COL334 Assignment 1

Siddhant Mago, 2017CS50419
Lakshay Saggi, 2017CS50412

August 2019

Local Network Analysis

a. **Wifi:**

```
dronemist > traceroute www.iitd.ac.in
traceroute to www.iitd.ac.in (10.7.174.111), 64 hops max, 52 byte packets
 1  10.184.32.14 (10.184.32.14)  9.893 ms  4.544 ms  5.465 ms
 2  10.254.236.18 (10.254.236.18)  5.479 ms  4.182 ms
    10.254.236.10 (10.254.236.10)  5.289 ms
 3  www.iitd.ac.in (10.7.174.111)  5.398 ms  2.967 ms  3.407 ms
```

Ethernet:

```
zion@ubuntu:~$ traceroute www.iitd.ac.in
traceroute to www.iitd.ac.in (10.7.174.111), 64 hops max
  1   10.243.144.1  0.646ms  0.722ms  1.715ms
  2   10.254.243.5  0.334ms  0.279ms  0.247ms
  3   10.254.239.5  0.516ms  0.438ms  0.467ms
  4   10.254.236.22  1.109ms  0.604ms  0.597ms
  5   10.7.174.111  0.265ms  0.243ms  0.214ms
```

b. We probed the above network segments at different times on different days but only found the same hosts up always:
For Wifi:

```
dronemist > nmap -sn 10.7.174.111/24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-08-10 17:39 IST
Nmap scan report for www.iitd.ac.in (10.7.174.111)
Host is up (0.0100s latency).
Nmap scan report for 10.7.174.113
Host is up (0.0091s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 16.99 seconds
```

```
dronemist > nmap -sn 10.254.236.18/24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-08-10 17:37 IST
Nmap scan report for 10.254.236.9
Host is up (0.0094s latency).
Nmap scan report for 10.254.236.10
Host is up (0.0093s latency).
Nmap scan report for 10.254.236.13
Host is up (0.0041s latency).
Nmap scan report for 10.254.236.14
Host is up (0.0040s latency).
Nmap scan report for 10.254.236.17
Host is up (0.0040s latency).
Nmap scan report for 10.254.236.18
Host is up (0.0041s latency).
Nmap scan report for 10.254.236.21
Host is up (0.0054s latency).
Nmap scan report for 10.254.236.22
Host is up (0.0053s latency).
Nmap done: 256 IP addresses (8 hosts up) scanned in 2.71 seconds
```

```
dronemist > nmap -sn 10.184.32.14/24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-08-10 17:37 IST
Nmap scan report for 10.184.32.1
Host is up (1.0s latency).
Nmap scan report for 10.184.32.2
Host is up (0.015s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 2.27 seconds
```

For Ethernet:

```
C:\Program Files (x86)\Nmap>nmap -sn 10.243.144.1/24
Starting Nmap 7.80 ( https://nmap.org ) at 2019-08-15 19:05 India Standard Time
Stats: 0:00:23 elapsed; 0 hosts completed (0 up), 256 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 75.78% done; ETC: 19:05 (0:00:07 remaining)
Stats: 0:00:34 elapsed; 0 hosts completed (0 up), 256 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 91.02% done; ETC: 19:05 (0:00:03 remaining)
Nmap scan report for 10.243.144.1
Host is up (0.019s latency).
MAC Address: 00:06:F6:43:29:C6 (Cisco Systems)
Nmap done: 256 IP addresses (1 host up) scanned in 58.75 seconds
```

```
C:\Program Files (x86)\Nmap>nmap -sn 10.254.243.1/24
Starting Nmap 7.80 ( https://nmap.org ) at 2019-08-15 19:20 India Standard Time
Nmap scan report for 10.254.243.1
Host is up (0.0010s latency).
Nmap scan report for 10.254.243.2
Host is up (0.0080s latency).
Nmap scan report for 10.254.243.5
Host is up (0.0080s latency).
Nmap scan report for 10.254.243.6
Host is up (0.0063s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 4.84 seconds
```

```
C:\Program Files (x86)\Nmap>nmap -sn 10.254.238.5/24
Starting Nmap 7.80 ( https://nmap.org ) at 2019-08-15 19:12 India Standard Time
Nmap scan report for 10.254.238.1
Host is up (0.0010s latency).
Nmap scan report for 10.254.238.2
Host is up (0.0034s latency).
Nmap scan report for 10.254.238.5
Host is up (0.0080s latency).
Nmap scan report for 10.254.238.6
Host is up (0.0070s latency).
Nmap scan report for 10.254.238.9
Host is up (0.0050s latency).
Nmap scan report for 10.254.238.10
Host is up (0.0036s latency).
Nmap done: 256 IP addresses (6 hosts up) scanned in 5.06 seconds
```

```
C:\Program Files (x86)\Nmap>nmap -sn 10.254.236.14/24
Starting Nmap 7.80 ( https://nmap.org ) at 2019-08-15 19:13 India Standard Time
Nmap scan report for 10.254.236.9
Host is up (0.0030s latency).
Nmap scan report for 10.254.236.10
Host is up (0.0020s latency).
Nmap scan report for 10.254.236.13
Host is up (0.0010s latency).
Nmap scan report for 10.254.236.14
Host is up (0.0019s latency).
Nmap scan report for 10.254.236.17
Host is up (0.0010s latency).
Nmap scan report for 10.254.236.18
Host is up (0.0010s latency).
Nmap scan report for 10.254.236.21
Host is up (0.0020s latency).
Nmap scan report for 10.254.236.22
Host is up (0.0020s latency).
Nmap done: 256 IP addresses (8 hosts up) scanned in 4.75 seconds
```

```
C:\Program Files (x86)\Nmap>nmap -sn 10.7.174.111/24
Starting Nmap 7.80 ( https://nmap.org ) at 2019-08-15 19:14 India Standard Time
Nmap scan report for www.iitd.ac.in (10.7.174.111)
Host is up (0.0020s latency).
Nmap scan report for 10.7.174.113
Host is up (0.0020s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 11.16 seconds
```

c. All of the devices were permanent and were mostly switches. They were running Cisco NX-OS, example:

```
Nmap scan report for 10.254.236.18
Host is up (0.0087s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
23/tcp  open  telnet
161/tcp open  snmp
Device type: switch
Running: Cisco NX-OS 5.X|6.X
OS CPE: cpe:/o:cisco:nexus_7000 cpe:/o:cisco:nx_os:5.2 cpe:/o:cisco:nx_os:6.0
OS details: Cisco Nexus 7000 switch (NX-OS 5.2(4)), Cisco Nexus switch (NX-OS 6.0(2))
Network Distance: 4 hops
```

One specific point(which was the last hop for `www.iitd.ac.in`) was running on Linux.

```
C:\Program Files (x86)\Nmap>nmap -O 10.7.174.111/25
Starting Nmap 7.80 ( https://nmap.org ) at 2019-08-15 19:30 India Standard Time
Nmap scan report for www.iitd.ac.in (10.7.174.111)
Host is up (0.0021s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.10, Linux 3.2 - 3.16
Network Distance: 5 hops
```

```
Nmap scan report for 10.7.174.113
Host is up (0.0023s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 5 hops
```

Internet Architecture

In this section we ran the traceroute from servers in Australia, Greece and Canada to the five servers specified in the assignment

Australia

Start Server(Country)	End Server	Number of hops	Average latency(in ms)
Australia	University of Waterloo (Canada east)	16	262.3
	University of Cape Town (South Africa)	17	333.3
	IIT Delhi (India)	Not Reached	NA
	Google	5	11.8
	Facebook	8	11.9

Greece

Start Server(Country)	End Server	Number of hops	Latency (in ms)
Greece	University of Waterloo (Canada east)	18	136.2
	University of Cape Town (South Africa)	21	219.4
	IIT Delhi (India)	Not Reached	NA
	Google	13	47.3
	Facebook	8	28.5

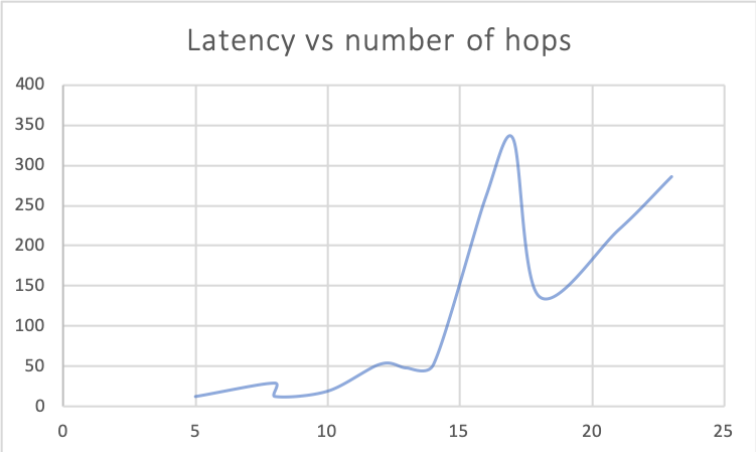
Canada

Start Server(Country)	End Server	Number of hops	Latency (in ms)
Canada	University of Waterloo (Canada east)	14	51.8
	University of Cape Town (South Africa)	23	285.5
	IIT Delhi (India)	Not Reached	NA
	Google	12	52.23
	Facebook	10	18.5

Answers:

2a Yes, as observed for University of Waterloo, the number of hops when a traceroute is called from Canada is 14 as opposed to 16 and 18 when called from Australia and Greece respectively.
Also, as observed from the tables it is evident that the number of hops to websites of large content providers like Facebook and Google are much less than to that of web servers of educational institutions.

2b The following graph was observed:
It is evident from the above graph (apart from the exception of one peek of traceroute to Cape Town from Australia) that as the number of hops increases the average latency between the traceroute servers and the web-servers also increases. However, the distance between the soutce and destination also plays a role in determining the latency.



2c The web servers of the educational institutions always resolved to the same IP address irrespective of from where we did a traceroute to them. While, on the other hand the web servers of Facebook and Google resolved to a different IP address each time. The main reason behind this we think was that large content providers have a lot of IP addresses assigned to them. We usually connect to the one which is reached in minimum number of hops. This is mainly used for load balancing.

2d It we observed that when we do traceroute from a single source to different IP addresses of the same web server, the routes taken were different. The path to the automatically chosen IP address was always the shortest among all the others. For example the traceroute from Greece to the automatically detected IP address of Facebook took 8 hops while from the same server to the IP address 157.240.3.35 (which is also one of the IP addresses of Facebook) took 15 jumps.

2e We observed traceroute from Australia, Czech Republic, Greece, Canada and India. From all these destinations facebook and google were reached with very little number of hops and with a very low latency which suggests that in all these places the local ISP have directly peered with google and facebook.

Local ISP

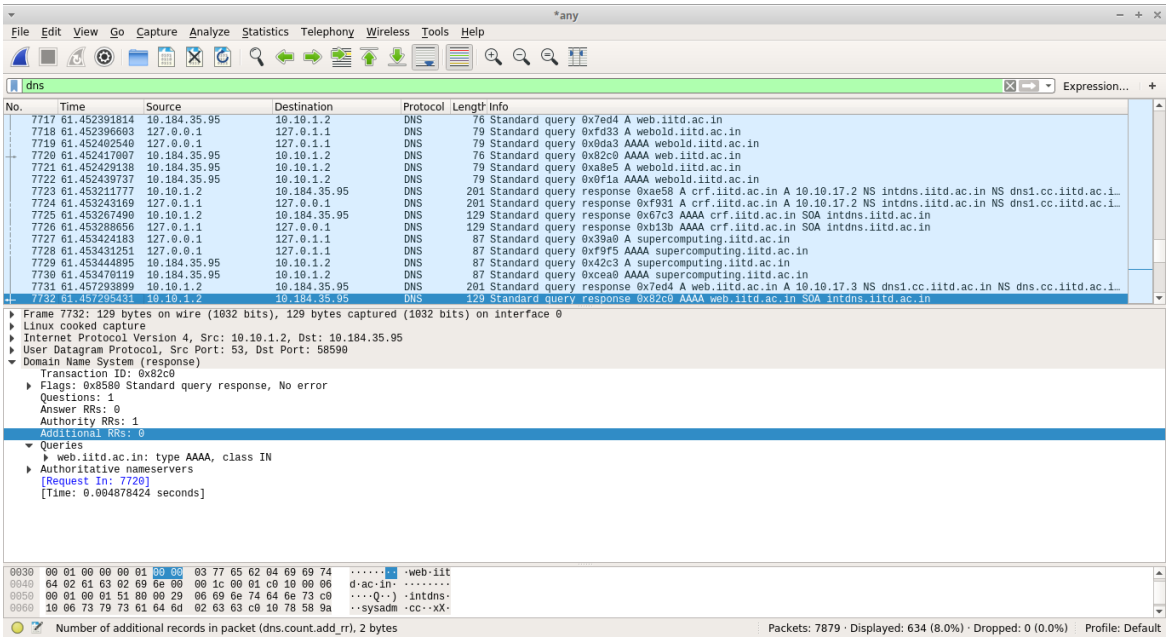
Destination IP	Inside Network		Final Destination	
	Number of hops	Latency (in ms)	Number of hops	Latency (in ms)
University of Waterloo (Canada east)	5	45.2	15	375.2
University of Cape Town (South Africa)	5	40	17	443.8
IIT Delhi (India)	NA	NA	NA	NA
Google	5	23.3	9	30.8
Facebook	5	31.2	9	27.6

2f From the readings, it is evident that the number of hops inside the network and the latency is far less than the total number of hops and latency. This tells us that the major latency is encountered when the data leaves the network of the local ISP.

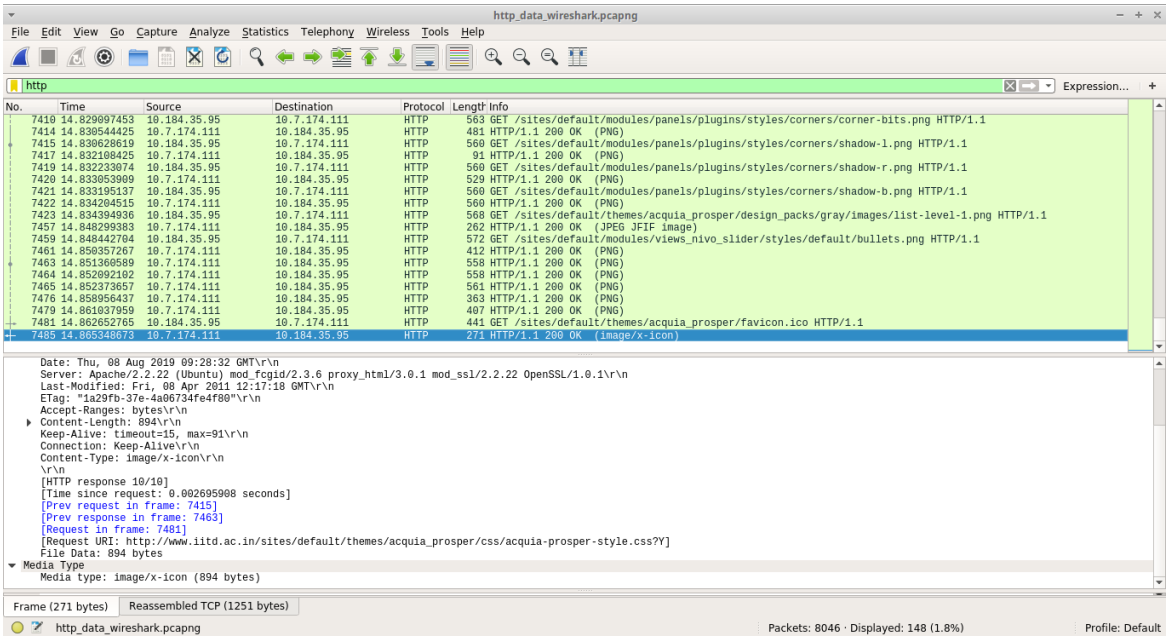
2g The cellular network doesn't show the best latency but it has performed relatively fair against most servers. The problem with the cellular networks is the (hops/latency) ratio which is far worse than any of the trace-servers.
The routes to USA from the local ISP were relatively shorter but that is also owed to the fact that large content providers like google and facebook have a lot of IP addresses, have peered directly with local ISP and do load balancing a lot better than the other websites.

Packet Analysis

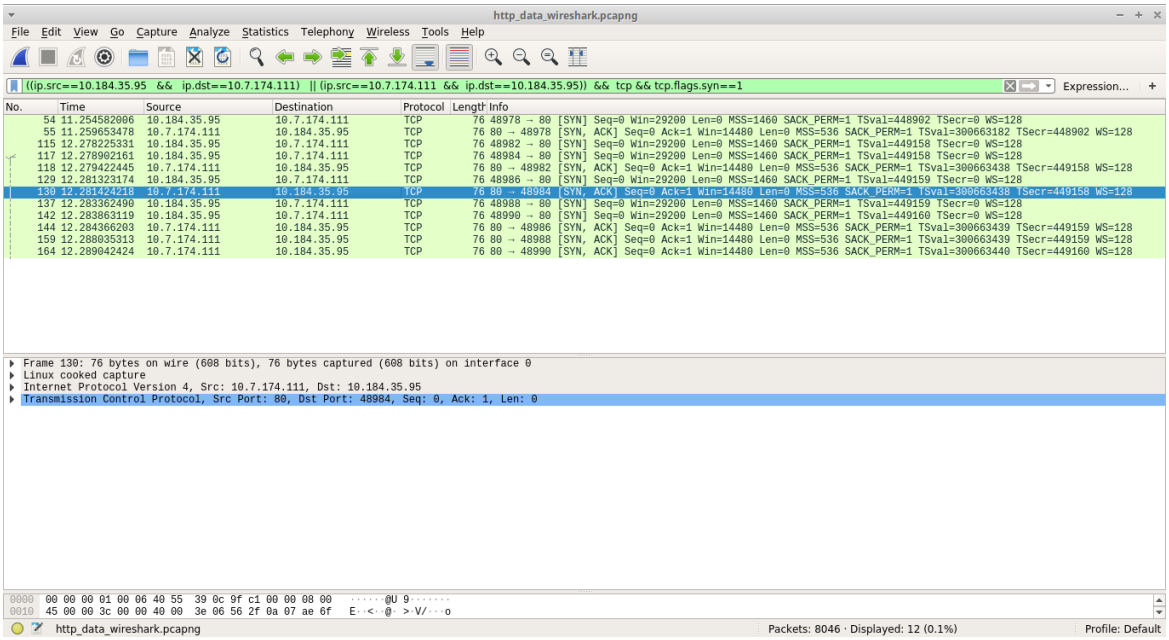
i. Yes, the highlighted response is the DNS response for `www.iitd.ac.in`. It took 0.005s to complete.



ii. There were 7500 requests generated and every request contained some part(HTML/CSS or JS) of the iitd website. This shows that web pages are structured in different parts of HTML/CSS and JS, which are being imported into webpage from various sources(eg: One JavaScript component was coming from `http://www.iitd.ac.in/sites/default/modules/panels/js/panels.js` and one CSS component was coming from `http://www.iitd.ac.in/modules/system/system-menus.css`). Hence, a browser renders complex pages by rendering multiple images/files over many http requests(All are not imported at once). Because of this, the smaller packets arrive earlier and hence, a basic version of website gets displayed first(most text loads first over images).



iii. Since there were 6 SYN messages sent by the browser, there were 6 TCP connections opened. While transferring multiple files or images, browser might be sending them in parts over the multiple TCP connections open between server and client. Yes, some objects were fetched over the same TCP connection.



iv. The entire content was fetched in about 7s. Hence we notice that even though loading of whole website took 7s, we were able to see the main contents of website in 2-3s only.(Because most lighter packets were received by then)

v. No, there was no http traffic, and we werent able to see the contents of any HTML or JS files being transferred. Yes, we were able to see them earlier(Screenshots posted in earlier answer).