

COL334 Assignment 1

Yash Bansal
2022CS51133

August 19, 2024

1 Measurement tools

1.1 Ping

1.1.1 Part A

```
yash@bansalss-MacBook-Air ~ % ping -c 10 google.com
PING google.com (142.250.286.142): 56 data bytes
64 bytes from 142.250.286.142: icmp_seq=0 ttl=117 time=8.179 ms
64 bytes from 142.250.286.142: icmp_seq=1 ttl=117 time=15.885 ms
64 bytes from 142.250.286.142: icmp_seq=2 ttl=117 time=15.882 ms
64 bytes from 142.250.286.142: icmp_seq=3 ttl=117 time=17.001 ms
64 bytes from 142.250.286.142: icmp_seq=4 ttl=117 time=15.720 ms
64 bytes from 142.250.286.142: icmp_seq=5 ttl=117 time=17.938 ms
64 bytes from 142.250.286.142: icmp_seq=6 ttl=117 time=15.038 ms
64 bytes from 142.250.286.142: icmp_seq=7 ttl=117 time=15.769 ms
64 bytes from 142.250.286.142: icmp_seq=8 ttl=117 time=14.236 ms
64 bytes from 142.250.286.142: icmp_seq=9 ttl=117 time=17.734 ms
--- google.com ping statistics ---
10 packets transmitted, 10 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 7.930/14.337/17.734/3.269 ms
yash@bansalss-MacBook-Air ~ |
```

google.com: avg. ping:- 14.33 ms

```
yash@bansalss-MacBook-Air ~ % ping -c 10 sigcomm.org
PING sigcomm.org (190.92.158.4): 56 data bytes
64 bytes from 190.92.158.4: icmp_seq=0 ttl=49 time=345.474 ms
64 bytes from 190.92.158.4: icmp_seq=1 ttl=49 time=364.350 ms
64 bytes from 190.92.158.4: icmp_seq=2 ttl=49 time=383.473 ms
64 bytes from 190.92.158.4: icmp_seq=3 ttl=49 time=401.950 ms
64 bytes from 190.92.158.4: icmp_seq=4 ttl=49 time=420.011 ms
64 bytes from 190.92.158.4: icmp_seq=5 ttl=49 time=337.001 ms
64 bytes from 190.92.158.4: icmp_seq=6 ttl=49 time=355.598 ms
64 bytes from 190.92.158.4: icmp_seq=7 ttl=49 time=375.736 ms
64 bytes from 190.92.158.4: icmp_seq=8 ttl=49 time=496.896 ms
64 bytes from 190.92.158.4: icmp_seq=9 ttl=49 time=413.682 ms
--- sigcomm.org ping statistics ---
10 packets transmitted, 10 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 337.001/389.416/496.896/44.617 ms
yash@bansalss-MacBook-Air ~ |
```

sigcomm.org: avg. ping:- 389.41 ms

Ping from IITD Network using IPv4

```
yash@bansalss-MacBook-Air ~ % ping -c 10 google.com
PING google.com (142.250.193.46): 56 data bytes
64 bytes from 142.250.193.46: icmp_seq=0 ttl=112 time=40.021 ms
64 bytes from 142.250.193.46: icmp_seq=1 ttl=112 time=34.117 ms
64 bytes from 142.250.193.46: icmp_seq=2 ttl=112 time=38.778 ms
64 bytes from 142.250.193.46: icmp_seq=3 ttl=112 time=42.748 ms
64 bytes from 142.250.193.46: icmp_seq=4 ttl=112 time=155.928 ms
64 bytes from 142.250.193.46: icmp_seq=5 ttl=112 time=73.104 ms
64 bytes from 142.250.193.46: icmp_seq=6 ttl=112 time=83.729 ms
64 bytes from 142.250.193.46: icmp_seq=7 ttl=112 time=69.727 ms
64 bytes from 142.250.193.46: icmp_seq=8 ttl=112 time=62.283 ms
64 bytes from 142.250.193.46: icmp_seq=9 ttl=112 time=68.571 ms
--- google.com ping statistics ---
10 packets transmitted, 10 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 34.117/66.901/155.928/33.840 ms
yash@bansalss-MacBook-Air ~ |
```

google.com: avg. ping:- 66.90 ms

```
yash@bansalss-MacBook-Air ~ % ping -c 10 sigcomm.org
PING sigcomm.org (190.92.158.4): 56 data bytes
64 bytes from 190.92.158.4: icmp_seq=0 ttl=46 time=613.143 ms
64 bytes from 190.92.158.4: icmp_seq=1 ttl=46 time=427.680 ms
64 bytes from 190.92.158.4: icmp_seq=2 ttl=46 time=350.316 ms
64 bytes from 190.92.158.4: icmp_seq=3 ttl=46 time=362.499 ms
64 bytes from 190.92.158.4: icmp_seq=4 ttl=46 time=381.719 ms
64 bytes from 190.92.158.4: icmp_seq=5 ttl=46 time=685.179 ms
64 bytes from 190.92.158.4: icmp_seq=6 ttl=46 time=623.885 ms
64 bytes from 190.92.158.4: icmp_seq=7 ttl=46 time=540.161 ms
64 bytes from 190.92.158.4: icmp_seq=8 ttl=46 time=486.761 ms
64 bytes from 190.92.158.4: icmp_seq=9 ttl=46 time=475.578 ms
--- sigcomm.org ping statistics ---
10 packets transmitted, 10 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 350.316/483.692/623.885/100.580 ms
yash@bansalss-MacBook-Air ~ |
```

sigcomm.org: avg. ping:- 483.69 ms

Ping from personal network using IPv4

Observations:-

1. The average ping latency for sigcomm.org is much higher than that of google.com. It could be because, on referring to traceroute results, fewer hops are required to reach google.com for both networks, as compared to sigcomm.org.
 - One reason for this can be peering with many networks by Google, which results in a smaller route.
 - Also, for sigcomm.org, there are a set of last few hops having similar IP addresses, which have a huge latency for traceroute. So, this slower internal network of sigcomm.org results in a higher ping.
2. The average ping latency for the IITD network is less than that of the personal network for both websites.
 - It is because, on seeing traceroute results, the IITD network is taking fewer hops to reach the destination website than the personal network, resulting in low ping latency for the IITD network.
 - Another reason could be the bandwidth of the network. IITD networks have higher individual bandwidth than personal networks, which have lower individual bandwidth due to more users.

1.1.2 Part B

1. The ping commands in the attached screenshots above use item IPv4 and ICMP(Internet Control Message Protocol) protocols. The following attached wireshark screenshot for the ping packet can also verify it.

The Wireshark screenshot displays a sequence of network frames. It shows five ICMP echo request (ping) frames (Frame 131 to 135) and three ICMP echo reply frames (Frame 132 to 134). The source IP for the requests is 10.184.36.66 and the destination IP for the replies is 10.184.36.66. The protocol headers and payload are visible, confirming the ICMP protocol used for the ping operation.

Wireshark screenshot for google.com ping packet

- When using ping, an ICMP echo request packet is sent to the target IP address. It requests the target to send an ICMP echo reply.
 - After the reply packet is received, the source machine calculates the round-trip time(RTT) to return the ping latency.
 - If the destination source is unavailable/configured not to reply to ICMP echo request, the request timed out is shown by the source machine.
 - All these addressing and routings are done using the IPv4 protocol, so changing the network protocol can also change the ping latency due to efficient headers and implementations.
2. The packet size for the ping requests is 64 bytes using IPv4 ping protocol (98 bytes, including headers, as detected by Wireshark).
 - The maximum packet size for an IPv4 packet can be 65,535 bytes with a 28-byte header. So, theoretically, ping packets can be as large as 65,507 bytes. But, normally, we need to keep the packet size as small as possible, as we need the RTT using ping, so just the required data is kept in the ping packet, namely source and destination IPs and the protocol headers.
 - No, I cannot ping with theoretical maximum packet size, as it is just theoretically achievable. Various other factors must be considered, like hardware limits in routers and switches, errors using larger packets, header size, etc.

1.1.3 Part C

Ping using IPv6 can be done by just changing the command from ping to ping6 in the terminal. The following wireshark screenshot can verify the protocols used.

The Wireshark screenshot displays a sequence of network frames. It shows four ICMPv6 echo request (ping) frames (Frame 98 to 101) and four ICMPv6 echo reply frames (Frame 99 to 102). The source IP for the requests is 2001:df4:e000:3fd2:: and the destination IP for the replies is 2001:df4:e000:3fd2::200e. The protocol headers and payload are visible, confirming the ICMPv6 protocol used for the ping operation.

Wireshark screenshot for google.com ping packet using IPv6

```
yash@bansalss-MacBook-Air ~ % ping6 -c 10 google.com
PING6(56=40+8+8 bytes) 2001:df4:e000:3fd2:fd61:7b69:5277:24f0 --> 2404:6800:4002
:82c::200e
16 bytes from 2404:6800:4002:82c::200e, icmp_seq=0 hlim=117 time=7.894 ms
16 bytes from 2404:6800:4002:82c::200e, icmp_seq=1 hlim=117 time=16.572 ms
16 bytes from 2404:6800:4002:82c::200e, icmp_seq=2 hlim=117 time=16.391 ms
16 bytes from 2404:6800:4002:82c::200e, icmp_seq=3 hlim=117 time=15.907 ms
16 bytes from 2404:6800:4002:82c::200e, icmp_seq=4 hlim=117 time=15.757 ms
16 bytes from 2404:6800:4002:82c::200e, icmp_seq=5 hlim=117 time=14.418 ms
16 bytes from 2404:6800:4002:82c::200e, icmp_seq=6 hlim=117 time=15.709 ms
16 bytes from 2404:6800:4002:82c::200e, icmp_seq=7 hlim=117 time=15.529 ms
16 bytes from 2404:6800:4002:82c::200e, icmp_seq=8 hlim=117 time=12.703 ms
16 bytes from 2404:6800:4002:82c::200e, icmp_seq=9 hlim=117 time=14.100 ms

--- google.com ping6 statistics ---
10 packets transmitted, 10 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 7.094/14.418/16.572/2.686 ms
yash@bansalss-MacBook-Air ~ %
```

google.com: avg. ping:- 14.41 ms

```
yash@bansalss-MacBook-Air ~ % ping6 -c 10 sigcomm.org
ping6: getaddrinfo -- nodename nor servname provided, or not known
yash@bansalss-MacBook-Air ~ %
```

sigcomm.org: Unable to ping

Ping from IITD Network using IPv6

```
yash@bansalss-MacBook-Air ~ % ping6 -c 10 google.com
PING6(56=40+8+8 bytes) 2409:4050:2d16:63d8:b157:931:4016:27fe --> 2404:6800:4002
:81a::200e
16 bytes from 2404:6800:4002:81a::200e, icmp_seq=0 hlim=116 time=38.551 ms
16 bytes from 2404:6800:4002:81a::200e, icmp_seq=1 hlim=116 time=42.819 ms
16 bytes from 2404:6800:4002:81a::200e, icmp_seq=2 hlim=116 time=57.568 ms
16 bytes from 2404:6800:4002:81a::200e, icmp_seq=3 hlim=116 time=62.805 ms
16 bytes from 2404:6800:4002:81a::200e, icmp_seq=4 hlim=116 time=58.418 ms
16 bytes from 2404:6800:4002:81a::200e, icmp_seq=5 hlim=116 time=62.742 ms
16 bytes from 2404:6800:4002:81a::200e, icmp_seq=6 hlim=116 time=58.095 ms
16 bytes from 2404:6800:4002:81a::200e, icmp_seq=7 hlim=116 time=75.882 ms
16 bytes from 2404:6800:4002:81a::200e, icmp_seq=8 hlim=116 time=76.645 ms
16 bytes from 2404:6800:4002:81a::200e, icmp_seq=9 hlim=116 time=60.462 ms

--- google.com ping6 statistics ---
10 packets transmitted, 10 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 38.551/59.399/76.645/11.439 ms
yash@bansalss-MacBook-Air ~ %
```

google.com: avg. ping:- 59.39 ms

```
yash@bansalss-MacBook-Air ~ % ping6 -c 10 sigcomm.org
ping6: getaddrinfo -- nodename nor servname provided, or not known
yash@bansalss-MacBook-Air ~ %
```

sigcomm.org: Unable to ping

Ping from personal network using IPv6

Observations:-

- For google.com, the average ping latency remains almost the same in the case of IPv6. This is because the total number of hops remained the same as for IPv4, both in the case of the IITD Network and personal network, which indicates that the path must have remained the same, just the protocol gets changed.
- sigcomm.org cannot be pinged using IPv6, nor can it be routed using IPv6 traceroute. This could be because sigcomm.org still does not support IPv6 in their servers, or there may be no path to sigcomm.org in which all the routers/switches support IPv6 protocol.
- The packet size for ping using IPv6 is 16 bytes, which is lower than that of the IPv4 protocol. Also, ICMPv6 is used in IPv6, as compared to ICMP in IPv4.

1.2 Traceroute

A. The attached screenshots contain the traceroute outputs. Autonomous systems are checked using the whois terminal command.

```
[yash@bansalss-MacBook-Air ~ % traceroute google.com
traceroute to google.com (142.250.206.142), 64 hops max, 40 byte packets
 1  10.184.32.13 (10.184.32.13)  5.555 ms  4.047 ms  4.566 ms
 2  10.255.107.3 (10.255.107.3)  4.066 ms  4.821 ms  4.322 ms
 3  10.119.233.65 (10.119.233.65)  5.280 ms  4.793 ms  5.263 ms
 4  * * *
 5  10.119.234.162 (10.119.234.162)  14.703 ms  8.036 ms  6.592 ms
 6  72.14.195.56 (72.14.195.56)  12.960 ms  11.962 ms  10.482 ms
 7  192.178.80.159 (192.178.80.159)  7.371 ms  7.459 ms  8.464 ms
 8  142.251.76.199 (142.251.76.199)  7.396 ms
    142.251.76.197 (142.251.76.197)  7.838 ms  6.944 ms
 9  del11s21-in-f14.1e100.net (142.250.206.142)  7.901 ms  7.840 ms  7.943 ms
yash@bansalss-MacBook-Air ~ % |
```

Traceroute to google.com using IITD Network

9 hops, 2 autonomous systems

```
[yash@bansalss-MacBook-Air ~ % traceroute google.com
traceroute to google.com (142.250.193.46), 64 hops max, 40 byte packets
 1  192.168.22.108 (192.168.22.108)  9.578 ms  33.570 ms  6.127 ms
 2  * * *
 3  56.14.87.161 (56.14.87.161)  60.491 ms
    56.14.87.133 (56.14.87.133)  38.772 ms
    56.14.87.165 (56.14.87.165)  41.659 ms
 4  192.168.44.234 (192.168.44.234)  38.320 ms  38.351 ms
    192.168.44.238 (192.168.44.238)  39.681 ms
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  209.85.148.118 (209.85.148.118)  63.885 ms
    142.251.54.117 (142.251.54.117)  40.690 ms
    209.85.148.118 (209.85.148.118)  40.172 ms
13  192.178.80.155 (192.178.80.155)  37.748 ms *
    142.251.54.117 (142.251.54.117)  57.707 ms
14  216.239.57.32 (216.239.57.32)  28.568 ms
    142.251.54.91 (142.251.54.91)  143.854 ms
    142.251.52.212 (142.251.52.212)  30.061 ms
15  142.251.54.93 (142.251.54.93)  31.927 ms
    216.239.62.180 (216.239.62.180)  38.228 ms
    del11s15-in-f14.1e100.net (142.250.193.46)  37.910 ms
yash@bansalss-MacBook-Air ~ %
```

Traceroute to google.com using personal network

15 hops, 3 autonomous systems

```
[yash@bansalss-MacBook-Air ~ % traceroute sigcomm.org
traceroute to sigcomm.org (190.92.158.4), 64 hops max, 40 byte packets
 1  10.184.32.13 (10.184.32.13)  5.077 ms  4.168 ms  4.200 ms
 2  10.255.107.3 (10.255.107.3)  5.380 ms  4.724 ms  4.202 ms
 3  10.119.233.65 (10.119.233.65)  4.451 ms  4.398 ms  4.162 ms
 4  * * *
 5  10.119.234.162 (10.119.234.162)  14.204 ms  8.060 ms  6.687 ms
 6  136.232.148.177 (136.232.148.177)  7.515 ms  7.379 ms  7.023 ms
 7  * * *
 8  * * *
 9  * * *
10  * 49.45.4.103 (49.45.4.103)  379.317 ms  362.771 ms
11  4.7.26.61 (4.7.26.61)  307.747 ms  324.632 ms  307.837 ms
12  a2-hosting.bar2.detroit1.level3.net (4.31.124.142)  409.442 ms
    ae6.6.bar2.detroit1.net.lumen.tech (4.69.151.134)  371.663 ms  314.838 ms
13  a2-hosting.bar2.detroit1.level3.net (4.31.124.142)  401.300 ms  407.853 ms
409.293 ms
14  e1-1.mi3-c1-e02.09-33.a2webhosting.com (69.48.136.9)  409.676 ms  407.012 ms
    server.hosting3.acm.org (190.92.158.4)  411.975 ms
yash@bansalss-MacBook-Air ~ % ]
```

Traceroute to sigcomm.org using IITD Network
14 hops, 3 autonomous systems

```
[yash@bansalss-MacBook-Air ~ % traceroute sigcomm.org
traceroute to sigcomm.org (190.92.158.4), 64 hops max, 40 byte packets
 1  192.168.22.108 (192.168.22.108)  9.579 ms  6.644 ms  7.966 ms
 2  * * *
 3  56.14.87.133 (56.14.87.133)  42.837 ms
    56.8.178.41 (56.8.178.41)  39.114 ms  48.589 ms
 4  192.168.44.234 (192.168.44.234)  29.026 ms  39.205 ms
    192.168.44.236 (192.168.44.236)  39.617 ms
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * 103.198.140.64 (103.198.140.64)  105.511 ms  93.427 ms
14  103.198.140.64 (103.198.140.64)  82.522 ms  69.877 ms  79.757 ms
15  49.45.4.103 (49.45.4.103)  331.933 ms *  426.241 ms
16  * * *
17  ae2.2.bar2.detroit1.net.lumen.tech (4.69.203.81)  312.392 ms  509.363 ms
    ae6.6.bar2.detroit1.net.lumen.tech (4.69.151.134)  614.939 ms
18  e1-1.mi3-c1-e02.09-33.a2webhosting.com (69.48.136.9)  408.918 ms
    a2-hosting.bar2.detroit1.level3.net (4.31.124.142)  515.703 ms
    e1-1.mi3-c1-e02.09-33.a2webhosting.com (69.48.136.9)  359.928 ms
19  e1-1.mi3-c1-e02.09-33.a2webhosting.com (69.48.136.9)  613.445 ms  612.875 ms
    614.716 ms
20  server.hosting3.acm.org (190.92.158.4)  718.131 ms  613.784 ms  409.343 ms
yash@bansalss-MacBook-Air ~ % ]
```

Traceroute to sigcomm.org using personal network
15 hops, 4 autonomous systems

- The * output in some IP addresses may be because the system does not receive the required packets from that particular IP address. It could be due to some security policies/blocking of particular ICMP/UDP packets by the systems.
- Yes, multiple IP addresses are available for some hop counts. It may be because of multiple servers for load balancing at the particular router or router changes between the packet transfer for faster transmission. It can be noted that the multiple IP addresses of the same hop count belong to the same autonomous system.
- The first IP address of the router while tracing google.com using IITD Network is 10.184.32.13. It is the IP address of the router nearest to me. No response can be received by pinging this using a personal network. It could be because IITD has an internal network that any outer service provider cannot access without a VPN.
- Yes, I observed a two-tiered structure while tracerouting google.com with IITD Network. It implies that IITD has directly peered with Google. Thus, only two autonomous systems(IITD and Google) are detected in the traceroute. However, while tracerouting with the personal network, a 3-tiered structure was observed.
- For sigcomm.org, multiple autonomous systems are observed in between, which means that the organization has not peered with many organizations. Thus, a longer route with more autonomous systems is detected.

Geolocations:-

IP Address	Location	Network	Postal Code	Approximate Latitude / Longitude*, and Accuracy Radius	ISP / Organization	Domain
10.184.32.13				⚠ The IP address '10.184.32.13' 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.).		
10.119.233.65				⚠ The IP address '10.119.233.65' is a reserved IP address (private, multicast, etc.).		
10.199.234.162				⚠ The IP address '10.199.234.162' is a reserved IP address (private, multicast, etc.).		
72.14.195.56	United States (US), North America	72.14.194.0/23	-	37.751, -97.822 (1000 km)	Google	-
192.178.80.159	United States (US), North America	192.178.80.0/22	-	37.751, -97.822 (1000 km)	Google	-
142.251.76.199	United States (US), North America	142.251.76.0/22	-	37.751, -97.822 (1000 km)	Google	-
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

Googl with IITD Network

IP Address	Location	Network	Postal Code	Approximate Latitude / Longitude*, and Accuracy Radius	ISP / Organization	Domain	Country
192.168.22.108	⚠ The IP address '192.168.22.108' is a reserved IP address (private, multicast, etc.).						
56.14.87.161	United States (US), North America	56.8.0.0/13	–	37.751, -97.822 (1000 km)	–	–	–
192.168.44.234	⚠ The IP address '192.168.44.234' is a reserved IP address (private, multicast, etc.).						
209.85.148.118	United States (US), North America	209.85.148.0/22	–	37.751, -97.822 (1000 km)	Google	–	Co
192.178.80.155	United States (US), North America	192.178.80.0/22	–	37.751, -97.822 (1000 km)	Google	–	Co
216.239.57.32	United States (US), North America	216.239.57.0/24	–	37.751, -97.822 (1000 km)	Google	–	Co
142.251.54.93	United States (US), North America	142.251.48.0/20	–	37.751, -97.822 (1000 km)	Google	–	Co

Google with personal network

IP Address	Location	Network	Code	Accuracy Radius	Orga
10.184.32.13	⚠ The IP address '10.184.32.13' is a reserved IP address (private, mostly used for loopback interfaces).				
10.255.107.3	⚠ The IP address '10.255.107.3' is a reserved IP address (private, mostly used for loopback interfaces).				
10.119.233.65	⚠ The IP address '10.119.233.65' is a reserved IP address (private, mostly used for loopback interfaces).				
10.119.234.162	⚠ The IP address '10.119.234.162' is a reserved IP address (private, mostly used for loopback interfaces).				
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
49.45.4.103	New Delhi, National Capital Territory of Delhi, India (IN), Asia	49.45.4.0/23	110043	28.652, 77.1663 (1000 km)	Jio, Reli Info Sing
4.7.26.61	San Bernardino, California, United States (US), North America	4.7.26.0/24	92407	34.2098, -117.3997 (20 km)	Lume
4.31.124.142	Detroit, Michigan, United States (US), North America	4.31.124.128/26	48213	42.3983, -82.992 (50 km)	Lume
4.69.151.134	United States (US), North America	4.69.151.128/27	-	37.751, -97.822 (1000 km)	Lume
69.48.136.9	United States (US), North America	69.48.136.0/23	-	37.751, -97.822 (1000 km)	A2 H

Sigcomm with IITD Network

IP Address	Location	Network	Postal Code	Longitude*, and Accuracy Radius	ISP / Organization
192.168.22.108				The IP address '192.168.22.108' is a reserved IP address (private, -)	
56.14.87.133	United States (US), North America	56.8.0.0/13	-	37.751, -97.822 (1000 km)	-
192.168.44.234				The IP address '192.168.44.234' is a reserved IP address (private, -)	
103.198.140.64	Singapore (SG), Asia	103.198.140.0/24	-	1.3673, 103.8014 (1000 km)	Reliance Infocom Singapore
49.45.4.103	New Delhi, National Capital Territory of Delhi, India (IN), Asia	49.45.4.0/23	110043	28.652, 77.1663 (1000 km)	Jio, Reliance Infocom Singapore
4.69.203.81	United States (US), North America	4.69.200.0/22	-	37.751, -97.822 (1000 km)	Lumen
4.69.151.134	United States (US), North America	4.69.151.128/27	-	37.751, -97.822 (1000 km)	Lumen
69.48.136.9	United States (US), North America	69.48.136.0/23	-	37.751, -97.822 (1000 km)	A2 Host
4.31.124.142	Detroit, Michigan, United States (US), North America	4.31.124.128/26	48213	42.3983, -82.992 (50 km)	Lumen
190.92.158.4	Michigan, United States (US), North America	190.92.152.0/21	-	42.4652, -83.3713 (1000 km)	A2 Host

Sigcomm with personal network

2 Network Data Collection and Header Analysis

We used Wireshark to collect the network traffic for the 2-person MS Teams video call.

This is the link for PCAP file:- [Click here](#)

2.1 Protocols identified

The following wireshark screenshot shows the protocols identified during the call.

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	44212	100.0	39582518	5187 k	0	0	0	44212
Ethernet	100.0	44212	1.6	618986	81 k	0	0	0	44212
Internet Protocol Version 6	0.2	81	0.0	3240	424	0	0	0	81
User Datagram Protocol	0.1	32	0.0	256	33	0	0	0	32
QUIC IETF	0.0	16	0.0	7138	935	16	7138	935	16
Domain Name System	0.0	16	0.0	1497	196	16	1497	196	16
Transmission Control Protocol	0.1	44	0.0	9668	1256	28	3596	471	44
Transport Layer Security	0.0	16	0.0	4965	650	16	4965	650	16
Internet Control Message Protocol v6	0.0	5	0.0	160	20	5	160	20	5
Internet Protocol Version 4	99.8	44130	2.2	882600	115 k	0	0	0	44130
User Datagram Protocol	99.6	44015	0.9	352120	46 k	0	0	0	44015
Session Traversal Utilities for NAT	0.6	256	0.1	24896	3262	244	22448	2941	256
Malformed Packet	0.0	12	0.0	0	0	12	0	0	12
Real-time Transport Control Protocol	0.3	132	0.0	14092	1846	46	4084	535	133
Malformed Packet	0.2	86	0.0	0	0	86	0	0	86
Data	98.7	43627	95.1	37636363	4932 k	43627	37636363	4932 k	43627
Transmission Control Protocol	0.3	115	0.1	23034	3018	70	15252	1998	115
Transport Layer Security	0.1	45	0.1	20001	2621	45	19663	2576	46
Address Resolution Protocol	0.0	1	0.0	46	6	1	46	6	1

Procols detected

- Link layer protocol :- Ethernet (used by IITD Wifi):- 100 %
- Network layer protocols
 1. IPv4:- used by MS teams
 2. IPv6:- background traffic
- Transport layer protocol:- User Datagram Protocol (UDP):- 100 %
- Application layer protocols
 1. Session traversal utilities for NAT (STUN):- 0.6 %
 2. Real-time transport control protocol (RTCP):- 0.3 %

2.2 Direct connection between hosts

Yes, we observed a direct connection between the two hosts. This is visible as the source and destination IP addresses match the IP addresses of my and my partner's computers.

10.184.45.87	10.184.18.215
10.184.45.87	10.184.18.215
10.184.18.215	10.184.45.87
10.184.18.215	10.184.45.87
10.184.45.87	10.184.18.215

Source and destination IPs

The screenshot shows the Network preferences window on macOS. The left sidebar lists network connections: **ITD_WIFI** (Connected), **TCP/IP**, **DNS**, **WINS**, **802.1X**, **Proxies**, and **Hardware**. The **ITD_WIFI** connection is highlighted with a blue bar at the top. A status message above the connection says: "WPA/WPA2 (TKIP) is not considered secure. If this is your Wi-Fi network, configure the router to use WPA2 (AES) or WPA3 security type." Below this is a link to "Learn more...". The main pane contains two sections: "Automatically join this network" (with a blue toggle switch) and "Low data mode" (with a grey toggle switch). The "Low data mode" section includes the text: "Low data mode helps reduce your Mac data usage over specific Wi-Fi networks you select." The bottom section, "Limit IP address tracking", includes the text: "Limit IP address tracking by hiding your IP address from known trackers in Mail and Safari." A red box highlights the "IP address" field, which shows the value **10.184.45.87**. The "Router" field shows the value **10.184.32.1**.

My IP address

```
C:\>ipconfig

Windows IP Configuration

Wireless LAN adapter Local Area Connection* 1:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

Wireless LAN adapter Local Area Connection* 2:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

Wireless LAN adapter Wi-Fi:
  Connection-specific DNS Suffix . . . . . : iit.ac.in
  IPv6 Address . . . . . : 2001:df4:e000:3fd1::553d
  Link-local IPv6 Address . . . . . : fe80::c137:656f:a8b8:3f7a%14
  IPv4 Address . . . . . : 10.184.18.215
  Subnet Mask . . . . . : 255.255.224.0
  Default Gateway . . . . . : fe80::255:242%14
                                10.184.0.1
```

Partner's IP address

2.3 Filtering Audio and Video packets

We filtered the audio and video packets using the following logic:-

- When we kept only videos on both ends, the UDP packets of only size greater than 500 were captured by Wireshark.
 - On the other hand, when only audio was kept on, only the packets of size less than 300 were captured.
 - When both were kept on, all the types of UDP packets occurred.
 - Also, for audio packets, when we were not speaking, audio packets were of size less than 100. While speaking, audio packets are larger than 100 but less than 400.
 - When both audio and videos are kept off, no UDP packets are detected. This procedure confirms that MS teams only use UDP packets of the size described above for audio and video.

Observations:-

- Total audio and video packets captured:- 44003
 - Total audio packets captured:- 6499
 - Total video packets captured:- 37504
 - % audio packets:- 14.76 %
 - % video packets:- 85.23 %

Apply a display filter... < / >						
#	Time	Source	Destination	Protocol	Length	Info
326,	26.81718	10..184.45.87	10..184..18..215	UDP	932	50836 - 50023 Len=898
326,	26.81722	10..184.45.87	10..184..18..215	UDP	930	50836 - 50023 Len=888
326,	26.81724	10..184.45.87	10..184..18..215	UDP	1011	50836 - 50023 Len=969
326,	26.81726	10..184.45.87	10..184..18..215	UDP	1011	50836 - 50023 Len=969
326,	26.81729	10..184.45.87	10..184..18..215	UDP	1011	50836 - 50023 Len=969
326,	26.81731	10..184.45.87	10..184..18..215	UDP	1011	50836 - 50023 Len=969
326,	26.81733	10..184.45.87	10..184..18..215	UDP	1011	50836 - 50023 Len=969
326,	26.81735	10..184.45.87	10..184..18..215	UDP	1009	50836 - 50023 Len=956
326,	26.81736	10..184.45.87	10..184..18..215	UDP	771	50836 - 50023 Len=729
326,	26.81738	10..184.45.87	10..184..18..215	UDP	771	50836 - 50023 Len=729
326,	26.81740	10..184.45.87	10..184..18..215	UDP	771	50836 - 50023 Len=729
326,	26.81742	10..184.45.87	10..184..18..215	UDP	771	50836 - 50023 Len=729
326,	26.81744	10..184.45.87	10..184..18..215	UDP	771	50836 - 50023 Len=729
326,	26.81746	10..184.45.87	10..184..18..215	UDP	1027	50836 - 50023 Len=985
326,	26.81747	10..184.45.87	10..184..18..215	UDP	1027	50836 - 50023 Len=985
326,	29.33663	10..184.45.87	10..184..18..215	UDP	372	50836 - 50023 Len=339
326,	29.33665	10..184.45.87	10..184..18..215	UDP	1027	50836 - 50023 Len=985
326,	29.33667	10..184.45.87	10..184..18..215	UDP	409	50836 - 50023 Len=448
326,	32.92020	10..184.45.87	10..184..18..215	UDP	1023	50836 - 50023 Len=981
326,	32.92026	10..184.45.87	10..184..18..215	UDP	911	50836 - 50023 Len=869
326,	32.92029	10..184.45.87	10..184..18..215	UDP	911	50836 - 50023 Len=869
326,	32.92255	10..184.45.87	10..184..18..215	UDP	1008	50836 - 50023 Len=966
326,	32.92256	10..184.45.87	10..184..18..215	UDP	1008	50836 - 50023 Len=966
326,	32.92258	10..184.45.87	10..184..18..215	UDP	1008	50836 - 50023 Len=966
326,	32.92259	10..184.45.87	10..184..18..215	UDP	1007	50836 - 50023 Len=965
326,	32.92261	10..184.45.87	10..184..18..215	UDP	1034	50836 - 50023 Len=992
326,	32.92263	10..184.45.87	10..184..18..215	UDP	1007	50836 - 50023 Len=965
326,	32.92264	10..184.45.87	10..184..18..215	UDP	1032	50836 - 50023 Len=998
326,	32.92266	10..184.45.87	10..184..18..215	UDP	1050	50836 - 50023 Len=1008
326,	32.92275	10..184..18..215	10..184..45..87	UDP	1229	50823 - 50023 Len=1197
326,	32.92276	10..184..18..215	10..184..45..87	UDP	1221	50823 - 50036 Len=1179
326,	32.92277	10..184..18..215	10..184..45..87	UDP	1221	50823 - 50036 Len=1179

Only video on

Apply a display filter: <ctrl>/>						
#	Time	Source	Destination	Protocol	Length	Info
250.	069.321918	10.184.18.215	10.184.45.87	UDP	756	50828 - 50828 Len=714
250..	069.321911	10.184.18.215	10.184.45.87	UDP	756	50828 - 50828 Len=714
250..	069.321912	10.184.18.215	10.184.45.87	UDP	756	50828 - 50828 Len=714
250..	069.321913	10.184.18.215	10.184.45.87	UDP	756	50828 - 50828 Len=714
250..	069.321915	10.184.18.215	10.184.45.87	UDP	756	50828 - 50828 Len=714
250..	069.327336	10.184.18.215	10.184.45.87	UDP	756	50828 - 50828 Len=714
250..	069.327337	10.184.18.215	10.184.45.87	UDP	756	50828 - 50828 Len=714
250..	069.327337	10.184.18.215	10.184.45.87	UDP	756	50828 - 50828 Len=714
250..	069.327338	10.184.18.215	10.184.45.87	UDP	756	50828 - 50828 Len=714
250..	069.327339	10.184.18.215	10.184.45.87	UDP	756	50828 - 50828 Len=714
250..	069.327340	10.184.18.215	10.184.45.87	UDP	756	50828 - 50828 Len=714
250..	069.327340	10.184.18.215	10.184.45.87	UDP	756	50828 - 50828 Len=714
250..	069.327341	10.184.18.215	10.184.45.87	UDP	756	50828 - 50828 Len=714
250..	069.331498	10.184.18.215	10.184.45.87	UDP	347	50814 - 50804 Len=395
250..	069.332940	10.184.18.215	10.184.45.87	UDP	337	50804 - 50814 Len=295
250..	069.335512	10.184.18.215	10.184.45.87	UDP	732	50828 - 50828 Len=698
250..	069.335522	10.184.18.215	10.184.45.87	UDP	731	50828 - 50828 Len=689
250..	069.335531	10.184.18.215	10.184.45.87	UDP	1046	50828 - 50828 Len=1884
250..	069.335533	10.184.18.215	10.184.45.87	UDP	1046	50828 - 50828 Len=1884
250..	069.335546	10.184.18.215	10.184.45.87	UDP	906	50828 - 50828 Len=866
250..	069.335546	10.184.18.215	10.184.45.87	UDP	906	50828 - 50828 Len=866
250..	069.335546	10.184.18.215	10.184.45.87	UDP	1021	50828 - 50828 Len=866
250..	069.335566	10.184.18.215	10.184.45.87	UDP	1191	50828 - 50828 Len=1149
250..	069.335577	10.184.18.215	10.184.45.87	UDP	1191	50828 - 50828 Len=1149
250..	069.335578	10.184.18.215	10.184.45.87	UDP	1191	50828 - 50828 Len=1149
250..	069.335582	10.184.18.215	10.184.45.87	UDP	1188	50828 - 50828 Len=1147
250..	069.335583	10.184.18.215	10.184.45.87	UDP	1287	50828 - 50828 Len=1165
250..	069.335594	10.184.18.215	10.184.45.87	UDP	1287	50828 - 50828 Len=1165
250..	069.335596	10.184.18.215	10.184.45.87	UDP	1287	50828 - 50828 Len=1165
250..	069.335599	10.184.18.215	10.184.45.87	UDP	1287	50828 - 50828 Len=1165
250..	069.335601	10.184.18.215	10.184.45.87	UDP	1287	50828 - 50828 Len=1165
250..	069.335613	10.184.18.215	10.184.45.87	UDP	1287	50828 - 50828 Len=1165

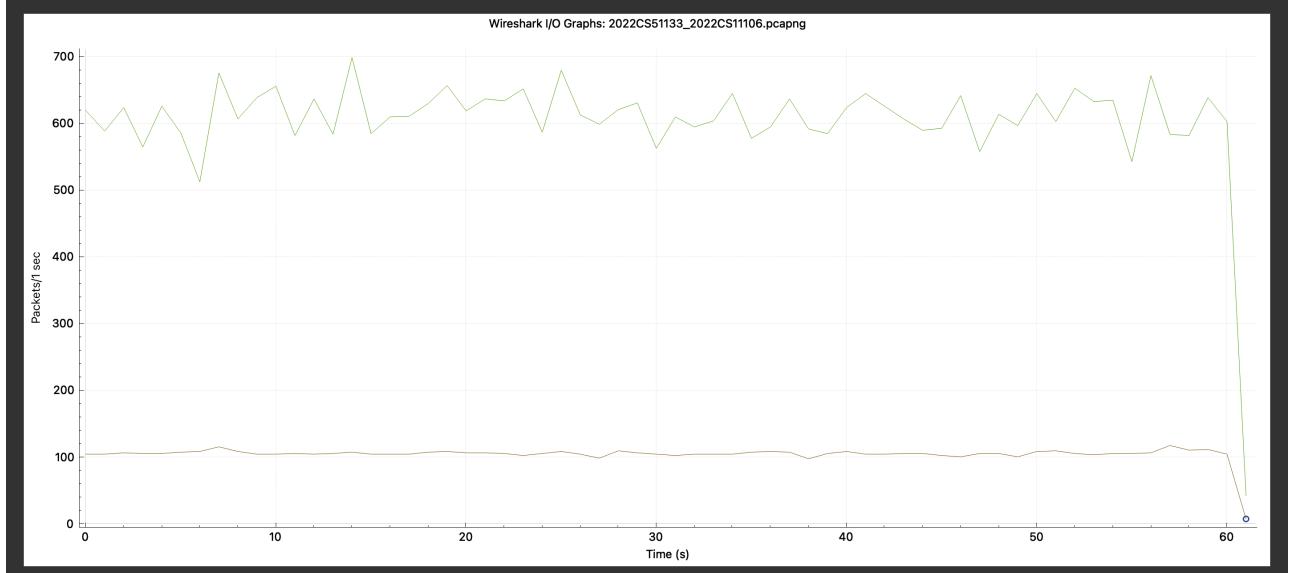
Both audio and video on

o.	Time	Source	Destination	Protocol	Length	Info
223674	423.946638	10.184.18.215	10.184.45.87	UDP	89	50014 - 50004 Len=47
223675	423.968223	10.184.45.87	10.184.18.215	UDP	89	50004 - 50014 Len=44
223676	423.969227	10.184.18.215	10.184.45.87	UDP	89	50014 - 50004 Len=47
223677	423.969228	10.184.18.215	10.184.45.87	UDP	89	50014 - 50004 Len=47
223678	423.9693752	10.184.18.215	10.184.45.87	UDP	86	50014 - 50004 Len=44
223679	424.007462	10.184.18.215	10.184.45.87	UDP	86	50014 - 50004 Len=47
223680	424.013966	10.184.45.87	10.184.18.215	UDP	86	50004 - 50014 Len=44
223681	424.026558	10.184.18.215	10.184.45.87	UDP	89	50014 - 50004 Len=47
223682	424.029174	10.184.45.87	10.184.18.215	UDP	94	50004 - 50014 Len=52
223683	424.048517	10.184.18.215	10.184.45.87	UDP	89	50014 - 50004 Len=47
223684	424.048970	10.184.45.87	10.184.18.215	UDP	86	50004 - 50014 Len=44
223685	424.049000	10.184.18.215	10.184.45.87	UDP	89	50014 - 50004 Len=47
223686	424.073124	10.184.45.87	10.184.18.215	UDP	86	50004 - 50014 Len=44
223687	424.084366	10.184.45.87	10.184.18.215	UDP	86	50004 - 50014 Len=44
223688	424.085591	10.184.18.215	10.184.45.87	UDP	97	50014 - 50004 Len=55
223689	424.18922	10.184.45.87	10.184.18.215	UDP	86	50004 - 50014 Len=44
223690	424.110809	10.184.18.215	10.184.45.87	UDP	89	50014 - 50004 Len=47
223691	424.128026	10.184.18.215	10.184.45.87	UDP	89	50014 - 50004 Len=47
223692	424.158635	10.184.45.87	10.184.18.215	UDP	86	50004 - 50014 Len=44
223693	424.158987	10.184.45.87	10.184.18.215	UDP	86	50004 - 50014 Len=44
223694	424.165938	10.184.45.87	10.184.18.215	UDP	86	50004 - 50014 Len=44
223695	424.198188	10.184.45.87	10.184.18.215	UDP	94	50004 - 50014 Len=52
223696	424.210381	10.184.45.87	10.184.18.215	UDP	86	50004 - 50014 Len=44
223697	424.235717	10.184.45.87	10.184.18.215	UDP	86	50004 - 50014 Len=44
223698	424.235788	10.184.18.215	10.184.45.87	UDP	89	50014 - 50004 Len=47
223699	424.235798	10.184.18.215	10.184.45.87	UDP	86	50014 - 50004 Len=44
223700	424.237782	10.184.18.215	10.184.45.87	UDP	89	50014 - 50004 Len=47
223701	424.237783	10.184.18.215	10.184.45.87	UDP	89	50014 - 50004 Len=47
223702	424.237783	10.184.18.215	10.184.45.87	UDP	89	50014 - 50004 Len=47
223703	424.245522	10.184.45.87	10.184.18.215	UDP	86	50004 - 50014 Len=44
223704	424.246665	10.184.18.215	10.184.45.87	UDP	97	50014 - 50004 Len=55
223705	424.268761	10.184.18.215	10.184.45.87	UDP	89	50014 - 50004 Len=47
223706	424.270870	10.184.45.87	10.184.18.215	UDP	86	50004 - 50014 Len=44

Only audio on with speaking without speaking

o.	Time	Source	Destination	Protocol	Length	Info
217928	372.455415	10.184.45.87	10.184.18.215	UDP	205	50004 - 50014 Len=163
217929	372.465265	10.184.18.215	10.184.45.87	UDP	184	50014 - 50004 Len=142
217930	372.466265	10.184.18.215	10.184.45.87	UDP	173	50014 - 50004 Len=131
217931	372.487233	10.184.18.215	10.184.45.87	UDP	221	50004 - 50014 Len=179
217932	372.490729	10.184.18.215	10.184.45.87	UDP	167	50014 - 50004 Len=125
217933	372.507108	10.184.18.215	10.184.45.87	UDP	201	50004 - 50014 Len=160
217934	372.524495	10.184.18.215	10.184.45.87	UDP	206	50014 - 50014 Len=164
217935	372.524995	10.184.18.215	10.184.45.87	UDP	157	50014 - 50004 Len=115
217936	372.528799	10.184.18.215	10.184.45.87	UDP	168	50014 - 50004 Len=111
217937	372.546741	10.184.18.215	10.184.45.87	UDP	203	50004 - 50014 Len=161
217938	372.551855	10.184.18.215	10.184.45.87	UDP	158	50014 - 50004 Len=116
217939	372.561218	10.184.18.215	10.184.45.87	UDP	202	50004 - 50014 Len=160
217940	372.561226	10.184.18.215	10.184.45.87	UDP	153	50014 - 50004 Len=121
217941	372.595118	10.184.18.215	10.184.45.87	UDP	218	50004 - 50014 Len=176
217942	372.606371	10.184.18.215	10.184.45.87	UDP	157	50014 - 50004 Len=115
217943	372.606472	10.184.18.215	10.184.45.87	UDP	196	50004 - 50014 Len=154
217944	372.627599	10.184.18.215	10.184.45.87	UDP	178	50014 - 50004 Len=128
217945	372.631295	10.184.18.215	10.184.45.87	UDP	162	50004 - 50014 Len=125
217946	372.631296	10.184.18.215	10.184.45.87	UDP	177	50004 - 50014 Len=135
217947	372.651226	10.184.18.215	10.184.45.87	UDP	181	50004 - 50014 Len=120
217948	372.666786	10.184.18.215	10.184.45.87	UDP	164	50014 - 50004 Len=122
217949	372.671516	10.184.18.215	10.184.45.87	UDP	187	50004 - 50014 Len=145
217950	372.687516	10.184.18.215	10.184.45.87	UDP	189	50004 - 50014 Len=147
217951	372.688164	10.184.18.215	10.184.45.87	UDP	174	50014 - 50004 Len=137
217952	372.700911	10.184.18.215	10.184.45.87	UDP	174	50004 - 50014 Len=125
217953	372.718911	10.184.18.215	10.184.45.87	UDP	182	50004 - 50014 Len=140
217954	372.726898	10.184.18.215	10.184.45.87	UDP	178	50014 - 50004 Len=136
217955	372.731886	10.184.18.215	10.184.45.87	UDP	198	50004 - 50014 Len=145
217956	372.744344	10.184.18.215	10.184.45.87	UDP	165	50014 - 50004 Len=123
217957	372.747545	10.184.18.215	10.184.45.87	UDP	194	50004 - 50014 Len=152
217958	372.767016	10.184.18.215	10.184.45.87	UDP	196	50004 - 50014 Len=154
217959	372.792887	10.184.18.215	10.184.45.87	UDP	185	50004 - 50014 Len=143

Only audio on with speaking without speaking



Bandwidth Utilisation by Audio and Video

3 Traffic Analysis and Network Performance

I used **dpkt** python library to read the given .pcapng file of the NDT7 speed test. On analyzing the given speed test file and a speed file I created using Wireshark, it can be seen that the NDT7 test handshakes 4 times during the complete speed test. In these 4 handshakes, the first is downloaded, and the second is uploaded to one IP address. Download and upload are done using a different IP address for the next two handshakes. NDT7 tests our network on two IP addresses for upload and download. The speed test file given to us truncates after the second download procedure, as seen in the graph below.

3.1 Percentage Traffic

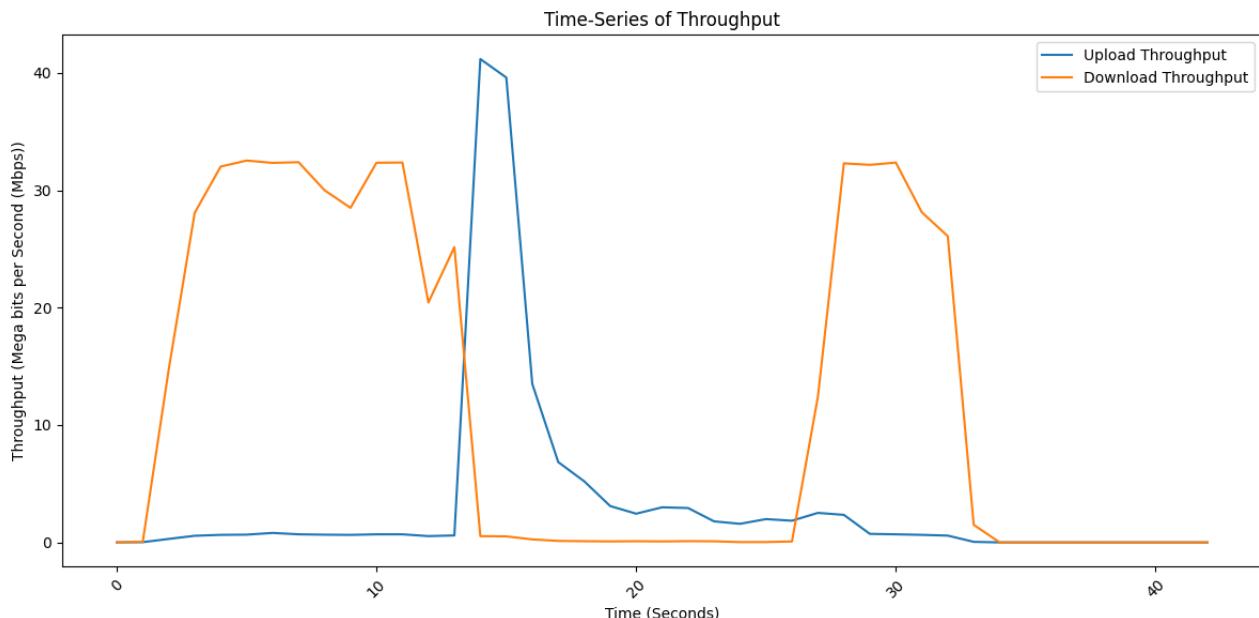
The NDT7 test uses TCP transport protocol and has port 443 on its server. So, the first filter is done based on protocol and port. Also, the packets which do not have any source/destination IP address are removed. The distinction between upload and download packets is based on the source and destination ports. Upload packets have destination port 443, while download packets have source port 443.

Percentage packets traffic for speed test:- 86.82 %

Percentage bytes traffic for speed test:- 88.45 %

3.2 Throughput

Upload and download packets are separated based on the port to calculate throughput. Then, for each second from the start of the file, the packets are accumulated for each second for both upload and download and then the graph is plotted. The following is the throughput graph for the given speed test file.



Throughput graph for upload and download

3.3 Upload and Download speed

For calculating the speed of upload/download, the maximum throughput per second is calculated, and then only that particular time frame is considered for which the throughput is greater than 25 %. This is because, at other times, it can be fairly assumed that the speed test was on the other phase.

Download speed in Megabits per second:- 28.023 Mbps

Upload speed in Megabits per second:- 31.432 Mbps