COL334 Assignment - 1

Aditya (2019CS50471)

21st August, 2021

Contents

1 Networking Tools

1.a *ifconfig*

I identified IP Address of my machine using *ifconfig* command. Here are the IP Addresses of my machine when connected to different service providers:

1. BSNL Wifi: 192.168.1.200

2. Airtel Wifi: 192.168.1.101

3. Jio Hotspot: 192.168.133.190

From these, we can notice that IP Address of my machine is changing if I change the service provider.

(a) IP Address of my PC (BSNL)   (b) IP Address of my PC (Airtel)

(c) IP Address of my PC (Jio)

1.b   *nslookup*

I identified the IP Address associated with www.google.com and www.facebook.com using *nslookup* command. IP Address of www.google.com is 142.250.193.164 and IP Address of www.facebook.com is 157.240.228.35.

After changing DNS Server:

1. Google Public DNS (8.8.8.8): IP Address of www.google.com is 142.250.196.4 and www.facebook.com is 157.240.228.35

2. Cisco OpenDNS (208.67.222.222): IP Address of www.google.com is 142.250.182.100 and www.facebook.com is 157.240.228.35

3. Quad9 (9.9.9.9): IP Address of www.google.com is 142.250.66.132 and www.facebook.com is 157.240.235.35

4. Cloudflare (1.1.1.1): IP Address of www.google.com is 142.250.183.4 and www.facebook.com is 31.13.79.35

We can notice that, IP Address depends on the DNS Server.

(a) IP Address associated with google

(b) IP Address associated with Facebook

(a) IP Address of google (Google Public DNS)

(b) IP Address of Facebook (Google Public DNS)

(a) IP Address of google (Cisco OpenDNS)

(b) IP Address of Facebook (Cisco OpenDNS)

(a) IP Address of google (Quad9)

(b) IP Address of Facebook (Quad9)

(a) IP Address of google (CloudFlare)

(b) IP Address of Facebook (CloudFlare)

1.c *ping*

Average RTT values for packets with size 56 bytes is 126.248 ms, size 100 bytes is 141.161 ms, size 250 bytes is 135.979 ms. The maximum size of ping packets that I am able to send is 1472(1500) data bytes. From the figure(c), we can see that for 1472(1500), we got response and for 1473(1501) we didn't get reply. It is not same for www.google.com and www.facebook.com
For www.google.com, this value is 68 data bytes and for www.facebook.com, this value is 1452 data bytes.

(a) Maximum packet size for www.google.com   (b) Maximum packet size for www.facebook.com

(c) Maximum packet size for www.iitd.ac.in

1.d *traceroute*

Traceroute for www.google.com via different service providers:

1. BSNL Wifi: No of hops - 10, No of routers responded - 9, No of routers didn't respond - 1

2. Airtel Wifi: No of hops - 12, No of routers responded - 11, No of routers didn't respond - 1

3. Jio Hotspot: No of hops - 14, No of routers responded - 12, No of routers didn't respond - 2

(a) Traceroute of Google (BSNL)   (b) Traceroute of Google (Airtel)

(c) Traceroute of Google (Jio)

Traceroute for www.facebook.com via different service providers:

1. BSNL Wifi: No of hops - 15, No of routers responded - 10, No of routers didn't respond - 5

2. Airtel Wifi: No of hops - 10, No of routers responded - 9, No of routers didn't respond - 1

3. Jio Hotspot: No of hops - 14, No of routers responded - 13, No of routers didn't respond - 1

(a) Traceroute of Facebook (BSNL)   (b) Traceroute of Facebook (Airtel)

(c) Traceroute of Facebook (Jio)

We can force the *traceroute* to use IPv4 by using -4 in the command.

Changes to *traceroute* request for some of the missing routers to reply:

1. We can use ICMP packets instead of UDP Packets by using -I in command, because UDP Packets are not reliable

2. We can increase the wait time of response by using -w <wait time>in command

2   Packet Analysis

Using wireshark, I grabbed all packets on your interface while visiting the website http://apache.org from the browser

2.a   DNS Filter

I applied DNS filter on the grabbed packets. The time stamp for DNS request is 5.9032 s and time stamp for DNS response is 5.9894. So, the time taken for DNS request - response is 86.2 ms. In the below figure, the DNS request is in No 223 and response is in No 242.

(a) DNS Request   (b) DNS Response

2.b   HTTP Filter

I applied http filter and the number of http requests generated are 28. From this we can say that web page consists of different objects (these can be images, HTML files, audio files) which are

stored on different web servers. So, for downloading each of these objects, a http request is sent and we receive the response message containing required object.

(a) HTTP Requests

2.c   Total Time

Time stamp when first DNS request generated is 5.9032 sec. Time stamp when last content object (last http response) was received is 7.9517 sec. So, the total time taken to download the entire web page is 2.0485 sec.

(a) First DNS Request

(b) Last Content response

2.d   HTTP Traffic

There is no http traffic when I visit http://www.cse.iitd.ac.in/. The reason is that, this webpage is secure. So, it follows https protocol and we can't find http traffic. But http://apache.org/ follows http protocol, so we can find http traffic easily.
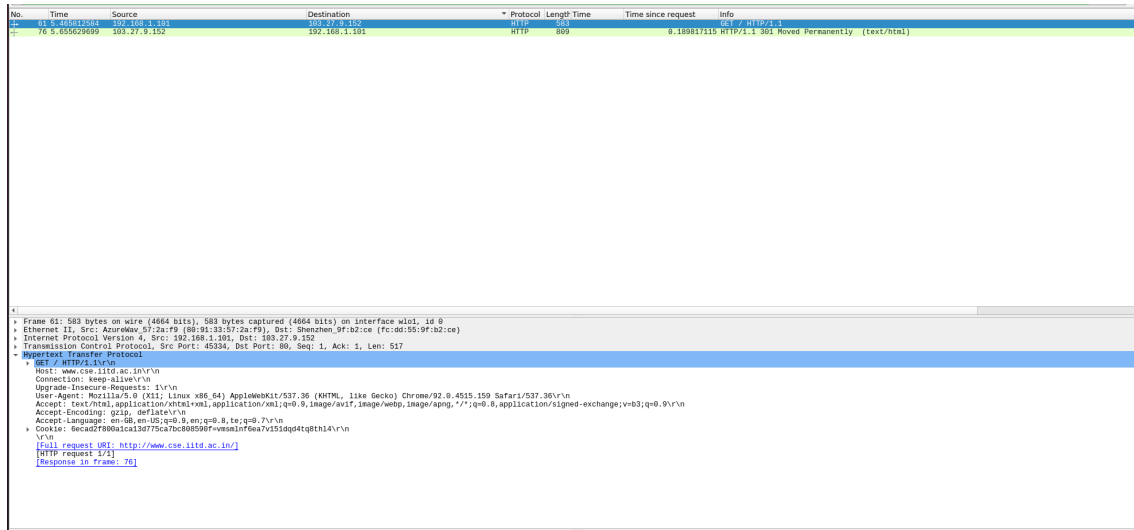
Figure 13: No http Traffic when we visit http://www.cse.iitd.ac.in/

3   Implementing Traceroute

I Implemented Trace route using scapy library. The program sends ICMP Packets with varying TTL values to get the IP Address of the hops in between and then calculates RTT values for these hops. Using matplotlib library, the graph of RTT vs hop number is plotted.

The following are the screenshots of output showing IP addresses of all the hops and RTT values for all these hops:
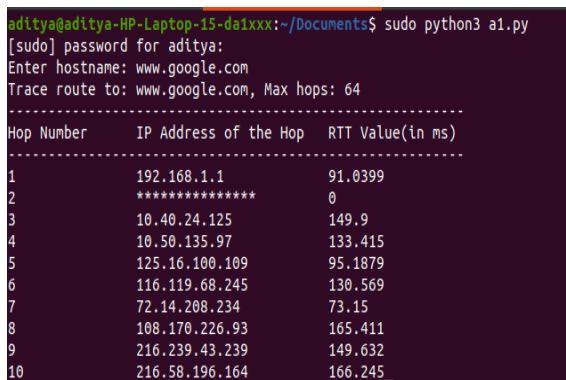
(a) Hops on the way to www.google.com
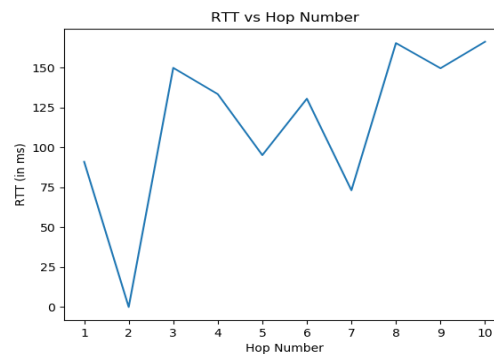
(b) RTT vs Hop Number for www.google.com
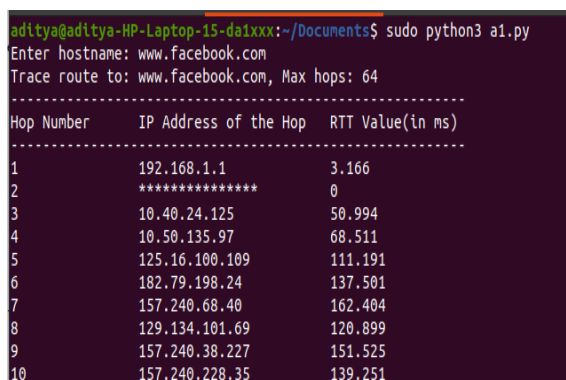
(a) Hops on the way to www.facebook.com
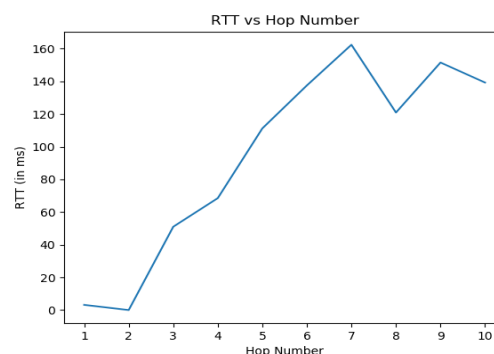
(b) RTT vs Hop Number for www.facebook.com

```
Enter hostname: www.iitd.ac.in
Trace route to: www.iitd.ac.in, Max hops: 64
--------------------------------------------------------
Hop Number     IP Address of the Hop   RTT Value(in ms)
--------------------------------------------------------
1              192.168.1.1             3.117
2              ***************         0
3              10.40.24.125            95.8669
4              10.50.135.97            108.404
5              125.16.100.109          95.503
6              116.119.68.108          166.575
7              ***************         0
8              115.255.253.237         110.345
9              115.249.198.97          115.941
10             10.255.222.3            0
11             ***************         0
12             ***************         0
13             ***************         0
14             ***************         0
15             ***************         0
16             103.27.9.24             158.743
17             103.27.9.24             94.417
18             103.27.9.24             160.656
```
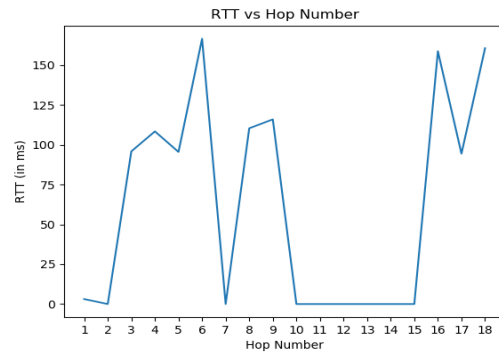
(a) Hops on the way to www.iitd.ac.in

(b) RTT vs Hop Number for www.iitd.ac.in

4   Appendix

1. Operating System: Linux (Ubuntu)