Assignment 1

Kappala Hemanth Krishna, 2021CS10102
Koduru Suchith, 2021CS10572

August, 13th 2023

1 Network Analysis

- I ran traceroute with wifi network and 4G network.

```
C:\Users\Suchith>tracert iitd.ac.in

Tracing route to iitd.ac.in [2001:df4:e000:29::212]
over a maximum of 30 hops:

  1     4 ms     3 ms     3 ms  2409:4050:e4c:9f48::5
  2     *        *        *     Request timed out.
  3    66 ms    44 ms    55 ms  2405:200:330:eeee:20::826
  4   122 ms    86 ms    56 ms  2405:200:801:300::e11
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9    42 ms    44 ms    44 ms  2405:203:982:68d::6
 10    37 ms    41 ms    66 ms  2405:203:982:68d::e
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14   124 ms    55 ms    29 ms  2001:4408:a::1
 15   206 ms    54 ms    54 ms  2405:8a00:a:2::c5
 16    46 ms    62 ms    77 ms  2405:8a00:a:2::c6
 17    42 ms    40 ms    58 ms  2001:df4:e000:108::2
 18   152 ms    44 ms    30 ms  2001:df4:e000:26::24
 19   111 ms    38 ms    69 ms  2001:df4:e000:29::212

Trace complete.
```

Figure 1: Results for the `tracert iitd.ac.in` command via 4G network.

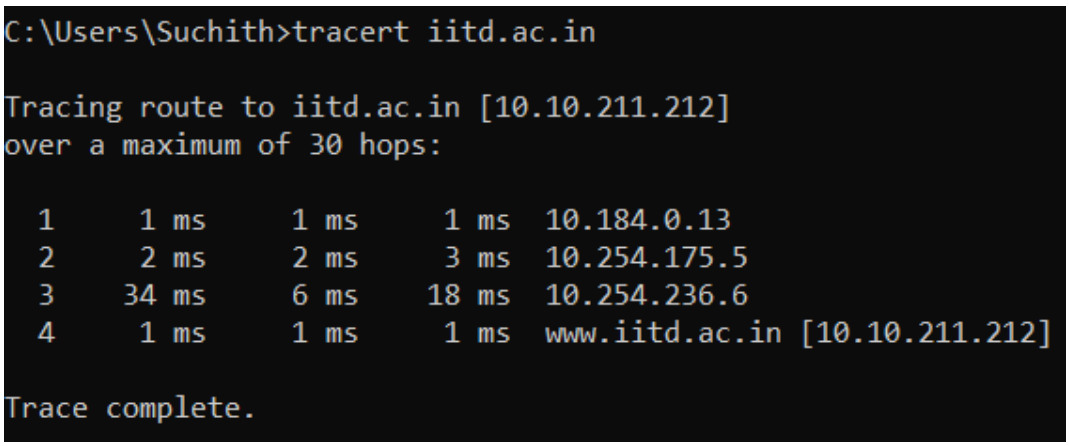

Figure 2: Results for the `tracert iitd.ac.in` command via IITD wifi.

- When I run traceroute command via 4G network, I got path that is default to IPv6. We can force traceroute to use IPv4 by adding -4 option in the command, then the command will be "tracert -4 iitd.ac.in".

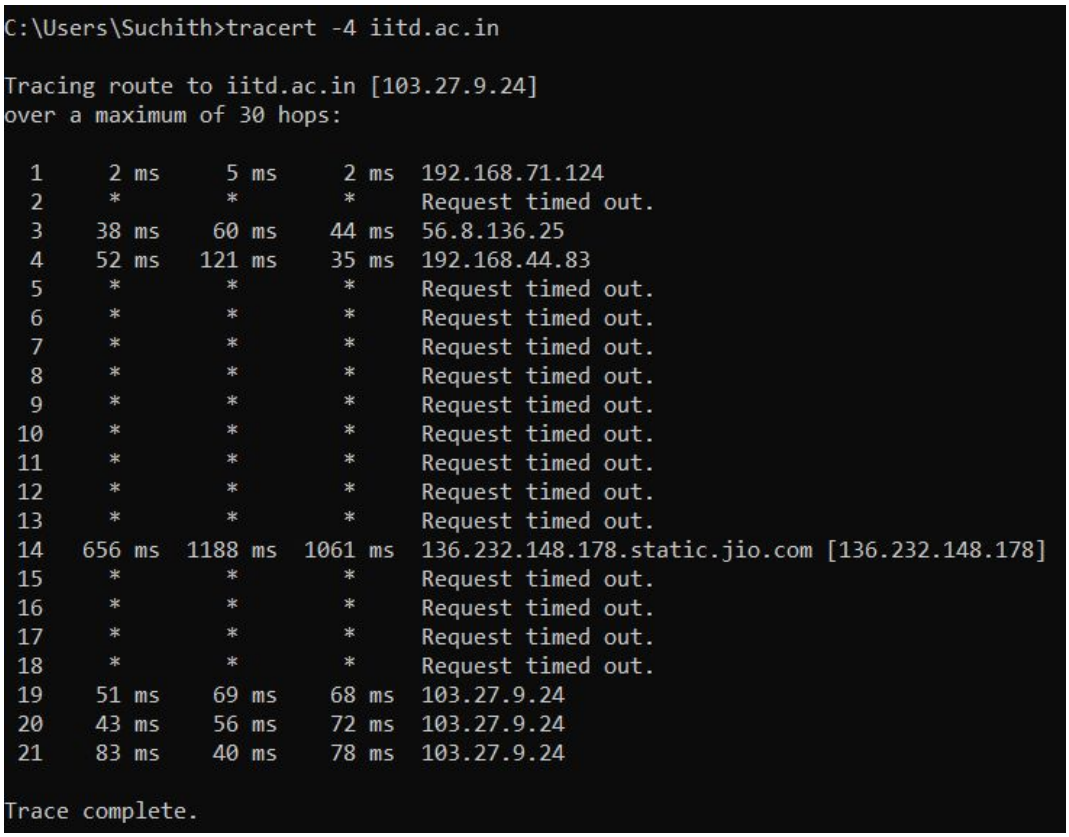

Figure 3: Results for the `tracert -4 iitd.ac.in` command via 4G network.

- In the path via IITD wifi, all the ip's in the path are private IP address, since I ran the command by using wifi so the tracert took the nearest routers in the campus which are private ip's of IIT Delhi campus.
- In the path via 4G network, only 1st and 3rd ip's in the path are private ip's, they are probably private ip's of jio network which are near to the campus.
- Maximum size of ping packets that I am able to send via 4G network connection is "1452". It was varying when I tried in different times, I also got it as "1472" otherday.

2 Replicating traceroute with ping

- We can replicate traceroute functionality using some option of the ping and loop.
- First I used ping command directly to the destination to get ip address of the destination.
- Then I initialized a ttl value with 1, empty list 'ans' and a boolean value "reached" and used it to loop through while loop, and change boolean value of "reached" to True, then the loop will stop.
- In the every iteration of while loop, I ran the ping command with options '-n' which specifies no of packets, '-i' which specifies ttl value to get the ip address which it reached in the middle of path with that ttl value.
- If the packets are blocked by ISP and I didn't get intermediate ip address I stored 'Request timed out' for that ttl, and stored the ip address for remaining.
- After getting intermediate ip addresses, I sent 3 packets using ping command and noted the RTT values for those. If the ip address matched with the destination ip address I changed the boolean value of 'reached' to True.
- Finally in every iteration I stored the ip address and 3 RTT's in the 'ans' list and incremented the ttl value by 1.

3 Internet architecture

a)

- **Table 1: No of Hops**

Server Name	Localhost	Germany	US(NYC)
iitd.ac.in	14hops	18hops	15hops
www.utah.edu	NA	NA	20hops (Ipv4)
www.uct.ac.za	NA	NA	NA
www.google.com	13hops	11hops	24hops
www.facebook.com	10hops	11hops	8hops

- NA means **not reached** (more than 30 hops)
- Geographical proximity can indeed result in fewer hops between traceroute sources and destinations. If two points are geographically close, there might be a more direct network path between them, potentially reducing the number of intermediate routers and hops.
- In the above table we can see that US(NYT)-IITD took less hops(15hops) compared to Germany-IITD even though Germany is geographically nearer than US(NYC).
- Yes,Google and Facebook, being two of the largest and most well-connected internet entities, often have robust network infrastructures and distributed data centers. This can lead to optimized routing and potentially fewer hops required to reach their servers. Additionally, they might have peering agreements with major ISPs, allowing for more direct paths.

b)

- **Table 2 : Latency**

Server Name	Localhost	Germany	US
iitd.ac.in	46ms	161.279ms	275.897ms
www.utah.edu	NA	NA	55.530ms (Ipv4)
www.uct.ac.za	NA	NA	NA
www.google.com	72.845ms	3.116ms	6.795ms
www.facebook.com	90.943	9.386	0.623ms

- **Latency and Hop Count:**In general, as the number of hops increases, the latency tends to increase as well. This is because each router along the path introduces processing time and potential transmission delays.Each router processes the packet, makes a forwarding decision, and introduces a certain amount of delay before passing it to the next hop. This cumulative processing time contributes to overall latency.
- **Routing Efficiency :**The routing decisions made by routers can influence the overall latency. Inefficient routing can lead to longer paths and higher latency.Sometimes, network congestion or suboptimal routing decisions can lead to higher latencies even with a smaller number of hops.

c)

- iitd.ac.in, www.utah.edu,www.uct.ac.za are resloved to the same IP address irrespective of the traceroute source and www.google.com and facebook.com resolved to different IP addresses. Although the servers of educational institutions are giving the same IP address, if we run traceroute command from IITD via Institute wifi, we get another IP address which is private since the network is also private.
- For the webservers of large content providers, there are multiple servers present across the globe. So we are getting different IP addresses for them when we run traceroute command from different source.

d)

- **Geographical Diversity:** Some paths might take more direct routes based on geographical proximity, while others might route through different locations due to network peering agreements.Here due to geographical proximity the paths are longer. Longer paths have higher hops.
- **Example:** NYC to faceboook(US) is 8 hops and NYC to facebook(India) is 18hops. geogrpahically facebook (India) is farther from facebook(US) which results in more hops than facebook(US).

e)

- Buenos Aires, AR for this country traceroute didn't reach destination for google and facebook.
- For other countries servers, traceroute path is complete mostly for google and facebook. So I didn't find any other country whose ISP is not directly peered with google and facebook.

4 Packet Analysis

a) DNS filter

we did packet trace for www.iitd.ac.in and applied dns filter.THe request-response time for A record(which resolves IP address)is 3.312ms and for https is 2.064ms.

b) HTTP filter

observations on apllying http filter to the act4d.iitd.ac.in

- number of http requests tha genereted are 12.
- **Multiple Requests :** It has generated multiple http requests to fetch all the js,css,html files.
- **Rendering Process :** Browser has started rendering the page as soon as it recieved the html file, they will pause rendering if they encounter external resources(images,stylesheets,scripts)referenced in HTML until those are fetched and loaded.

- **Paraller Fetching :** Browsers can fetch resources in parallel to improve page loading speed. This allows browser to efficiently retrieve multiple resources simultaneously,making use of available network bandwith
- **asynchronous Loding :**To optimize performance, web developers often use techniques like asynchronous loading of scripts and lazy loading of images. This means some resources might be fetched after the main page is displayed, further improving perceived page load times.

c) TCP connection

- **No of TCP connections :** 6
- **Number of TCP Connections vs. Number of HTTP Requests:**No of TCP connections and HTTP requests we got in the previous part are not same. Because here a single TCP connection can serve multiple HTTP requests using techniwues like HTTP/1.1 pipeling.
- **Content Objects Over the Same TCP Connection:**Yes, content objects can be fetched over the same TCP connection. Modern browsers and web servers often use techniques to optimize performance, such as keeping connections open and reusing them for fetching multiple resources. This reduces the overhead of establishing new TCP connections for each resource.

d) Indian Express

- **HTTP Traffic:** There is HTTP traffic. which sent a request to http:/indianexpress.com/
- **Content:**there is only one html file.
- **Analysis:**What happende is browser is making HTTP requests to the websites server for various resiources,including HTML files(whihc define the structres of the web page). These resources are fetched using HTTP GET requests. Browser then processses this content to render the webpage correctly.