icmp_seq=4 ttl=118 time=25.6 ms
64 bytes from del11s21-in-x0e.1e100.net (2404:6800:4002:82c::200e): icmp_seq=5 ttl=118 time=21.6 ms
64 bytes from del11s21-in-x0e.1e100.net (2404:6800:4002:82c::200e): icmp_seq=6 ttl=118 time=22.2 ms
64 bytes from del11s21-in-x0e.1e100.net (2404:6800:4002:82c::200e): icmp_seq=7 ttl=118 time=19.9 ms
64 bytes from del11s21-in-x0e.1e100.net (2404:6800:4002:82c::200e): icmp_seq=8 ttl=118 time=25.6 ms
64 bytes from del11s21-in-x0e.1e100.net (2404:6800:4002:82c::200e): icmp_seq=9 ttl=118 time=21.4 ms
64 bytes from del11s21-in-x0e.1e100.net (2404:6800:4002:82c::200e): icmp_seq=10 ttl=118 time=6.29 ms

--- google.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9016ms
rtt min/avg/max/mdev = 6.291/20.338/25.622/5.227 ms
anup@anup:~$ |
```

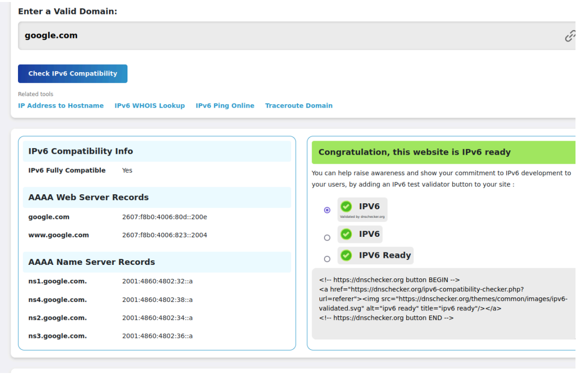
Ipv6 sigcomm

Couldnt ping sigcomm with ipv6 since it does not support ipv6.



```
anup@anup:~$ ping sigcomm.org -c 10 -6
ping: sigcomm.org: Address family for hostname not supported
anup@anup:~$ |
```

PROOF: Google is compatible with ipv6 but sigcomm is not.



Enter a Valid Domain: google.com

IPv6 Compatibility Info

IPv6 Fully Compatible	Yes

AAAA Web Server Records

google.com	2607:f8b0:4006:80d::200e
www.google.com	2607:f8b0:4006:823::2004

AAAA Name Server Records

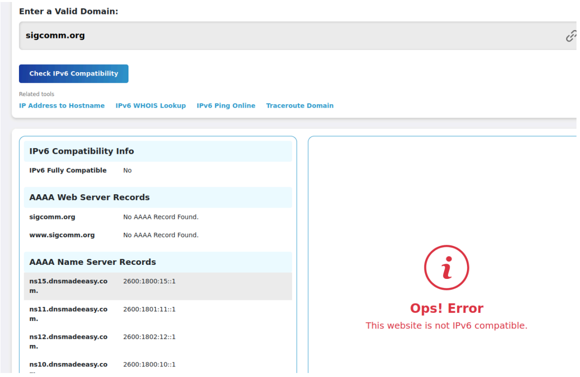
ns1.google.com.	2001:4860:4802:32::a
ns4.google.com.	2001:4860:4802:38::a
ns2.google.com.	2001:4860:4802:34::a
ns3.google.com.	2001:4860:4802:36::a

Congratulation, this website is IPv6 ready

You can help raise awareness and show your commitment to IPv6 development to your users, by adding an IPv6 test validator button to your site :

● IPV6
○ IPV6
○ IPV6 Ready

```
<!-- https://dnschecker.org button BEGIN -->
<a href="https://dnschecker.org/ipv6-compatibility-checker.php?
url=referer"><img src="https://dnschecker.org/themes/common/images/ipv6-
validated.svg" alt="ipv6 ready" title="ipv6 ready"/></a>
<!-- https://dnschecker.org button END -->
```



Enter a Valid Domain: sigcomm.org

IPv6 Compatibility Info

IPv6 Fully Compatible	No

AAAA Web Server Records

sigcomm.org	No AAAA Record Found.
www.sigcomm.org	No AAAA Record Found.

AAAA Name Server Records

ns15.dnsmadeeasy.com.	2600:1800:15::1
ns11.dnsmadeeasy.com.	2600:1801:11::1
ns12.dnsmadeeasy.com.	2600:1802:12::1
ns10.dnsmadeeasy.co	2600:1800:10::1

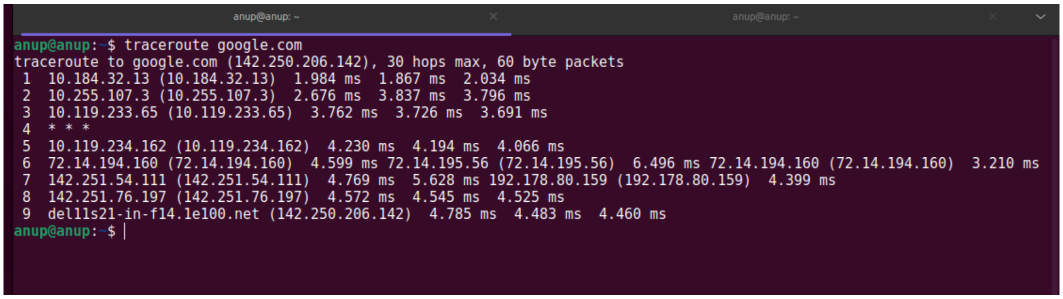
Ops! Error

This website is not IPv6 compatible.

Traceroute

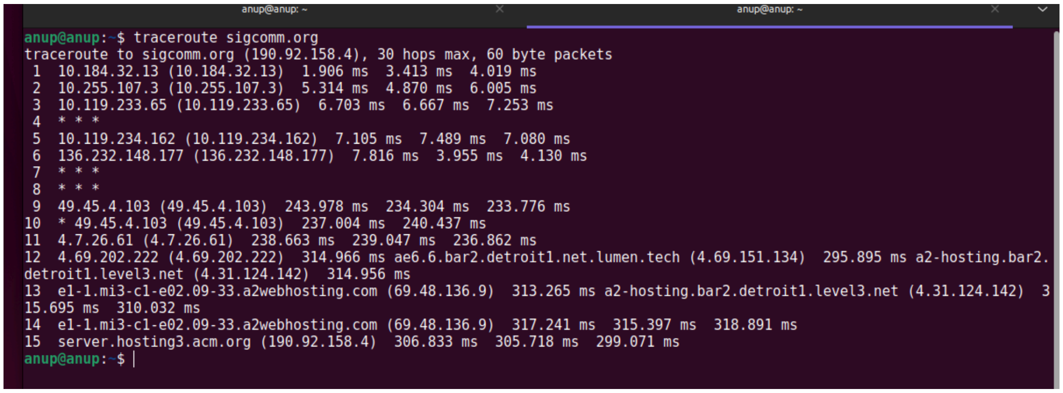
IITD NETWORK

1. google.com



```
anup@anup:~$ traceroute google.com
traceroute to google.com (142.250.206.142), 30 hops max, 60 byte packets
 1  10.184.32.13 (10.184.32.13)  1.984 ms  1.867 ms  2.034 ms
 2  10.255.107.3 (10.255.107.3)  2.676 ms  3.837 ms  3.796 ms
 3  10.119.233.65 (10.119.233.65)  3.762 ms  3.726 ms  3.691 ms
 4  * * *
 5  10.119.234.162 (10.119.234.162)  4.230 ms  4.194 ms  4.066 ms
 6  72.14.194.160 (72.14.194.160)  4.599 ms 72.14.195.56 (72.14.195.56)  6.496 ms 72.14.194.160 (72.14.194.160)  3.210 ms
 7  142.251.54.111 (142.251.54.111)  4.769 ms  5.628 ms 192.178.80.159 (192.178.80.159)  4.399 ms
 8  142.251.76.197 (142.251.76.197)  4.572 ms  4.545 ms  4.525 ms
 9  del11s21-in-f14.1e100.net (142.250.206.142)  4.785 ms  4.483 ms  4.460 ms
anup@anup:~$ |
```

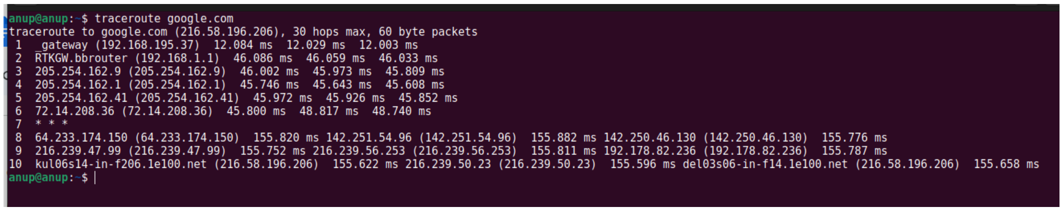
2. sigcomm.org



```
anup@anup:~$ traceroute sigcomm.org
traceroute to sigcomm.org (190.92.158.4), 30 hops max, 60 byte packets
 1  10.184.32.13 (10.184.32.13)  1.906 ms  3.413 ms  4.019 ms
 2  10.255.107.3 (10.255.107.3)  5.314 ms  4.870 ms  6.005 ms
 3  10.119.233.65 (10.119.233.65)  6.703 ms  6.667 ms  7.253 ms
 4  * * *
 5  10.119.234.162 (10.119.234.162)  7.105 ms  7.489 ms  7.080 ms
 6  136.232.148.177 (136.232.148.177)  7.816 ms  3.955 ms  4.130 ms
 7  * * *
 8  * * *
 9  49.45.4.103 (49.45.4.103)  243.978 ms  234.304 ms  233.776 ms
10  * 49.45.4.103 (49.45.4.103)  237.004 ms  240.437 ms
11  4.7.26.61 (4.7.26.61)  238.663 ms  239.047 ms  236.862 ms
12  4.69.202.222 (4.69.202.222)  314.966 ms ae6.6.bar2.detroit1.net.lumen.tech (4.69.151.134)  295.895 ms a2-hosting.bar2.
detroit1.level3.net (4.31.124.142)  314.956 ms
13  e1-1.mi3-c1-e02.09-33.a2webhosting.com (69.48.136.9)  313.265 ms a2-hosting.bar2.detroit1.level3.net (4.31.124.142)  3
15.695 ms  310.032 ms
14  e1-1.mi3-c1-e02.09-33.a2webhosting.com (69.48.136.9)  317.241 ms  315.397 ms  318.891 ms
15  server.hosting3.acm.org (190.92.158.4)  306.833 ms  305.718 ms  299.071 ms
anup@anup:~$ |
```

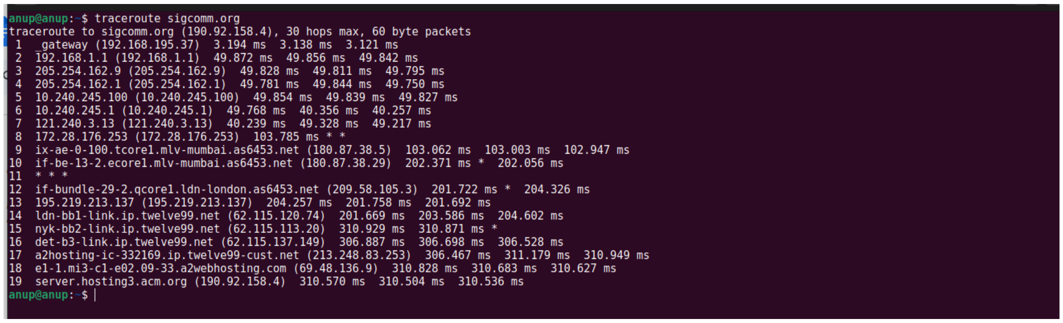
MOBILE HOTSPOT

1. google.com



```
anup@anup:~$ traceroute google.com
traceroute to google.com (216.58.196.206), 30 hops max, 60 byte packets
 1  _gateway (192.168.195.37)  12.084 ms  12.029 ms  12.003 ms
 2  RTKGW.bbrouter (192.168.1.1)  46.086 ms  46.059 ms  46.033 ms
 3  205.254.162.9 (205.254.162.9)  46.002 ms  45.973 ms  45.809 ms
 4  205.254.162.1 (205.254.162.1)  45.746 ms  45.643 ms  45.608 ms
 5  205.254.162.41 (205.254.162.41)  45.972 ms  45.926 ms  45.852 ms
 6  72.14.208.36 (72.14.208.36)  45.800 ms  48.817 ms  48.740 ms
 7  * * *
 8  64.233.174.150 (64.233.174.150)  155.820 ms 142.251.54.96 (142.251.54.96)  155.882 ms 142.250.46.130 (142.250.46.130)  155.776 ms
 9  216.239.47.99 (216.239.47.99)  155.752 ms 216.239.56.253 (216.239.56.253)  155.811 ms 192.178.82.236 (192.178.82.236)  155.787 ms
10  kul06s14-in-f206.1e100.net (216.58.196.206)  155.622 ms 216.239.50.23 (216.239.50.23)  155.596 ms del03s06-in-f14.1e100.net (216.58.196.206)  155.658 ms
anup@anup:~$ |
```

2. sigcomm.org



```
anup@anup:~$ traceroute sigcomm.org
traceroute to sigcomm.org (190.92.158.4), 30 hops max, 60 byte packets
 1  _gateway (192.168.195.37)  3.194 ms  3.138 ms  3.121 ms
 2  192.168.1.1 (192.168.1.1)  49.872 ms  49.856 ms  49.842 ms
 3  205.254.162.9 (205.254.162.9)  49.828 ms  49.811 ms  49.795 ms
 4  205.254.162.1 (205.254.162.1)  49.781 ms  49.844 ms  49.750 ms
 5  10.240.245.100 (10.240.245.100)  49.854 ms  49.839 ms  49.827 ms
 6  10.240.245.1 (10.240.245.1)  49.768 ms  40.356 ms  40.257 ms
 7  121.240.3.13 (121.240.3.13)  40.239 ms  49.328 ms  49.217 ms
 8  172.28.176.253 (172.28.176.253)  103.785 ms * *
 9  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net (180.87.38.5)  103.062 ms  103.003 ms  102.947 ms
10  if-be-13-2.ecore1.mlv-mumbai.as6453.net (180.87.38.29)  202.371 ms *  202.056 ms
11  * * *
12  if-bundle-29-2.qcore1.ldn-london.as6453.net (209.58.105.3)  201.722 ms *  204.326 ms
13  195.219.213.137 (195.219.213.137)  204.257 ms  201.758 ms  201.692 ms
14  ldn-bb1-link.ip.twelve99.net (62.115.120.74)  201.669 ms  203.586 ms  204.602 ms
15  nyk-bb2-link.ip.twelve99.net (62.115.113.20)  310.929 ms  310.871 ms *
16  det-b3-link.ip.twelve99.net (62.115.137.149)  306.887 ms  306.698 ms  306.528 ms
17  a2hosting-ic-332169.ip.twelve99-cust.net (213.248.83.253)  306.467 ms  311.179 ms  310.949 ms
18  e1-1.mi3-c1-e02.09-33.a2webhosting.com (69.48.136.9)  310.828 ms  310.683 ms  310.627 ms
19  server.hosting3.acm.org (190.92.158.4)  310.570 ms  310.504 ms  310.536 ms
anup@anup:~$ |
```

A. IP Hops and Autonomous systems

Hop Count:

- Number of Hops:
    - IITD Network:
        - google.com: 9 hops
        - sigcomm.org: 15 hops
    - Mobile Network:
        - google.com: 10 hops
        - sigcomm.org: 19 hops

Autonomous systems:

IITD

1. google.com

Private IPs

72.14.194.160	AS -15169	Google
142.251.54.111	AS -15169	Google
142.251.76.197	AS -15169	Google
142.250.206.142	AS- 15169	Google

2. sigcomm.org

Private IPs

136.232.148.177	AS- 55836	RELIANCEJIO-IN Reliance Jio Infocom Limited, IN
4.7.26.61	AS-3356	LEVEL3
4.69.202.222	AS-3356	LEVEL3
4.31.124.142	AS-3356	LEVEL3
190.92.158.4	AS-55293	A2HOSTING

Mobile Data

1. google.com

205.254.162.9	AS-133982	EXCITEL-AS-IN Excitel Broadband Private Limited, IN
64.233.174.150	AS-15169	GOOGLE
216.239.47.99	AS- 15169	GOOGLE
216.58.200.206	AS- 15169	GOOGLE

2. sigcomm.org

205.254.162.9	AS-133982	EXCITEL-AS-IN Excitel Broadband Private Limited, IN
121.240.3.13	AS-4755	TATACOMM-AS TATA Communications formerly VSNL is Leading ISP, IN
180.87.38.5	AS-6453	AS6453
62.115.120.74	AS-1299	TWELVE99 Arelion, fka Telia Carrier, SE
38.142.132.58	AS-174	COGENT-174
69.48.136.9	AS-55293	A2HOSTING190.92.158.4 AS-55293 A2HOSTING

B. ‘*’ in traceroute output

Yes, ‘*’ is observed in traceroute results. In a traceroute output, an asterisk typically indicates that the probe packet sent to a particular hop along the route did not receive a response within the timeout period. This can happen for several reasons:

1. **Packet Loss:** The packet might have been dropped due to network congestion or other issues.
2. **Firewall or Security Settings:** Some routers or devices may be configured to block ICMP or UDP responses, which are commonly used in traceroute operations. As a result, they do not reply to the probe packets.
3. **Rate Limiting:** Some routers are set up to limit the number of responses they send to traceroute probes to avoid being overwhelmed by excessive requests.
4. **Non-Responsive Device:** The device might not be configured to respond to traceroute requests, or it might simply be ignoring them.

C. Multiple IP Addresses

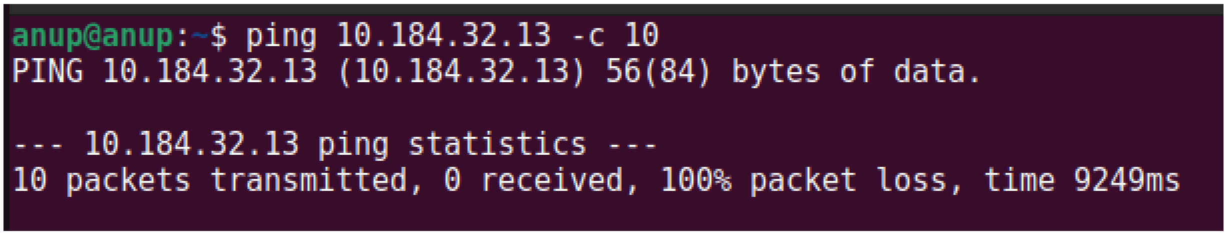
Yes, multiple IP addresses can appear at the same hop count in a network trace. This happens because:

1. **Load Balancing**: Traffic is spread across different paths that have the same hop count.
2. **Redundancy**: Networks often have backup routes, leading to different IPs showing up at the same hop.
3. **Dynamic Routing**: The network may change paths on the fly, so different IPs might appear in the same position.
4. **Anycast**: Multiple devices might share the same IP but show up with different addresses depending on the path.

These factors make it normal to see different IP addresses at the same hop in a trace.

D. First Hop router

IP address of first hop router : 10.184.32.13



```
anup@anup:~$ ping 10.184.32.13 -c 10
PING 10.184.32.13 (10.184.32.13) 56(84) bytes of data.

--- 10.184.32.13 ping statistics ---
10 packets transmitted, 0 received, 100% packet loss, time 9249ms
```

- Mobile data ping response to this IP: Expected to fail due to network restrictions or different routing paths. This IP address can be accessed by IITD internet only according to me.
- This IP address is restricted to the IITD network only and hence cannot be accessed by mobile data, just like academic erp, etc.

E. Internet Architecture

IITD network:

google.com -> 2 Tier (IITD, Google)

sigcomm.org -> 3 Tier (IITD, Reliance, Sigcomm[A2 hosting])

Mobile Hotspot:

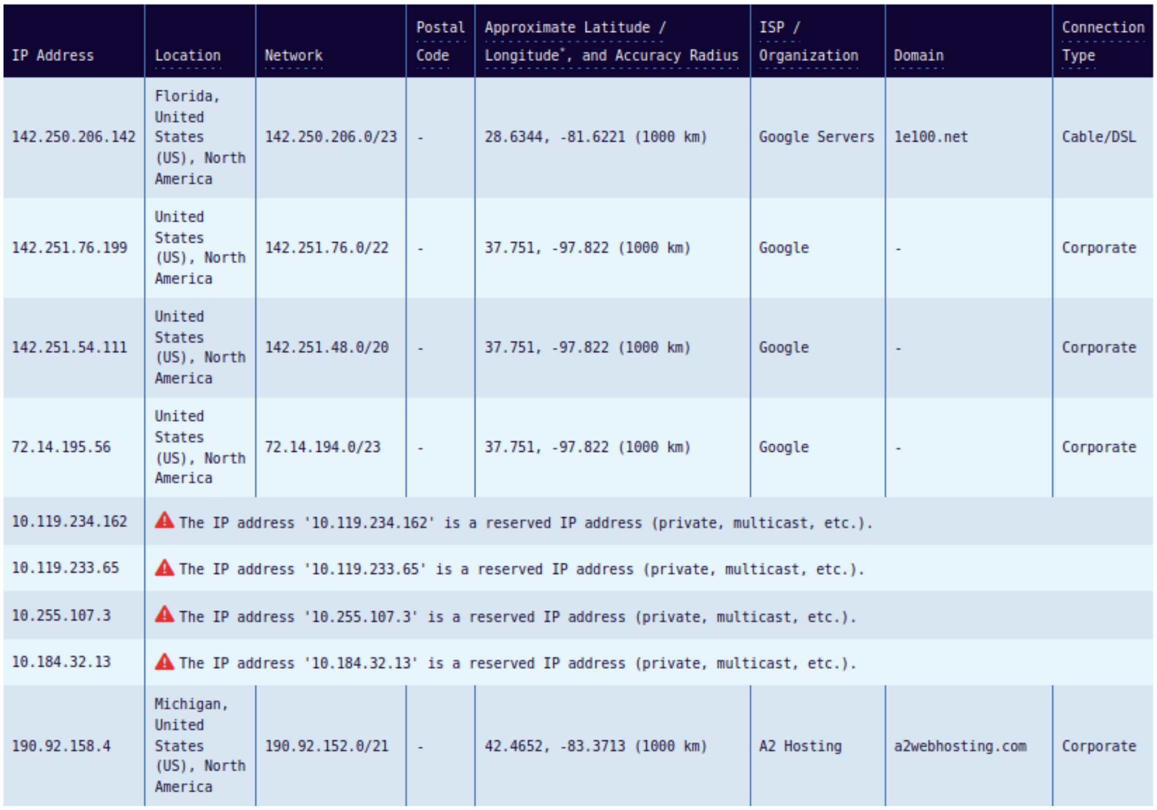
google.com -> 2 Tier (EXCITEL, Google)

sigcomm.org -> 3 Tier (EXCITEL, TATA, Sigcomm[A2 hosting])

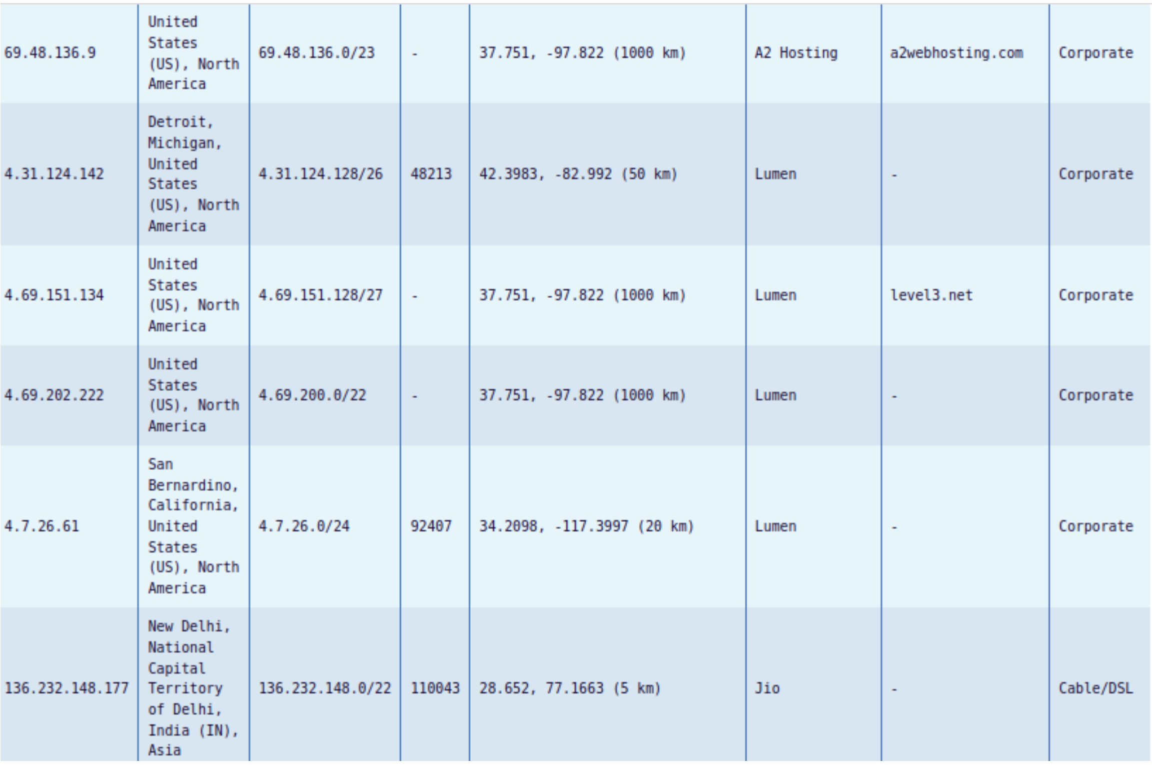
Since Google is highly connected to regional ISPs directly as a content ISP, as discussed in class, in case of google we see only 2 Tiers.

F. Geolocation of IPs

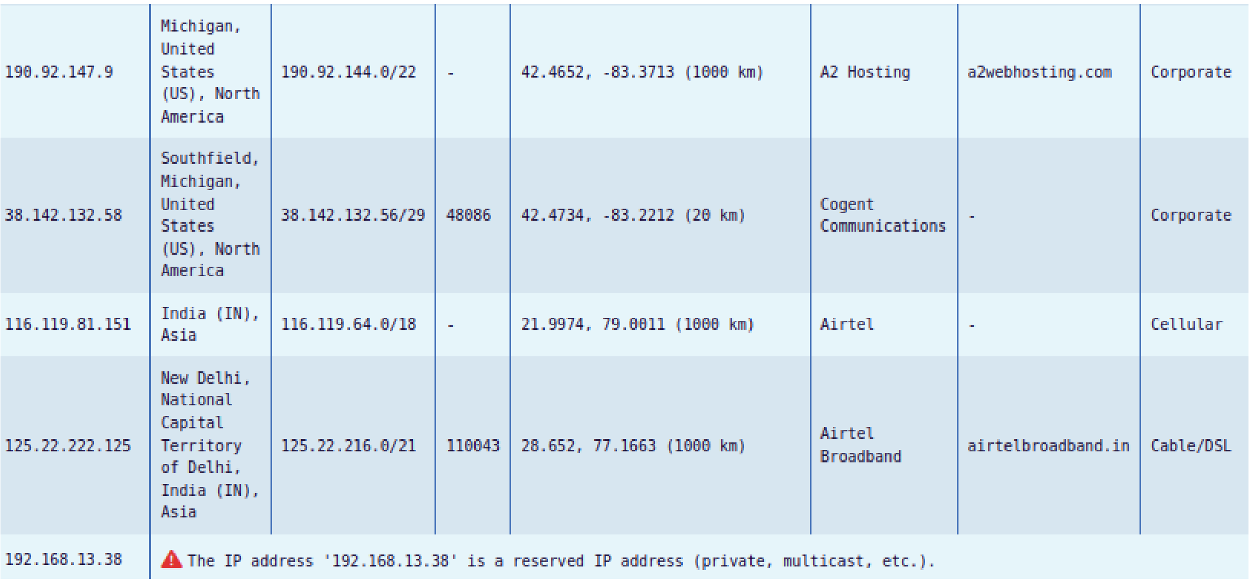
- maxmind database (cross checked with reverse DNS lookup)



IP Address	Location	Network	Postal Code	Approximate Latitude / Longitude*, and Accuracy Radius	ISP / Organization	Domain	Connection Type
142.250.206.142	Florida, United States (US), North America	142.250.206.0/23	-	28.6344, -81.6221 (1000 km)	Google Servers	1e100.net	Cable/DSL
142.251.76.199	United States (US), North America	142.251.76.0/22	-	37.751, -97.822 (1000 km)	Google	-	Corporate
142.251.54.111	United States (US), North America	142.251.48.0/20	-	37.751, -97.822 (1000 km)	Google	-	Corporate
72.14.195.56	United States (US), North America	72.14.194.0/23	-	37.751, -97.822 (1000 km)	Google	-	Corporate
10.119.234.162	⚠ The IP address '10.119.234.162' is a reserved IP address (private, multicast, etc.).						
10.119.233.65	⚠ The IP address '10.119.233.65' is a reserved IP address (private, multicast, etc.).						
10.255.107.3	⚠ The IP address '10.255.107.3' is a reserved IP address (private, multicast, etc.).						
10.184.32.13	⚠ The IP address '10.184.32.13' is a reserved IP address (private, multicast, etc.).						
190.92.158.4	Michigan, United States (US), North America	190.92.152.0/21	-	42.4652, -83.3713 (1000 km)	A2 Hosting	a2webhosting.com	Corporate



69.48.136.9	United States (US), North America	69.48.136.0/23	-	37.751, -97.822 (1000 km)	A2 Hosting	a2webhosting.com	Corporate
4.31.124.142	Detroit, Michigan, United States (US), North America	4.31.124.128/26	48213	42.3983, -82.992 (50 km)	Lumen	-	Corporate
4.69.151.134	United States (US), North America	4.69.151.128/27	-	37.751, -97.822 (1000 km)	Lumen	level3.net	Corporate
4.69.202.222	United States (US), North America	4.69.200.0/22	-	37.751, -97.822 (1000 km)	Lumen	-	Corporate
4.7.26.61	San Bernardino, California, United States (US), North America	4.7.26.0/24	92407	34.2098, -117.3997 (20 km)	Lumen	-	Corporate
136.232.148.177	New Delhi, National Capital Territory of Delhi, India (IN), Asia	136.232.148.0/22	110043	28.652, 77.1663 (5 km)	Jio	-	Cable/DSL



190.92.147.9	Michigan, United States (US), North America	190.92.144.0/22	-	42.4652, -83.3713 (1000 km)	A2 Hosting	a2webhosting.com	Corporate
38.142.132.58	Southfield, Michigan, United States (US), North America	38.142.132.56/29	48086	42.4734, -83.2212 (20 km)	Cogent Communications	-	Corporate
116.119.81.151	India (IN), Asia	116.119.64.0/18	-	21.9974, 79.0011 (1000 km)	Airtel	-	Cellular
125.22.222.125	New Delhi, National Capital Territory of Delhi, India (IN), Asia	125.22.216.0/21	110043	28.652, 77.1663 (1000 km)	Airtel Broadband	airtelbroadband.in	Cable/DSL
192.168.13.38	⚠ The IP address '192.168.13.38' is a reserved IP address (private, multicast, etc.).						

Geographical Path and RTT Analysis

When comparing the geographical path with the observed Round-Trip Times (RTTs), there's a noticeable pattern: as the location of the IP addresses gets farther away from New Delhi, the RTT increases. This makes sense because, generally, the farther data has to travel, the longer it takes, leading to higher RTTs. This relationship between distance and RTT matches what you'd expect based on how networks operate, where longer distances and more network hops naturally introduce more delay.

Network Data Collection and Header Analysis

B) Protocols Used During the Meeting:

Network Layer Protocols Used:
- ICMPv6
- IGMP
- ARP

Transport Layer Protocols Used:
- TCP
- UDP
- TLS

Application Layer Protocols Used:
- STUN
- RTCP
- NTP
- MDNS
- DNS

Packet Distribution:
- UDP – 99.3% (48,384 Packets)
- STUN – 50.2% (22,191 Packets)
- RTCP – 1.2% (518 Packets)
- ARP – 0.1% (46 Packets)
- IGMPv3 – 0.01% (2 Packets)
- ICMPv6 – 0.01% (1 Packet)
- MDNS – 0.01% (2 Packets)
- TLS – 0.1% (48 Packets)
- TCP – 0.6% (280 Packets)
- DNS – 0.03% (6 Packets)

C) Host Connection Analysis:

No there is no direct connection between the two hosts.
Endpoint for one host is 52.113.11.11 or 52.113.11.19. It is a Microsoft datacentre in Pune.
Endpoint for the other host is 52.113.11.11 or 52.113.11.19(Same as Above).
Yes, the endpoint for each host is same. It means that we are connected to the same datacentre in Pune which hosts the meeting for us. The meeting call is centralized and thus ensures reliable connectivity by hosting at a datacentre instead at one participant.

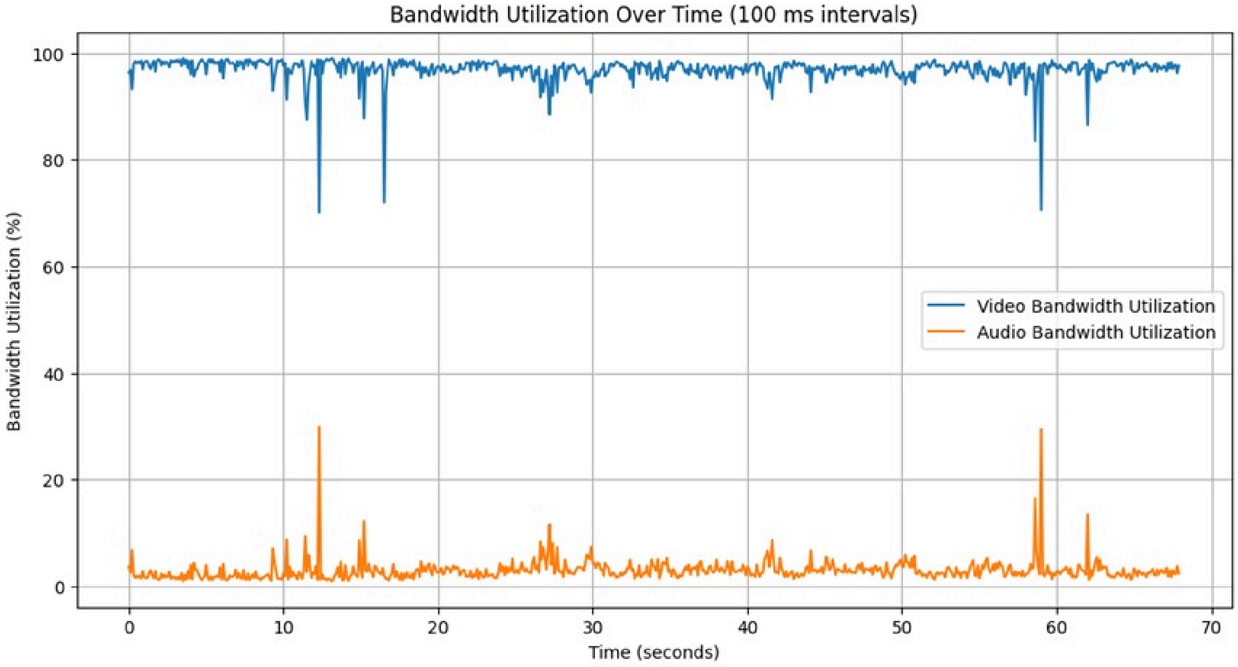
D) Port Analysis for Teams Meeting:

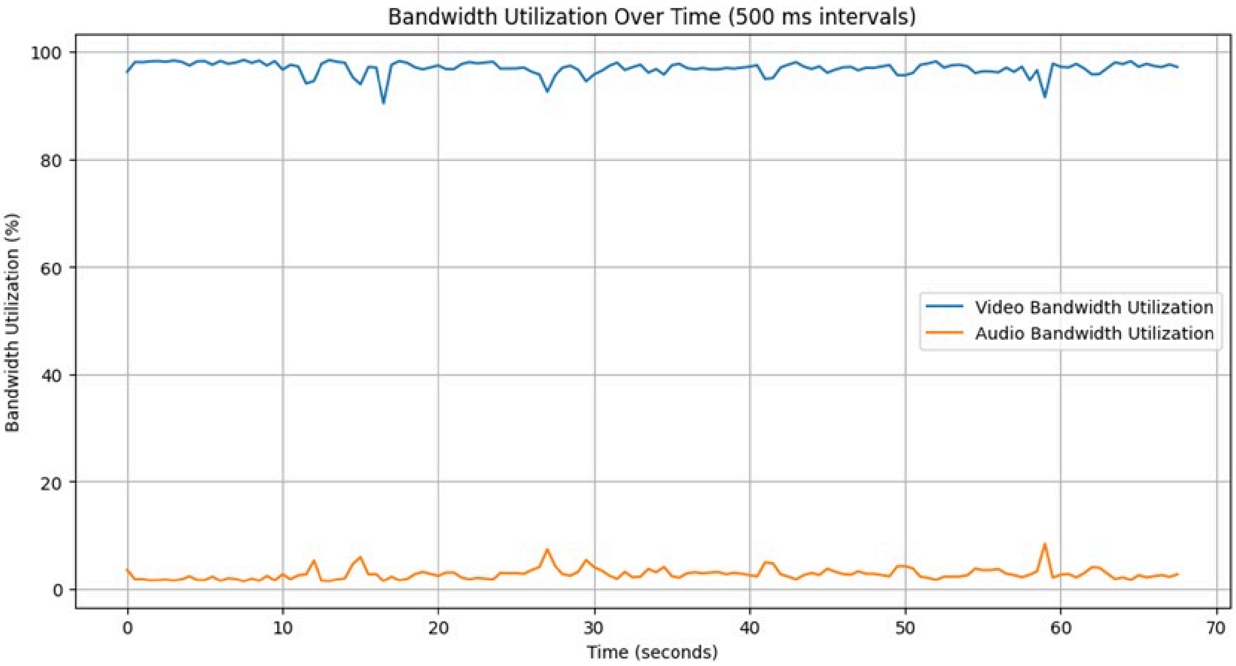
According to Microsoft documentation, Teams meeting audio packets are transmitted over UDP ports 50000-50019, while video packets are transmitted over UDP ports 50020-50039.

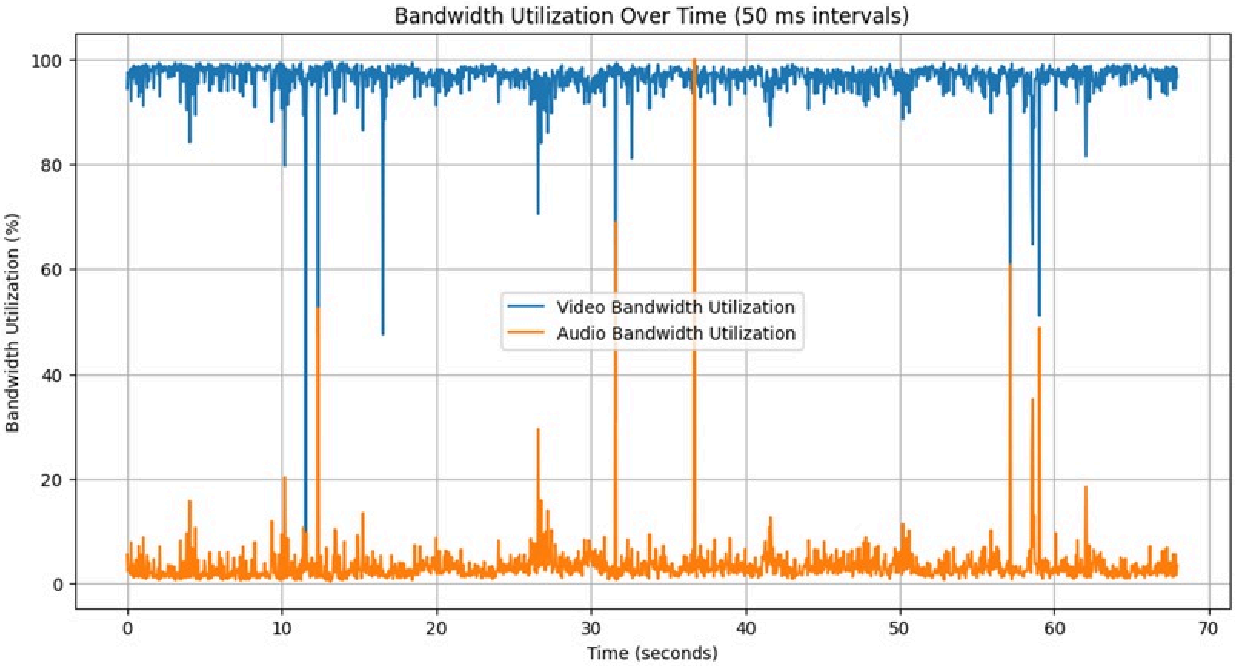
In this case:
- Audio packets are sent through port 50016, totaling 7,195 packets.
- Video packets are sent through port 50020, totaling 36,628 packets.

Steps to Plot Bandwidth Utilization:
1. Apply the appropriate filters and export the packets as CSV files for both audio and video. Export all packets as CSV as well.
2. Use Python to distribute the packets into time intervals (e.g., 100ms, 500ms, 50ms) and plot a graph showing the percentage of packets used for video and audio during those intervals using PyPlot.

Filters used in WinShark:
Audio filters = ((udp.srcport>= 50000) &&(udp.srcport<=5019)) || ((udp.dstport>=50000) &&(udp.dstport <=50019)).
Video filters = ((udp.srcport>= 50020) &&(udp.srcport<=5039)) || ((udp.dstport>=50020) &&(udp.dstport <=50039)).




Bandwidth Utilization Over Time (500 ms intervals)
Bandwidth Utilization (%)
Time (seconds)
0
20
40
60
80
100
0
10
20
30
40
50
60
70
Video Bandwidth Utilization
Audio Bandwidth Utilization


Bandwidth Utilization Over Time (50 ms intervals)
Bandwidth Utilization (%)
Time (seconds)
0
20
40
60
80
100
0
10
20
30
40
50
60
70
Video Bandwidth Utilization
Audio Bandwidth Utilization

Traffic Analysis and Network Performance

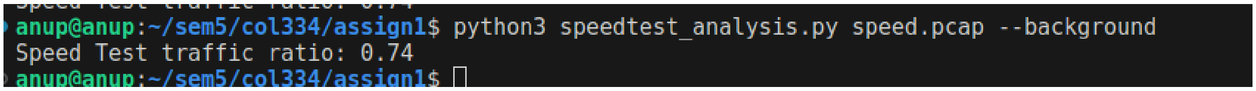
Overview of Code:

1. Find out Client and Server ISP:
   As observed from the trace file, and also by doing a speed test on my laptop and observing the pcap file, I could concur the type of protocols used during the test. Also, the IP with highest frequency in conversation could be chosen as client, and second highest as server, rest is background traffic.
2. Parse the pcap file:
   Parsed the pcap file and completed primary filtering of only IP conversations. Stored conversations between client and server in download and upload arrays respectively.
3. Filtering the download and upload data:
   Filtered out noise data values from upload/download vector by applying a filter of atleast 1Mbps speed during the speed test.
4. Plotting the throughput:
   Plotted the primarily filtered data (bytes) w.r.t time for both upload and download cases.
5. Found out speed test traffic to total traffic ratio using the filtered data.
6. Calculated the throughput values using the filtered data and corresponding time intervals.

A. Isolating Speed Test Traffic

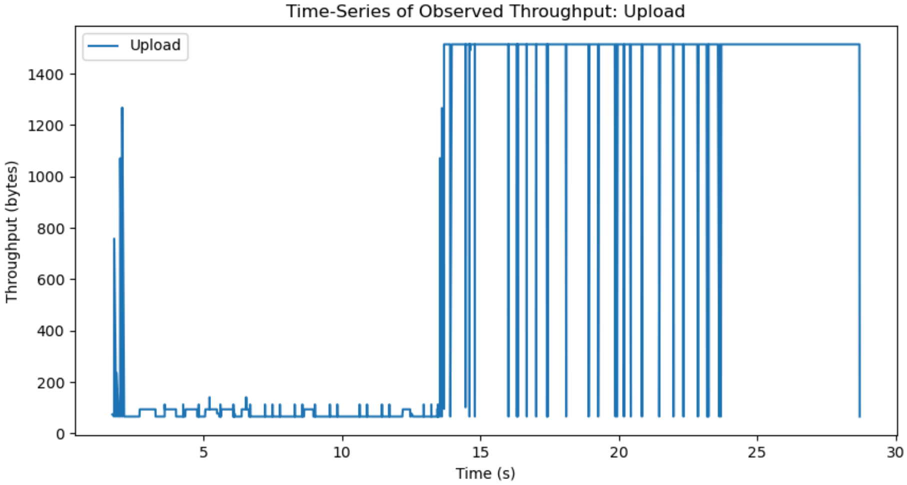
- speed test traffic ratio was calculated as (speed test traffic/(speed test traffic+backgrounf traffic)
- speed test traffic was filtered out of total traffic as times when total upload/download speeds are >= 1 Mbps
- all the intervals satisfying the above condition and conversation is between server_ip and client_ip is considered as speed test traffic.

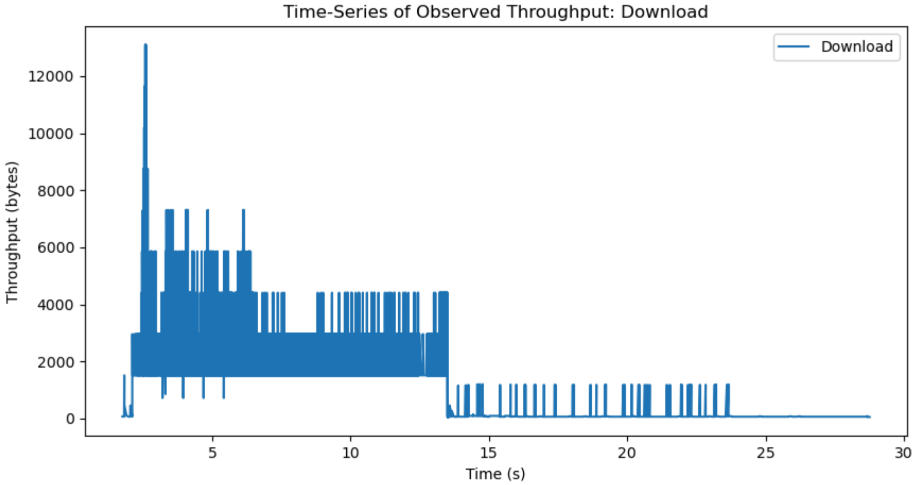
For the given pcap file, speed test traffic ratio was 0.74



```
Speed Test traffic ratio: 0.74
anup@anup:~/sem5/col334/assign1$ python3 speedtest_analysis.py speed.pcap --background
Speed Test traffic ratio: 0.74
anup@anup:~/sem5/col334/assign1$ 
```

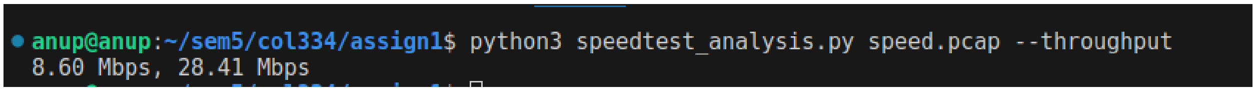
B. Time-Series Plot





C. Average Speeds

- Upload speed: 8.60 Mbps, Download speed: 28.41 Mbps



```
● anup@anup:~/sem5/col334/assign1$ python3 speedtest_analysis.py speed.pcap --throughput
  8.60 Mbps, 28.41 Mbps
```