Assignment 1

Gohil Dwijesh
2017CS50407

Prafful
2017CS10369

August 2019

1 Local network analysis

Day-1	11/8/19
Afternoon	Afternoon(3pm)
10.243.144.0: 10.243.144.1, 10.243.144.164	**10.243.144.0:** 10.243.144.1, 10.243.144.164
10.254.243.0: 10.254.243.1, 10.254.243.2, 10.254.243.5, 10.254.243.6	**10.254.243.0:** 10.254.243.1, 10.254.243.2, 10.254.243.5, 10.254.243.6
10.254.239.0: 10.254.239.1, 10.254.239.2, 10.254.239.5, 10.254.239.6	**10.254.239.0:** 10.254.239.1, 10.254.239.2, 10.254.239.5, 10.254.239.6
10.254.236.0: 10.254.236.9, 10.254.236.10, 10.254.236.13, 10.254.236.14, 10.254.236.17, 10.254.236.18, 10.254.236.21, 10.254.236.22	**10.254.236.0:** 10.254.236.9, 10.254.236.10, 10.254.236.13, 10.254.236.14, 10.254.236.17, 10.254.236.18, 10.254.236.21, 10.254.236.22

Table 1: Analysis over Ethernet

7/8/19		8/8/19		11/8/19	
Afternoon(15:57)	Night(21.14)	Afternoon(11:40)	Night(19:28)	Afternoon(12:00)	Night
10.184.0.14: 10.184.0.1, 10.184.0.2, 10.184.0.13, 10.184.0.14	**10.184.0.14:** 10.184.0.1, 10.184.0.2, 10.184.0.13, 10.184.0.14	**10.184.0.14:** 10.184.0.1, 10.184.0.2, 10.184.0.13, 10.184.0.14	**10.184.0.14:** 10.184.0.1, 10.184.0.2, 10.184.0.13, 10.184.0.14	**10.184.0.14:** 10.184.0.1, 10.184.0.2, 10.184.0.13, 10.184.0.14	**10.184.0.14:** 10.184.0.1, 10.184.0.2, 10.184.0.13, 10.184.0.14
10.254.236.18: 10.254.236.9, 10.254.236.10, 10.254.236.13, 10.254.236.14, 10.254.236.17, 10.254.236.18, 10.254.236.21, 10.254.236.22	**10.254.236.18:** 10.254.236.9, 10.254.236.10, 10.254.236.13, 10.254.236.14, 10.254.236.17, 10.254.236.18, 10.254.236.21, 10.254.236.22	**10.254.236.18:** 10.254.236.9, 10.254.236.10, 10.254.236.13, 10.254.236.14, 10.254.236.17, 10.254.236.18, 10.254.236.21, 10.254.236.22	**10.254.236.18:** 10.254.236.9, 10.254.236.10, 10.254.236.13, 10.254.236.14, 10.254.236.17, 10.254.236.18, 10.254.236.21, 10.254.236.22	**10.254.236.18:** 10.254.236.9, 10.254.236.10, 10.254.236.13, 10.254.236.14, 10.254.236.17, 10.254.236.18, 10.254.236.21, 10.254.236.22	**10.254.236.18:** 10.254.236.9, 10.254.236.10, 10.254.236.13, 10.254.236.14, 10.254.236.17, 10.254.236.18, 10.254.236.21, 10.254.236.22
10.7.174.111: 10.7.174.111, 10.7.174.113	**10.7.174.111:** 10.7.174.111, 10.7.174.113	**10.7.174.111:** 10.7.174.111, 10.7.174.113	**10.7.174.111:** 10.7.174.111, 10.7.174.113	**10.7.174.111:** 10.7.174.111, 10.7.174.113	**10.7.174.111:** 10.7.174.111, 10.7.174.113

Table 2: Analysis over WiFi

ip	os	ip	os	ip	os
10.184.0.14	Cisco NX-OS	10.184.0.1	Cisco NX-OS	10.184.0.2	Apple Apple TV 5.X (86%)
10.184.0.13	Cisco NX-OS	10.254.236.9	Cisco NX-OS	10.254.236.10	Cisco NX-OS
10.254.236.13	Cisco NX-OS	10.254.236.14	Cisco NX-OS	10.254.236.17	Cisco NX-OS
10.254.236.18	Cisco NX-OS	10.254.236.21	Cisco NX-OS	10.254.236.22	Cisco NX-OS
10.7.174.111	Linux(95%)	10.7.174.113	Linux(95%)	**10.243.144.1**	Cisco switch(97%)
10.254.243.1	Cisco switch(95%)	**10.254.239.1**	Cisco switch	**10.254.236.21**	Cisco NX-OS

Table 3: IP vs OS

2 Internet Architecture

Servers	Waterloo		Capetown		IIT Delhi		Google		Facebook	
	# Hops	latency(ms)	# Hops	latency(ms)	# Hops	latency(ms)	# Hops	latency(ms)	# Hops	latency(ms)
s1(Czech)	17	123.7	18	200.9	-1	-1	6	6.5	6	5.73
s2(USA)	13	20.4	15	217.4	-1	-1	7	3.0	8	18.7
s3(Australia)	17	208.5	21	417.3	-1	-1	14	208.1	11	189.1

Table 4: Tracerouting through servers from different continents

RTT	Waterloo		CapeTown		IIT Delhi		Google		Facebook	
	# Hops	latency	# Hops	latency	# Hops	latency	# Hops	latency	# Hops	latency
Total path	14	476	17	682.5	-1	-1	10	78.4	9	52.2
last router in local ISP	6	560.7	6	223.8	-1	-1	5	38.3	6	54.4

Table 5: Tracerouting from IIT Delhi using Airtel 4G

a)

- Yes, the number of hops between nodes of same continent are lower when compared to nodes on different continents. This can be attributed to the fact that more distance is to be travelled (hence more hops) when the connection has to established overseas.
- **Few hops for google and facebook** can be due to
  - direct peering with the local ISPs.
  - duplicating the original content to web servers in many continents to reduce the latency over the network.

b) **# hops vs latency:**

- **# hops:** In reality, traceroute's hop count does not reflect the actual number of hops between source and the destination ip. It can be more than or less than the hop count. Reasons for that can be transparent firewall, or switches. Trace route only shows level 3 hops.
- **Latency:** Latency is not strictly related to #hops. Table 4 reflects this fact. Consider (15, 217.4), (17, 123.7), (17, 208.5) pairs.

c) Web servers of University of Waterloo, University of Capetown are always resorted to the same IP address and the Google, Facebook resorts to different web servers when trace routed from different continents. Reasons can be:

- Google and Facebook both duplicate their web content to web servers in different continents, because of to reduce the latency, reduce the network congestion. As a result tracerouting from different continents gives different IP address. While for the Universities, web content must be accessed from the same web server irrespective of the continent.
- There can be duplication on the same web server to incorporate the traffic. Here we can have round robin protocol or similar. This type of duplication can also result in tracerouting to different IP address.

d) Yes, the paths appear different. The different ip addresses found for the same domain name (google and facebook) are because of different web servers owned by the same company (provider), which are located in different locations of the world. When probed with the domain name, the server which is closely accessible from the client's location is set up. Hence, the paths obtained for corresponding ip addresses(the server when tracerouted with the domain name) are relatively shorter when compared to other addresses related to the same host name. An example to demonstrate this: the resultant addresses when probed for www.google.com from Czech Republic, USA and Sydney are 172.217.23.228, 172.3.100 and 172.217.6.36 respectively. The #hops and latency when these 3 ip addresses are probed from Sydney are:

- Czech : 18 hops and 330 ms
- USA : 13 hops and 240 ms
- Sydney : 11 hops and 184 ms

e) If the local ISPs peer with google or facebook, the data packets flow through the peered exchange point and reach the google server(google data center) directly. Else, they flow through a longer path through different countries. The following countries do not have their local ISPs peered with

- Google: South Korea (Japan), Dijbouti (Dubai), New Zealand (Japan), some parts of Australia(Japan) The places in the brackets are the corresponding places where the google's POP is reached. Most of the European countries like Germany, France, Italy etc; Asian countries like India, Japan, UAE and both American continents have good amount of peering with google
- Facebook : Denmark, Colombo, South Korea

f) Latency incurred within the ISP is greater than the latency caused by remaining network in most of the cases (Refer Table 5). The major causes for latency are transmission mediums, propagation delays, routers and storage delays. The higher latency with my local ISP can be due to the Storage delays that occur at switches and bridges.

g) Yes, there is difference in the connectivity of my ISP with rest of the world. It is very well connected with the USA and UK networks when compared to other regions. This can also be attributed to the heavier traffic across these regions relative to others from India.
NOTE: IIT Delhi web server blocks traceroute request from any server. So, whenever www.iitd.ac.in is tracerouted it reaches max hop limit (30 or 64) with all the TTLs after 10th or 11th hop having all the 3 packets timed out(returning *). Because of which, accurate #hops and latency could not be concluded.

3 Packet Analysis

a) Grabbing and analysing packets while visiting www.iitd.ac.in website

i) DNS filter

- My laptop(10.184.52.92) sends DNS query to IIT Delhi DNS server(10.10.2.2)
- Asking for IP addresses for the requested domain name (iitd.ac.in) and all the domain names which are linked with that web page(i.e., library.iitd.ac.in)
- IIT Delhi DNS server replies with IP address of the queried domain name. For example, reply for iitd.ac.in domain name is 10.7.174.111
- Time taken for the both query and reply for iitd.ac.in domain name is 0.008394231 seconds
- Total time taken to resolve all DNS queries is: 3.67165445 seconds

ii) HTTP filter

- 150 HTTP requests found
- My laptop(10.184.52.92) sends an HTTP request to iitd.ac.in(10.7.174.111) website host, asking for the html(or similar) code of the web-page
- Host(10.7.174.111) sends an HTTP respond to me(10.184.52.92), sending the web-page code
- Complex web-pages consist of references to many other files(.css, .js, etc.), photos, gifs, etc. in its HTML code
- My browser starts rendering the received code. As soon as it finds references to any file that is located in the server, it sends a new HTTP request, asking for the content of that file
- As the browser encounters file references while rendering, it keeps asking for the content via HTTP requests

iii) TCP filter

- Optimization done by the browser:
  - There are multiple TCP connections made from source port to destination port(80). Each TCP connection defers in source port(43001-43187). By default each connection is persistent unless client explicitly signals the closing of TCP connection
  - Multiple HTTP requests-responses can be made on the same TCP connection. In general these requests are pipe-lined
  - Such HTTP requests-responses can be made on all the TCP connections between the source and the destination host
  - This configuration makes TCP protocols to work more efficiently, and reduces the network traffic.
  - Total 6 TCP connections were established between localhost(me) and the destination server, that includes the following destination ports: 43082, 43084, 43086, 43088, 43090, 43092
- Yes, there are some content objects that are fetched on the same TCP port because of multiple HTTP requests can be made on the same TCP connection
- After any TCP connection is established, client sends an HTTP request to server and as soon as the server receives the request it sends back a TCP ack packet to the client and vice versa

iv) Time taken to download the complete web-page

- Time at the first DNS query: 2.311199694 sec
- Time at the last HTTP response: 5.853938462 sec
- Total time taken to download the complete web-page is: 3.54273877 sec

v) HTTP vs HTTPS protocols

- Observations:
  - After tracing for http://www.indianexpress.com website and analyzing the packets we could find exactly one HTTP packet and instead we found TLSv1.2 packets
- HTTP vs HTTPS:
  - HTTP response packet contains:

```
HTTP/1.1 301 Moved Permanently
 Location: https://indianexpress.com
```

  - HTTPS is more secure than HTTP. It consists of SSL certificate that encrypts the data being transferred on the network for the security purposes. It also uses TLS(Transport Layer Security) protocol to prevent the data being modified or corrupted
  - That is why we see TLSv1.2 packets instead of HTTP packets
- Take home message:
  - Sensitive websites that involve routing of sensitive user data, prefer secure connection. Indianexpress also uses the secure connection, so we can not see the data being transffered(in this case: the webpage content), because it is encrypted using SSL certificate.

4 Tinkering with the network setting

4.1 Where to configure IP address and DNS server

- Linux: add the following to /etc/network/interfaces file.

```
auto eth0
iface eth0 inet static
    address 10.0.0.41
    netmask 255.255.255.0
    network 10.0.0.0
    broadcast 10.0.0.255
    gateway 10.0.0.1
    dns-nameservers 10.0.0.1 8.8.8.8
    dns-domain acme.com
    dns-search acme.com
```

4.2 Configure static IP address on android

- wifi settings -> networks details -> IP setting(change it from DHCP to Static) -> (fill the details)

4.3 Static IP Assignment vs Dynamic IP Assignment

- Static IP addresses are the fixed IP addresses given to any device on internet and Dynamic IP addresses change over time(dynamically assigned).
- Static IP addresses are more vulnerable compared to Dynamic ones. So mail servers, gaming servers which are not worried about their locations, generally use static IP addressing, while business, offices, etc. uses dynamic IP addressing.