

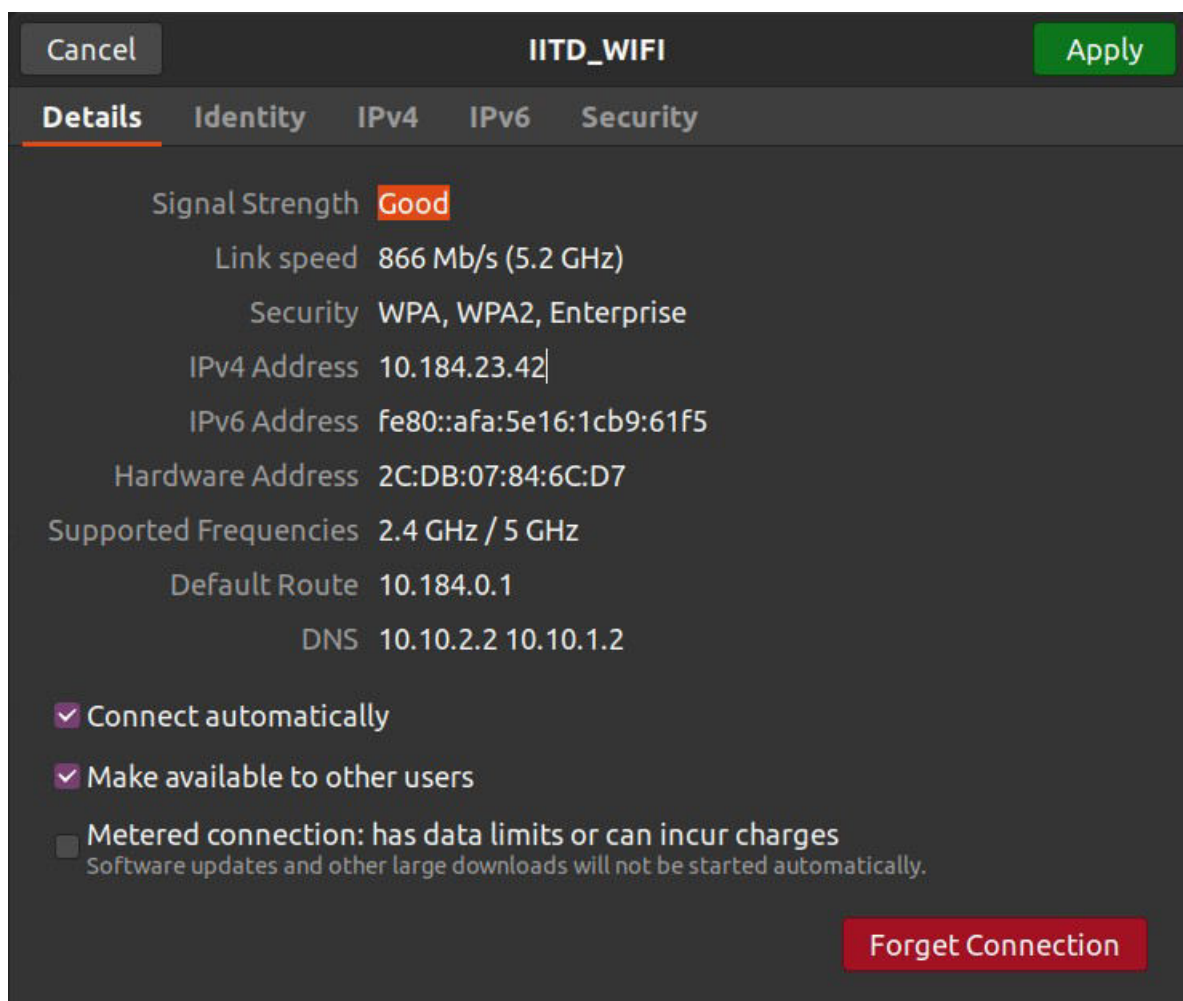
Assignment 1

Shreyansh Singh

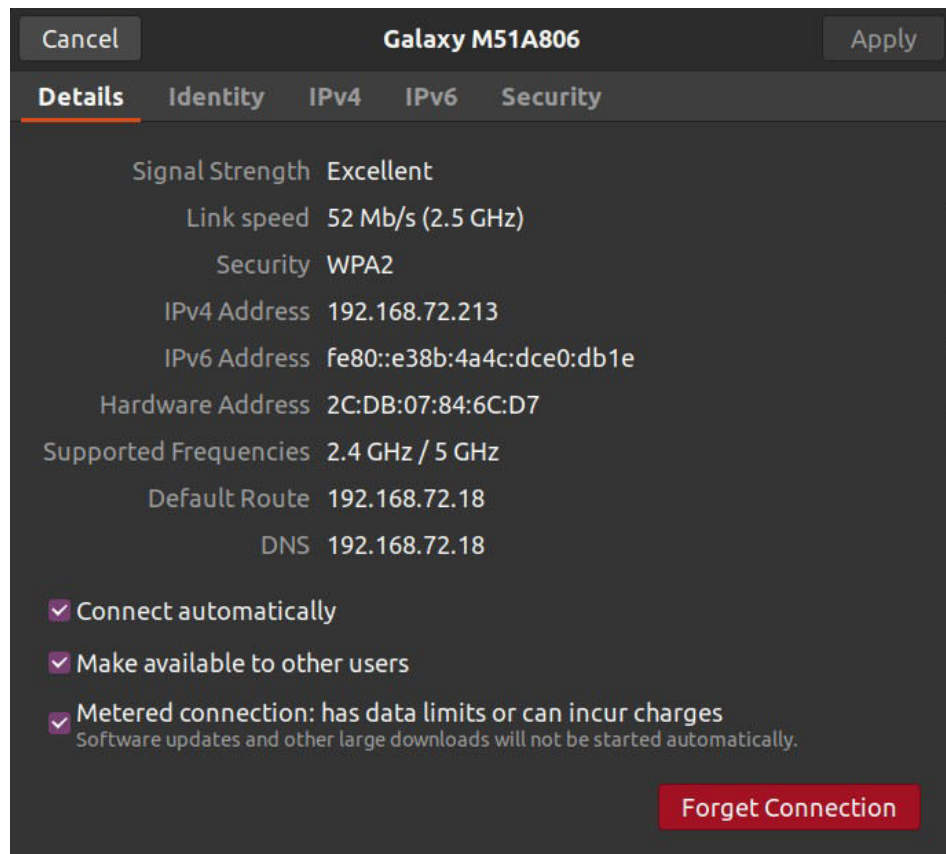
2020CS10385

Networking Tools

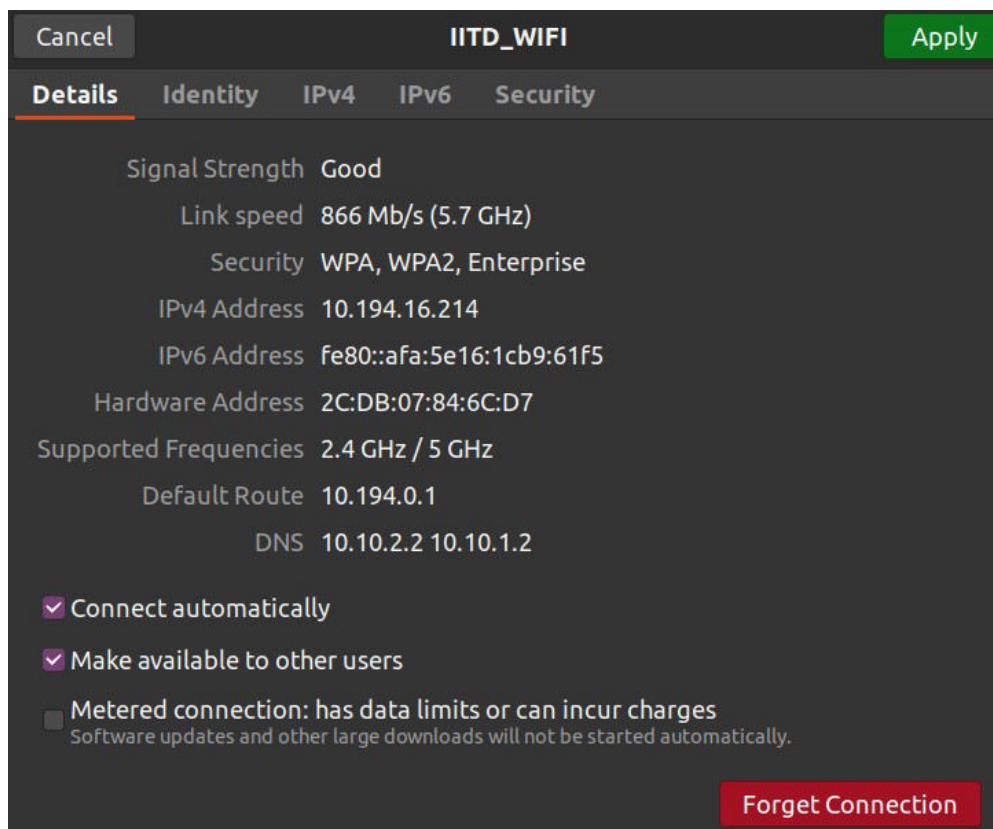
1. a) IP address of IITD Hostel Wifi : 10.184.23.42 (IPv4)



b) IP address of mobile network : 192.168.72.213 (IPv4)



c) IP address of IITD Library Wifi : 10.194.16.214 (IPv4)



2. a) IP address associated with google.com and facebook.com

```
shreyansh@shreyansh-HP-Pavilion-Laptop-14-ce3xxx:~$ nslookup www.google.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.183.164
Name:   www.google.com
Address: 2404:6800:4002:82b::2004

shreyansh@shreyansh-HP-Pavilion-Laptop-14-ce3xxx:~$ nslookup www.facebook.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
www.facebook.com canonical name = star-mini.c10r.facebook.com.
Name:   star-mini.c10r.facebook.com
Address: 157.240.16.35
Name:   star-mini.c10r.facebook.com
Address: 2a03:2880:f12f:183:face:b00c:0:25de
```

b) IP address associated with google.com and facebook.com using different DNS server. As a result of different DNS server the IP address of both of them changes.

```
shreyansh@shreyansh-HP-Pavilion-Laptop-14-ce3xxx:~$ nslookup www.google.com 149.112.112.112
Server:      149.112.112.112
Address:     149.112.112.112#53

Non-authoritative answer:
Name:   www.google.com
Address: 172.217.16.132
Name:   www.google.com
Address: 2a00:1450:4001:806::2004

shreyansh@shreyansh-HP-Pavilion-Laptop-14-ce3xxx:~$ nslookup www.facebook.com 149.112.112.112
Server:      149.112.112.112
Address:     149.112.112.112#53

Non-authoritative answer:
www.facebook.com canonical name = star-mini.c10r.facebook.com.
Name:   star-mini.c10r.facebook.com
Address: 157.240.195.35
Name:   star-mini.c10r.facebook.com
Address: 2a03:2880:f11c:8083:face:b00c:0:25de
```

3. a) Ping of google.com

```
shreyansh@shreyansh-HP-Pavilion-Laptop-14-ce3xxx:~$ ping google.com
PING google.com (142.250.193.206) 56(84) bytes of data.
64 bytes from del11s17-in-f14.1e100.net (142.250.193.206): icmp_seq=1 ttl=118 time=6.86 ms
64 bytes from del11s17-in-f14.1e100.net (142.250.193.206): icmp_seq=2 ttl=118 time=8.14 ms
64 bytes from del11s17-in-f14.1e100.net (142.250.193.206): icmp_seq=3 ttl=118 time=41.2 ms
64 bytes from del11s17-in-f14.1e100.net (142.250.193.206): icmp_seq=4 ttl=118 time=20.9 ms
64 bytes from del11s17-in-f14.1e100.net (142.250.193.206): icmp_seq=5 ttl=118 time=7.69 ms
64 bytes from del11s17-in-f14.1e100.net (142.250.193.206): icmp_seq=6 ttl=118 time=25.0 ms
64 bytes from del11s17-in-f14.1e100.net (142.250.193.206): icmp_seq=7 ttl=118 time=26.2 ms
^C
--- google.com ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6009ms
rtt min/avg/max/mdev = 6.862/19.431/41.183/11.807 ms
```

b) Ping after increasing ping time interval. As a result the time taken increases but ping remains nearly same.

```
shreyansh@shreyansh-HP-Pavilion-Laptop-14-ce3xxx:~$ ping -i 5 google.com
PING google.com (142.250.193.206) 56(84) bytes of data.
64 bytes from del11s17-in-f14.1e100.net (142.250.193.206): icmp_seq=1 ttl=117 time=4.71 ms
64 bytes from del11s17-in-f14.1e100.net (142.250.193.206): icmp_seq=2 ttl=117 time=68.4 ms
64 bytes from del11s17-in-f14.1e100.net (142.250.193.206): icmp_seq=3 ttl=117 time=6.45 ms
64 bytes from del11s17-in-f14.1e100.net (142.250.193.206): icmp_seq=4 ttl=117 time=6.24 ms
64 bytes from del11s17-in-f14.1e100.net (142.250.193.206): icmp_seq=5 ttl=117 time=141 ms
^C
--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 20022ms
rtt min/avg/max/mdev = 4.714/45.315/140.785/53.540 ms
```

c) Ping after changing TTL.

```
shreyansh@shreyansh-HP-Pavilion-Laptop-14-ce3xxx:~$ ping -t 90 google.com
PING google.com (142.250.193.206) 56(84) bytes of data.
64 bytes from del11s17-in-f14.1e100.net (142.250.193.206): icmp_seq=1 ttl=117 time=76.1 ms
64 bytes from del11s17-in-f14.1e100.net (142.250.193.206): icmp_seq=2 ttl=117 time=241 ms
64 bytes from del11s17-in-f14.1e100.net (142.250.193.206): icmp_seq=3 ttl=117 time=63.7 ms
64 bytes from del11s17-in-f14.1e100.net (142.250.193.206): icmp_seq=4 ttl=117 time=11.0 ms
64 bytes from del11s17-in-f14.1e100.net (142.250.193.206): icmp_seq=5 ttl=117 time=6.31 ms
64 bytes from del11s17-in-f14.1e100.net (142.250.193.206): icmp_seq=6 ttl=117 time=8.31 ms
64 bytes from del11s17-in-f14.1e100.net (142.250.193.206): icmp_seq=7 ttl=117 time=7.27 ms
^C
--- google.com ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6009ms
rtt min/avg/max/mdev = 6.307/59.112/241.067/79.093 ms
```


d) Ping after decreasing ping packet size, this causes to reduce the ping value.

```
shreyansh@shreyansh-HP-Pavilion-Laptop-14-ce3xxx:~$ ping -s 24 -w 7 google.com
PING google.com (142.250.67.238) 24(52) bytes of data:
32 bytes from bom07s24-in-f14.1e100.net (142.250.67.238): icmp_seq=1 ttl=117 time=23.8 ms
32 bytes from bom07s24-in-f14.1e100.net (142.250.67.238): icmp_seq=2 ttl=117 time=29.0 ms
32 bytes from bom07s24-in-f14.1e100.net (142.250.67.238): icmp_seq=3 ttl=117 time=24.7 ms
32 bytes from bom07s24-in-f14.1e100.net (142.250.67.238): icmp_seq=4 ttl=117 time=29.5 ms
32 bytes from bom07s24-in-f14.1e100.net (142.250.67.238): icmp_seq=5 ttl=117 time=28.1 ms
32 bytes from bom07s24-in-f14.1e100.net (142.250.67.238): icmp_seq=6 ttl=117 time=28.9 ms
32 bytes from bom07s24-in-f14.1e100.net (142.250.67.238): icmp_seq=7 ttl=117 time=29.8 ms

--- google.com ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6007ms
rtt min/avg/max/mdev = 23.816/27.671/29.802/2.233 ms
```

4. Traceroute

**** Using IITD WiFi**

a) iitd.ac.in. Traceroute is done successfully with no request timeout.

```
shreyansh@shreyansh-HP-Pavilion-Laptop-14-ce3xxx:~$ traceroute www.iitd.ac.in
traceroute to www.iitd.ac.in (10.10.211.212), 30 hops max, 60 byte packets
 1  10.194.0.14 (10.194.0.14)  2.516 ms  2.473 ms  2.456 ms
 2  10.254.238.1 (10.254.238.1)  2.475 ms  2.458 ms  2.442 ms
 3  10.254.236.18 (10.254.236.18)  2.439 ms  2.424 ms  10.254.236.10 (10.254.236.10)  2.360 ms
 4  www.iitd.ac.in (10.10.211.212)  2.407 ms  2.392 ms  2.377 ms
```

b) google.com. Except first two requests all the rest are timed out.

```
shreyansh@shreyansh-HP-Pavilion-Laptop-14-ce3xxx:~$ traceroute www.google.com
traceroute to www.google.com (172.217.161.4), 30 hops max, 60 byte packets
 1  10.194.0.14 (10.194.0.14)  169.736 ms  169.702 ms  169.687 ms
 2  10.254.238.1 (10.254.238.1)  169.674 ms  169.662 ms  169.650 ms
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

c) facebook.com. Same result as with google.com

```
shreyansh@shreyansh-HP-Pavilion-Laptop-14-ce3xxx:~$ traceroute www.facebook.com
traceroute to www.facebook.com (157.240.16.35), 30 hops max, 60 byte packets
 1  10.194.0.14 (10.194.0.14)  1.696 ms  1.652 ms  1.634 ms
 2  10.254.238.5 (10.254.238.5)  1.585 ms  2.192 ms  2.175 ms
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

d) Forcing IPv4 on iitd.ac.in. Traceroute is done successfully with no request timeout.

```
shreyansh@shreyansh-HP-Pavilion-Laptop-14-ce3xxx:~$ traceroute -4 www.iitd.ac.in
traceroute to www.iitd.ac.in (10.10.211.212), 30 hops max, 60 byte packets
 1  10.194.0.14 (10.194.0.14)  4.028 ms  3.987 ms  3.972 ms
 2  10.254.238.1 (10.254.238.1)  4.646 ms  5.118 ms  4.616 ms
 3  10.254.236.10 (10.254.236.10)  3.897 ms  10.254.236.18 (10.254.236.18)  3.811 ms  10.254.236.10 (10.254.236.10)  3.869 ms
 4  www.iitd.ac.in (10.10.211.212)  3.795 ms  3.778 ms  3.763 ms
shreyansh@shreyansh-HP-Pavilion-Laptop-14-ce3xxx:~$ traceroute -4 www.iitd.ac.in
```

e) Forcing IPv4 and IPv6 on google.com. No difference when Ipv4 is enforced and on enforcing IPv6 it is not able to connect.

```
shreyansh@shreyansh-HP-Pavilion-Laptop-14-ce3xxx:~$ traceroute -4 www.google.com
traceroute to www.google.com (172.217.161.4), 30 hops max, 60 byte packets
 1  10.194.0.14 (10.194.0.14)  4.671 ms  4.604 ms  4.588 ms
 2  10.254.238.1 (10.254.238.1)  4.574 ms  4.559 ms  4.544 ms
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
shreyansh@shreyansh-HP-Pavilion-Laptop-14-ce3xxx:~$ traceroute -6 www.google.com
traceroute to www.google.com (2404:6800:4009:830::2004), 30 hops max, 80 byte packets
connect: Network is unreachable
```

**** Using mobile network**

a) facebook.com

```
shreyansh@shreyansh-HP-Pavilion-Laptop-14-ce3xxx:~$ traceroute www.facebook.com
traceroute to www.facebook.com (157.240.239.35), 30 hops max, 60 byte packets
 1 _gateway (192.168.67.212) 11.165 ms 11.587 ms 11.708 ms
 2 * * *
 3 56.14.87.5 (56.14.87.5) 157.407 ms 56.8.178.105 (56.8.178.105) 157.428 ms 56.14.86.245 (56.14.86.245) 157.380 ms
 4 192.168.44.236 (192.168.44.236) 157.400 ms 192.168.44.234 (192.168.44.234) 157.349 ms 192.168.44.238 (192.168.44.238) 157.334 ms
 5 * * *
 6 * * *
 7 * * *
 8 * * *
 9 * * *
10 * * *
11 * * *
12 * * *
13 ae4.pr02.del1.tfbnw.net (157.240.73.118) 198.974 ms * *
14 173.252.67.213 (173.252.67.213) 721.451 ms ae4.pr02.del1.tfbnw.net (157.240.73.118) 721.433 ms po102.psw01.del1.tfbnw.net (31.13.24.7) 522.271 ms
15 edge-star-mini-shv-02-del1.facebook.com (157.240.239.35) 522.219 ms po102.psw01.del1.tfbnw.net (31.13.24.7) 522.203 ms po102.psw02.del1.tfbnw.net (74.119.78.33) 522.186 ms
```

b) forcing IPv6 on google.com works using mobile network but not with IITD WiFi

```
shreyansh@shreyansh-HP-Pavilion-Laptop-14-ce3xxx:~$ traceroute -6 www.google.com
traceroute to www.google.com (2404:6800:4002:80c::2004), 30 hops max, 80 byte packets
 1 2409:4050:2d18:a688::7 (2409:4050:2d18:a688::7) 16.119 ms 16.045 ms 16.013 ms
 2 * * *
 3 2405:200:331:eeee:20::1292 (2405:200:331:eeee:20::1292) 109.425 ms 115.906 ms 124.469 ms
 4 2405:200:801:300::e72 (2405:200:801:300::e72) 127.919 ms 2405:200:801:300::e76 (2405:200:801:300::e76) 129.672 ms 2405:200:801:300::e72 (2405:200:801:300::e72) 156.380 ms
 5 * * *
 6 * * *
 7 * * *
 8 2001:4860:1:1::1ef4 (2001:4860:1:1::1ef4) 118.464 ms 118.411 ms 2001:4860:1:1::15b4 (2001:4860:1:1::15b4) 118.499 ms
 9 2404:6800:812a::1 (2404:6800:812a::1) 125.446 ms 2404:6800:812f::1 (2404:6800:812f::1) 48.622 ms 63.523 ms
10 2001:4860:0:1::54e6 (2001:4860:0:1::54e6) 63.477 ms 2001:4860:0:1::5396 (2001:4860:0:1::5396) 65.441 ms 2001:4860:0:1::53a0 (2001:4860:0:1::53a0) 79.549 ms
11 * 2001:4860:0:1::1687 (2001:4860:0:1::1687) 80.858 ms 71.947 ms
12 del03s17-in-x04.1e100.net (2404:6800:4002:80c::2004) 55.610 ms 2001:4860::1c:4000:eaf6 (2001:4860::1c:4000:eaf6) 47.434 ms del03s17-in-x04.1e100.net (2404:6800:4002:80c::2004) 50.057 ms
```

c) iitd.ac.in Most of requests are timed out only few are successful

```
shreyansh@shreyansh-HP-Pavilion-Laptop-14-ce3xxx:~$ traceroute www.iitd.ac.in
traceroute to www.iitd.ac.in (103.27.9.24), 30 hops max, 60 byte packets
 1 _gateway (192.168.67.212) 123.916 ms 123.876 ms 131.463 ms
 2 * * *
 3 56.8.178.93 (56.8.178.93) 193.589 ms 56.14.86.249 (56.14.86.249) 193.575 ms 56.14.87.5 (56.14.87.5) 193.559 ms
 4 192.168.44.234 (192.168.44.234) 208.784 ms 192.168.44.236 (192.168.44.236) 208.773 ms 208.761 ms
 5 * * *
 6 * * *
 7 * * *
 8 * * *
 9 * * *
10 * * *
11 * 136.232.148.254.static.jio.com (136.232.148.254) 97.950 ms *
12 * * 136.232.148.254.static.jio.com (136.232.148.254) 107.251 ms
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *
```


d) Forcing IPv4 on iitd.ac.in

```
shreyansh@shreyansh-HP-Pavilion-Laptop-14-ce3xxx:~$ traceroute -4 www.iitd.ac.in
traceroute to www.iitd.ac.in (103.27.9.24), 30 hops max, 60 byte packets
 1 _gateway (192.168.67.212)  9.832 ms  9.790 ms  13.066 ms
 2 * * *
 3 56.14.86.237 (56.14.86.237)  68.172 ms 56.14.87.9 (56.14.87.9)  68.154 ms  71.208 ms
 4 192.168.44.234 (192.168.44.234)  71.307 ms 192.168.44.238 (192.168.44.238)  127.250 ms  127.238 ms
 5 * * *
 6 * * *
 7 * * *
 8 * * *
 9 * * *
10 * * *
11 * * *
12 * * *
13 136.232.148.254.static.jio.com (136.232.148.254)  367.192 ms * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *
```

e) Forcing IP 192.168.43.45 on google.com. All requests are not shown.

```
shreyansh@shreyansh-HP-Pavilion-Laptop-14-ce3xxx:~$ traceroute -g 192.168.43.45 www.iitd.ac.in
traceroute to www.iitd.ac.in (10.10.211.212), 30 hops max, 72 byte packets
 1 * * *
 2 * * *
 3 * * *
 4 * * *
 5 * * *
 6 * * *
 7 * * *
 8 * * *
 9 * * *
10 * * *
11 * * *
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *
```

Packet Analysis

1. DNS Task

Source	Destination	Protocol	Length	Info
2409:4050:2e38:ddd8:a72e:80d1:a006:cdb9	2409:4050:2e38:ddd8::3d	DNS	98	Standard query 0xb0c6 A www.cse.iitd.ac.in
2409:4050:2e38:ddd8:a72e:80d1:a006:cdb9	2409:4050:2e38:ddd8::3d	DNS	98	Standard query 0xe332 AAAA www.cse.iitd.ac.in
2409:4050:2e38:ddd8:a72e:80d1:a006:cdb9	2409:4050:2e38:ddd8::3d	DNS	98	Standard query 0xe332 AAAA www.cse.iitd.ac.in
192.168.190.213	192.168.190.244	DNS	78	Standard query 0xb0c6 A www.cse.iitd.ac.in
2409:4050:2e38:ddd8::3d	2409:4050:2e38:ddd8:a72e:80d1:a006:cdb9	DNS	149	Standard query response 0xe332 AAAA www.cse.iitd.ac.in SOA dns8.iitd.ac.in
192.168.190.244	192.168.190.213	DNS	94	Standard query response 0xb0c6 A www.cse.iitd.ac.in A 103.27.9.152

Fig. Image of all queries and responses.

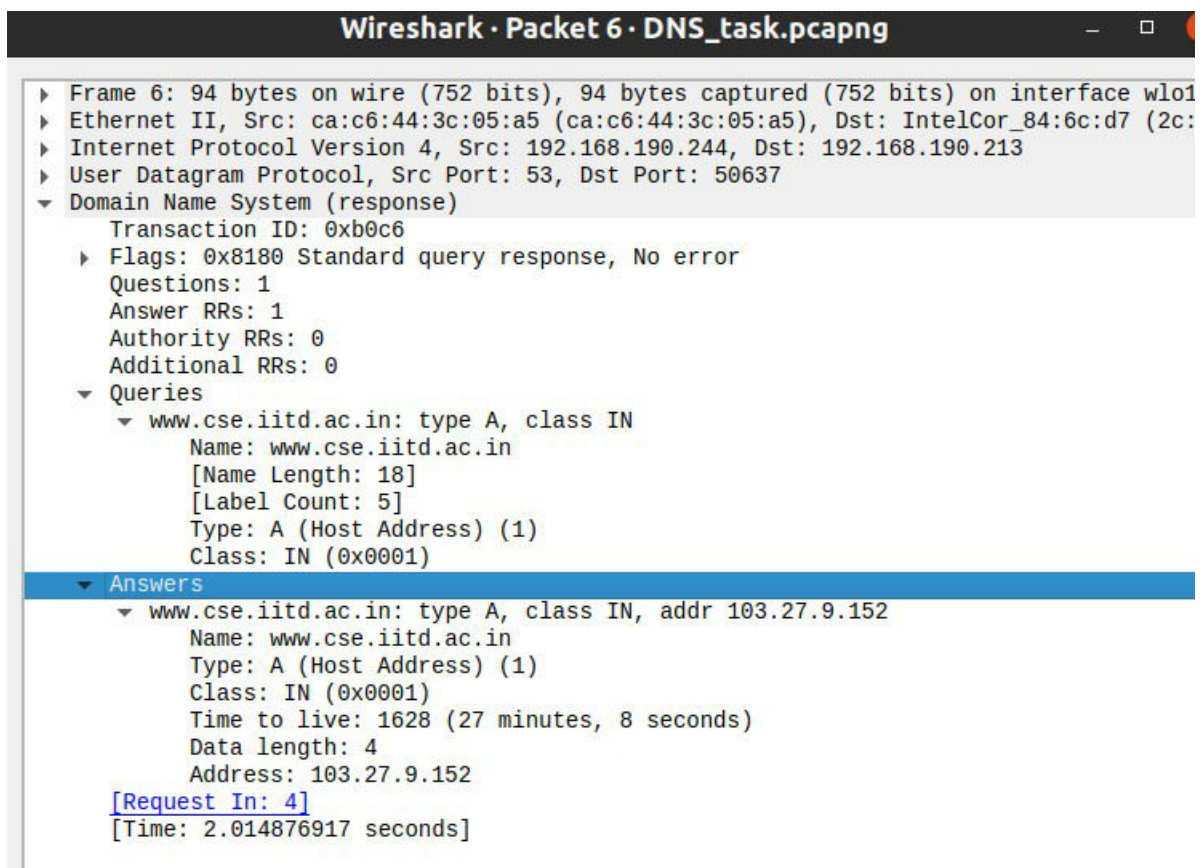


Fig. Query response in which answer is returned

1. They are sent over UDP.
2. 4 queries are sent in total, out of which 2 are of type "A" and rest 2 are of type "AAAA".
3. 2 DNS servers are involved.
4. DNS server with IP address 192.168.190.244

5. One DNS server responds to query of type “A” which has the IP address of the site and One DNS server responds to query of type “AAAA” which has no answer.

6.

	IP type	Name	Value	Type	TTL (in sec)
Query	IP6	www.cse.iitd.ac.in	-	A	-
Query	IP6	www.cse.iitd.ac.in	-	AAAA	-
Query	IP6	www.cse.iitd.ac.in	-	AAAA	-
Query	IP4	www.cse.iitd.ac.in	-	A	-
Response	IP6	www.cse.iitd.ac.in	-	AAAA	3418
Response	IP4	www.cse.iitd.ac.in	103.27.9.152	A	1628

2. Iperf Task

1. 977 packets.
2. Bulk data is send from server to client and average size of packet is 1356.
3. Throughput from terminal is 1.07 Mbits/s i.e. 0.13375 Mb/s.

In wireshark the time taken for all packets is
 $12.328 - 0.244 = 12.084$ s.

UDP length (packet size) = 1400 bytes.

Throughput is (no. of packets * packet size) / Total time
i.e $977 * 1400 / 12.084 = 0.1131$ Mb/s.

Both the values are nearly same.

```
shreyansh@shreyansh-HP-Pavilion-Laptop-14-ce3xxx:~$ iperf3 -u -t 10 -c ping.online.net -p 5208 -R
Connecting to host ping.online.net, port 5208
Reverse mode, remote host ping.online.net is sending
[ 5] local 192.168.190.213 port 53704 connected to 62.210.18.40 port 5208
[ ID] Interval           Transfer     Bitrate      Jitter    Lost/TOTAL  Datagrams
[ 5]  0.00-1.00   sec    129 KBytes    1.05 Mbits/sec  211687239.823 ms  0/97 (0%)
[ 5]  1.00-2.00   sec    129 KBytes    1.05 Mbits/sec  404497.684 ms  0/97 (0%)
[ 5]  2.00-3.00   sec    127 KBytes    1.04 Mbits/sec  833.248 ms  0/96 (0%)
[ 5]  3.00-4.00   sec    115 KBytes    945 Kbits/sec   7.139 ms  0/87 (0%)
[ 5]  4.00-5.00   sec    127 KBytes    1.04 Mbits/sec   5.334 ms  0/96 (0%)
[ 5]  5.00-6.00   sec    142 KBytes    1.16 Mbits/sec   1.557 ms  0/107 (0%)
[ 5]  6.00-7.00   sec    127 KBytes    1.04 Mbits/sec   2.305 ms  0/96 (0%)
[ 5]  7.00-8.00   sec    129 KBytes    1.05 Mbits/sec   1.933 ms  0/97 (0%)
[ 5]  8.00-9.00   sec    127 KBytes    1.04 Mbits/sec   2.132 ms  0/96 (0%)
[ 5]  9.00-10.00  sec    129 KBytes    1.05 Mbits/sec   2.437 ms  0/97 (0%)
- - - - -
[ ID] Interval           Transfer     Bitrate      Jitter    Lost/TOTAL  Datagrams
[ 5]  0.00-10.00  sec    1.28 MBytes    1.07 Mbits/sec   0.000 ms  0/966 (0%)  sender
[ 5]  0.00-10.00  sec    1.25 MBytes    1.05 Mbits/sec   2.437 ms  0/966 (0%)  receiver
iperf Done.
```


Wireshark · Capture File Properties · iperf3_filtered_final.pcapng

Details

Hash (SHA256): 0a18fa5953de0f541773fdded5b27dc78453eb317685b5d2dc92cda30ea387f6

Hash (RIPEMD160): 64f1fd4afc0fe9462bf2099ec9a9a9c1481bb4de

Hash (SHA1): a3fe3c7a6b2a0dfb3198c8ee65e0f5d7bc652b5f

Format: Wireshark/... - pcapng

Encapsulation: Ethernet

Time

First packet: 2022-08-29 23:07:41

Last packet: 2022-08-29 23:07:54

Elapsed: 00:00:12

Capture

Hardware: Intel(R) Core(TM) i5-1035G1 CPU @ 1.00GHz (with SSE4.2)

OS: Linux 5.15.0-46-generic

Application: Dumpcap (Wireshark) 3.6.5 (Git v3.6.5 packaged as 3.6.5-1~ubuntu20.04.0+wiresharkdevstable)

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
wlo1	Unknown	none	Ethernet	262144 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	1019	1019 (100.0%)	—
Time span, s	12.328	12.328	—
Average pps	82.7	82.7	—
Average packet size, B	1356	1356	—
Bytes	1381897	1381897 (100.0%)	0
Average bytes/s	112 k	112 k	—
Average bits/s	896 k	896 k	—

Capture file comments

Help

Refresh

Copy To Clipboard

Close

Save Comments

File Properties

3. HTTP Task

1. 9 packets of HTTP/2 and 2 of HTTP/1.1
2. 4 packets are exchanged.
3. HTTP/2 has all the header lines of HTTP/1.1 along with some other lines. These are : x-backend-header-rtt, via, x-frame-options, x-xss-protection, x-content-type-options.

```
▶ Header: :status: 200 OK
▶ Header: date: Sun, 12 Aug 2018 17:30:41 GMT
▶ Header: content-type: text/plain
▶ Header: last-modified: Tue, 08 May 2018 13:53:22 GMT
▶ Header: etag: "5af1abd2-3e"
▶ Header: accept-ranges: bytes
▶ Header: content-length: 62
▶ Header: x-backend-header-rtt: 0.002645
▶ Header: server: nghttpx
▶ Header: via: 2 nghttpx
▶ Header: x-frame-options: SAMEORIGIN
▶ Header: x-xss-protection: 1; mode=block
▶ Header: x-content-type-options: nosniff
```

Header of HTTP/2

4. Ping Task

** I have used 1000 as packet size because for larger sizes there was 100% packet loss.

1. Total 12 IP packets are shared of which 2 are DNS packets
5 are ping request packets and 5 are ping reply packets (no packets were lost.)
2. Total size of packet is 1008 bytes of which 992 bytes data is there.
- 3.

	Fragmented	Length of packet (bytes)	Time of sending	Time of recieving	Actual length of data (bytes)
Query	No	1008	16:48:15.0197	-	992
Response	No	1008	-	16:48:15.7568	992
Query	No	1008	16:48:16.0210	-	992
Response	No	1008	-	16:48:17.0231	992
Query	No	1008	16:48:17.0257	-	992
Response	No	1008	-	16:48:18.0250	992
Query	No	1008	16:48:18.1576	-	992
Response	No	1008	-	16:48:18.8910	992
Query	No	1008	16:48:19.0254	-	992
Response	No	1008	-	16:48:20.0173	992

```
shreyansh@shreyansh-HP-Pavilion-Laptop-14-ce3xxx:~$ ping -s 1000 ping-ams1.online.net -c 5
PING ping-ams1.online.net (163.172.208.7) 1000(1028) bytes of data.
1008 bytes from ping-ams1.online.net (163.172.208.7): icmp_seq=1 ttl=49 time=737 ms
1008 bytes from ping-ams1.online.net (163.172.208.7): icmp_seq=2 ttl=49 time=1005 ms
1008 bytes from ping-ams1.online.net (163.172.208.7): icmp_seq=3 ttl=49 time=1135 ms
1008 bytes from ping-ams1.online.net (163.172.208.7): icmp_seq=4 ttl=49 time=866 ms
1008 bytes from ping-ams1.online.net (163.172.208.7): icmp_seq=5 ttl=49 time=992 ms

--- ping-ams1.online.net ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 737.110/946.855/1134.526/135.007 ms, pipe 2
```

5. Traceroute Task

** I have used 1000 as packet size because for larger sizes I was getting only * after 2 lines.

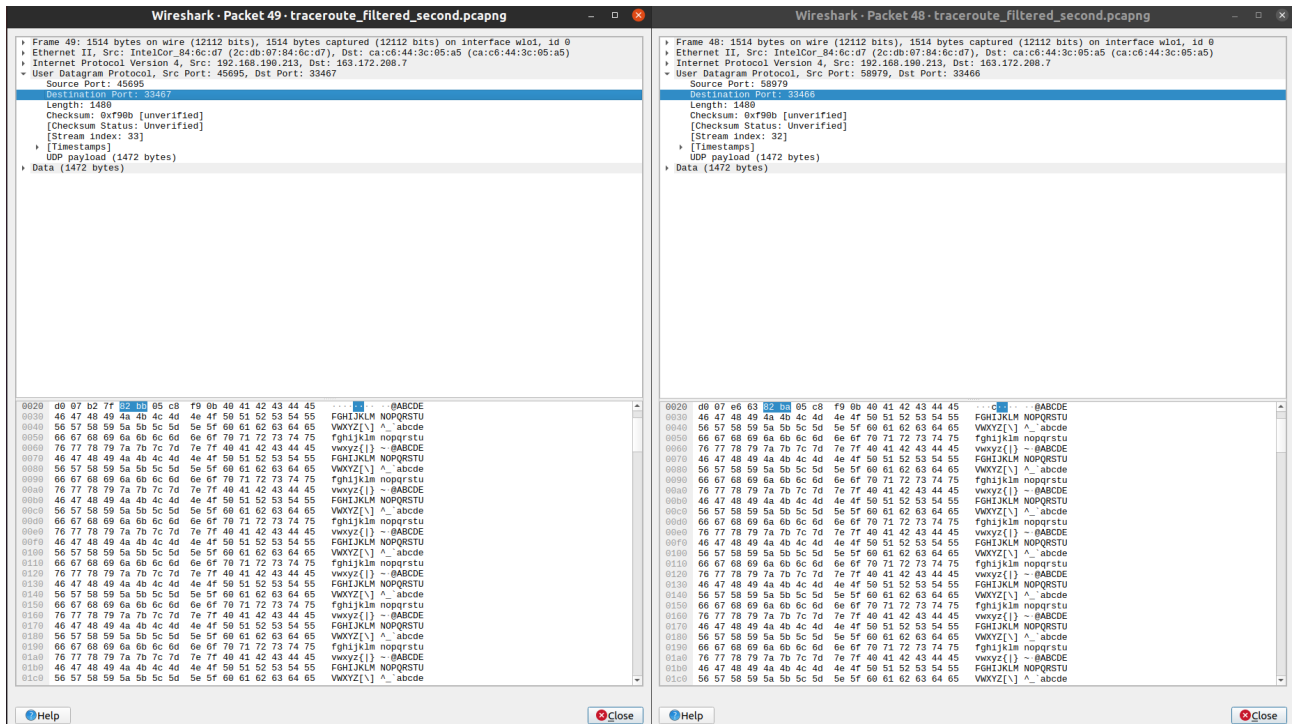
1. 21 hops
2. Total 122 packets are exchanged, of which 116 are sent from client to remote machine and 6 are sent from remote machine to the client.
3. Destination port increases by one and source port changes arbitrarily. Length, check sum, UDP payload remains same.

Checksum and IP should remain same since IP of destination must be same and checksum to verify that message is intact.

The source port and destination port must change because UDP is used and it sends packets one after the other and waits for replies to distinguish between different responses, so it changes the port number.

```
shreyansh@shreyansh-HP-Pavilion-Laptop-14-cd3xxx:~$ traceroute -q 5 ping-ansi.online.net 1000
traceroute to ping-ansi.online.net (163.172.208.7), 30 hops max, 1000 byte packets
 1  _gateway (192.168.14.50)  8.979 ms  9.007 ms  9.255 ms  9.426 ms  9.588 ms
 2  * * * * *
 3  10.72.243.229 (10.72.243.229)  1446.208 ms  56.8.123.73 (56.8.123.73)  1567.655 ms  56.8.123.53 (56.8.123.53)  1799.361 ms * *
 4  * 192.168.44.236 (192.168.44.236)  659.705 ms 192.168.44.232 (192.168.44.232)  1383.159 ms 192.168.44.238 (192.168.44.238)  1648.980 ms *
 5  * * * * *
 6  * * * * *
 7  * * * * *
 8  * * * * *
 9  * * * * *
10  * * * * *
11  * * * * *
12  * * * * *
13  103.198.140.174 (103.198.140.174)  333.651 ms  333.961 ms  333.945 ms * *
14  103.198.140.56 (103.198.140.56)  274.565 ms 103.198.140.29 (103.198.140.29)  274.522 ms 103.198.140.27 (103.198.140.27)  183.454 ms 103.198.140.176 (103.198.140.176)  92.812 ms 103.198.140.174 (103.198.140.174)  90.398 ms
15  * * * * *
16  103.198.140.107 (103.198.140.107)  429.244 ms 195.154.2.103 (195.154.2.103)  429.224 ms 62.210.0.135 (62.210.0.135)  429.280 ms * 195.154.2.103 (195.154.2.103)  429.230 ms
17  195.154.2.103 (195.154.2.103)  429.217 ms * grokoulk.poneytelecom.eu (62.210.175.218)  429.214 ms 62.210.0.135 (62.210.0.135)  429.201 ms 429.188 ms
18  grokoulk.poneytelecom.eu (62.210.175.218)  429.174 ms 306.988 ms 62.210.0.135 (62.210.0.135)  306.926 ms grokoulk.poneytelecom.eu (62.210.175.218)  306.918 ms 306.901 ms
19  195.154.2.104 (195.154.2.104)  306.878 ms grokoulk.poneytelecom.eu (62.210.175.218)  306.861 ms 306.847 ms 306.832 ms 195.154.2.104 (195.154.2.104)  306.798 ms
20  195.154.2.104 (195.154.2.104)  306.766 ms 306.781 ms * 51.158.0.168 (51.158.0.168)  306.796 ms 195.154.2.104 (195.154.2.104)  306.737 ms
21  * 51.158.0.168 (51.158.0.168)  306.753 ms 195.154.2.104 (195.154.2.104)  306.694 ms 51.158.143.1 (51.158.143.1)  341.701 ms ping-ansi.online.net (163.172.208.7)  409.186 ms
```

Output on terminal



Datagram of two consecutive packets