COL334 Assignment-1

Shrey J. Patel, 2019CS10400

August 2021

1 Networking Tools

1.1 *ifconfig*

I use both my ISPs in wireless configuration. So, both the IP addresses are of the wlp3s0 type.

1. **ISP 1(Vodafone)**
   - **IPv4:** 192.168.1.102
   - **IPv6:** fe80::98a4:e1eb:6fa1:ae04
2. **ISP 2(Reliance Jio)**
   - **IPv4:** 192.168.144.31
   - **IPv6:** fe80::6c32:c7a3:e9ca:5928

1.2 *nslookup*

1.2.1 ISP 1

1. **Local DNS server:** 127.0.0.53
   - **google:** 172.217.19.132
   - **facebook:** 31.13.79.35
2. **Public DNS server(Google):** 8.8.8.8
   - **google:** 142.250.77.68
   - **facebook:** 157.240.16.35
3. **Public DNS server(Cloudfare):** 1.1.1.1
   - **google:** 142.250.192.132
   - **facebook:** 157.240.7.35

1.2.2 ISP 2

1. **Local DNS server:** 127.0.0.53
   - **google:** 142.250.193.4
   - **facebook:** 157.240.16.35
2. **Public DNS server(Google):** 8.8.8.8
   - **google:** 142.251.42.36
   - **facebook:** 31.13.79.35
3. **Public DNS server(Cloudfare):** 1.1.1.1
   - **google:** 142.250.76.196
   - **facebook:** 31.13.79.35

1.2.3 Observations

1. All the above query answers are non-authoritative, which means the query for a particular domain name is requested through a non-authoritative DNS server, like the local host or the public non-authoritative server. A list of authoritative server for a particular domain can be fetched from the command:

   host -t ns domainName

   However, regardless of the type of server used, the IP address is the same and it is sent by the authoritative server, although in case of a non-authoritative answer, the query reply is sent indirectly i.e. forwarded through the local/public DNS server.

2. Different host DNS servers give different IP addresses for the same domain name, which can be attributed to the fact that the same domain name my be assigned to multiple different servers, which is natural for domains that receive heavy traffic. So, different DNS servers may access a different server with the same domain name. The same reason can be applied to explain the fact that even different access networks(i.e. ISPs) also return different IPs for the same domain name. And the number of different servers is fairly representative of the amount of traffic on that site. For instance, Google seems to have the largest number of servers as expected, followed by Facebook. While a relatively less known domain such as IITD home site seems to have a single IP address(103.27.9.24).

3. Even when the ISP is changed, the IP address for the local DNS server is the same i.e. 127.0.0.53#53 (53 denotes the port used by the DNS server). But 127.0.0.53 points to the system's local cache which depends on the operating system. So, all the DNS queries which use the local DNS server(provided by the ISP) ago through this cache first.

1.3 *ping*

I have created a bash shell script named *ping.sh*, which uses ping command on console on different packet sizes and TTF values to perform **binary search** on the maximum value of packet size and the minimum TTL value required for the packet to reach the destination.

1.4 ISP 1

1) www.iitd.ac.in:
Maximum packet size = 1452 + 8 header bytes
Minimum TTL value = 16

2) www.google.com:
Maximum packet size = 68 + 8 header bytes
Minimum TTL value = 18

3) www.facebook.com:
Maximum packet size = 1452 + 8 header bytes
Minimum TTL value = 9

1.5 ISP 2

1) www.iitd.ac.in:
Maximum packet size = 1472 + 8 header bytes
Minimum TTL value = 21

2) www.google.com:
Maximum packet size = 68 + 8 header bytes
Minimum TTL value = 12

3) www.facebook.com:
Maximum packet size = 1452 + 8 header bytes
Minimum TTL value = 12

1.6 Observations

1. The maximum packet size may be dependant on the size allowance of the intermediate routers and switches, and since each of the packets follow different routes to reach different domains, and even same domains but on different access networks, the packet sizes are bound to be different.

2. Similarly, the minimum TTL value is dependant on the length of the route to the destination, and so different domains and different ISP networks have different TTL values.

1.7 *traceroute*

Traceroute implements the ping to send ICMP packets hop-by-hop i.e. for increasing TTL values. It exploits the feature of ping, by which if the packet doesn't reach the destination for the current hop value, then the last router on the path sends an ICMP error report(mostly) before discarding the packet. In this way, traceroute traces the path of routers and switches by their IPs until the destination. I have implemented a traceroute script using this method.

1.7.1 ISP 1: 192.168.1.102

```
shrey@shrey-Inspiron-7570:~/Shrey/COL334/Basic-Networking/Part1$ traceroute www.iitd.ac.in -I
traceroute to www.iitd.ac.in (103.27.9.24), 64 hops max
  1   192.168.1.1  4.531ms  3.851ms  1.993ms
  2   192.168.0.1  2.194ms  2.101ms  1.961ms
  3   100.76.0.1  13.736ms  11.339ms  16.915ms
  4   203.187.200.184  16.307ms  15.269ms  17.230ms
  5   118.185.41.10  12.888ms  11.008ms  11.363ms
  6   182.19.106.103  21.609ms  25.558ms  22.673ms
  7   14.142.18.97  22.770ms  22.509ms  22.367ms
  8   *  *  *
  9   *  *  *
 10   14.140.210.22  36.134ms  36.297ms  36.505ms
 11   *  *  *
 12   *  *  *
 13   *  *  *
 14   103.27.9.24  37.901ms  43.561ms  45.224ms
```

1.7.2 ISP 2: 192.168.144.31

```
shrey@shrey-Inspiron-7570:~/Shrey/COL334/Basic-Networking/Part1$ traceroute www.iitd.ac.in -I
traceroute to www.iitd.ac.in (103.27.9.24), 64 hops max
  1   192.168.58.113  3.102ms  3.463ms  2.255ms
  2   *  *  *
  3   56.8.119.1  46.521ms  56.8.119.13  37.265ms  56.8.119.9  50.556ms
  4   192.168.38.2  39.778ms  39.617ms  192.168.38.0  39.034ms
  5   192.168.21.235  60.065ms  40.787ms  39.212ms
  6   172.26.101.4  39.791ms  30.227ms  40.013ms
  7   172.26.100.242  30.047ms  39.883ms  38.634ms
  8   192.168.38.23  40.794ms  192.168.38.25  39.830ms  192.168.38.23  54.377ms
  9   192.168.38.24  35.469ms  40.169ms  39.839ms
 10   172.26.40.5  43.681ms  49.519ms  74.146ms
 11   172.16.25.2  51.678ms  50.670ms  63.175ms
 12   172.16.1.218  66.083ms  58.891ms  58.568ms
 13   *  *  *
 14   *  *  *
 15   14.140.210.22  88.991ms  96.869ms  79.608ms
 16   *  *  *
 17   *  *  *
 18   *  *  *
 19   103.27.9.24  151.479ms  76.513ms  73.920ms
```

1.7.3 Observations:

1. According to the implementation of the traceroute, the total number of intermediate routers that the traceroute should encounter must be equal to the minimum TTL value, because this TTL value is the exact length of the route between the source and the destination.

   However, in the case of www.iitd.ac.in, I obtained the number of hops to be equal to **2 less than the minimum TTL value**, and on verifying with the ping command, I found that the

the last three hops in both ISPs all correspond to the routers whose IP address matches with the destination IP address. This might suggest that the Linux implementation of traceroute might be trying to find the first matching IP address for finding the destination instead of the actual destination based on the TTL values.

For instance, the TTL value for ISP 1 is 16, but the hop count of traceroute is 14, while the same for ISP 2 is 21 and its hop count is 19.

2. For the traceroute to get the information regarding the IP address of an intermediate router, the router must send back necessary information back to the source after discarding the packet. However some routers either don't respond to the pings or are not able able to send back the request before the timeout (which is set to 3 by default). The traceroute command sends the next ping and classifies the current router as private/hidden if it doesn't send any response before the timeout.

   So, one way to allow the identification of more routers on the path is to increase the timeout value of every ping. This can be done by using -w tag followed by the desired timeout value. However, this strategy might not be useful for routers which don't respond at all. This might be fixed by using the -I tag to prompt the traceroute to send ICMP packets instead of UDP packets as the routers sometimes don't respond to them because of unreliability.

3. The traceroutes for more traffic heavy domains like Google consist of variable number hops because of existence of multiple different servers and therefore multiple routes and destinations. However, I found that the number of hidden/private routers are comparatively lesser in these cases, the reason of which is not quite clear to me.

2 Packet Analysis

3 Traceroute using Ping