Assignment 1, COL334

Sarthak Singla

08/21/21

1 Networking Tools

a) **IP Address of machine** - The IP Address of a machine can be determined by using the *ipconfig* tool. The IP Address of my machine when connected to different service providers is as follows -

- Home Broadband (Airtel, 5GHz) : 192.168.1.24
- Home Broadband (Airtel, 2.4GHz) : 192.168.1.12
- Mobile Hotspot (Jio) : 192.168.8.126

The IP Address of our machine is not fixed as it is not a public IP Address. It is a private IP Address allocated by the wifi router or mobile's inbuilt router. Therefore it depends on which service provider we are using.

b) **IP Address of websites** - The IP Address of a can be determined using the *nslookup* tool. We need to provide IP Address of a DNS server for lookup. If a DNS server is not specified, the default DNS server is used.

Website/DNS server	default	8.8.8.8	1.1.1.1	9.9.9.9
www.google.com	142.250.194.14	142.250.194.14	142.250.194.238	216.58.220.206
www.facebook.com	192.168.1.1	157.240.239.35	157.240.239.35	157.240.235.35

We observe that the IP Address varies with DNS Server used because of different IPs stored. Even the same DNS Server stores multiple IP Addresses for the same domain which it gives in rotation to do load balancing.

c) **Ping** - An IP Address can be pinged using the *ping* command. It helps to verify IP-level connectivity by sending ICMP(Internet Message Control Protocol) request messages. Ping command can be used with various parameters like number of requests, size of data field in request, time to live of the request and timeout period for reply.

The maximum size of packet sent can be found out by manually adjusting the value of size of data field in a *ping* request in a binary search fashion. The maximum size of packet sent (data field only) for various domains is as follows -

- *www.google.com*: 1464 bytes
- *www.facebook.com*: 1464 bytes
- *www.iitd.ac.in*: 1472 bytes

We observe that the maximum size of the packet varies as it depends upon the server configuration.

We also observe that on decreasing TTL values below a certain threshhold, we see that "TTL expired in transit" message is returned, implying that the number of hops to reach the destination is more than the TTL value specified.

d) **Traceroute** - Traceroute can be performed by the *tracert* command. It finds out the path taken between the host and the destination over the network.

Traceroute to iitd.ac.in for 2 ISPs is as follows -

- **Airtel**

```
Tracing route to iitd.ac.in [103.27.9.24]
over a maximum of 30 hops:

  1     2 ms     1 ms     1 ms  192.168.1.1
  2     6 ms     5 ms     4 ms  122.169.34.1
  3     6 ms     7 ms     6 ms  182.78.219.41
  4     7 ms     7 ms     6 ms  182.79.141.216
  5     8 ms    11 ms     8 ms  115.110.232.173
  6     *        *        *     Request timed out.
  7     8 ms     8 ms     8 ms  14.140.210.22
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11    10 ms    10 ms    10 ms  103.27.9.24
 12    20 ms    10 ms    10 ms  103.27.9.24
 13    10 ms    10 ms     9 ms  103.27.9.24
```

Figure 1: Airtel

- **Jio**

```
Tracing route to iitd.ac.in [103.27.9.24]
over a maximum of 30 hops:

  1     8 ms     4 ms     2 ms  192.168.8.206
  2     *        *        *     Request timed out.
  3    66 ms    24 ms    36 ms  10.71.80.2
  4    69 ms    30 ms    48 ms  172.26.100.116
  5    71 ms    24 ms    38 ms  172.26.100.98
  6    69 ms    45 ms    37 ms  192.168.44.26
  7    50 ms    24 ms    38 ms  192.168.44.27
  8    65 ms    34 ms    48 ms  172.16.18.33
  9    39 ms    26 ms    41 ms  172.16.18.0
 10    59 ms    67 ms    59 ms  115.249.187.169
 11    62 ms    57 ms    56 ms  115.255.253.18
 12    72 ms    59 ms    54 ms  115.249.198.97
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19    50 ms    59 ms    57 ms  103.27.9.24
 20    57 ms    68 ms    65 ms  103.27.9.24
 21    82 ms    53 ms    68 ms  103.27.9.24
```

Figure 2: Jio

Observations -

- We use -4 to force tracert to use IPv4.
- -d flag can be added to stop tracert from resolving IPs to names. This helps speeding up tracert.
- We can specify the maximum hops to destination using -h ¡maximumhops¿ flag
- Some routers do not return time exceeded messages for packets with expired TTL, hence are not visible to tracert. They are represented as *. This may be due to RTT exceeding default timeout of 4s. -w ¡timeout¿ flag can be used to increase timeout in such cases.
- Some private IP addresses (10.*.*.* and 192.168.*.*) were observed.

2 Packet Analysis

Wireshark is used to grab all packets while visiting http://apache.org with the following observations -

a) After applying the *DNS* filter, the time taken for the DNS request response to complete is 11.638686 - 11.617220 = 0.021466 seconds.

b) After applying the *HTTP* filter, the number of HTTP requests generated were found to be around 30. This suggests that the various components of a complex webpage HTML, stylesheets, javascript, images, etc. need to be requested separately by the browser. The browser puts together these various objects to display a webpage.

c) The total time to download the entire webpage is the time between the first DNS request and the time when the last content object was received, that is 13.913203 - 11.617220 = 2.295983 seconds.

d) Packet trace for *http://cse.iitd.ac.in* doesn't reveal any HTTP traffic. Only a single HTTP response, 301 Moved Permanently is observed. This is because it is a HTTPS only website, therefore it gets redirected to *https://cse.iitd.ac.in*. In HTTPS, data is encrypted as TLS, therefore, it is not identified as HTTP traffic by wireshark, making it difficult to sniff data. However *http://apache.org* supports HTTP and therefore data is visible to wireshark.

3 Traceroute using Ping

I implemented traceroute using ping command of Powershell in Python using os interface. Sample output for destination iitd.ac.in has been shown below -

```
Enter domain name / IP Address of destination
iitd.ac.in
Enter max hops(or blank to use default)

hop 1 192.168.1.1
hop 2 122.169.34.1
hop 3 182.78.219.37
hop 4 182.79.181.255
hop 5 115.110.232.173
hop 6 *
hop 7 14.140.210.22
hop 8 *
hop 9 *
hop 10 *
hop 11 103.27.9.24
hop 12 103.27.9.24
hop 13 103.27.9.24
traceroute for iitd.ac.in successful!
plot saved at iitd.ac.in.png
```

Figure 3: Output

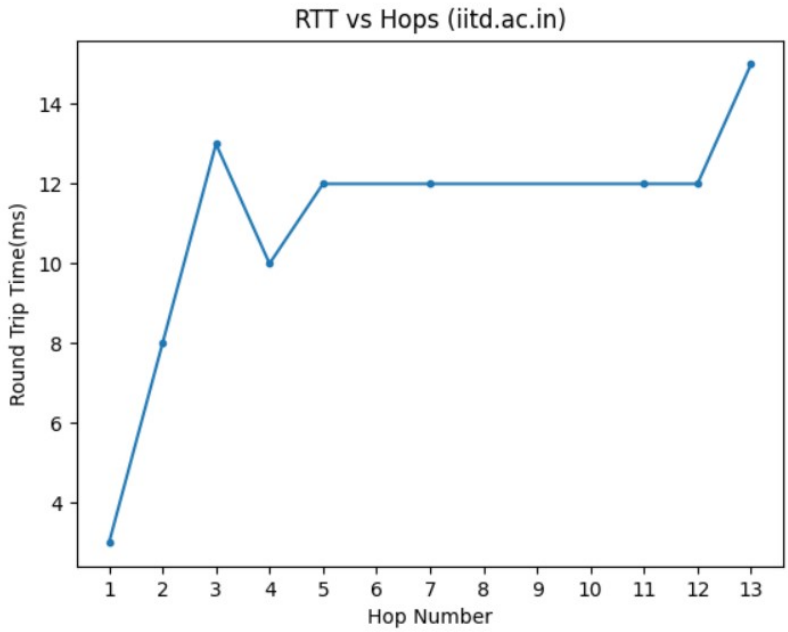

Figure 4: RTT vs Hops plot