Name : Vaidehi Vatsaraj

Branch : TE Comps

Batch : D
UID : 2018130060

Experiment 2 :

Basic Network Utilities

Aim: To study and understand some basic command line network utilities.

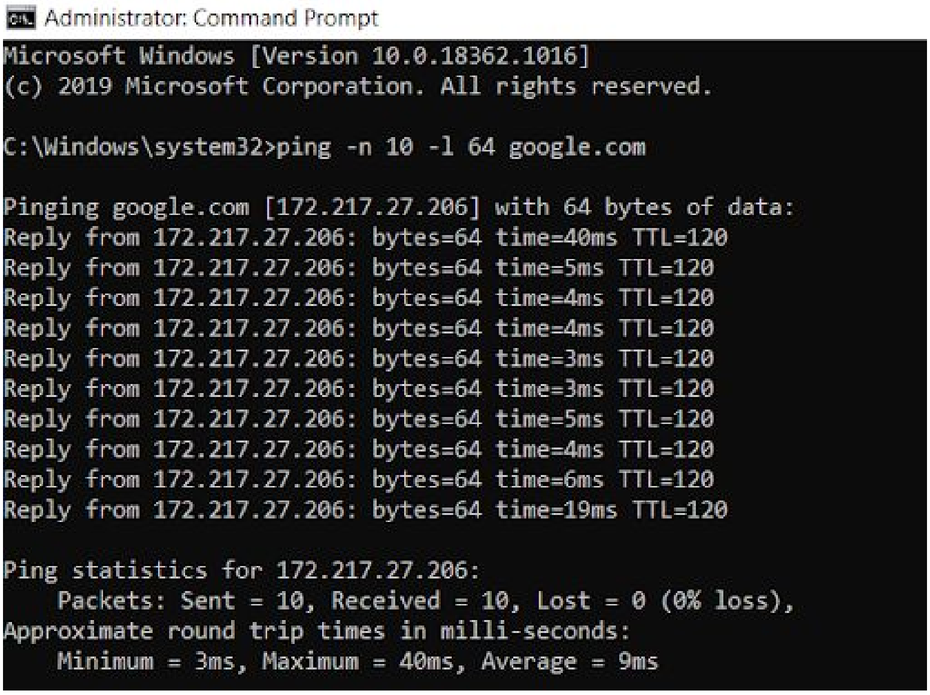
Command : PING

Description : Ping comes from a term used in sonar technology that sends out pulses of sound, and then listens for the echo to return. On a computer network, a ping tool is built into most operating systems that works in much the same way. You issue the ping command along with a specific URL or IP address. Your computer sends several packets of information out to that device, and then waits for a response. When it gets the response, the ping tool shows you how long each packet took to make the round trip—or tells you there was no reply

Experiments with Ping

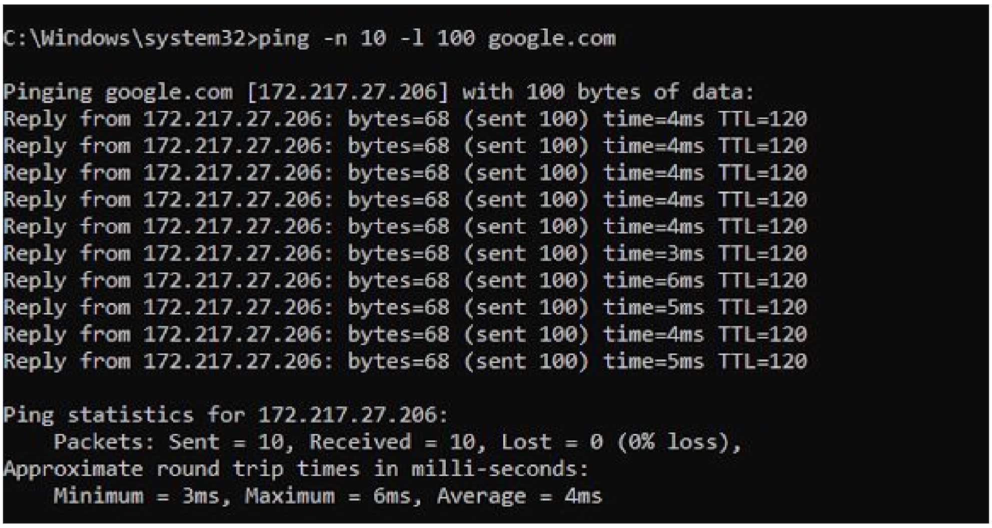
1. Ping the any hosts 10 times (i.e., packet count is 10) with a packet size of 64 bytes, 100 bytes, 500 bytes, 1000 bytes, 1400 bytes

- ping -n 10 -l 64 google.com



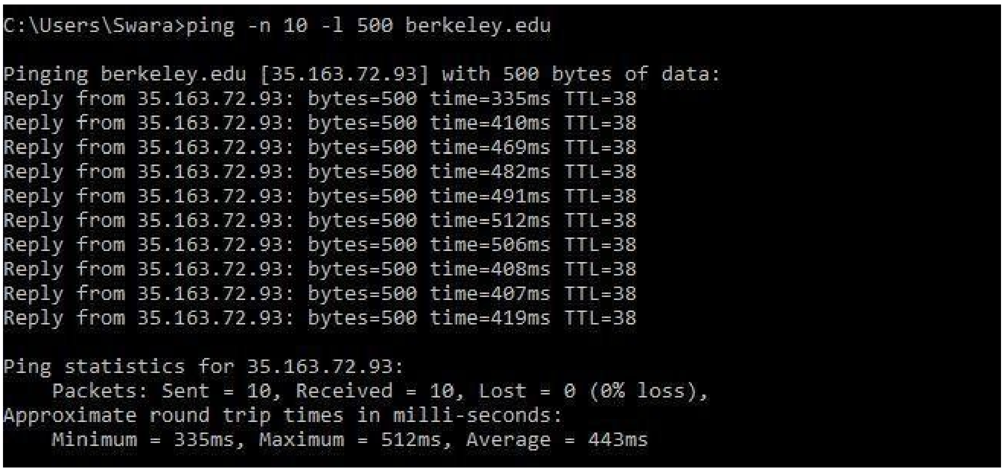
```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.18362.1016]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ping -n 10 -l 64 google.com

Pinging google.com [172.217.27.206] with 64 bytes of data:
Reply from 172.217.27.206: bytes=64 time=40ms TTL=120
Reply from 172.217.27.206: bytes=64 time=5ms TTL=120
Reply from 172.217.27.206: bytes=64 time=4ms TTL=120
Reply from 172.217.27.206: bytes=64 time=4ms TTL=120
Reply from 172.217.27.206: bytes=64 time=3ms TTL=120
Reply from 172.217.27.206: bytes=64 time=3ms TTL=120
Reply from 172.217.27.206: bytes=64 time=5ms TTL=120
Reply from 172.217.27.206: bytes=64 time=4ms TTL=120
Reply from 172.217.27.206: bytes=64 time=6ms TTL=120
Reply from 172.217.27.206: bytes=64 time=19ms TTL=120

Ping statistics for 172.217.27.206:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 40ms, Average = 9ms
```

- ping -n 10 -l 100 google.com



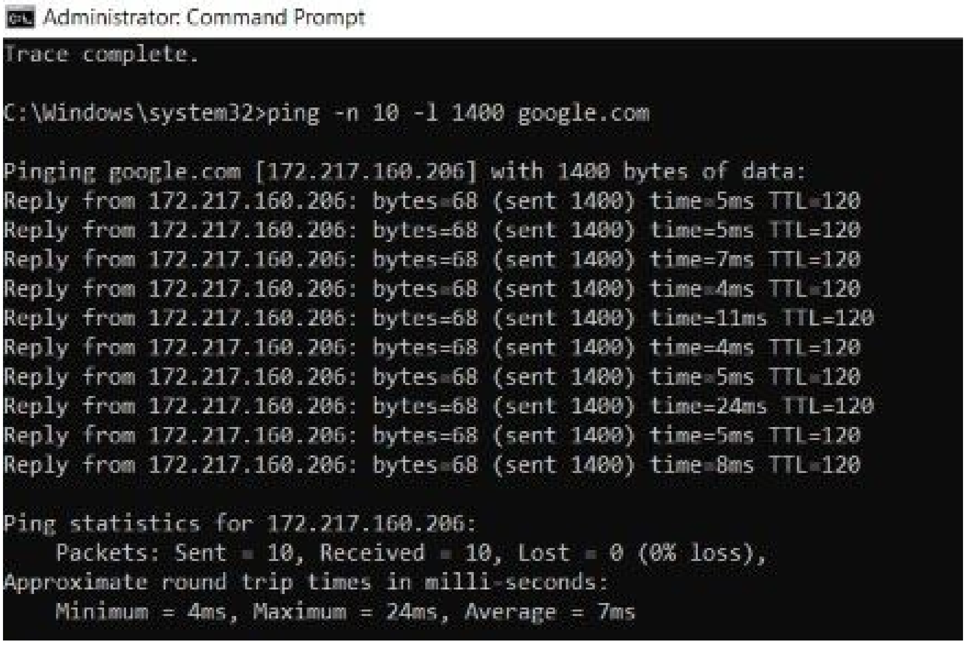
```
C:\Windows\system32>ping -n 10 -l 100 google.com

Pinging google.com [172.217.27.206] with 100 bytes of data:
Reply from 172.217.27.206: bytes=68 (sent 100) time=4ms TTL=120
Reply from 172.217.27.206: bytes=68 (sent 100) time=4ms TTL=120
Reply from 172.217.27.206: bytes=68 (sent 100) time=4ms TTL=120
Reply from 172.217.27.206: bytes=68 (sent 100) time=4ms TTL=120
Reply from 172.217.27.206: bytes=68 (sent 100) time=4ms TTL=120
Reply from 172.217.27.206: bytes=68 (sent 100) time=3ms TTL=120
Reply from 172.217.27.206: bytes=68 (sent 100) time=6ms TTL=120
Reply from 172.217.27.206: bytes=68 (sent 100) time=5ms TTL=120
Reply from 172.217.27.206: bytes=68 (sent 100) time=4ms TTL=120
Reply from 172.217.27.206: bytes=68 (sent 100) time=5ms TTL=120

Ping statistics for 172.217.27.206:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 6ms, Average = 4ms
```

- ping -n 10 -l 500 berkeley.edu



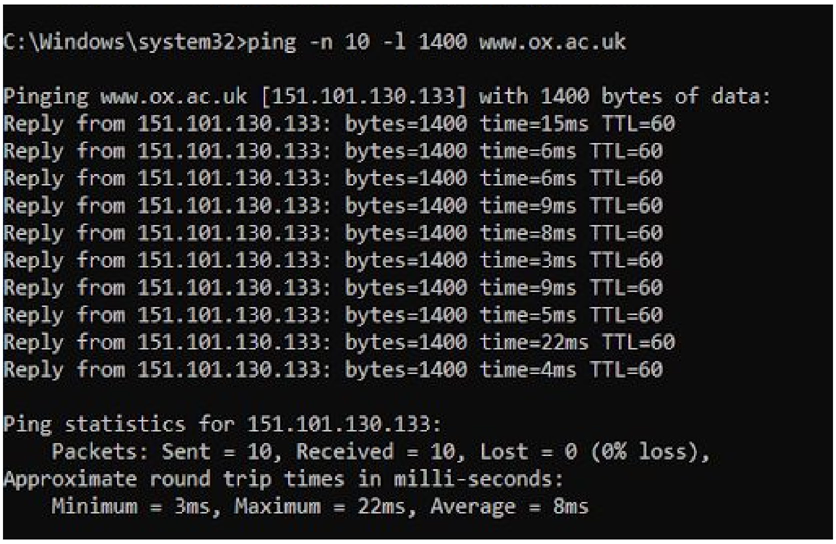
```
C:\Users\Swara>ping -n 10 -l 500 berkeley.edu

Pinging berkeley.edu [35.163.72.93] with 500 bytes of data:
Reply from 35.163.72.93: bytes=500 time=335ms TTL=38
Reply from 35.163.72.93: bytes=500 time=410ms TTL=38
Reply from 35.163.72.93: bytes=500 time=469ms TTL=38
Reply from 35.163.72.93: bytes=500 time=482ms TTL=38
Reply from 35.163.72.93: bytes=500 time=491ms TTL=38
Reply from 35.163.72.93: bytes=500 time=512ms TTL=38
Reply from 35.163.72.93: bytes=500 time=506ms TTL=38
Reply from 35.163.72.93: bytes=500 time=408ms TTL=38
Reply from 35.163.72.93: bytes=500 time=407ms TTL=38
Reply from 35.163.72.93: bytes=500 time=419ms TTL=38

Ping statistics for 35.163.72.93:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 335ms, Maximum = 512ms, Average = 443ms
```

- ping -n 10 -l 1000 google.com



```
Trace complete.

C:\Windows\system32>ping -n 10 -l 1400 google.com

Pinging google.com [172.217.160.206] with 1400 bytes of data:
Reply from 172.217.160.206: bytes=68 (sent 1400) time=5ms TTL=120
Reply from 172.217.160.206: bytes=68 (sent 1400) time=5ms TTL=120
Reply from 172.217.160.206: bytes=68 (sent 1400) time=7ms TTL=120
Reply from 172.217.160.206: bytes=68 (sent 1400) time=4ms TTL=120
Reply from 172.217.160.206: bytes=68 (sent 1400) time=11ms TTL=120
Reply from 172.217.160.206: bytes=68 (sent 1400) time=4ms TTL=120
Reply from 172.217.160.206: bytes=68 (sent 1400) time=5ms TTL=120
Reply from 172.217.160.206: bytes=68 (sent 1400) time=24ms TTL=120
Reply from 172.217.160.206: bytes=68 (sent 1400) time=5ms TTL=120
Reply from 172.217.160.206: bytes=68 (sent 1400) time=8ms TTL=120

Ping statistics for 172.217.160.206:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 24ms, Average = 7ms
```

- ping -n 10 -l 1400 www.ox.ac.uk



```
C:\Windows\system32>ping -n 10 -l 1400 www.ox.ac.uk

Pinging www.ox.ac.uk [151.101.130.133] with 1400 bytes of data:
Reply from 151.101.130.133: bytes=1400 time=15ms TTL=60
Reply from 151.101.130.133: bytes=1400 time=6ms TTL=60
Reply from 151.101.130.133: bytes=1400 time=6ms TTL=60
Reply from 151.101.130.133: bytes=1400 time=9ms TTL=60
Reply from 151.101.130.133: bytes=1400 time=8ms TTL=60
Reply from 151.101.130.133: bytes=1400 time=3ms TTL=60
Reply from 151.101.130.133: bytes=1400 time=9ms TTL=60
Reply from 151.101.130.133: bytes=1400 time=5ms TTL=60
Reply from 151.101.130.133: bytes=1400 time=22ms TTL=60
Reply from 151.101.130.133: bytes=1400 time=4ms TTL=60

Ping statistics for 151.101.130.133:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 22ms, Average = 8ms
```

Questions About Latency

Now look at the results you gathered and answer the following questions about latency. Store your answers in a file named ping.txt.

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

   List of factors affecting RTT:
   1 . The nature of the transmission medium
   2. Local area network (LAN) traffic
   3. Server response time
   4. Node count and congestion
   5. Physical distance

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

why?

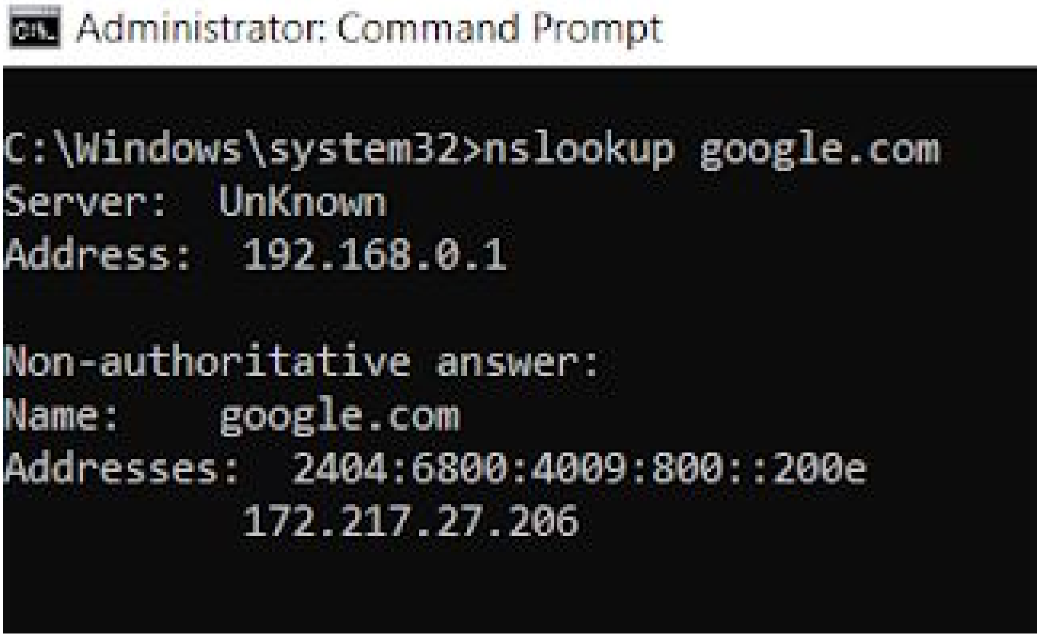
Ans: RTT increases with increase in packet size. There would be increased latency for increased packet size due to transmission delay and propagation delay.

Exercise 1: 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. Here are few places from who to get replies: www.uw.edu, www.cornell.edu, berkeley.edu, www.uchicago.edu, www.ox.ac.uk (England), www.u-tokyo.ac.jp (Japan).

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

- 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.
- 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.
- 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

nslookup — 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 nslokup by adding the server name or IP address to the command: nslookup <host> <server>:

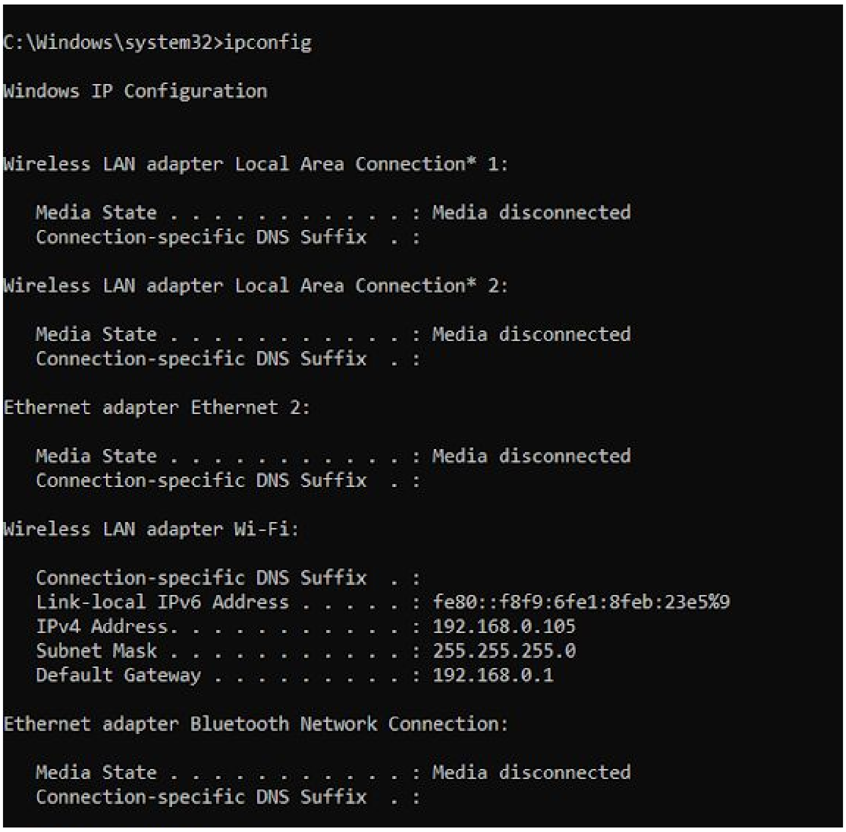


```
C:\Windows\system32>nslookup google.com
Server:  UnKnown
Address:  192.168.0.1

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4009:800::200e
          172.217.27.206
```

Command :ifconfig

You used ifconfig in the previous lab. When used with no parameters, ifconfig reports some information about the computer's network interfaces. This usually includes lo which stands for localhost; it can be used for communication between programs running on the same computer. Linux often has an interface named eth0, which is the first ethernet card. The information is different on Mac OS and Linux, but includes the IP or "inet" address and ethernet or "hardware" address for an ethernet card. On Linux, you get the number of packets received (RX) and sent (TX), as well as the number of bytes transmitted and received. (A better place to monitor network bytes on our Linux computers is in the GUI program System Monitor, if it is installed!!

Screenshot :

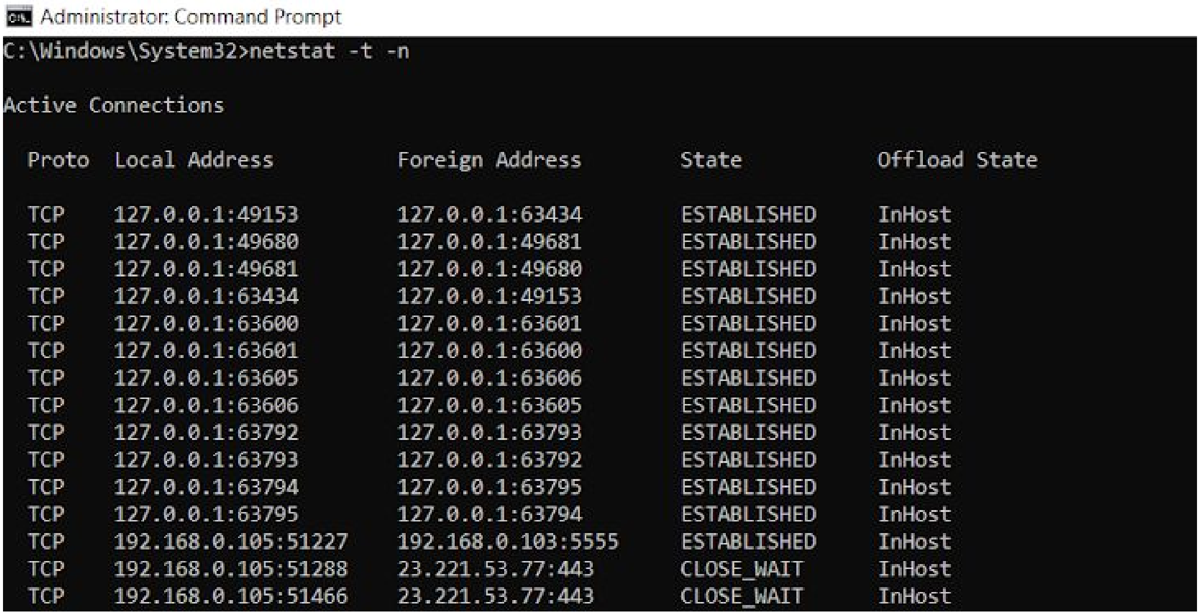


```
C:\Windows\system32>ipconfig

Windows IP Configuration


Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::f8f9:6fe1:8feb:23e5%9
   IPv4 Address. . . . . . . . . . . : 192.168.0.105
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

netstat — 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.)

Screenshot:



```
C:\Windows\System32>netstat -t -n

Active Connections

  Proto  Local Address          Foreign Address        State           Offload State

  TCP    127.0.0.1:49153        127.0.0.1:63434        ESTABLISHED     InHost
  TCP    127.0.0.1:49680        127.0.0.1:49681        ESTABLISHED     InHost
  TCP    127.0.0.1:49681        127.0.0.1:49680        ESTABLISHED     InHost
  TCP    127.0.0.1:63434        127.0.0.1:49153        ESTABLISHED     InHost
  TCP    127.0.0.1:63600        127.0.0.1:63601        ESTABLISHED     InHost
  TCP    127.0.0.1:63601        127.0.0.1:63600        ESTABLISHED     InHost
  TCP    127.0.0.1:63605        127.0.0.1:63606        ESTABLISHED     InHost
  TCP    127.0.0.1:63606        127.0.0.1:63605        ESTABLISHED     InHost
  TCP    127.0.0.1:63792        127.0.0.1:63793        ESTABLISHED     InHost
  TCP    127.0.0.1:63793        127.0.0.1:63792        ESTABLISHED     InHost
  TCP    127.0.0.1:63794        127.0.0.1:63795        ESTABLISHED     InHost
  TCP    127.0.0.1:63795        127.0.0.1:63794        ESTABLISHED     InHost
  TCP    192.168.0.105:51227    192.168.0.103:5555     ESTABLISHED     InHost
  TCP    192.168.0.105:51288    23.221.53.77:443       CLOSE_WAIT      InHost
  TCP    192.168.0.105:51466    23.221.53.77:443       CLOSE_WAIT      InHost
```

Comamnd : tracert

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

Experiments with Traceroute

From your machine traceroute to the following hosts:

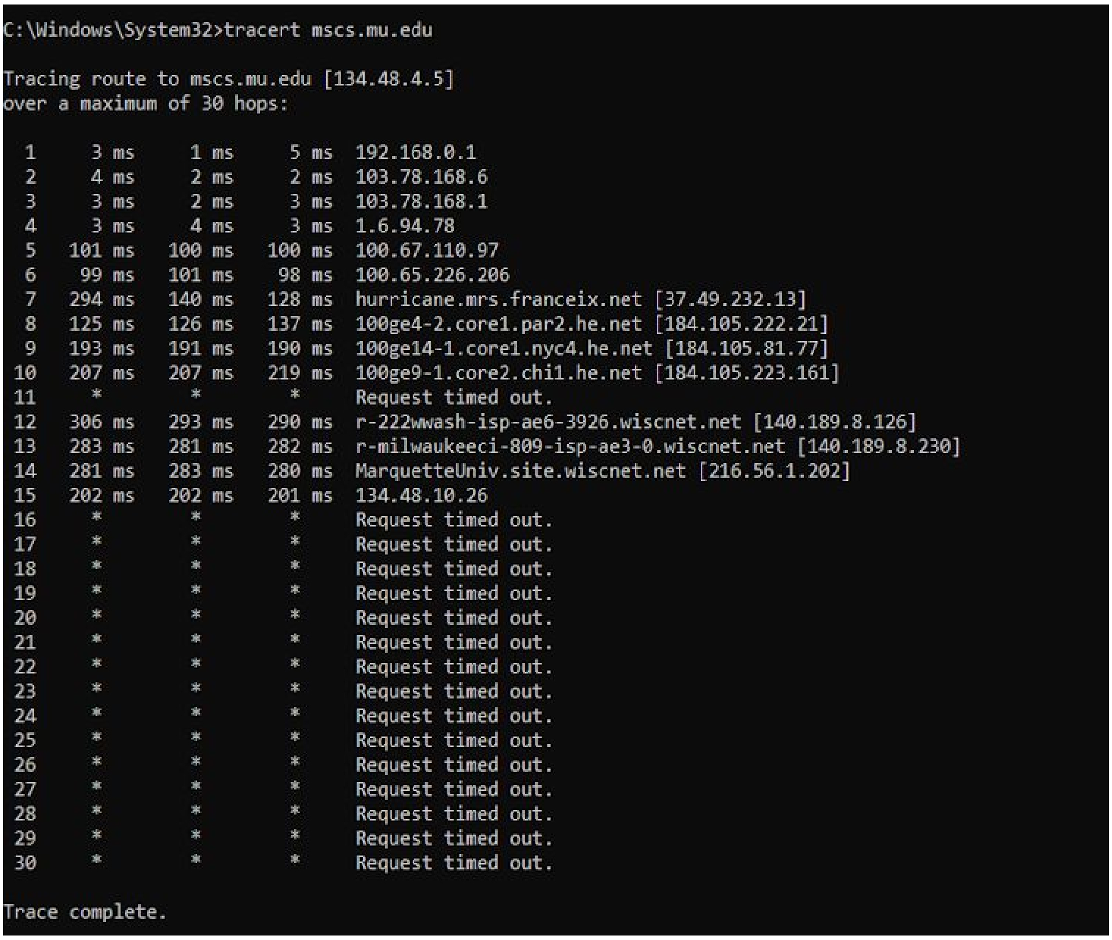
- ee.iitb.ac.in
- mscs.mu.edu
- www.cs.grinnell.edu
- csail.mit.edu
- cs.stanford.edu
- cs.manchester.ac.uk

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).

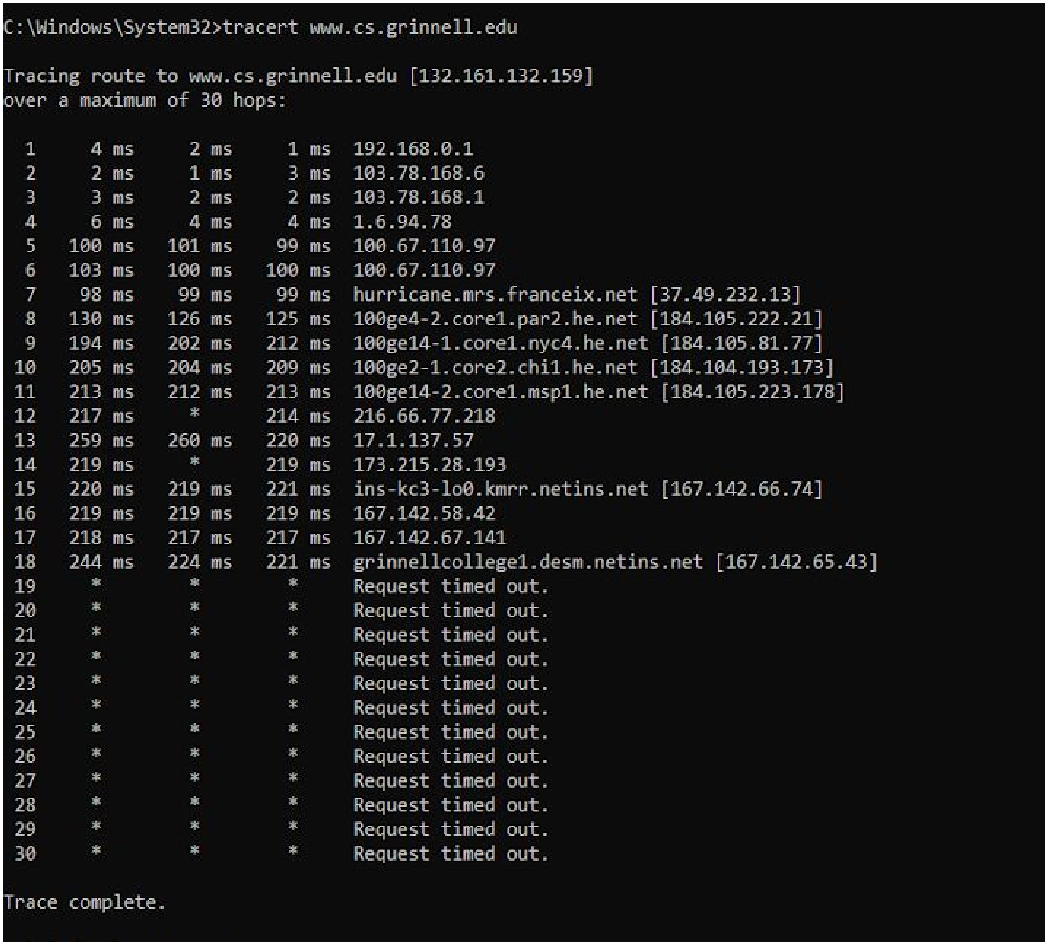
Screenshots :

1) mscs.mu.edu



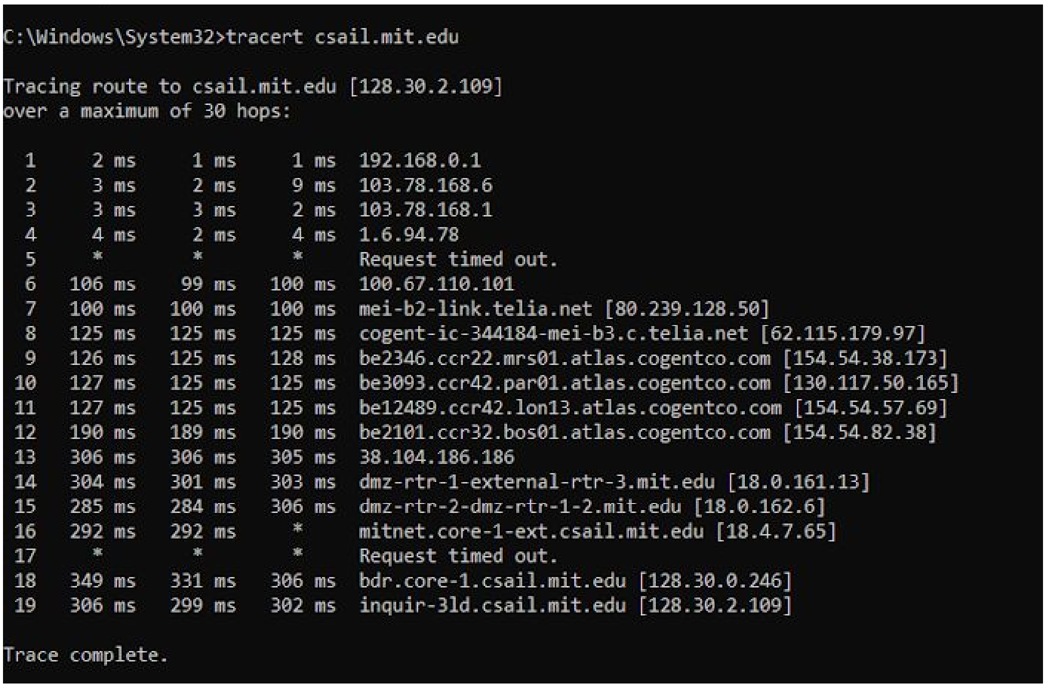
```
C:\Windows\System32>tracert mscs.mu.edu

Tracing route to mscs.mu.edu [134.48.4.5]
over a maximum of 30 hops:

  1     3 ms     1 ms     5 ms  192.168.0.1
  2     4 ms     2 ms     2 ms  103.78.168.6
  3     3 ms     2 ms     3 ms  103.78.168.1
  4     3 ms     4 ms     3 ms  1.6.94.78
  5   101 ms   100 ms   100 ms  100.67.110.97
  6    99 ms   101 ms    98 ms  100.65.226.206
  7   294 ms   140 ms   128 ms  hurricane.mrs.franceix.net [37.49.232.13]
  8   125 ms   126 ms   137 ms  100ge4-2.core1.par2.he.net [184.105.222.21]
  9   193 ms   191 ms   190 ms  100ge14-1.core1.nyc4.he.net [184.105.81.77]
 10   207 ms   207 ms   219 ms  100ge9-1.core2.chi1.he.net [184.105.223.161]
 11     *        *        *     Request timed out.
 12   306 ms   293 ms   290 ms  r-222wwash-isp-ae6-3926.wiscnet.net [140.189.8.126]
 13   283 ms   281 ms   282 ms  r-milwaukeeci-809-isp-ae3-0.wiscnet.net [140.189.8.230]
 14   281 ms   283 ms   280 ms  MarquetteUniv.site.wiscnet.net [216.56.1.202]
 15   202 ms   202 ms   201 ms  134.48.10.26
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```

2) www.cs.grinnell.edu



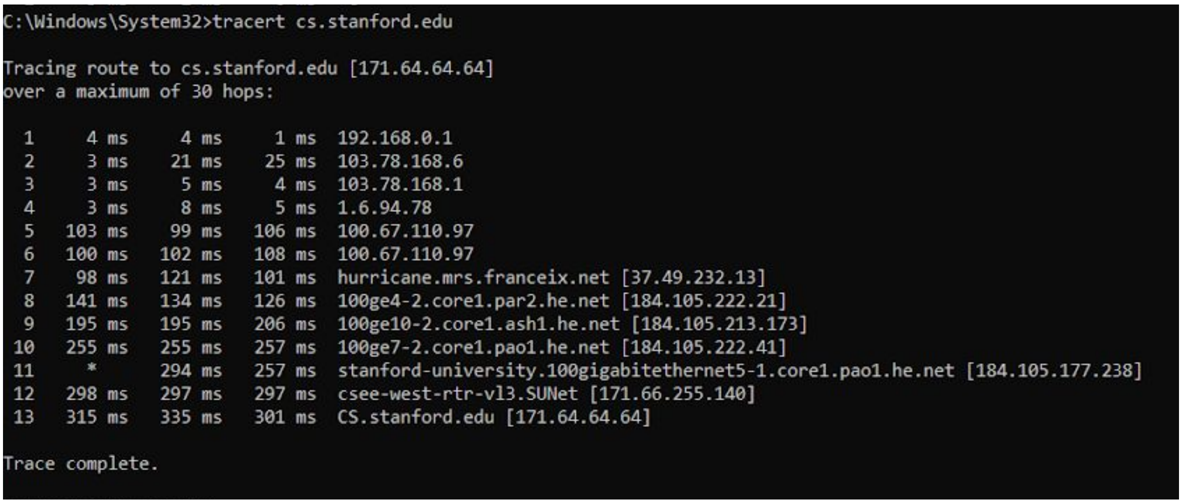
```
C:\Windows\System32>tracert www.cs.grinnell.edu

Tracing route to www.cs.grinnell.edu [132.161.132.159]
over a maximum of 30 hops:

  1     4 ms     2 ms     1 ms  192.168.0.1
  2     2 ms     1 ms     3 ms  103.78.168.6
  3     3 ms     2 ms     2 ms  103.78.168.1
  4     6 ms     4 ms     4 ms  1.6.94.78
  5   100 ms   101 ms    99 ms  100.67.110.97
  6   103 ms   100 ms   100 ms  100.67.110.97
  7    98 ms    99 ms    99 ms  hurricane.mrs.franceix.net [37.49.232.13]
  8   130 ms   126 ms   125 ms  100ge4-2.core1.par2.he.net [184.105.222.21]
  9   194 ms   202 ms   212 ms  100ge14-1.core1.nyc4.he.net [184.105.81.77]
 10   205 ms   204 ms   209 ms  100ge2-1.core2.chi1.he.net [184.104.193.173]
 11   213 ms   212 ms   213 ms  100ge14-2.core1.msp1.he.net [184.105.223.178]
 12   217 ms     *      214 ms  216.66.77.218
 13   259 ms   260 ms   220 ms  17.1.137.57
 14   219 ms     *      219 ms  173.215.28.193
 15   220 ms   219 ms   221 ms  ins-kc3-lo0.kmrr.netins.net [167.142.66.74]
 16   219 ms   219 ms   219 ms  167.142.58.42
 17   218 ms   217 ms   217 ms  167.142.67.141
 18   244 ms   224 ms   221 ms  grinnellcollege1.desm.netins.net [167.142.65.43]
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```

3)csail.mit.edu



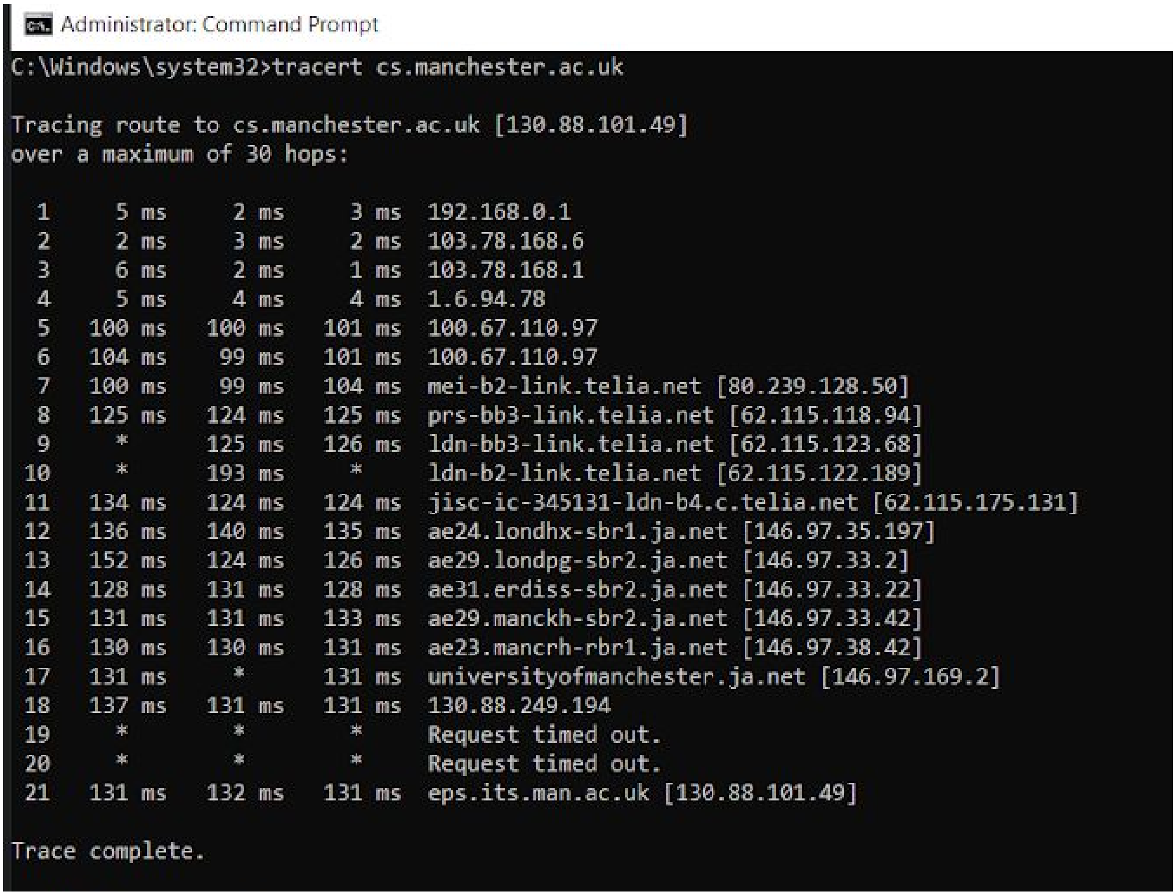
```
C:\Windows\System32>tracert csail.mit.edu

Tracing route to csail.mit.edu [128.30.2.109]
over a maximum of 30 hops:

  1     2 ms     1 ms     1 ms  192.168.0.1
  2     3 ms     2 ms     9 ms  103.78.168.6
  3     3 ms     3 ms     2 ms  103.78.168.1
  4     4 ms     2 ms     4 ms  1.6.94.78
  5     *        *        *     Request timed out.
  6   106 ms    99 ms   100 ms  100.67.110.101
  7   100 ms   100 ms   100 ms  mei-b2-link.telia.net [80.239.128.50]
  8   125 ms   125 ms   125 ms  cogent-ic-344184-mei-b3.c.telia.net [62.115.179.97]
  9   126 ms   125 ms   128 ms  be2346.ccr22.mrs01.atlas.cogentco.com [154.54.38.173]
 10   127 ms   125 ms   125 ms  be3093.ccr42.par01.atlas.cogentco.com [130.117.50.165]
 11   127 ms   125 ms   125 ms  be12489.ccr42.lon13.atlas.cogentco.com [154.54.57.69]
 12   190 ms   189 ms   190 ms  be2101.ccr32.bos01.atlas.cogentco.com [154.54.82.38]
 13   306 ms   306 ms   305 ms  38.104.186.186
 14   304 ms   301 ms   303 ms  dmz-rtr-1-external-rtr-3.mit.edu [18.0.161.13]
 15   285 ms   284 ms   306 ms  dmz-rtr-2-dmz-rtr-1-2.mit.edu [18.0.162.6]
 16   292 ms   292 ms     *      mitnet.core-1-ext.csail.mit.edu [18.4.7.65]
 17     *        *        *     Request timed out.
 18   349 ms   331 ms   306 ms  bdr.core-1.csail.mit.edu [128.30.0.246]
 19   306 ms   299 ms   302 ms  inquir-3ld.csail.mit.edu [128.30.2.109]

Trace complete.
```

4)cs.stanford.edu



```
C:\Windows\System32>tracert cs.stanford.edu

Tracing route to cs.stanford.edu [171.64.64.64]
over a maximum of 30 hops:

  1     4 ms     4 ms     1 ms  192.168.0.1
  2     3 ms    21 ms    25 ms  103.78.168.6
  3     3 ms     5 ms     4 ms  103.78.168.1
  4     3 ms     8 ms     5 ms  1.6.94.78
  5   103 ms    99 ms   106 ms  100.67.110.97
  6   100 ms   102 ms   108 ms  100.67.110.97
  7    98 ms   121 ms   101 ms  hurricane.mrs.franceix.net [37.49.232.13]
  8   141 ms   134 ms   126 ms  100ge4-2.core1.par2.he.net [184.105.222.21]
  9   195 ms   195 ms   206 ms  100ge10-2.core1.ash1.he.net [184.105.213.173]
 10   255 ms   255 ms   257 ms  100ge7-2.core1.pao1.he.net [184.105.222.41]
 11     *      294 ms   257 ms  stanford-university.100gigabitethernet5-1.core1.pao1.he.net [184.105.177.238]
 12   298 ms   297 ms   297 ms  csee-west-rtr-vl3.SUNet [171.66.255.140]
 13   315 ms   335 ms   301 ms  CS.stanford.edu [171.64.64.64]

Trace complete.
```

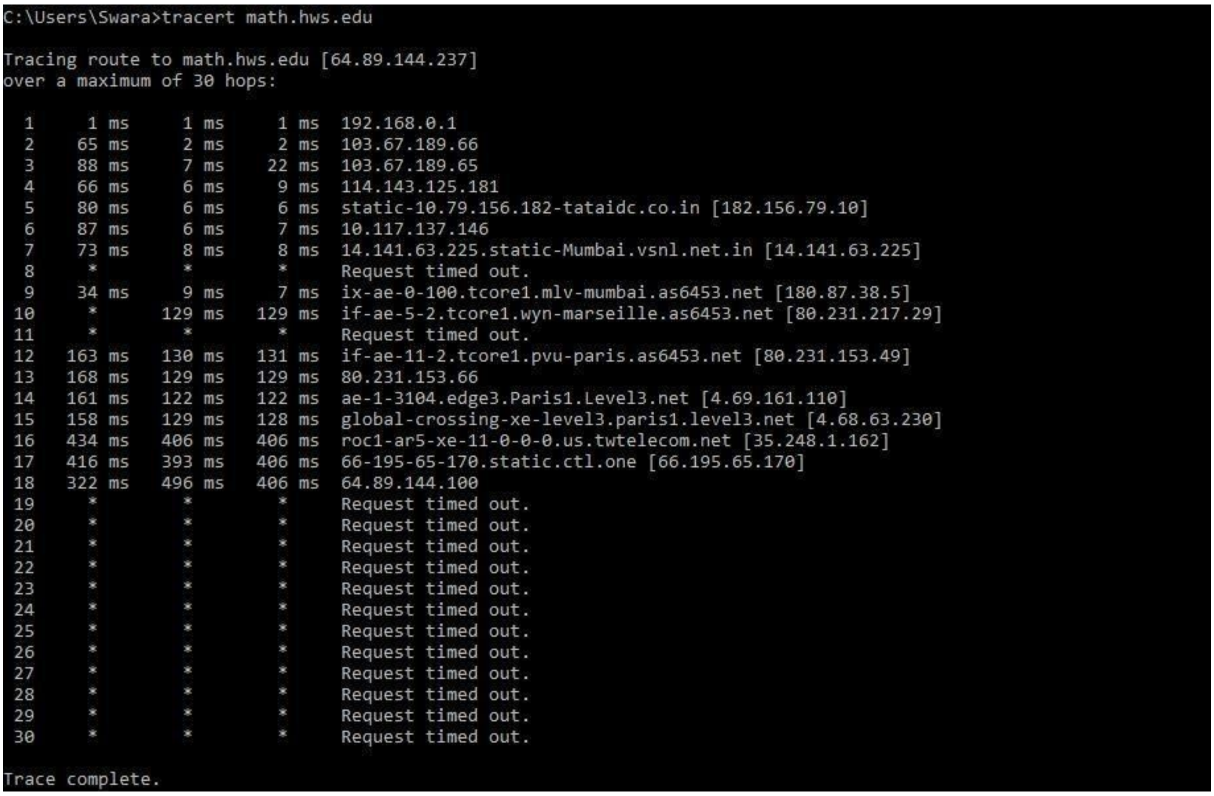
5) cs.manchester.ac.uk



```
C:\Windows\system32>tracert cs.manchester.ac.uk

Tracing route to cs.manchester.ac.uk [130.88.101.49]
over a maximum of 30 hops:

  1     5 ms     2 ms     3 ms  192.168.0.1
  2     2 ms     3 ms     2 ms  103.78.168.6
  3     6 ms     2 ms     1 ms  103.78.168.1
  4     5 ms     4 ms     4 ms  1.6.94.78
  5   100 ms   100 ms   101 ms  100.67.110.97
  6   104 ms    99 ms   101 ms  100.67.110.97
  7   100 ms    99 ms   104 ms  mei-b2-link.telia.net [80.239.128.50]
  8   125 ms   124 ms   125 ms  prs-bb3-link.telia.net [62.115.118.94]
  9     *      125 ms   126 ms  ldn-bb3-link.telia.net [62.115.123.68]
 10     *      193 ms     *     ldn-b2-link.telia.net [62.115.122.189]
 11   134 ms   124 ms   124 ms  jisc-ic-345131-ldn-b4.c.telia.net [62.115.175.131]
 12   136 ms   140 ms   135 ms  ae24.londhx-sbr1.ja.net [146.97.35.197]
 13   152 ms   124 ms   126 ms  ae29.londpg-sbr2.ja.net [146.97.33.2]
 14   128 ms   131 ms   128 ms  ae31.erdiss-sbr2.ja.net [146.97.33.22]
 15   131 ms   131 ms   133 ms  ae29.manckh-sbr2.ja.net [146.97.33.42]
 16   130 ms   130 ms   131 ms  ae23.mancrh-rbr1.ja.net [146.97.38.42]
 17   131 ms     *      131 ms  universityofmanchester.ja.net [146.97.169.2]
 18   137 ms   131 ms   131 ms  130.88.249.194
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21   131 ms   132 ms   131 ms  eps.its.man.ac.uk [130.88.101.49]

Trace complete.
```

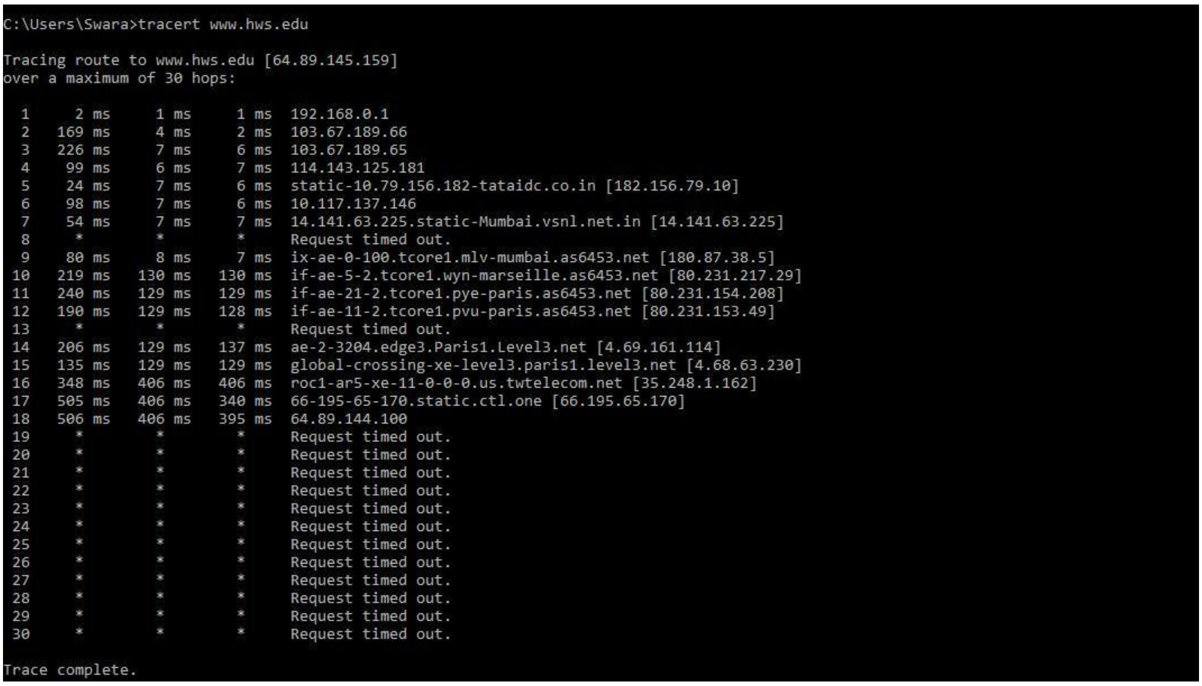
Exercise 2: (Very short.) Use traceroute to trace the route from your computer to math.hws.edu and to www.hws.edu. Explain the difference in the results.

maths.hws.edu



```
C:\Users\Swara>tracert math.hws.edu

Tracing route to math.hws.edu [64.89.144.237]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  192.168.0.1
  2    65 ms     2 ms     2 ms  103.67.189.66
  3    88 ms     7 ms    22 ms  103.67.189.65
  4    66 ms     6 ms     9 ms  114.143.125.181
  5    80 ms     6 ms     6 ms  static-10.79.156.182-tataidc.co.in [182.156.79.10]
  6    87 ms     6 ms     7 ms  10.117.137.146
  7    73 ms     8 ms     8 ms  14.141.63.225.static-Mumbai.vsnl.net.in [14.141.63.225]
  8     *        *        *     Request timed out.
  9    34 ms     9 ms     7 ms  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net [180.87.38.5]
 10     *      129 ms   129 ms  if-ae-5-2.tcore1.wyn-marseille.as6453.net [80.231.217.29]
 11     *        *        *     Request timed out.
 12   163 ms   130 ms   131 ms  if-ae-11-2.tcore1.pvu-paris.as6453.net [80.231.153.49]
 13   168 ms   129 ms   129 ms  80.231.153.66
 14   161 ms   122 ms   122 ms  ae-1-3104.edge3.Paris1.Level3.net [4.69.161.110]
 15   158 ms   129 ms   128 ms  global-crossing-xe-level3.paris1.level3.net [4.68.63.230]
 16   434 ms   406 ms   406 ms  roc1-ar5-xe-11-0-0-0.us.twtelecom.net [35.248.1.162]
 17   416 ms   393 ms   406 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 18   322 ms   496 ms   406 ms  64.89.144.100
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```

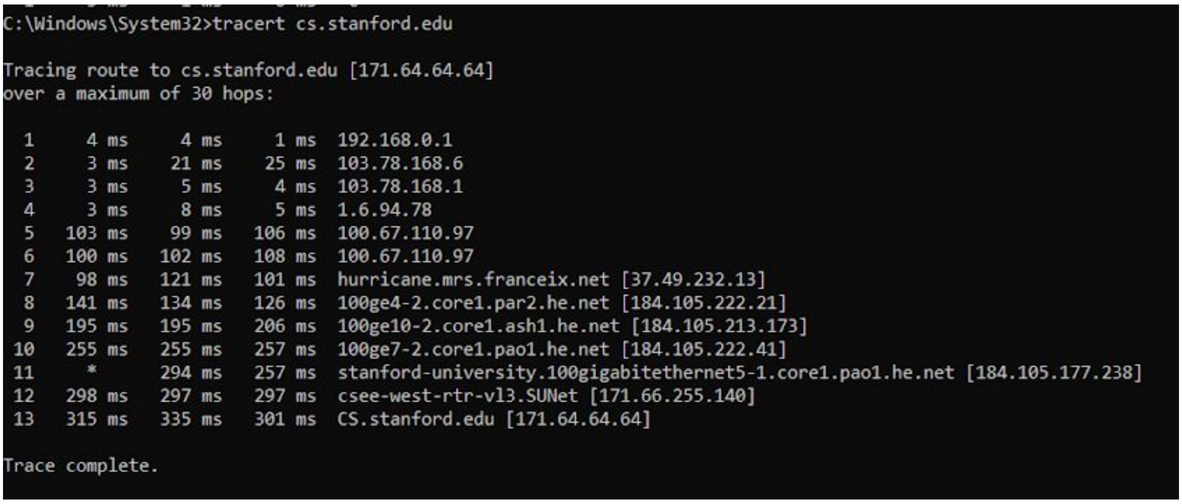
www.hws.edu



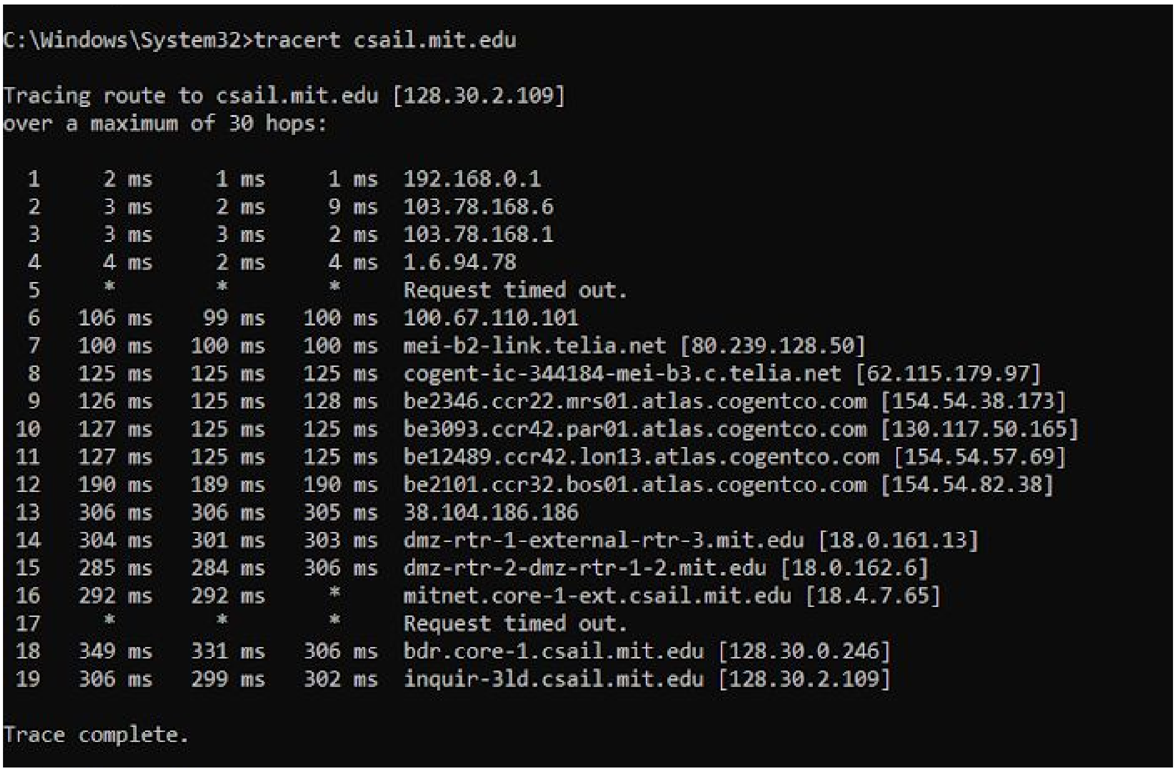
```
C:\Users\Swara>tracert www.hws.edu

Tracing route to www.hws.edu [64.89.145.159]
over a maximum of 30 hops:

  1     2 ms     1 ms     1 ms  192.168.0.1
  2   169 ms     4 ms     2 ms  103.67.189.66
  3   226 ms     7 ms     6 ms  103.67.189.65
  4    99 ms     6 ms     7 ms  114.143.125.181
  5    24 ms     7 ms     6 ms  static-10.79.156.182-tataidc.co.in [182.156.79.10]
  6    98 ms     7 ms     6 ms  10.117.137.146
  7    54 ms     7 ms     7 ms  14.141.63.225.static-Mumbai.vsnl.net.in [14.141.63.225]
  8     *        *        *     Request timed out.
  9    80 ms     8 ms     7 ms  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net [180.87.38.5]
 10   219 ms   130 ms   130 ms  if-ae-5-2.tcore1.wyn-marseille.as6453.net [80.231.217.29]
 11   240 ms   129 ms   129 ms  if-ae-21-2.tcore1.pye-paris.as6453.net [80.231.154.208]
 12   190 ms   129 ms   128 ms  if-ae-11-2.tcore1.pvu-paris.as6453.net [80.231.153.49]
 13     *        *        *     Request timed out.
 14   206 ms   129 ms   137 ms  ae-2-3204.edge3.Paris1.Level3.net [4.69.161.114]
 15   135 ms   129 ms   129 ms  global-crossing-xe-level3.paris1.level3.net [4.68.63.230]
 16   348 ms   406 ms   406 ms  roc1-ar5-xe-11-0-0-0.us.twtelecom.net [35.248.1.162]
 17   505 ms   406 ms   340 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 18   506 ms   406 ms   395 ms  64.89.144.100
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```

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 math.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.

<u>Exercise 3:</u> 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.



```
C:\Windows\System32>tracert cs.stanford.edu

Tracing route to cs.stanford.edu [171.64.64.64]
over a maximum of 30 hops:

  1     4 ms     4 ms     1 ms  192.168.0.1
  2     3 ms    21 ms    25 ms  103.78.168.6
  3     3 ms     5 ms     4 ms  103.78.168.1
  4     3 ms     8 ms     5 ms  1.6.94.78
  5   103 ms    99 ms   106 ms  100.67.110.97
  6   100 ms   102 ms   108 ms  100.67.110.97
  7    98 ms   121 ms   101 ms  hurricane.mrs.franceix.net [37.49.232.13]
  8   141 ms   134 ms   126 ms  100ge4-2.core1.par2.he.net [184.105.222.21]
  9   195 ms   195 ms   206 ms  100ge10-2.core1.ash1.he.net [184.105.213.173]
 10   255 ms   255 ms   257 ms  100ge7-2.core1.pao1.he.net [184.105.222.41]
 11     *      294 ms   257 ms  stanford-university.100gigabitethernet5-1.core1.pao1.he.net [184.105.177.238]
 12   298 ms   297 ms   297 ms  csee-west-rtr-vl3.SUNet [171.66.255.140]
 13   315 ms   335 ms   301 ms  CS.stanford.edu [171.64.64.64]

Trace complete.
```



```
C:\Windows\System32>tracert csail.mit.edu

Tracing route to csail.mit.edu [128.30.2.109]
over a maximum of 30 hops:

  1     2 ms     1 ms     1 ms  192.168.0.1
  2     3 ms     2 ms     9 ms  103.78.168.6
  3     3 ms     3 ms     2 ms  103.78.168.1
  4     4 ms     2 ms     4 ms  1.6.94.78
  5     *        *        *     Request timed out.
  6   106 ms    99 ms   100 ms  100.67.110.101
  7   100 ms   100 ms   100 ms  mei-b2-link.telia.net [80.239.128.50]
  8   125 ms   125 ms   125 ms  cogent-ic-344184-mei-b3.c.telia.net [62.115.179.97]
  9   126 ms   125 ms   128 ms  be2346.ccr22.mrs01.atlas.cogentco.com [154.54.38.173]
 10   127 ms   125 ms   125 ms  be3093.ccr42.par01.atlas.cogentco.com [130.117.50.165]
 11   127 ms   125 ms   125 ms  be12489.ccr42.lon13.atlas.cogentco.com [154.54.57.69]
 12   190 ms   189 ms   190 ms  be2101.ccr32.bos01.atlas.cogentco.com [154.54.82.38]
 13   306 ms   306 ms   305 ms  38.104.186.186
 14   304 ms   301 ms   303 ms  dmz-rtr-1-external-rtr-3.mit.edu [18.0.161.13]
 15   285 ms   284 ms   306 ms  dmz-rtr-2-dmz-rtr-1-2.mit.edu [18.0.162.6]
 16   292 ms   292 ms     *      mitnet.core-1-ext.csail.mit.edu [18.4.7.65]
 17     *        *        *     Request timed out.
 18   349 ms   331 ms   306 ms  bdr.core-1.csail.mit.edu [128.30.0.246]
 19   306 ms   299 ms   302 ms  inquir-3ld.csail.mit.edu [128.30.2.109]

Trace complete.
```

Questions About Paths

Now look at the results you gathered and answer the following questions about the paths taken by your packets. Store your answers in a file named `traceroute.txt`.

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

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?

   No, there is no proportional relationship between the number of nodes and location of the host.

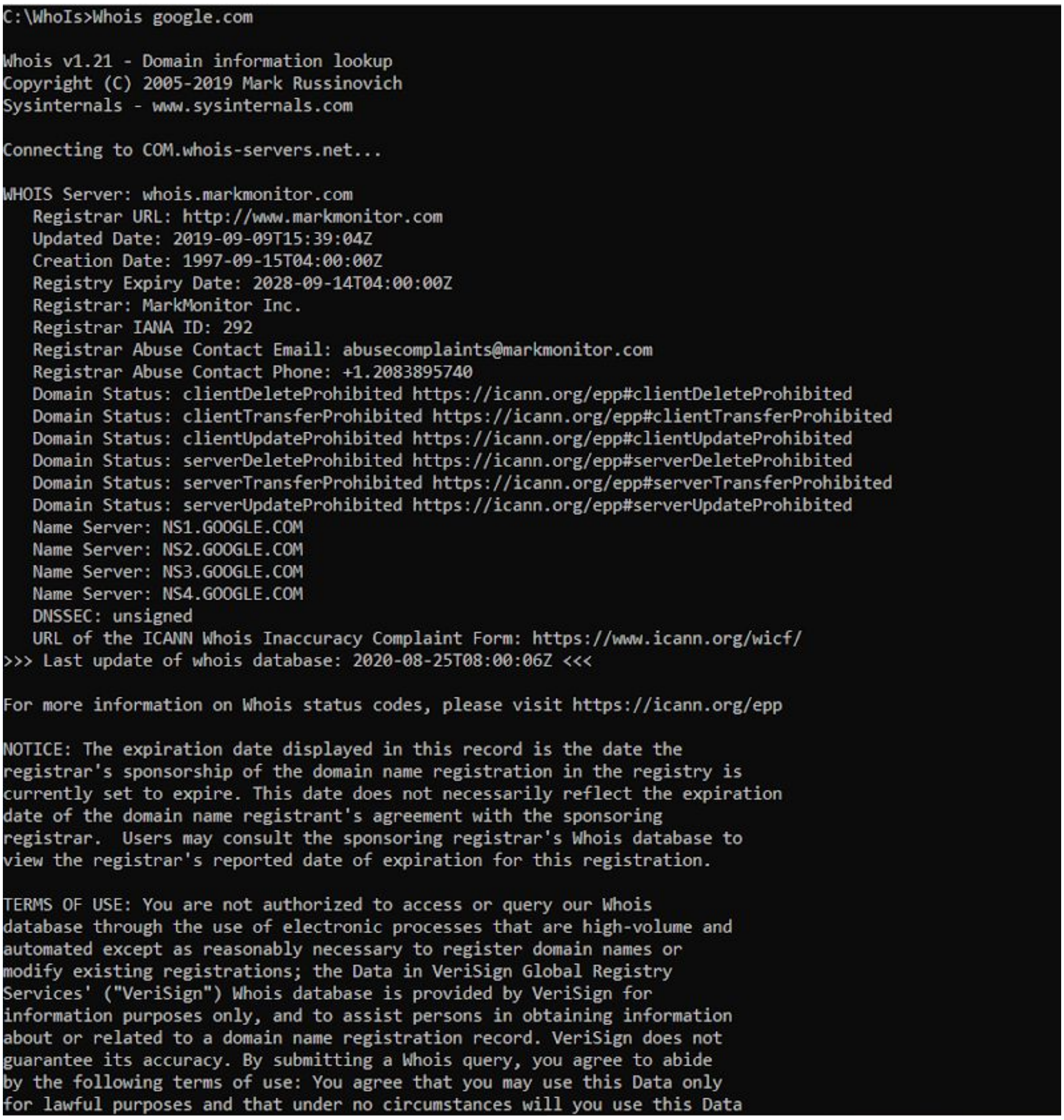
3. Is there a relationship between the number of nodes that show up in the traceroute and latency of the host (from your ping results above)? Does the same relationship hold for all hosts?
   There is a direct relationship between the number of nodes and latency of the host. The amount of latency is largely dependent on how far the visitor is from the server location and how many nodes signal has to travel through.

WHOIS

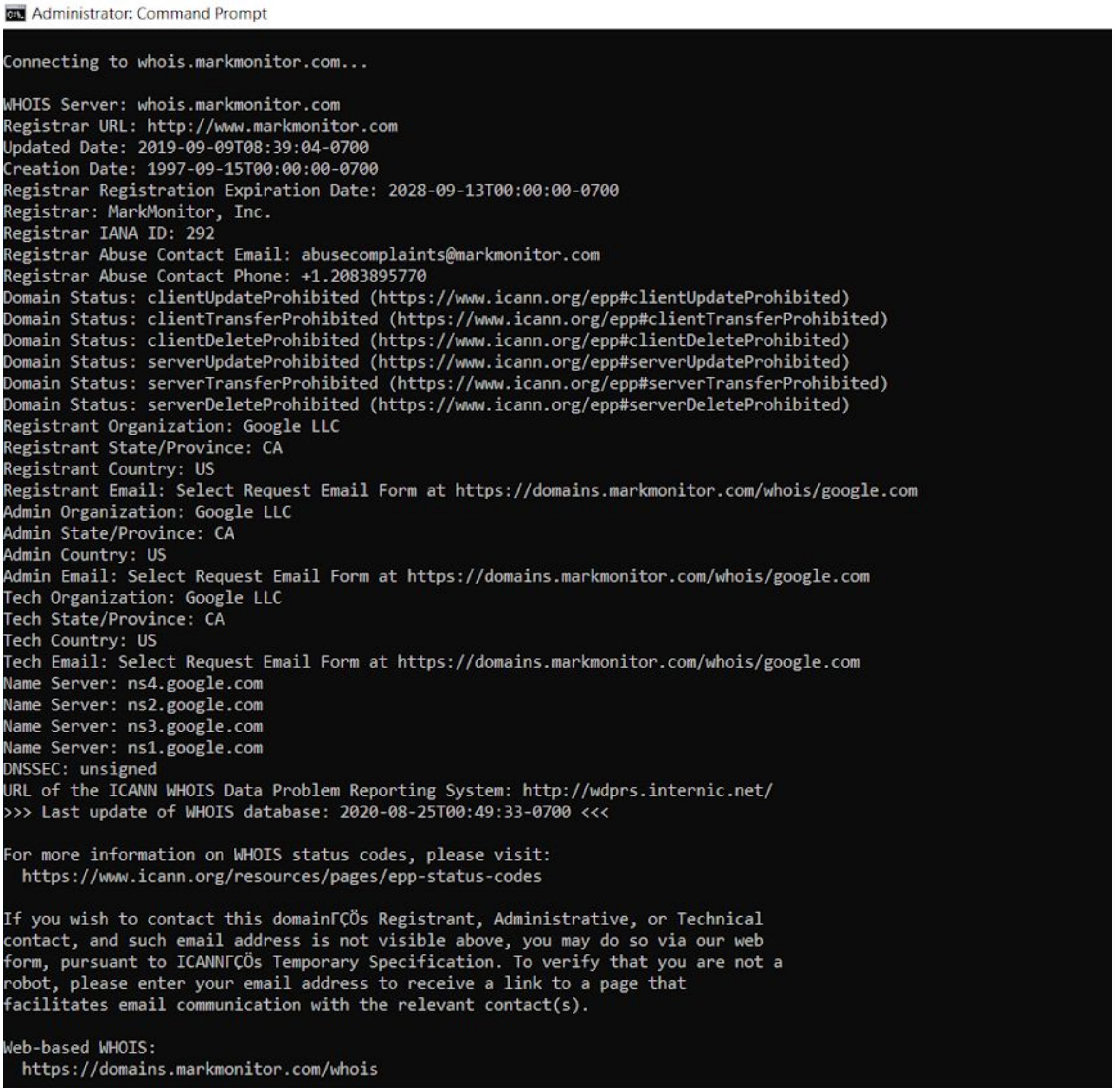
Whois — The *whois* command can give detailed information about domain names and IP addresses. If it is not installed on the computers then install it with command sudo apt-get install whois in.

Whois can tell you what organization owns or is responsible for the name or address and where to contact them. It often includes a list of domain name servers for the organization. When using *whois* to look up a domain name, use the simple two-part network name, not an individual computer name (for example, *whois spit.ac.in*).

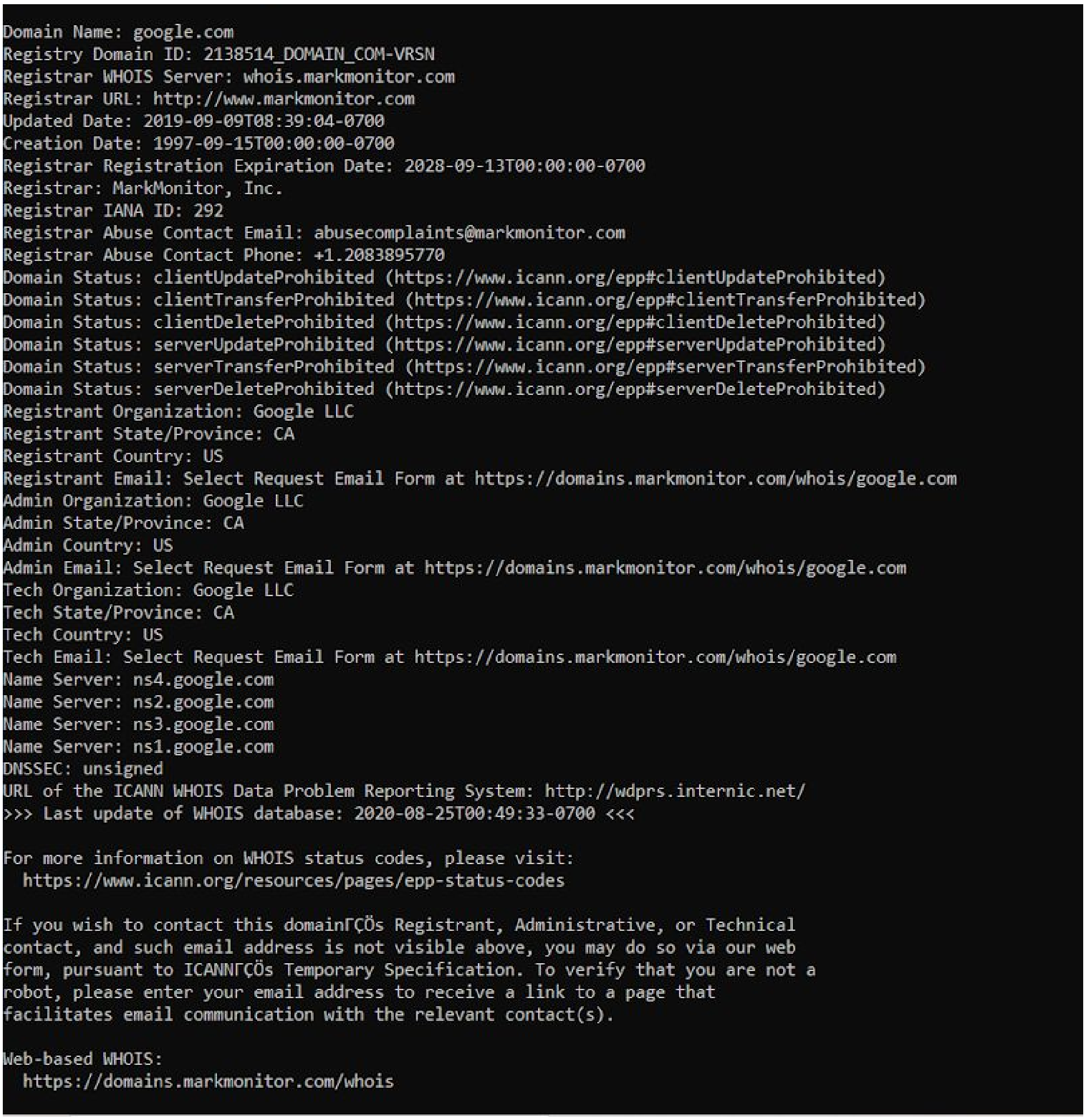
Exercise 4: (Short.) Use *whois* to investigate a well-known web site such as google.com or amazon.com, and write a couple of sentences about what you find out.



```
C:\WhoIs>Whois google.com

Whois v1.21 - Domain information lookup
Copyright (C) 2005-2019 Mark Russinovich
Sysinternals - www.sysinternals.com

Connecting to COM.whois-servers.net...

WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2019-09-09T15:39:04Z
   Creation Date: 1997-09-15T04:00:00Z
   Registry Expiry Date: 2028-09-14T04:00:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2083895740
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: NS1.GOOGLE.COM
   Name Server: NS2.GOOGLE.COM
   Name Server: NS3.GOOGLE.COM
   Name Server: NS4.GOOGLE.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2020-08-25T08:00:06Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

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
```



```
Connecting to whois.markmonitor.com...

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: ns4.google.com
Name Server: ns2.google.com
Name Server: ns3.google.com
Name Server: ns1.google.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2020-08-25T00:49:33-0700 <<<

For more information on WHOIS status codes, please visit:
  https://www.icann.org/resources/pages/epp-status-codes

If you wish to contact this domainΓÇÖs Registrant, Administrative, or Technical
contact, and such email address is not visible above, you may do so via our web
form, pursuant to ICANNΓÇÖs Temporary Specification. To verify that you are not a
robot, please enter your email address to receive a link to a page that
facilitates email communication with the relevant contact(s).

Web-based WHOIS:
  https://domains.markmonitor.com/whois
```



```
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: ns4.google.com
Name Server: ns2.google.com
Name Server: ns3.google.com
Name Server: ns1.google.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2020-08-25T00:49:33-0700 <<<

For more information on WHOIS status codes, please visit:
  https://www.icann.org/resources/pages/epp-status-codes

If you wish to contact this domainΓÇÖs Registrant, Administrative, or Technical
contact, and such email address is not visible above, you may do so via our web
form, pursuant to ICANNΓÇÖs Temporary Specification. To verify that you are not a
robot, please enter your email address to receive a link to a page that
facilitates email communication with the relevant contact(s).

Web-based WHOIS:
  https://domains.markmonitor.com/whois
```

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.

Exercise 5: (Should be short.) Because of NAT, the domain name *spit.ac.in* has a different IP address outside of SPIT than it does on campus. Using information in this lab and working on a home computer, find the outside IP address for spit.ac.in. Explain how you did it.

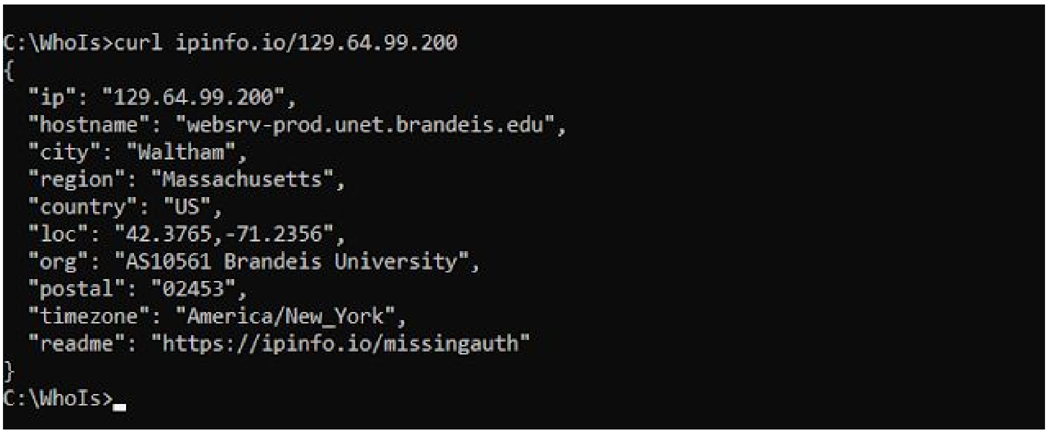
Geolocation — A geolocation service tries to tell, approximately, where a given IP address is located physically. They can't be completely accurate—but they probably get at least the country right most of the time.

This geolocation program is not installed on our computers, but you can access one on the command line using the *curl* command, which can send HTTP requests and display the response. The following command uses *curl* to contact a public web service that will look up an IP address for you: curl ipinfo.io/<IP-address>. For a specific example:

curl ipinfo.io/129.64.99.200

(As you can see, you get back more than just the location.)

Screenshot:



```
C:\WhoIs>curl ipinfo.io/129.64.99.200
{
  "ip": "129.64.99.200",
  "hostname": "websrv-prod.unet.brandeis.edu",
  "city": "Waltham",
  "region": "Massachusetts",
  "country": "US",
  "loc": "42.3765,-71.2356",
  "org": "AS10561 Brandeis University",
  "postal": "02453",
  "timezone": "America/New_York",
  "readme": "https://ipinfo.io/missingauth"
}
C:\WhoIs>_
```

Conclusion:

1. Learnt about some basic command line network utilities.
2. Learnt about Network Latency, RTT and the factors impacting RTT.

References :

1. https://www.geeksforgeeks.org/packet-switching-and-delays-in-computer-network/
2. https://www.sciencedirect.com/topics/computer-science/traceroute-command