Name : Soham Vaidya
Branch : TE Computer
Batch : D
UID : 2018130058

EXPERIMENT 2

Basic Network Utilities

Command : ping

Description : PING (Packet Internet Groper) command is used to check the network connectivity between host and server/host. This command takes as input the IP address or the URL and sends a data packet to the specified address with the message “PING” and gets a response from the server/host this time is recorded which is called latency. Fast ping low latency means faster connection. Ping uses ICMP(Internet Control Message Protocol) to send an ICMP echo message to the specified host if that host is available then it sends an ICMP reply message. Ping is generally measured in millisecond every modern operating system has this ping pre-installed.

Experiments :

1. Ping the any hosts 10 times (i.e., packet count is 10) with a packet size of 64 bytes, 100 bytes, 500 bytes, 1000 bytes, 1400 bytes.

1.*ping -c 10 -s 64 google.com*

```
soham@soham-H81M-S1:~$ ping -c 10 -s 64 google.com
PING google.com (142.250.67.238) 64(92) bytes of data.
72 bytes from bom07s24-in-f14.1e100.net (142.250.67.238): icmp_seq=1 ttl=118 time=9.89 ms
72 bytes from bom07s24-in-f14.1e100.net (142.250.67.238): icmp_seq=2 ttl=118 time=6.96 ms
72 bytes from bom07s24-in-f14.1e100.net (142.250.67.238): icmp_seq=3 ttl=118 time=8.94 ms
72 bytes from bom07s24-in-f14.1e100.net (142.250.67.238): icmp_seq=4 ttl=118 time=4.94 ms
72 bytes from bom07s24-in-f14.1e100.net (142.250.67.238): icmp_seq=5 ttl=118 time=11.2 ms
72 bytes from bom07s24-in-f14.1e100.net (142.250.67.238): icmp_seq=6 ttl=118 time=5.77 ms
72 bytes from bom07s24-in-f14.1e100.net (142.250.67.238): icmp_seq=7 ttl=118 time=9.37 ms
72 bytes from bom07s24-in-f14.1e100.net (142.250.67.238): icmp_seq=8 ttl=118 time=11.1 ms
72 bytes from bom07s24-in-f14.1e100.net (142.250.67.238): icmp_seq=9 ttl=118 time=4.11 ms
72 bytes from bom07s24-in-f14.1e100.net (142.250.67.238): icmp_seq=10 ttl=118 time=3.64 ms

--- google.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9011ms
rtt min/avg/max/mdev = 3.640/7.605/11.243/2.735 ms
```

2. ping -c 10 -s 100 www.geeksforgeeks.org

```
soham@soham-H81M-S1:~$ ping -c 10 -s 100 www.geeksforgeeks.org
PING a1991.dscr.akamai.net (183.87.86.208) 100(128) bytes of data.
108 bytes from 208-86-87-183.mysipl.com (183.87.86.208): icmp_seq=1 ttl=60 time=2.28 ms
108 bytes from 208-86-87-183.mysipl.com (183.87.86.208): icmp_seq=2 ttl=60 time=2.44 ms
108 bytes from 208-86-87-183.mysipl.com (183.87.86.208): icmp_seq=3 ttl=60 time=3.94 ms
108 bytes from 208-86-87-183.mysipl.com (183.87.86.208): icmp_seq=4 ttl=60 time=3.17 ms
108 bytes from 208-86-87-183.mysipl.com (183.87.86.208): icmp_seq=5 ttl=60 time=3.37 ms
108 bytes from 208-86-87-183.mysipl.com (183.87.86.208): icmp_seq=6 ttl=60 time=4.64 ms
108 bytes from 208-86-87-183.mysipl.com (183.87.86.208): icmp_seq=7 ttl=60 time=9.31 ms
108 bytes from 208-86-87-183.mysipl.com (183.87.86.208): icmp_seq=8 ttl=60 time=5.61 ms
108 bytes from 208-86-87-183.mysipl.com (183.87.86.208): icmp_seq=9 ttl=60 time=10.1 ms
108 bytes from 208-86-87-183.mysipl.com (183.87.86.208): icmp_seq=10 ttl=60 time=6.03 ms

--- a1991.dscr.akamai.net ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9012ms
rtt min/avg/max/mdev = 2.282/5.098/10.157/2.603 ms
```

3. ping -c 10 -s 500 www.geeksforgeeks.org

```
soham@soham-H81M-S1:~$ ping -c 10 -s 500 www.geeksforgeeks.org
PING a1991.dscr.akamai.net (183.87.86.208) 500(528) bytes of data.
508 bytes from 208-86-87-183.mysipl.com (183.87.86.208): icmp_seq=1 ttl=60 time=4.83 ms
508 bytes from 208-86-87-183.mysipl.com (183.87.86.208): icmp_seq=2 ttl=60 time=2.43 ms
508 bytes from 208-86-87-183.mysipl.com (183.87.86.208): icmp_seq=3 ttl=60 time=2.06 ms
508 bytes from 208-86-87-183.mysipl.com (183.87.86.208): icmp_seq=4 ttl=60 time=4.84 ms
508 bytes from 208-86-87-183.mysipl.com (183.87.86.208): icmp_seq=5 ttl=60 time=8.61 ms
508 bytes from 208-86-87-183.mysipl.com (183.87.86.208): icmp_seq=6 ttl=60 time=4.17 ms
508 bytes from 208-86-87-183.mysipl.com (183.87.86.208): icmp_seq=7 ttl=60 time=2.18 ms
508 bytes from 208-86-87-183.mysipl.com (183.87.86.208): icmp_seq=8 ttl=60 time=9.62 ms
508 bytes from 208-86-87-183.mysipl.com (183.87.86.208): icmp_seq=9 ttl=60 time=2.79 ms
508 bytes from 208-86-87-183.mysipl.com (183.87.86.208): icmp_seq=10 ttl=60 time=5.05 ms

--- a1991.dscr.akamai.net ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9014ms
rtt min/avg/max/mdev = 2.067/4.661/9.621/2.490 ms
```

4. ping -c 10 -s 1000 www.geeksforgeeks.org

```
soham@soham-H81M-S1:~$ ping -c 10 -s 1000 www.geeksforgeeks.org
PING a1991.dscr.akamai.net (183.87.86.243) 1000(1028) bytes of data.
1008 bytes from 243-86-87-183.mysipl.com (183.87.86.243): icmp_seq=1 ttl=60 time=2.97 ms
1008 bytes from 243-86-87-183.mysipl.com (183.87.86.243): icmp_seq=2 ttl=60 time=3.92 ms
1008 bytes from 243-86-87-183.mysipl.com (183.87.86.243): icmp_seq=3 ttl=60 time=2.41 ms
1008 bytes from 243-86-87-183.mysipl.com (183.87.86.243): icmp_seq=4 ttl=60 time=2.89 ms
1008 bytes from 243-86-87-183.mysipl.com (183.87.86.243): icmp_seq=5 ttl=60 time=2.81 ms
1008 bytes from 243-86-87-183.mysipl.com (183.87.86.243): icmp_seq=6 ttl=60 time=8.50 ms
1008 bytes from 243-86-87-183.mysipl.com (183.87.86.243): icmp_seq=7 ttl=60 time=2.66 ms
1008 bytes from 243-86-87-183.mysipl.com (183.87.86.243): icmp_seq=8 ttl=60 time=3.75 ms
1008 bytes from 243-86-87-183.mysipl.com (183.87.86.243): icmp_seq=9 ttl=60 time=2.76 ms
1008 bytes from 243-86-87-183.mysipl.com (183.87.86.243): icmp_seq=10 ttl=60 time=4.01 ms

--- a1991.dscr.akamai.net ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9015ms
rtt min/avg/max/mdev = 2.411/3.671/8.502/1.697 ms
```

5. ping -c 10 -l 1400 www.geeksforgeeks.org

```
soham@soham-H81M-S1:~$ ping -c 10 -s 1400 www.geeksforgeeks.org
PING a1991.dscr.akamai.net (183.87.86.208) 1400(1428) bytes of data.
From _gateway (192.168.2.1) icmp_seq=1 Frag needed and DF set (mtu = 1392)
1408 bytes from 208-86-87-183.mysipl.com (183.87.86.208): icmp_seq=2 ttl=60 time=3.88 ms
1408 bytes from 208-86-87-183.mysipl.com (183.87.86.208): icmp_seq=3 ttl=60 time=3.51 ms
1408 bytes from 208-86-87-183.mysipl.com (183.87.86.208): icmp_seq=4 ttl=60 time=3.80 ms
1408 bytes from 208-86-87-183.mysipl.com (183.87.86.208): icmp_seq=5 ttl=60 time=3.09 ms
1408 bytes from 208-86-87-183.mysipl.com (183.87.86.208): icmp_seq=6 ttl=60 time=3.19 ms
1408 bytes from 208-86-87-183.mysipl.com (183.87.86.208): icmp_seq=7 ttl=60 time=3.15 ms
1408 bytes from 208-86-87-183.mysipl.com (183.87.86.208): icmp_seq=8 ttl=60 time=3.66 ms
1408 bytes from 208-86-87-183.mysipl.com (183.87.86.208): icmp_seq=9 ttl=60 time=3.35 ms
1408 bytes from 208-86-87-183.mysipl.com (183.87.86.208): icmp_seq=10 ttl=60 time=7.88 ms

--- a1991.dscr.akamai.net ping statistics ---
10 packets transmitted, 9 received, +1 errors, 10% packet loss, time 9013ms
rtt min/avg/max/mdev = 3.093/3.949/7.885/1.418 ms
```

Questions on Latency :

1. Does the average RTT vary between different hosts? What aspects of latency (transmit, propagation, and queueing delay) might impact this and why?

   From the above figures, we can clearly conclude that the RTT is dependent on the host on which the ‘ping’ command is used. Transmission delay is the time taken to put a packet onto a link or simply, the time required to put data bits on the wire/communication medium. It depends on the size of the packet and the bandwidth of the network. Since the hosts are the only parameters changed, there is no transmission delay in the two cases. Propagation delay is the time taken by the first bit to travel from sender to receiver end of the link or simply the time required for bits to reach the destination from the start point. Factors on which propagation delay depends are distance and propagation speed. So, there exists a propagation delay in the two cases. Queueing delay is the time difference between when the packet arrived at its destination and when the packet data was processed or executed. It depends on the number of packets, size of the packet and bandwidth of the network. Since all the parameters are non-varying in both cases, there is hardly any queueing delay.

2. Does the average RTT vary with different packet sizes? What aspects of latency (transmit, propagation, and queueing delay) might impact this and why?

   From the above images, we can say that the Round Trip Time is impacted due to the difference in the size of the packets. This is because of the Transmission delay and the Queueing delay which depend on the size of the packets.

Exercise :

Experiment with ping to find the round trip times to a variety of destinations. Write up any interesting observations, including in particular how the round trip time compares to the physical distance.

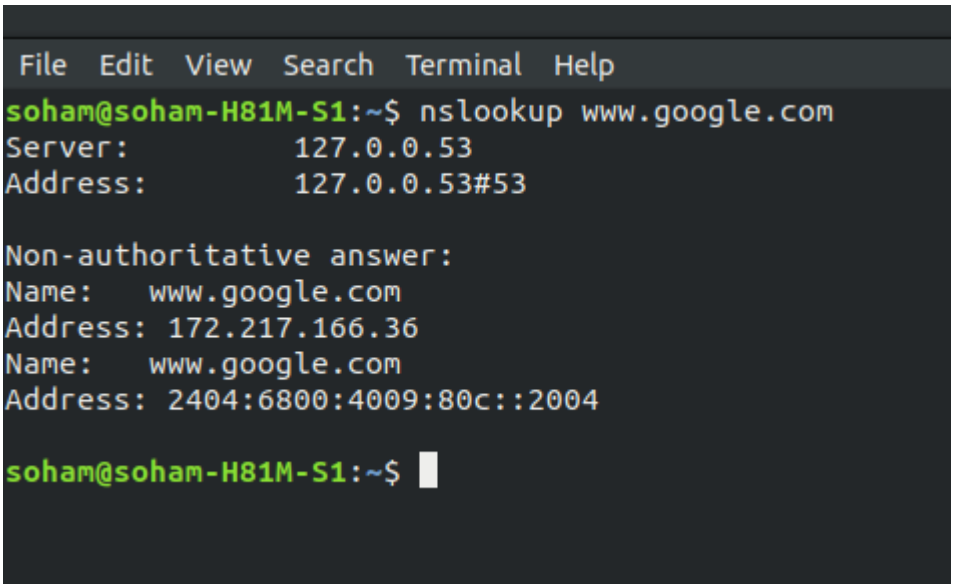
From the images shown above, the following observations can be made :

(1) The length a signal has to travel correlates with the time taken for a request to reach a server and a response to reach a browser.
(2) The medium used to route a signal (e.g., copper wire, fiber optic cables) can impact how quickly a request is received by a server and routed back to a user.
(3) Intermediate routers or servers take time to process a signal, increasing RTT. The more hops a signal has to travel through, the higher the RTT.
(4) RTT typically increases when a network is congested with high levels of traffic. Conversely, low traffic times can result in decreased RTT.
(5) The time taken for a target server to respond to a request depends on its processing capacity, the number of requests being handled and the nature of the request (i.e., how much server-side work is required). A longer server response time increases RTT.

Command : nslookup

Description : The command nslookup <host> will do a DNS query to find and report the IP address (or addresses) for a domain name or the domain name corresponding to an IP address. To do this, it contacts a "DNS server." Default DNS servers are part of a computer's network configuration. (For a static IP address in Linux, they are configured in the file /etc/network/interfaces that you encountered in the last lab.) You can specify a different DNS server to be used by nslookup by adding the server name or IP address to the command: nslookup <host> <server>

Screenshot :



Command : ifconfig

Description : Displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. Used without parameters, ipconfig displays Internet Protocol version 4 (IPv4) and IPv6 addresses, subnet mask, and default gateway for all adapters.

Screenshots :

```
soham@soham-H81M-S1:~$ ifconfig -a
enp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.2.113  netmask 255.255.255.0  broadcast 192.168.2.255
        inet6 fe80::229e:d0e7:7f5a:bbe0  prefixlen 64  scopeid 0x20<link>
        ether 94:de:80:fb:d2:18  txqueuelen 1000  (Ethernet)
        RX packets 25322  bytes 26765140 (26.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 18189  bytes 2144249 (2.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 2925  bytes 270372 (270.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2925  bytes 270372 (270.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Command : netstat

Description : The netstat command gives information about network connections. I often use netstat -t -n which lists currently open TCP connections (that's the "-t" option) by IP address rather than domain name (that's the "-n" option). Add the option "-l" (lower case ell) to list listening sockets, that is sockets that have been opened by server programs to wait for connection requests from clients: netstat -t -n -l. (On Mac, use netstat -p tcp to list tcp connections, and add "-a" to include listening sockets in the list.)

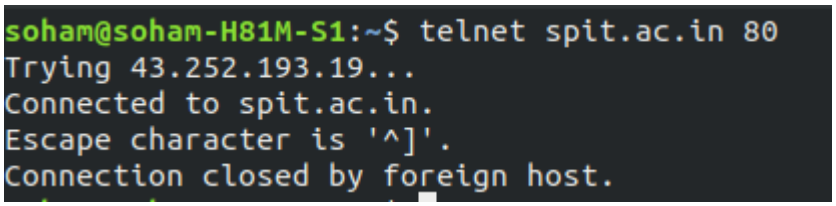
Screenshots :

```
soham@soham-H81M-S1:~$ netstat -t -n
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.2.113:54250     45.55.41.223:80         CLOSE_WAIT
tcp        0      0 192.168.2.113:43062     52.35.6.89:443          TIME_WAIT
tcp        0      0 192.168.2.113:40734     172.217.26.227:443      ESTABLISHED
tcp        0      0 192.168.2.113:47360     142.250.67.142:443      ESTABLISHED
tcp        0      0 192.168.2.113:42174     172.217.160.170:443     ESTABLISHED
tcp        1      0 192.168.2.113:41760     172.217.160.170:443     CLOSE_WAIT
tcp        0      0 192.168.2.113:47358     142.250.67.142:443      ESTABLISHED
tcp        0      0 192.168.2.113:34706     172.217.166.36:443      ESTABLISHED
tcp        0      0 192.168.2.113:45526     34.212.188.196:443      ESTABLISHED
tcp        0      0 192.168.2.113:41110     172.217.194.189:443     ESTABLISHED
```

Command : telnet

Description : Telnet is an old program for remote login. It's not used so much for that any more, since it has no security features. But basically, all it does is open a connection to a server and allow the server and client to send lines of plain text to each other. It can be used to check that it's possible to connect to a server and, if the server communicates in plain text, even to interact with the server by hand. Since the Web uses a plain text protocol, you can use telnet to connect to a web client and play the part of the web browser. I will suggest that you do this with your own web server when you write it, but you might want to try it now. When you use telnet in this way, you need to specify both the host and the port number to which you want to connect: telnet <host> <port>. For example, to connect to the web server on www.spit.ac.in: telnet spit.ac.in 80

Screenshots :



A blank command prompt screen appears showing that the connection is established.

Command : traceroute

Description : The tracert diagnostic utility determines the route to a destination by sending Internet Control Message Protocol (ICMP) echo packets to the destination. In these packets, traceroute uses varying IP Time-To-Live (TTL) values. Because each router along the path is required to decrement the packet's TTL by at least 1 before forwarding the packet, the TTL is effectively a hop counter. When the TTL on a packet reaches zero (0), the router sends an ICMP "Time Exceeded" message back to the source computer.

Experiment :

From your machine traceroute to the following hosts:

1. ee.iitb.ac.in

2. mscs.mu.edu

3. www.cs.grinnell.edu

4. csail.mit.edu

5. cs.stanford.edu

6. cs.manchester.ac.uk

Store the output of each traceroute command in a separate file named traceroute_HOSTNAME.log, replacing HOSTNAME with the hostname for end-host you pinged

(e.g., traceroute_ee.iitb.ac.in.log).

Screenshots :

```
soham@soham-H81M-S1:~$ traceroute iitb.ac.in
traceroute to iitb.ac.in (103.21.127.114), 30 hops max, 60 byte packets
 1  _gateway (192.168.2.1)  0.804 ms  1.210 ms  1.608 ms
 2  10.200.100.4 (10.200.100.4)  8.179 ms  8.399 ms  8.593 ms
 3  10.200.100.254 (10.200.100.254)  9.122 ms  8.864 ms  9.302 ms
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  46-97-87-183.mysipl.com (183.87.97.46)  12.979 ms 42-97-87-183.mysipl.com (183.87.97.42)  7.368 ms 38-97-87-183.mysipl.com (183.87.97.38)  7.617
ms
 9  172.23.78.237 (172.23.78.237)  7.942 ms  5.606 ms 115.110.234.170.static.Mumbai.vsnl.net.in (115.110.234.170)  6.458 ms
10  172.23.78.234 (172.23.78.234)  5.890 ms  6.075 ms  7.960 ms
11  115.110.234.170.static.Mumbai.vsnl.net.in (115.110.234.170)  9.089 ms  9.300 ms *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
soham@soham-H81M-S1:~$
```

```
soham@soham-H81M-S1:~$ traceroute www.cs.grinnell.edu
traceroute to www.cs.grinnell.edu (132.161.132.159), 30 hops max, 60 byte packets
 1  _gateway (192.168.2.1)  0.707 ms  1.260 ms  1.683 ms
 2  10.200.100.4 (10.200.100.4)  8.457 ms  8.667 ms  8.872 ms
 3  10.200.100.254 (10.200.100.254)  9.168 ms  9.398 ms  9.608 ms
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  38-97-87-183.mysipl.com (183.87.97.38)  6.596 ms  6.357 ms 42-97-87-183.mysipl.com (183.87.97.42)  11.183 ms
 9  172.23.78.237 (172.23.78.237)  11.468 ms 172.23.78.233 (172.23.78.233)  5.241 ms 172.23.78.237 (172.23.78.237)  5.450 ms
10  172.31.244.45 (172.31.244.45)  27.128 ms  27.331 ms  22.951 ms
11  ix-ae-4-2.tcore2.cxr-chennai.as6453.net (180.87.37.1)  32.273 ms  32.710 ms  32.455 ms
12  if-ae-9-2.tcore2.mlv-mumbai.as6453.net (180.87.37.10)  249.287 ms  241.007 ms  241.032 ms
13  if-ae-2-2.tcore1.mlv-mumbai.as6453.net (180.87.38.1)  237.115 ms  244.801 ms  236.238 ms
14  * * *
15  if-ae-2-2.tcore2.wyn-marseille.as6453.net (80.231.217.2)  242.719 ms  245.877 ms  243.512 ms
16  if-ae-9-2.tcore2.l78-london.as6453.net (80.231.200.14)  238.502 ms  242.826 ms  240.641 ms
17  if-ae-8-49.tcore2.nto-newyork.as6453.net (216.6.81.34)  238.106 ms  239.952 ms if-ae-15-2.tcore2.ldn-london.as6453.net (80.231.131.118)  241.248
ms
18  if-ae-32-2.tcore2.nto-newyork.as6453.net (63.243.216.22)  240.496 ms if-ae-26-2.tcore1.ct8-chicago.as6453.net (216.6.81.29)  241.776 ms  248.921
ms
19  if-ae-26-2.tcore1.ct8-chicago.as6453.net (216.6.81.29)  248.665 ms *  247.697 ms
20  * * *
21  * et3-1-0-0.agr03.desm01-ia.us.windstream.net (40.128.250.43)  244.514 ms *
22  et4-1-0-0.agr04.desm01-ia.us.windstream.net (40.136.117.253)  248.941 ms ae4-0.pe04.grnl01-ia.us.windstream.net (40.128.248.35)  243.898 ms et4-1
-0-0.agr04.desm01-ia.us.windstream.net (40.136.117.253)  246.780 ms
23  ae4-0.pe05.grnl01-ia.us.windstream.net (40.128.251.179)  251.445 ms ae4-0.pe04.grnl01-ia.us.windstream.net (40.128.248.35)  257.197 ms  254.375 m
s
24  h29.127.138.40.static.ip.windstream.net (40.138.127.29)  248.436 ms * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

```
soham@soham-H81M-S1:~$ traceroute csail.mit.edu
traceroute to csail.mit.edu (128.30.2.109), 30 hops max, 60 byte packets
 1  _gateway (192.168.2.1)  0.631 ms  1.040 ms  1.430 ms
 2  10.200.100.4 (10.200.100.4)  7.972 ms  8.229 ms  8.429 ms
 3  10.200.100.254 (10.200.100.254)  8.964 ms  8.697 ms  9.130 ms
 4  * * 21.9.106.27.mysipl.com (27.106.9.21)  29.559 ms
 5  * * *
 6  * * *
 7  * * *
 8  46-97-87-183.mysipl.com (183.87.97.46)  6.020 ms  6.226 ms  6.755 ms
 9  * 172.23.78.237 (172.23.78.237)  7.737 ms  5.406 ms
10  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net (180.87.38.5)  5.700 ms  6.103 ms  5.823 ms
11  if-ae-2-2.tcore2.mlv-mumbai.as6453.net (180.87.38.2)  207.378 ms if-ae-5-2.tcore1.wyn-marseille.as6453.net (80.231.217.29)  205.867 ms if-ae-2-2.
tcore2.mlv-mumbai.as6453.net (180.87.38.2)  208.309 ms
12  if-ae-12-2.tcore1.l78-london.as6453.net (180.87.39.21)  198.910 ms  207.005 ms if-ae-2-2.tcore2.wyn-marseille.as6453.net (80.231.217.2)  204.032
ms
13  if-ae-9-2.tcore2.l78-london.as6453.net (80.231.200.14)  205.485 ms if-ae-17-2.tcore1.ldn-london.as6453.net (80.231.130.130)  206.704 ms if-ae-9-2
.tcore2.l78-london.as6453.net (80.231.200.14)  202.473 ms
14  if-ae-15-2.tcore2.ldn-london.as6453.net (80.231.131.118)  202.828 ms if-ae-26-2.tcore2.ldn-london.as6453.net (80.231.62.57)  206.253 ms if-ae-18-
2.tcore1.nto-newyork.as6453.net (80.231.131.73)  198.297 ms
15  if-ae-32-3.tcore2.nto-newyork.as6453.net (80.231.20.107)  201.231 ms if-ae-12-2.tcore1.n75-newyork.as6453.net (66.110.96.5)  200.040 ms if-ae-2-2
.tcore1.n0v-newyork.as6453.net (216.6.90.21)  207.487 ms
16  be-10390-cr02.newyork.ny.ibone.comcast.net (68.86.83.89)  212.076 ms if-ae-7-2.tcore1.nto-newyork.as6453.net (63.243.128.25)  202.446 ms 66.110.9
6.146 (66.110.96.146)  198.385 ms
17  be-10390-cr02.newyork.ny.ibone.comcast.net (68.86.83.89)  200.330 ms be-1302-cs03.newyork.ny.ibone.comcast.net (96.110.38.41)  209.019 ms  208.47
1 ms
18  be-1302-cs03.newyork.ny.ibone.comcast.net (96.110.38.41)  198.963 ms 66.110.96.130 (66.110.96.130)  201.822 ms 96.110.42.10 (96.110.42.10)  213.6
50 ms
19  be-10390-cr02.newyork.ny.ibone.comcast.net (68.86.83.89)  205.825 ms be-1302-cs03.newyork.ny.ibone.comcast.net (96.110.38.41)  205.368 ms ae0-0-e
g-bstpmall74w.boston.ma.boston.comcast.net (68.86.238.34)  217.264 ms
20  50-201-57-174-static.hfc.comcastbusiness.net (50.201.57.174)  214.482 ms be-1302-cs03.newyork.ny.ibone.comcast.net (96.110.38.41)  202.958 ms ae0
-0-eg-bstpmall74w.boston.ma.boston.comcast.net (68.86.238.34)  205.015 ms
21  50-201-57-174-static.hfc.comcastbusiness.net (50.201.57.174)  205.476 ms dmz-rtr-1-external-rtr-3.mit.edu (18.0.161.13)  214.936 ms  215.863 ms
22  dmz-rtr-2-dmz-rtr-1-2.mit.edu (18.0.162.6)  216.447 ms  210.382 ms dmz-rtr-2-dmz-rtr-1-1.mit.edu (18.0.161.6)  216.005 ms
23  dmz-rtr-1-external-rtr-3.mit.edu (18.0.161.13)  210.520 ms dmz-rtr-2-dmz-rtr-1-1.mit.edu (18.0.161.6)  206.320 ms mitnet.core-1-ext.csail.mit.edu
 (18.4.7.65)  217.487 ms
24  mitnet.core-1-ext.csail.mit.edu (18.4.7.65)  206.552 ms dmz-rtr-1-external-rtr-3.mit.edu (18.0.161.13)  210.026 ms *
25  * dmz-rtr-2-dmz-rtr-1-1.mit.edu (18.0.161.6)  208.105 ms *
26  * * bdr.core-1.csail.mit.edu (128.30.0.246)  209.241 ms
```

```
27  * bdr.core-1.csail.mit.edu (128.30.0.246)  210.918 ms *
28  * bdr.core-1.csail.mit.edu (128.30.0.246)  210.783 ms  217.082 ms
29  * * *
30  * * *
```

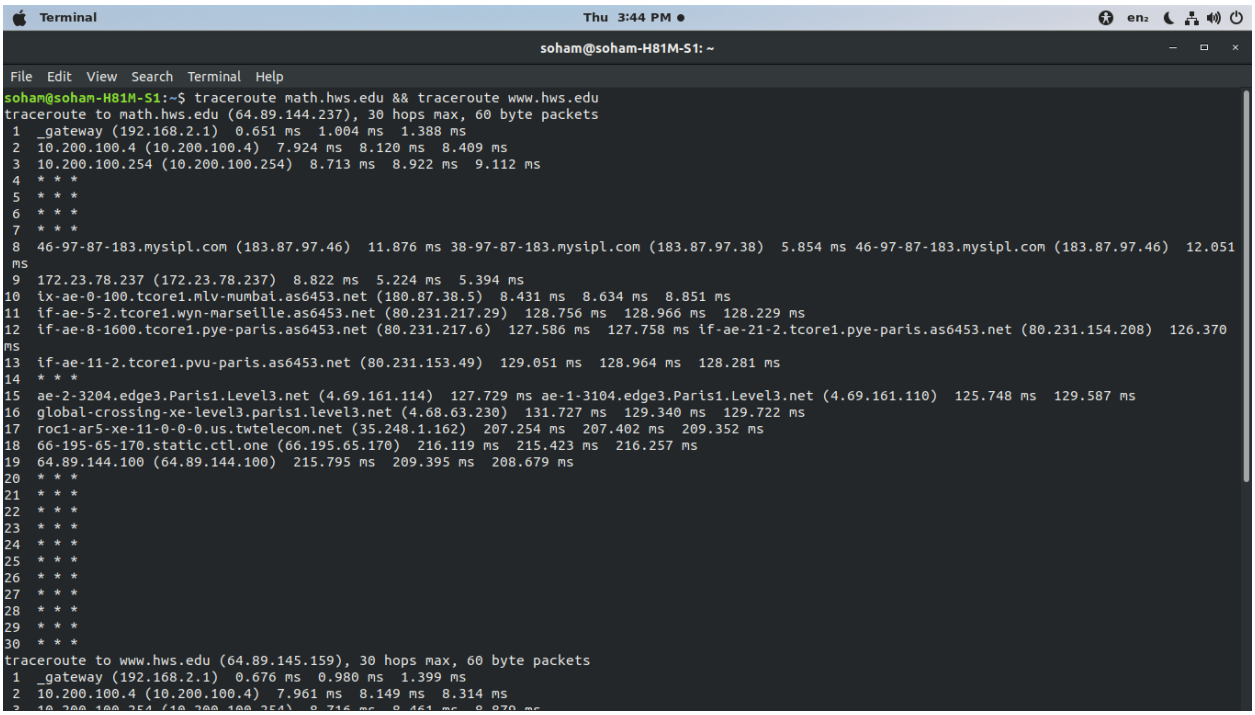
```
soham@soham-H81M-S1:~$ traceroute cs.stanford.edu
traceroute to cs.stanford.edu (171.64.64.64), 30 hops max, 60 byte packets
 1  _gateway (192.168.2.1)  0.655 ms  1.026 ms  1.403 ms
 2  10.200.100.4 (10.200.100.4)  7.955 ms  8.122 ms  8.313 ms
 3  10.200.100.254 (10.200.100.254)  8.587 ms  8.876 ms  9.072 ms
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  42-97-87-183.mysipl.com (183.87.97.42)  11.279 ms  11.463 ms 38-97-87-183.mysipl.com (183.87.97.38)  6.971 ms
 9  172.23.78.237 (172.23.78.237)  11.727 ms  5.329 ms  5.507 ms
10  172.31.244.45 (172.31.244.45)  22.062 ms  27.041 ms  23.749 ms
11  ix-ae-4-2.tcore2.cxr-chennai.as6453.net (180.87.37.1)  31.283 ms  24.031 ms  32.312 ms
12  * * *
13  if-ae-7-2.tcore2.lvw-losangeles.as6453.net (180.87.15.26)  238.949 ms  232.846 ms  234.657 ms
14  if-ae-2-2.tcore1.lvw-losangeles.as6453.net (66.110.59.1)  231.890 ms  229.975 ms  232.438 ms
15  las-b24-link.telia.net (80.239.128.214)  231.661 ms  233.817 ms  228.120 ms
16  * palo-b24-link.telia.net (62.115.119.90)  245.017 ms  243.697 ms
17  palo-b1-link.telia.net (62.115.122.169)  252.618 ms  251.440 ms  249.251 ms
18  hurricane-ic-308019-palo-b1.c.telia.net (80.239.167.174)  250.729 ms  247.807 ms  242.053 ms
19  stanford-university.100gigabitethernet5-1.core1.pao1.he.net (184.105.177.238)  242.281 ms  239.818 ms  242.637 ms
20  csee-west-rtr-vl3.SUNet (171.66.255.140)  253.225 ms  247.703 ms  249.784 ms
21  CS.stanford.edu (171.64.64.64)  256.499 ms  254.332 ms  256.982 ms
soham@soham-H81M-S1:~$
```

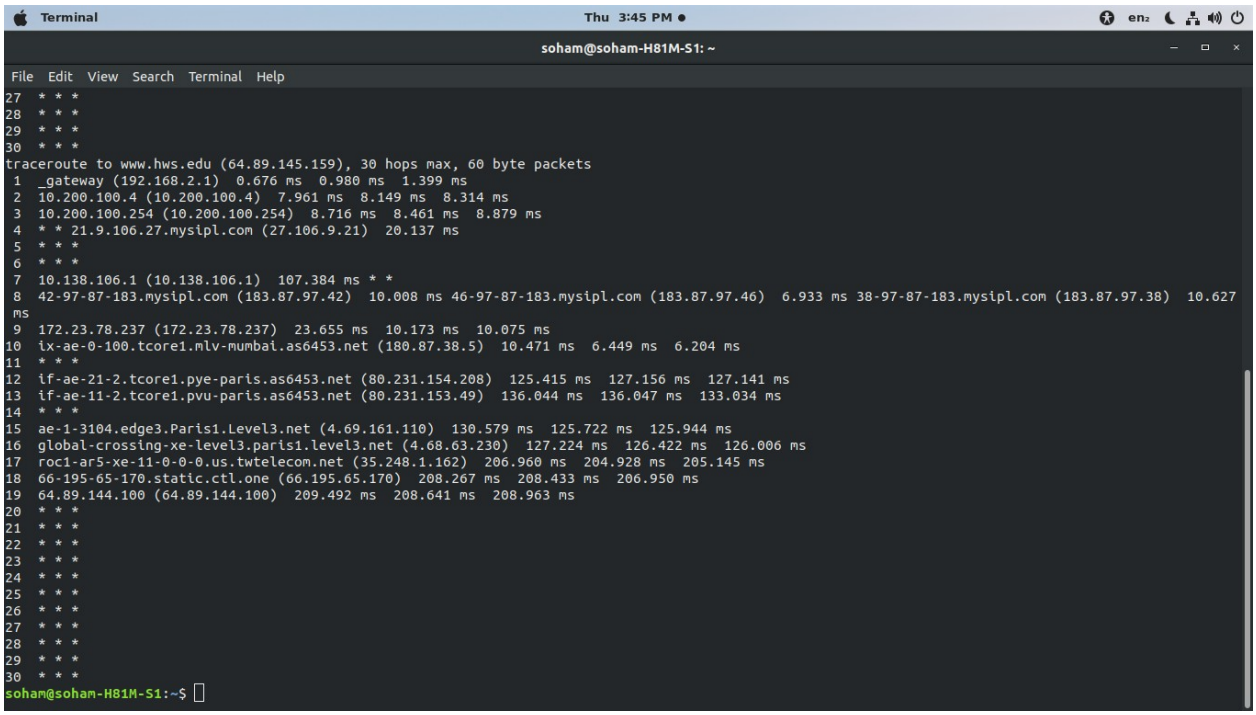
```
soham@soham-H81M-S1:~$ traceroute cs.manchester.ac.uk
traceroute to cs.manchester.ac.uk (130.88.101.49), 30 hops max, 60 byte packets
 1  _gateway (192.168.2.1)  0.693 ms  1.089 ms  1.488 ms
 2  10.200.100.4 (10.200.100.4)  8.290 ms  8.486 ms  8.726 ms
 3  10.200.100.254 (10.200.100.254)  9.113 ms  9.314 ms  9.516 ms
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  42-97-87-183.mysipl.com (183.87.97.42)  5.910 ms 46-97-87-183.mysipl.com (183.87.97.46)  5.598 ms 42-97-8
7-183.mysipl.com (183.87.97.42)  7.583 ms
 9  172.23.78.237 (172.23.78.237)  10.781 ms  5.681 ms 172.23.78.233 (172.23.78.233)  6.437 ms
10  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net (180.87.38.5)  6.723 ms  7.414 ms  8.099 ms
11  if-ae-29-8.tcore1.wyn-marseille.as6453.net (80.231.217.110)  116.071 ms if-ae-5-2.tcore1.wyn-marseille.as
6453.net (80.231.217.29)  115.728 ms if-ae-29-8.tcore1.wyn-marseille.as6453.net (80.231.217.110)  116.836 ms
12  if-ae-8-1600.tcore1.pye-paris.as6453.net (80.231.217.6)  114.867 ms if-ae-21-2.tcore1.pye-paris.as6453.ne
t (80.231.154.208)  114.747 ms  112.817 ms
13  if-ae-11-2.tcore1.pvu-paris.as6453.net (80.231.153.49)  113.396 ms  112.902 ms  112.815 ms
14  * * *
15  ae-1-9.bear1.Manchesteruk1.Level3.net (4.69.167.38)  127.410 ms  127.865 ms  127.616 ms
16  JANET.bear1.Manchester1.Level3.net (212.187.174.238)  128.840 ms  127.485 ms  127.979 ms
17  ae22.manckh-sbr2.ja.net (146.97.35.189)  128.530 ms  129.563 ms  128.711 ms
18  ae23.mancrh-rbr1.ja.net (146.97.38.42)  131.536 ms  132.792 ms  131.731 ms
19  * * universityofmanchester.ja.net (146.97.169.2)  128.217 ms
20  130.88.249.194 (130.88.249.194)  129.262 ms  128.420 ms  128.177 ms
21  * * *
22  * * *
23  eps.its.man.ac.uk (130.88.101.49)  129.174 ms  127.563 ms  128.184 ms
```

```
soham@soham-H81M-S1:~$ traceroute mscs.mu.edu
traceroute to mscs.mu.edu (134.48.4.5), 30 hops max, 60 byte packets
 1  _gateway (192.168.2.1)  0.629 ms  1.017 ms  1.401 ms
 2  10.200.100.4 (10.200.100.4)  8.114 ms  8.313 ms  8.498 ms
 3  10.200.100.254 (10.200.100.254)  8.773 ms  8.955 ms  9.139 ms
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  38-97-87-183.mysipl.com (183.87.97.38)  6.402 ms 42-97-87-183.mysipl.com (183.87.97.42)  6.085 ms 46-97-87-183.mysipl.com (183.87.97.46)  11.085
ms
 9  172.23.78.237 (172.23.78.237)  10.748 ms  5.058 ms 172.23.78.233 (172.23.78.233)  10.872 ms
10  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net (180.87.38.5)  6.027 ms  5.829 ms  8.179 ms
11  if-ae-5-2.tcore1.wyn-marseille.as6453.net (80.231.217.29)  128.213 ms  128.443 ms  128.999 ms
12  if-ae-21-2.tcore1.pye-paris.as6453.net (80.231.154.208)  130.626 ms if-ae-8-1600.tcore1.pye-paris.as6453.net (80.231.217.6)  125.433 ms if-ae-21-
2.tcore1.pye-paris.as6453.net (80.231.154.208)  128.861 ms
13  if-ae-11-2.tcore1.pvu-paris.as6453.net (80.231.153.49)  127.522 ms  126.464 ms  126.777 ms
14  * * *
15  * * *
16  MARQUETTE-U.ear3.Chicago2.Level3.net (4.16.38.70)  222.094 ms  218.738 ms  220.044 ms
17  134.48.10.27 (134.48.10.27)  220.548 ms  220.284 ms  220.712 ms
18  * * *
19  * * *
20  euclid.mscs.mu.edu (134.48.4.5)  219.582 ms  219.758 ms  219.731 ms
```

Exercise 2 :

Use traceroute to trace the route from your computer to math.hws.edu and to www.hws.edu. Explain the difference in the results.





From the above images, the first row shows that the process of route tracing has started as the last column shows the Default Gateway of the user. The

next three rows in both the cases are similar as the route is being traced starting from the ISP (Internet service provider) of the user. The next few rows, after which the tracing reaches the common IP address of 66.195.65.170 and then nat.hws.edu [64.89.144.100], clearly show that the route is completely different after crossing the ISP for both the cases. A domain name might have multiple IP addresses associated. If this is the case, multiple traces may access two or more IP addresses. This will yield trace paths that differ from one another, even if the origin and destinations are the same.

Domains may also use multiple servers for its subdomains. Tracing the path to the base domain might result in a completely different path when tracing to the subdomain. A URL with the www prefix is technically a subdomain, so it's possible that traces to example.com and www.example.com follow two very different paths.

Many domains use separate hosting for email. If you try to trace the domain, you'll get data for the website server, not the email server. This concept is popularly known as Caveats (Reference: https://network-tools.com/trace/).

Exercise 3 :

Two packets sent from the same source to the same destination do not necessarily follow the same path through the net. Experiment with some sources that are fairly far away. Can you find cases where packets sent to the same destination follow different paths? How likely does it seem to be? What about when the packets are sent at very different times? Save some of the outputs from traceroute. (You can copy them from the Terminal window by highlighting and right-clicking, then paste into a text editor.) Come back sometime next week, try the same destinations again, and compare the results with the results from today. Report your observations.

```
soham@soham-H81M-S1:~$ traceroute cs.stanford.edu
traceroute to cs.stanford.edu (171.64.64.64), 30 hops max, 60 byte packets
 1  _gateway (192.168.2.1)  0.655 ms  1.026 ms  1.403 ms
 2  10.200.100.4 (10.200.100.4)  7.955 ms  8.122 ms  8.313 ms
 3  10.200.100.254 (10.200.100.254)  8.587 ms  8.876 ms  9.072 ms
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  42-97-87-183.mysipl.com (183.87.97.42)  11.279 ms  11.463 ms 38-97-87-183.mysipl.com (183.87.97.38)  6.971 ms
 9  172.23.78.237 (172.23.78.237)  11.727 ms  5.329 ms  5.507 ms
10  172.31.244.45 (172.31.244.45)  22.062 ms  27.041 ms  23.749 ms
11  ix-ae-4-2.tcore2.cxr-chennai.as6453.net (180.87.37.1)  31.283 ms  24.031 ms  32.312 ms
12  * * *
13  if-ae-7-2.tcore2.lvw-losangeles.as6453.net (180.87.15.26)  238.949 ms  232.846 ms  234.657 ms
14  if-ae-2-2.tcore1.lvw-losangeles.as6453.net (66.110.59.1)  231.890 ms  229.975 ms  232.438 ms
15  las-b24-link.telia.net (80.239.128.214)  231.661 ms  233.817 ms  228.120 ms
16  * palo-b24-link.telia.net (62.115.119.90)  245.017 ms  243.697 ms
17  palo-b1-link.telia.net (62.115.122.169)  252.618 ms  251.440 ms  249.251 ms
18  hurricane-ic-308019-palo-b1.c.telia.net (80.239.167.174)  250.729 ms  247.807 ms  242.053 ms
19  stanford-university.100gigabitethernet5-1.core1.pao1.he.net (184.105.177.238)  242.281 ms  239.818 ms  242.637 ms
20  csee-west-rtr-vl3.SUNet (171.66.255.140)  253.225 ms  247.703 ms  249.784 ms
21  CS.stanford.edu (171.64.64.64)  256.499 ms  254.332 ms  256.982 ms
soham@soham-H81M-S1:~$
```

Questions :

(1) Is any part of the path common for all hosts you tracerouted ?

Yes, the tracerouting follows a particular path from the user's IP address through the IP addresses of the ISP and then the path really depends on which access point is ready to respond and which access points or routers have firewalls configured for blocking the requests and accordingly, the destination can be reached through different paths at different times.

(2) Is there a relationship between the number of nodes that show up in the traceroute and the location of the host? If so, what is this relationship?

A hop is limited only to a specific distance and also depends largely on the bandwidth and the traffic present on the network. If the distance between the location of the user and that of the destination url is more, then more hops will be required in order to reach the destination as more number of access points will be used for routing and the greater the number of access points involved, the greater are the chances of access points failing to respond and similarly for searching the alternative optimal path towards the destination.

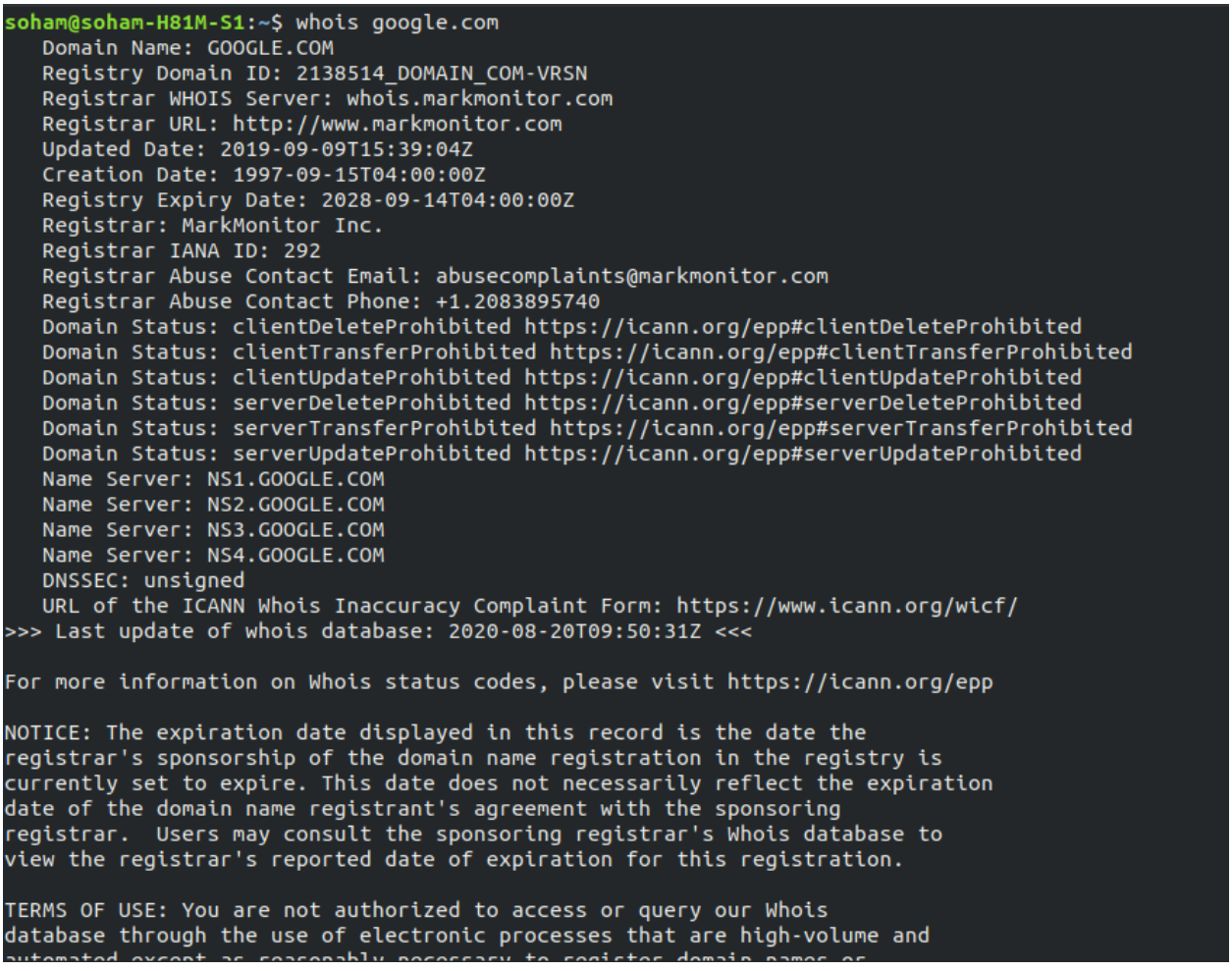
(3) Is there a relationship between the number of nodes that show up in the traceroute and latency of the host (from your ping results above)? Does the same relationship hold for all hosts?

If the latency of the host causes the traceroute request to get timed out even after the conventional three tries, then it keeps on sending the data packets until the host responds or upto a certain maximum hops. The same relationship may not hold for each host as it really depends on the time which the host takes to respond. If the host responds in the first request itself, the tracerouting stops with a success message.

Command : whois

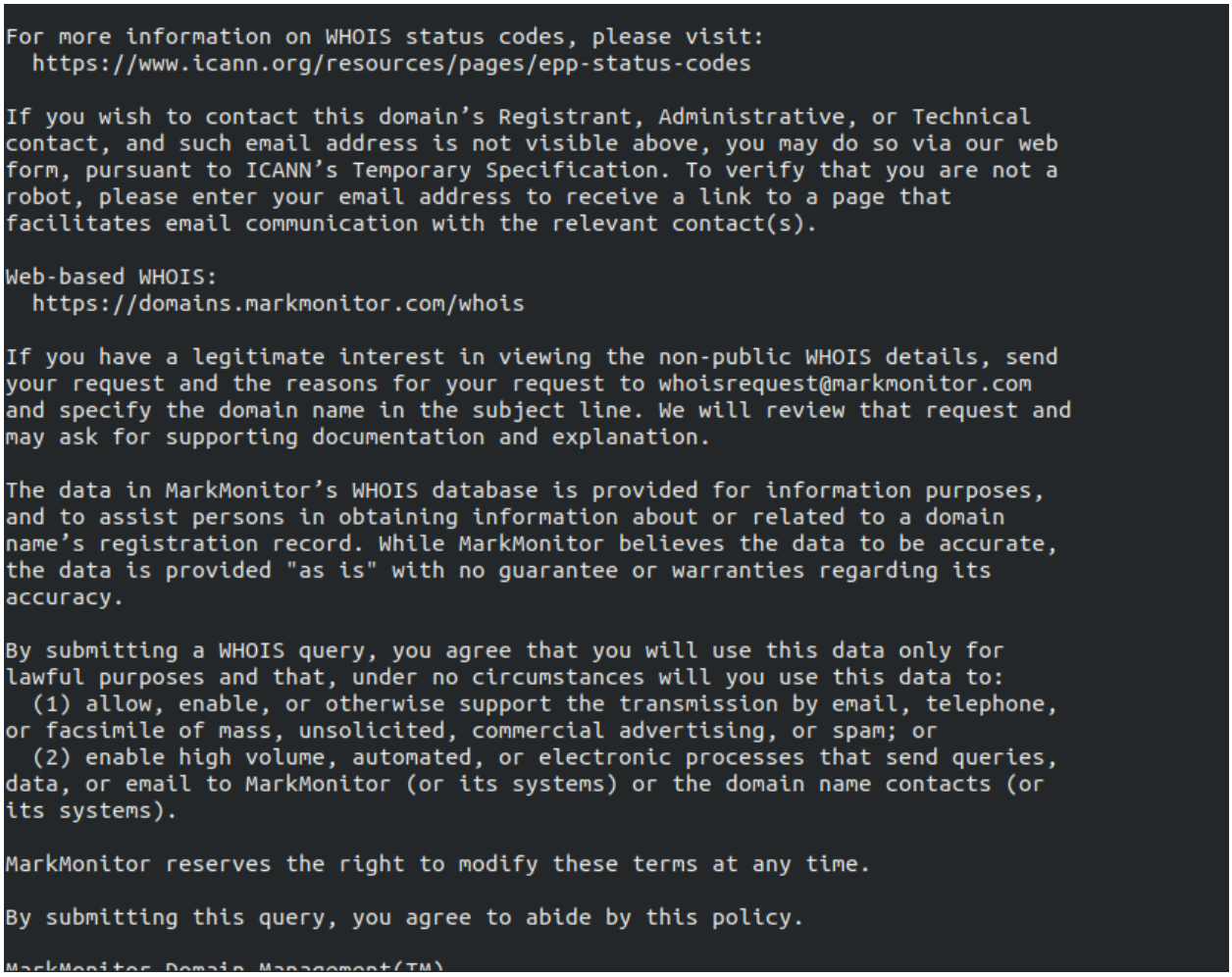
Description : The whois command can give detailed information about the domain names and IP addresses.

Exercise 4 : Use whois to investigate a well-known web site such as google.com or amazon.com, and write a couple of sentences about what you find out.



```
TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability.  VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.
```

```
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: google.com
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-09-09T08:39:04-0700
Creation Date: 1997-09-15T00:00:00-0700
Registrar Registration Expiration Date: 2028-09-13T00:00:00-0700
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895770
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Registrant Organization: Google LLC
Registrant State/Province: CA
Registrant Country: US
Registrant Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Admin Organization: Google LLC
Admin State/Province: CA
Admin Country: US
Admin Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Tech Organization: Google LLC
Tech State/Province: CA
Tech Country: US
Tech Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Name Server: ns2.google.com
Name Server: ns4.google.com
Name Server: ns1.google.com
Name Server: ns3.google.com
```



As shown in the above image, the whois command gives information about the domain name, the Registry Domain ID and some other details such as the details of the Registrar and the Registrant. For example, in case of google.com (domain name), the Registrant Organization is Google LLC, the Registrant State/Province is California and the Registrant Country is the United States. It also provides the domain expiry date.

References

1) https://www.paessler.com/it-explained/ping
2) https://www.geeksforgeeks.org/curl-command-in-linux-with-examples/
3) https://searchnetworking.techtarget.com/definition/Telnet
4) https://tldp.org/LDP/nag2/x-087-2-iface.netstat.html
5) https://geek-university.com/linux/whois-command/
6) https://www.geeksforgeeks.org/traceroute-command-in-linux-with-examples/

Conclusion:

I implemented various commands used in computer networking in a linux based system such as ping traceroute and etc. This practical also helped me to understand the path taken by a packet from source to destination.