Computer Networks (COL334)
Assignment 1

Pratyush Saini (2019CS10444)

21 August 2021

1 Networking Tools

1.1 IP Detection

a) IITD WiFi
IPv4 : 10.194.12.226
IPv6 : fe80::145d:e88f:6798:9b49

```
en0: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether 1c:91:80:cb:7a:75
        inet6 fe80::145d:e88f:6798:9b49%en0 prefixlen 64 secured scopeid 0xc
        inet 10.194.12.226 netmask 0xffffe000 broadcast 10.194.31.255
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
```

b) Jio
IPv4 : 192.168.43.231
IPv6 : 2409:4050:2ec2:33fb:94a9:b3e0:1e29:db06

c) Airtel
IPv4 : 192.168.1.100
IPv6 : 2401:4900:446f:31e:6031:1e09:68f0:59e7

Results: The IP address provided by different service providers is dynamic in nature and varies accordingly depending on different network connections. New DHCP servers, would assign a new IP address when connected to different service providers.

1.2 nslookup

a) Domain Server : www.google.com

i) IITD DNS Server : dns.cc.iitd.ac.in
IP obtained : 142.250.77.228 (Non-authoritative)

ii) Google DNS : ns1.google.com (216.239.32.1053)
IP obtained : 172.217.167.196

iii) CISCO DNS : 208.67.220.22053
IP obtained : 142.250.194.164 (Non-authoritative)

```
pratyushsaini@Pratyushs-MacBook-Air ~ % nslookup www.google.com dns.cc.iitd.ac.in
Server:         dns.cc.iitd.ac.in
Address:        10.10.1.2#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.77.228

pratyushsaini@Pratyushs-MacBook-Air ~ % nslookup www.google.com ns1.google.com
Server:         ns1.google.com
Address:        216.239.32.10#53

Name:   www.google.com
Address: 172.217.167.196

pratyushsaini@Pratyushs-MacBook-Air ~ % nslookup www.google.com 208.67.220.220
Server:         208.67.220.220
Address:        208.67.220.220#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.194.164
```

b) Domain Server : www.facebook.com

i) IITD DNS Server : dns.cc.iitd.ac.in
IP obtained : 157.240.16.35 (Non-authoritative)

ii) Facebook DNS : a.ns.facebook.com (129.134.30.1253)
IP obtained : 157.240.16.35

iii) CISCO DNS : 208.67.220.22053
IP obtained : 157.240.16.35 (Non-authoritative)

```
pratyushsaini@Pratyushs-MacBook-Air ~ % nslookup www.facebook.com dns.cc.iitd.ac.in
Server:         dns.cc.iitd.ac.in
Address:        10.10.1.2#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

pratyushsaini@Pratyushs-MacBook-Air ~ % nslookup www.facebook.com a.ns.facebook.com
Server:         a.ns.facebook.com
Address:        129.134.30.12#53

www.facebook.com        canonical name = star-mini.c10r.facebook.com.

pratyushsaini@Pratyushs-MacBook-Air ~ % nslookup www.facebook.com 208.67.220.220
Server:         208.67.220.220
Address:        208.67.220.220#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
```

1.3 Ping

Service Provider : **IITD WiFi**
Maximum allowed packet size : 8192 bytes (Including header)

```
pratyushsaini@Pratyushs-MacBook-Air ~ % ping www.iitd.ac.in -c 4 -s 8184
PING www.iitd.ac.in (10.10.211.212): 8184 data bytes
8192 bytes from 10.10.211.212: icmp_seq=0 ttl=61 time=19.267 ms
8192 bytes from 10.10.211.212: icmp_seq=1 ttl=61 time=15.548 ms
8192 bytes from 10.10.211.212: icmp_seq=2 ttl=61 time=13.914 ms
8192 bytes from 10.10.211.212: icmp_seq=3 ttl=61 time=10.205 ms

--- www.iitd.ac.in ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 10.205/14.733/19.267/3.256 ms
pratyushsaini@Pratyushs-MacBook-Air ~ % ping www.iitd.ac.in -c 4 -s 8185
PING www.iitd.ac.in (10.10.211.212): 8185 data bytes
ping: sendto: Message too long
ping: sendto: Message too long
Request timeout for icmp_seq 0
ping: sendto: Message too long
Request timeout for icmp_seq 1
ping: sendto: Message too long
Request timeout for icmp_seq 2
```

Server : **www.facebook.com**
Maximum allowed packet size : 1480 bytes (Including header)

Server : **www.google.com**
Maximum allowed packet size : 76/1480 bytes (Including header)

```
pratyushsaini@Pratyushs-MacBook-Air ~ % ping www.facebook.com -c 4 -s 1472
PING star-mini.c10r.facebook.com (157.240.16.35): 1472 data bytes
1480 bytes from 157.240.16.35: icmp_seq=0 ttl=53 time=29.335 ms
1480 bytes from 157.240.16.35: icmp_seq=1 ttl=53 time=29.180 ms
^C
--- star-mini.c10r.facebook.com ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 29.180/29.258/29.335/0.078 ms
pratyushsaini@Pratyushs-MacBook-Air ~ % ping www.facebook.com -c 4 -s 1474
PING star-mini.c10r.facebook.com (157.240.16.35): 1474 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
```

Pinging with different TTL values

Service Provider : **IITD WiFi**

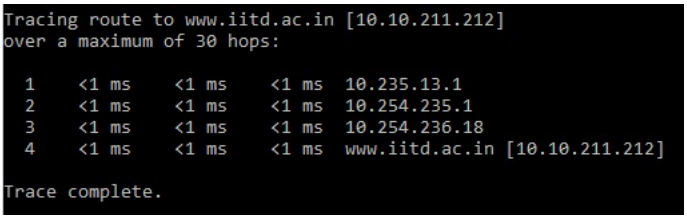
```
--- www.iitd.ac.in ping statistics ---
1 packets transmitted, 0 packets received, 100.0% packet loss
pratyushsaini@Pratyushs-MacBook-Air ~ % ping www.iitd.ac.in -c 1 -m 3
PING www.iitd.ac.in (10.10.211.212): 56 data bytes
36 bytes from 10.254.236.14: Time to live exceeded
Vr HL TOS  Len   ID Flg  off TTL Pro  cks      Src      Dst
 4  5  00 5400 3afa   0 0000  01  01 9153 10.194.4.188  10.10.211.212


--- www.iitd.ac.in ping statistics ---
1 packets transmitted, 0 packets received, 100.0% packet loss
pratyushsaini@Pratyushs-MacBook-Air ~ % ping www.iitd.ac.in -c 1 -m 4
PING www.iitd.ac.in (10.10.211.212): 56 data bytes
64 bytes from 10.10.211.212: icmp_seq=0 ttl=61 time=3.664 ms

--- www.iitd.ac.in ping statistics ---
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 3.664/3.664/3.664/0.000 ms
pratyushsaini@Pratyushs-MacBook-Air ~ % ping www.iitd.ac.in -c 1 -m 10
PING www.iitd.ac.in (10.10.211.212): 56 data bytes
64 bytes from 10.10.211.212: icmp_seq=0 ttl=61 time=11.704 ms
```

Service Provider : **Jio**

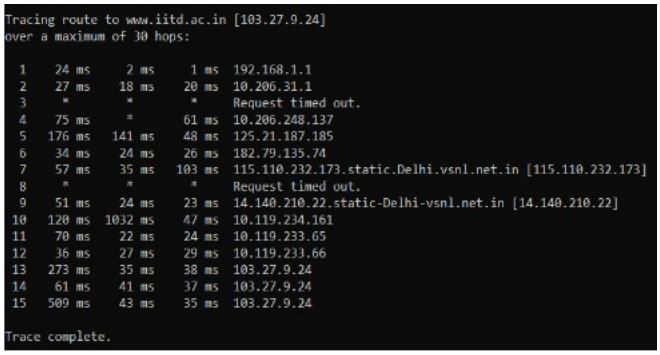
```
--- www.iitd.ac.in ping statistics ---
1 packets transmitted, 0 packets received, 100.0% packet loss
(pratyushsaini@Pratyushs-MacBook-Air ~ % ping www.iitd.ac.in -c 1 -m 10
PING www.iitd.ac.in (103.27.9.24): 56 data bytes
76 bytes from 172.26.14.73: Time to live exceeded
Vr HL TOS  Len   ID Flg  off TTL Pro  cks      Src      Dst
 4  5  28 5400 32a1   0 0000  01  01 2a1e 192.168.43.231  103.27.9.24


--- www.iitd.ac.in ping statistics ---
1 packets transmitted, 0 packets received, 100.0% packet loss
(pratyushsaini@Pratyushs-MacBook-Air ~ % ping www.iitd.ac.in -c 1 -m 18
PING www.iitd.ac.in (103.27.9.24): 56 data bytes
36 bytes from 103.27.9.24: Time to live exceeded
Vr HL TOS  Len   ID Flg  off TTL Pro  cks      Src      Dst
 4  5  28 5400 83c5   0 0000  01  01 d8f9 192.168.43.231  103.27.9.24


--- www.iitd.ac.in ping statistics ---
1 packets transmitted, 0 packets received, 100.0% packet loss
(pratyushsaini@Pratyushs-MacBook-Air ~ % ping www.iitd.ac.in -c 1 -m 25
PING www.iitd.ac.in (103.27.9.24): 56 data bytes
64 bytes from 103.27.9.24: icmp_seq=0 ttl=45 time=122.406 ms

--- www.iitd.ac.in ping statistics ---
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 122.406/122.406/122.406/0.000 ms
```

1.4 Traceroute

Traceroute implementation using IITD WiFi



Traceroute implementation using Airtel



To obtain results in IPv4 form, we can use -4 flag.

To receive the IP address of routers which do not reply to requests, we can try obtaining their IPs by changing the protocol.
By using the -I flag, we can send packets using ICMP protocols rather than UDP protocol by default. Some routers do not repond to UDP packets due to it's unreliability. Routers which do not reply even on using the icmp packets, it is not possible to get their ip (it might be using firewall).

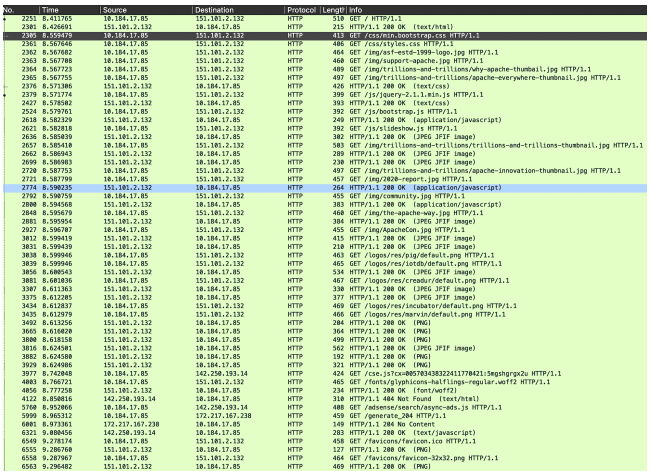
2 Packet Analysis

2.1 DNS Response request

2246	8.399058	10.184.17.85	10.10.2.2	DNS	70	Standard query 0x9013 A apache.org
2247	8.403928	10.10.2.2	10.184.17.85	DNS	404	Standard query response 0x9013 A apache.org A 151.101.2

Time Taken for DNS Response Request: 8.404 - 8.399 = 0.005 seconds

2.2 HTTP Requests



Approx number of HTTP Request generated = 27 (25 + 2 (Advertisements))
A web browser is a piece of software that requests and loads file from a remote server and displays them accordingly for user interaction. We observe that website data (Images and Files) are sent as chunks in the form of data packets over Internet and then, the browser renders them accordingly. Each data packets has a header associated with it which stores information about the previous and next data packets, which allows the browser to collect and render data in order.

2.3 Total time to download the webpage

Time of receiving last data packet = 9.296 seconds.
Total time to download = 9.296 - 8.399 = 0.897 seconds.

2.4 Packet tracing for cse.iitd.ac.in

No.	Time	Source	Destination	Protocol	Length	Info
423	11.258617	10.194.4.188	10.208.20.4	HTTP	518	GET / HTTP/1.1
426	11.262155	10.208.20.4	10.194.4.188	HTTP	285	HTTP/1.1 301 Moved Permanently (text/html)
461	11.466616	10.194.4.188	104.71.61.81	HTTP	421	GET /MFgwVqADAgEAME8wTTBLMAkGBSsOAwIaBQAEFEjayaD7K
464	11.565545	104.71.61.81	10.194.4.188	OCSP	431	Response

There is very less traffic on https://www.cse.iitd.ac.in as compared to http://apache.org
This is because the apache.org is not secured so we can easily filter is using http and but as the cse.iitd.ac.in is secured as it is https so we can't see it's traffic by filtering through http. HTTPS is used to provide encrytion to the data. Wireshark can not decrypt the content, because the used protocol inside the TLS connection is unknown to Wireshark. .We can use tls or tcp.port==443 to obtain https packets.

3 Traceroute using ping

```
pratyushsaini@Pratyushs-MacBook-Air COL334 % ./main www.geeksforgeeks.org
1       RTT = 16.170ms          IPv4 = 10.184.0.14
2       RTT = 09.634ms          IPv4 = 10.255.1.34
3       RTT = 15.259ms          IPv4 = 10.119.233.65
4       RTT = 15.105ms          IPv4 = 10.1.207.69
5       RTT = 07.141ms          IPv4 = 10.119.234.162
6       RTT = 11.677ms          IPv4 = 10.184.17.85
7       RTT = 07.396ms          IPv4 = 23.15.35.9
```