# COL334 Assignment 1

Dipen Kumar (2018CS50098)

October 23, 2020

## 1. Network Analysis

1. Run traceroute via Nepal Telecom DSL broadband network (via wifi) for www.google.com

```
(base) Dipens-MacBook-Air:~ dipenkumar$ traceroute www.google.com
traceroute to www.google.com (216.58.196.196), 64 hops max, 52 byte packets
 1  192.168.1.1 (192.168.1.1)  1.959 ms  11.315 ms  1.376 ms
 2  1-adsl.ntc.net.np (49.244.128.1)  41.936 ms  38.242 ms  63.786 ms
 3  202.70.88.181 (202.70.88.181)  39.150 ms  38.222 ms  39.726 ms
 4  10.26.213.41 (10.26.213.41)  39.777 ms  46.367 ms  60.350 ms
 5  * * bhr.ger-04.ge1-1.ntc.net.np (202.70.93.97)  44.654 ms
 6  202.70.93.190 (202.70.93.190)  41.842 ms  42.933 ms  42.476 ms
 7  bhr.core-but.core.ntc.net.np (202.70.93.158)  143.204 ms  45.853 ms  41.365 ms
 8  74.125.119.92 (74.125.119.92)  71.031 ms  68.093 ms  68.854 ms
 9  108.170.251.113 (108.170.251.113)  130.639 ms  129.117 ms
    108.170.251.97 (108.170.251.97)  129.567 ms
10  216.239.47.99 (216.239.47.99)  128.929 ms
    216.239.56.253 (216.239.56.253)  131.161 ms  133.068 ms
11  kul06s14-in-f196.1e100.net (216.58.196.196)  129.772 ms  129.789 ms  129.911 ms
```

2. I have been using macOS and don't find any path that defaults to IPv6. Although, we can use -4 with tracert command in windows to force traceroute to use IPv4. I have seen 10.26.213.41 and 192.168.1.1 which are private IP addresses. Two occurrences of missing routers along the path that do not seem to reply to the traceroute requests.

3. Ping command when used with -s in macOS allows us to specify the size of packets to send. In my case the maximum size of ping packets that I am able to send is 1451 data bytes.

```
(base) Dipens-MacBook-Air:~ dipenkumar$ ping -t 1 -s 1452 www.google.com
PING www.google.com (216.58.196.196): 1452 data bytes

--- www.google.com ping statistics ---
1 packets transmitted, 0 packets received, 100.0% packet loss
(base) Dipens-MacBook-Air:~ dipenkumar$ ping -t 1 -s 1451 www.google.com
PING www.google.com (216.58.196.196): 1451 data bytes
76 bytes from 216.58.196.196: icmp_seq=0 ttl=56 time=173.972 ms
wrong total length 96 instead of 1479

--- www.google.com ping statistics ---
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 173.972/173.972/173.972/0.000 ms
```

## 2. Traceroute Script

Yes we can replicate the traceroute functionality using ping. Ping command when used with -m in macOS allows us to initialize a TTL.

I have given my python script replicating traceroute command using ping along with this report in zip format.

```
(base) Dipens-MacBook-Air:2018CS50098 dipenkumar$ python traceroute.py
traceroute www.iitd.ac.in
traceroute to www.iitd.ac.in (103.27.9.24), 64 hops max
 1  192.168.1.1  1.257 ms  11.501 ms  4.304 ms
 2  49.244.128.1  52.047 ms  173.696 ms  51.234 ms
 3  202.70.88.181  182.395 ms  109.348 ms  36.524 ms
 4  * * *
 5  202.70.93.201  54.950 ms  169.145 ms  239.144 ms
 6  180.87.39.193  1040.593 ms  387.610 ms  326.492 ms
 7  180.87.39.26  445.848 ms  325.216 ms  60.316 ms
 8  172.17.125.238  *  *  *
 9  14.140.210.22  141.514 ms  178.112 ms  225.567 ms
10  10.119.234.161  *  *  *
11  10.119.233.65  *  *  *
12  10.119.233.66  *  *  *
13  * * *
14  103.27.9.24  349.513 ms  254.983 ms  47.265 ms
```

## 3. Internet architecture

1. Yes, the number of hops between nodes in the same continent lower than the number of hops between nodes in different continents. This is because our packet is travelling through many ISP network to reach the destination in the other continent w.r.t when the destination is in the same continent. Yes, Google and Facebook differ from the others in the number of hops required to reach them because they have create their own large network and they directly peer with many local/regional ISP networks to decrease the latency and save cost (money otherwise they would have to give to Tier 1 ISP). The number of hops required to reach them is fairly small from almost every part of world when compared with others end systems separated by continents and large distance. In case of Google and Facebook our packet is not travelling through too many intermediate ISP networks and hence number of hops is small.

| | Google | Facebook | IITD | University of Utah | University of Cape Town |
|---|---|---|---|---|---|
| Germany | 9 | 9 | 30+ | 29 | 30+ |
| USA | 8 | 14 | 30+ | 20 | 30+ |
| My System | 11 | 15 | 14 | 32 | 30+ |

2. Yes, the latency seem to be related to the number of hops, being higher when there are more hops because the number of hops specifies the number of packet switches that were traversed through by our packet to reach the destination. each packet switch will add its processing, queuing, transmission and propagation delay to the overall delay for a packet to reach the destination from the source. This will increase the latency when for more hops.

| | Google | Facebook | IITD | University of Utah | University of Cape Town |
|---|---|---|---|---|---|
| Germany | 3.883 ms | 3.682 ms | time out | 153.429 ms | time out |
| USA | 2.776 ms | 39.821 ms | time out | 51.936 ms | time out |
| My System | 71.220 ms | 139.104 ms | 110.857 ms | 351.664 ms | time out |

3. Web servers of universities are resolved to the same IP address irrespective of from where we do a traceroute to them because they have a single server located fixed in the world. Whereas web servers of of big content and service providers like facebook and google have multiple data centers with multiple servers all around the world. They have created their own network and hence DNS will lookup the address and get reply from authoritative DNS server with an IP address optimized for the client location. When enquired from different part of the world, different DNS servers respond and each will respond with the different addresses optimized for them. Hence they are resolved to different IP addresses when queried from different parts of the world. We can use nslookup to change the DNS server that we want to use and hence will get IP address accordingly. Also busy sites replicated over multiple servers, with each running one different end system and each having different IP address. DNS replies with different IP addresses to distribute the traffic among replicated servers.

4. Yes, the paths are different. Those paths are longer where destination IP address was fetched by traceroute server sitting on some other continent because in that case that IP address is optimized for that traceroute server in that continent and hence our packet will need to traverse more through many ISP networks to reach that destination IP address and thus hops number increases, path length increases and changes accordingly to reach that destination IP address.

5. It is very difficult to find such country. So far all the countries I checked have local ISP directly peered to Google and Facebook. We have to check every IP address in the path and track the path to see if our data is going from regional to tier 1 ISP and then to Google and Facebook in that case we can say local ISP is not directly peered to Google and Facebook. Whois services is limited to check extensively every IP address. We can get rough idea from number of hops, if it is large implies not directly peered and going through many intermediate ISP networks. But if it is low the we can say it is directly peered to local ISP network and immediately our packet get into Google or Facebook network. In my case I am using service of Nepal Telecom and it then forward the packet to Japan Tokyo Google Llc, that local ISP Nepal Telecom is directly peered with google.