NAME: ASHUTOSH NAIK
CLASS: TE COMPS
BATCH: C
ROLL NO: 35
UID: 2018130030
DATE: 14/08/2020

CEL 51, DCCN, Monsoon 2020
Lab 2: Basic Network Utilities

This lab introduces some basic network monitoring/analysis tools. There are a few exercises along the way. You should write up answers to the ***ping*** and ***traceroute*** exercises and turn them in next lab. (You should try out each tool, whether it is needed for an exercise or not!).

Prerequisite: Basic understanding of command line utilities of Linux Operating system.

Some Basic command line Networking utilities

Start with a few of the most basic command line tools. These commands are available on Unix, including Linux (and the first two, at least, are also for Windows). Some parameters or options might differ on different operating systems. Remember that you can use man <command> to get information about a command and its options.

ping — The command ping <host> sends a series of packets and expects to receieve a response to each packet. When a return packet is received, ping reports the round trip time (the time between sending the packet and receiving the response). Some routers and firewalls block ping requests, so you might get no reponse at all. Ping can be used to check whether a computer is up and running, to measure network delay time, and to check for dropped packets indicating network congestion. Note that <host> can be either a domain name or an IP address. By default, ping will send a packet every second indefinitely; stop it with Control-C

Network latency, specifically round trip time (RTT), can be measured using `ping`, which sends ICMP packets. The syntax for the command in Linux or Mac OS is:

```
ping [-c <count>] [-s <packetsize>] <hostname>
```

The syntax in Windows is:

```
ping [-n <count>] [-l <packetsize>] <hostname>
```

The default number of ICMP packets to send is either infinite (in Linux and Mac OS) or 4 (in Windows). The default packet size is either 64 bytes (in Linux) or 32 bytes (in Windows). You can specify either a hostname (e.g., `spit.ac.in`) or an IP address.

To save the output from `ping` to a file, include a greater than symbol and a file name at the end of the command. For example:

```
ping -c 10 google.com > ping_c10_s64_google.log
```

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

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?**

   Answer -

   In telecommunications, the **round-trip time** is the length of time it takes for a signal to be sent plus the length of time it takes for an acknowledgement of that signal to be received. This time delay includes the propagation times for the paths between the two communication endpoints. [1]

   Transmission delay is a function of the packet's length and has nothing to do with the distance between the two nodes.

   Propagation delay is the amount of time it takes for the head of the signal to travel from the sender to the receiver. It can be computed as the ratio between the link length and the propagation speed over the specific medium.

   Queuing delay is the time a job waits in a queue until it can be executed.

   Yes, Average RTT does vary between different hosts due to queuing delay as we can see in above example the average RTT calculated for **google.com, uw.edu** and **ox.ac.uk** differs. This can mostly be due to **propagation delay**

as it depends on distance and due to **queuing delay** as the packet may be in queue.

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

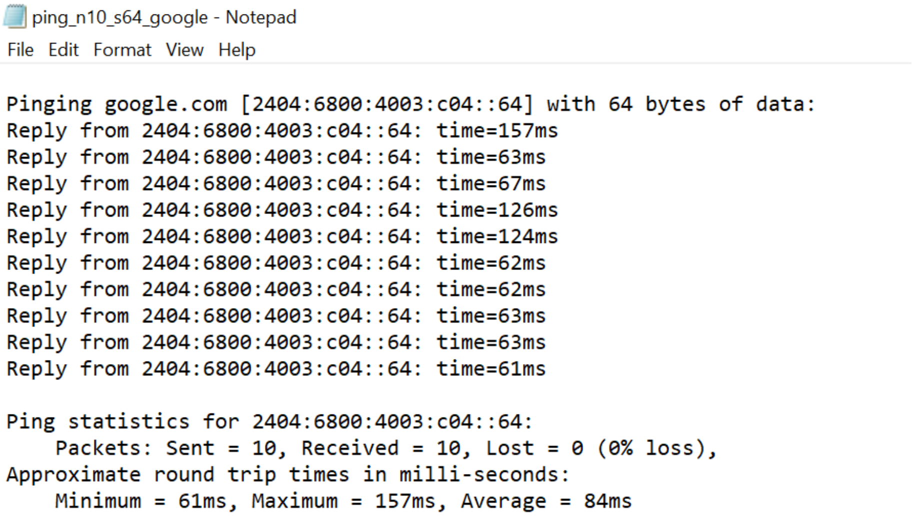
Answer -

The host google.com was pinged with 64, 100, 500, 1000 and 1400 bytes of data. The average RTT did not vary much as per the packet size. However, theoretically RTT should have increased because of increased **transmission delay** as it is dependent on packet size and **queue delay.**

Observations:
The average RTT varies for different hosts for same packet size. It is observed that the RTT for US servers are quite high compared to England servers. RTT can vary according to nature of transmission media and physical distance.

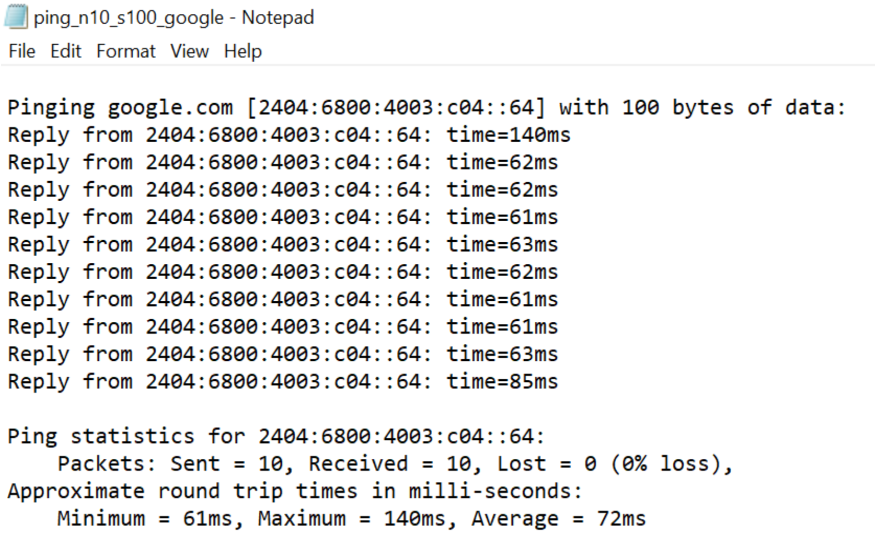
Exercise 1: Experiment with ping to find the round trip times to a variety of destinations. Write up any interesting observations, including in particular how the round trip time compares to the physical distance. Here are few places from who to get replies: www.uw.edu, www.cornell.edu, berkeley.edu, www.uchicago.edu, www.ox.ac.uk (England), www.u-tokyo.ac.jp (Japan).

64 bytes google.com



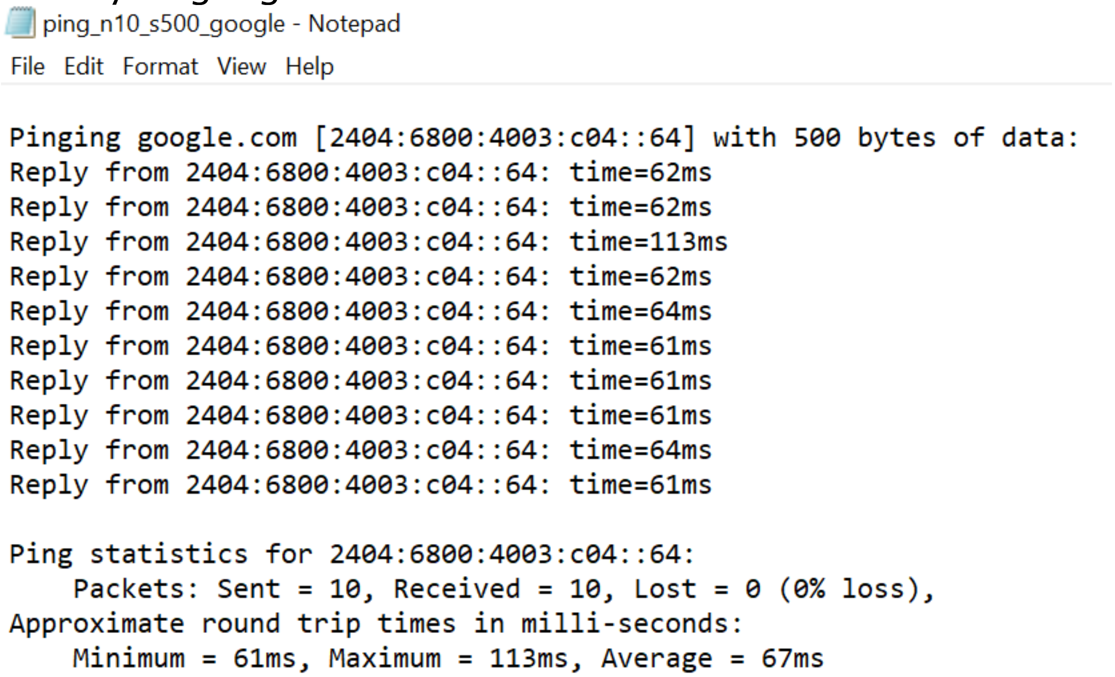
```
Pinging google.com [2404:6800:4003:c04::64] with 64 bytes of data:
Reply from 2404:6800:4003:c04::64: time=157ms
Reply from 2404:6800:4003:c04::64: time=63ms
Reply from 2404:6800:4003:c04::64: time=67ms
Reply from 2404:6800:4003:c04::64: time=126ms
Reply from 2404:6800:4003:c04::64: time=124ms
Reply from 2404:6800:4003:c04::64: time=62ms
Reply from 2404:6800:4003:c04::64: time=62ms
Reply from 2404:6800:4003:c04::64: time=63ms
Reply from 2404:6800:4003:c04::64: time=63ms
Reply from 2404:6800:4003:c04::64: time=61ms

Ping statistics for 2404:6800:4003:c04::64:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 61ms, Maximum = 157ms, Average = 84ms
```

100 bytes google.com



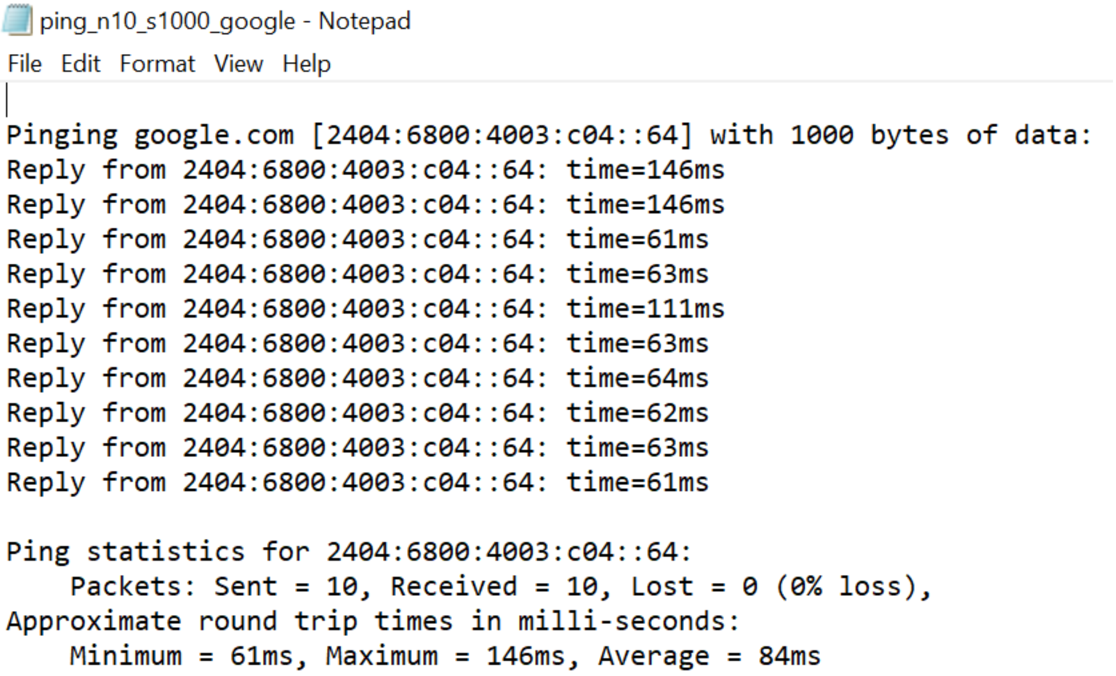
```
Pinging google.com [2404:6800:4003:c04::64] with 100 bytes of data:
Reply from 2404:6800:4003:c04::64: time=140ms
Reply from 2404:6800:4003:c04::64: time=62ms
Reply from 2404:6800:4003:c04::64: time=62ms
Reply from 2404:6800:4003:c04::64: time=61ms
Reply from 2404:6800:4003:c04::64: time=63ms
Reply from 2404:6800:4003:c04::64: time=62ms
Reply from 2404:6800:4003:c04::64: time=61ms
Reply from 2404:6800:4003:c04::64: time=61ms
Reply from 2404:6800:4003:c04::64: time=63ms
Reply from 2404:6800:4003:c04::64: time=85ms

Ping statistics for 2404:6800:4003:c04::64:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 61ms, Maximum = 140ms, Average = 72ms
```

500 bytes google.com



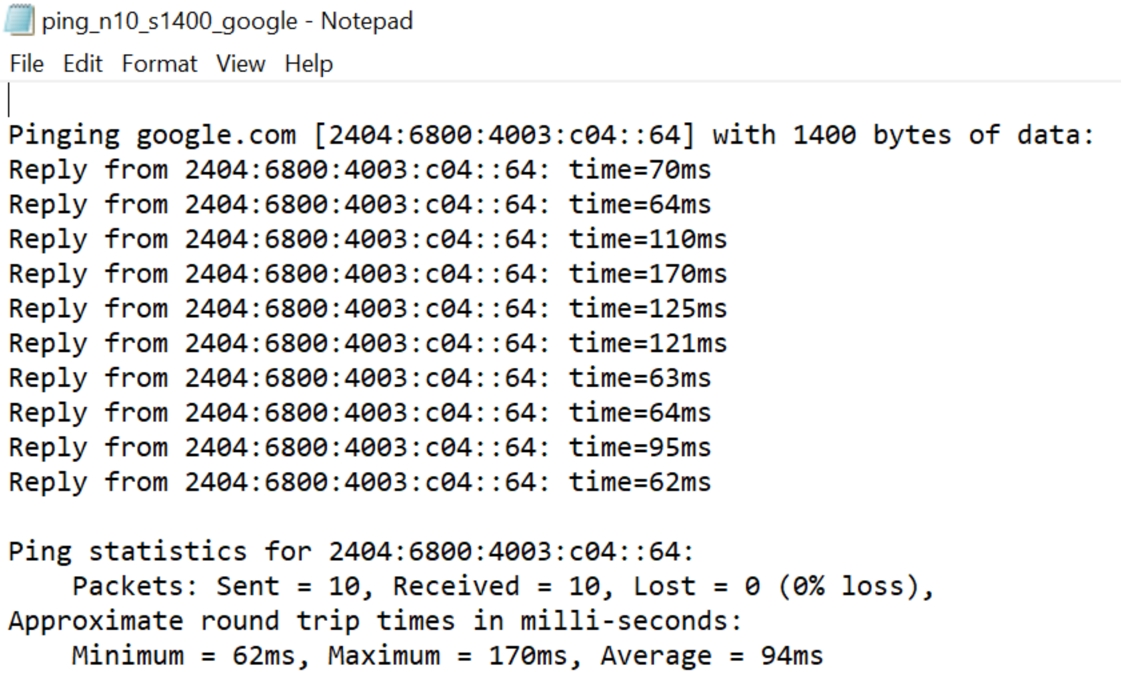
```
Pinging google.com [2404:6800:4003:c04::64] with 500 bytes of data:
Reply from 2404:6800:4003:c04::64: time=62ms
Reply from 2404:6800:4003:c04::64: time=62ms
Reply from 2404:6800:4003:c04::64: time=113ms
Reply from 2404:6800:4003:c04::64: time=62ms
Reply from 2404:6800:4003:c04::64: time=64ms
Reply from 2404:6800:4003:c04::64: time=61ms
Reply from 2404:6800:4003:c04::64: time=61ms
Reply from 2404:6800:4003:c04::64: time=61ms
Reply from 2404:6800:4003:c04::64: time=64ms
Reply from 2404:6800:4003:c04::64: time=61ms

Ping statistics for 2404:6800:4003:c04::64:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 61ms, Maximum = 113ms, Average = 67ms
```

1000 bytes google.com



```
Pinging google.com [2404:6800:4003:c04::64] with 1000 bytes of data:
Reply from 2404:6800:4003:c04::64: time=146ms
Reply from 2404:6800:4003:c04::64: time=146ms
Reply from 2404:6800:4003:c04::64: time=61ms
Reply from 2404:6800:4003:c04::64: time=63ms
Reply from 2404:6800:4003:c04::64: time=111ms
Reply from 2404:6800:4003:c04::64: time=63ms
Reply from 2404:6800:4003:c04::64: time=64ms
Reply from 2404:6800:4003:c04::64: time=62ms
Reply from 2404:6800:4003:c04::64: time=63ms
Reply from 2404:6800:4003:c04::64: time=61ms

Ping statistics for 2404:6800:4003:c04::64:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 61ms, Maximum = 146ms, Average = 84ms
```

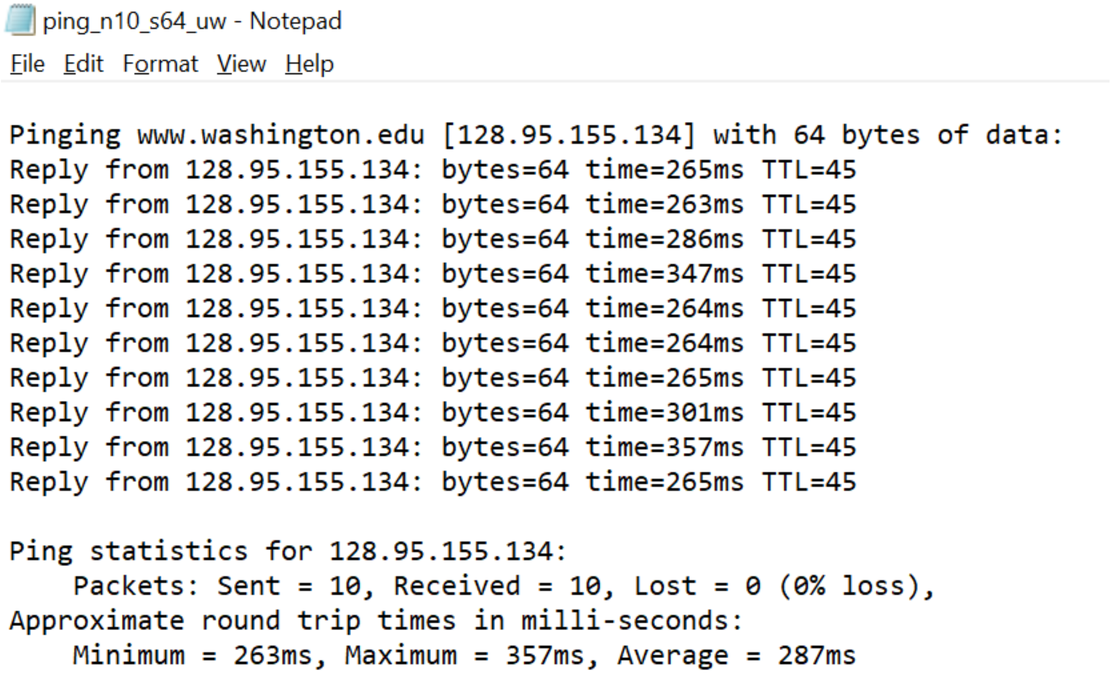
1400 bytes google.com



```
Pinging google.com [2404:6800:4003:c04::64] with 1400 bytes of data:
Reply from 2404:6800:4003:c04::64: time=70ms
Reply from 2404:6800:4003:c04::64: time=64ms
Reply from 2404:6800:4003:c04::64: time=110ms
Reply from 2404:6800:4003:c04::64: time=170ms
Reply from 2404:6800:4003:c04::64: time=125ms
Reply from 2404:6800:4003:c04::64: time=121ms
Reply from 2404:6800:4003:c04::64: time=63ms
Reply from 2404:6800:4003:c04::64: time=64ms
Reply from 2404:6800:4003:c04::64: time=95ms
Reply from 2404:6800:4003:c04::64: time=62ms

Ping statistics for 2404:6800:4003:c04::64:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 62ms, Maximum = 170ms, Average = 94ms
```

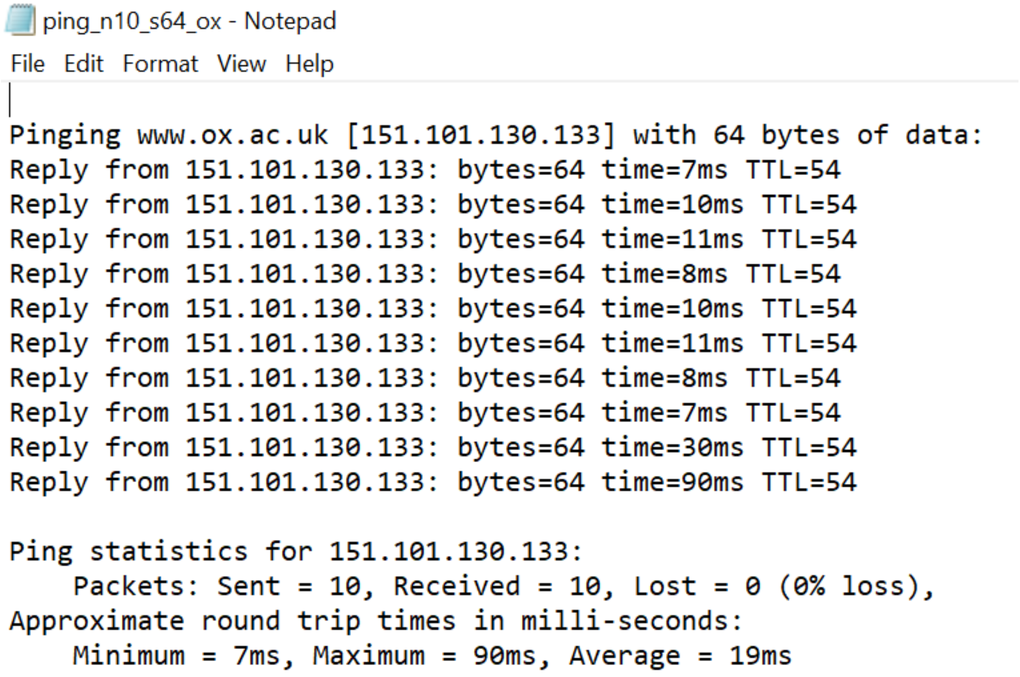
Ping to other hosts

64 bytes
www.uw.edu



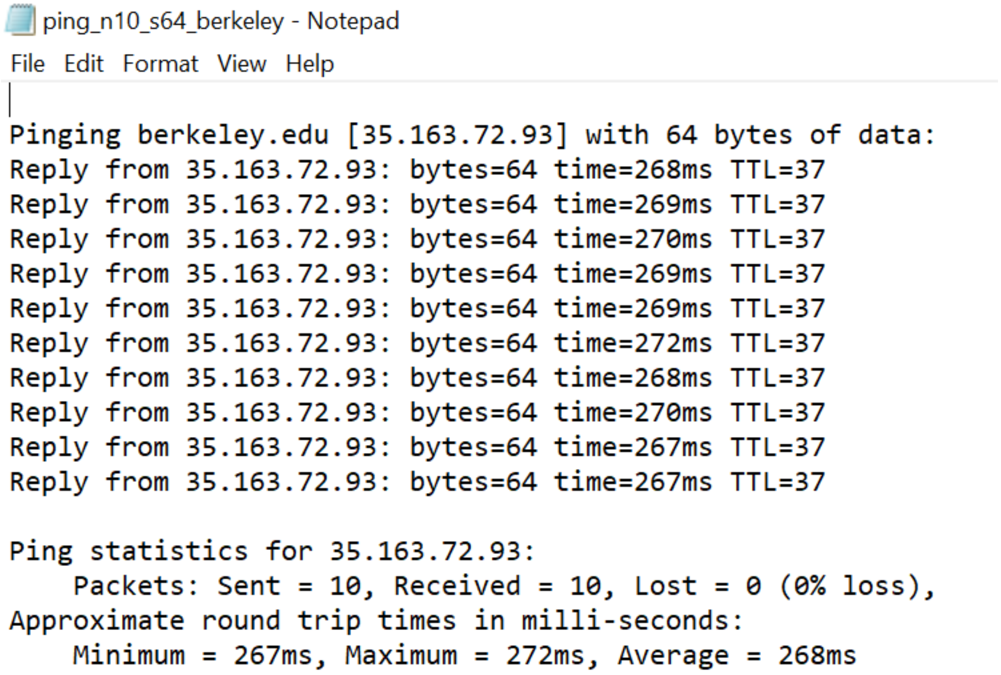
```
Pinging www.washington.edu [128.95.155.134] with 64 bytes of data:
Reply from 128.95.155.134: bytes=64 time=265ms TTL=45
Reply from 128.95.155.134: bytes=64 time=263ms TTL=45
Reply from 128.95.155.134: bytes=64 time=286ms TTL=45
Reply from 128.95.155.134: bytes=64 time=347ms TTL=45
Reply from 128.95.155.134: bytes=64 time=264ms TTL=45
Reply from 128.95.155.134: bytes=64 time=264ms TTL=45
Reply from 128.95.155.134: bytes=64 time=265ms TTL=45
Reply from 128.95.155.134: bytes=64 time=301ms TTL=45
Reply from 128.95.155.134: bytes=64 time=357ms TTL=45
Reply from 128.95.155.134: bytes=64 time=265ms TTL=45

Ping statistics for 128.95.155.134:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 263ms, Maximum = 357ms, Average = 287ms
```

64 bytes www.ox.ac.uk



```
Pinging www.ox.ac.uk [151.101.130.133] with 64 bytes of data:
Reply from 151.101.130.133: bytes=64 time=7ms TTL=54
Reply from 151.101.130.133: bytes=64 time=10ms TTL=54
Reply from 151.101.130.133: bytes=64 time=11ms TTL=54
Reply from 151.101.130.133: bytes=64 time=8ms TTL=54
Reply from 151.101.130.133: bytes=64 time=10ms TTL=54
Reply from 151.101.130.133: bytes=64 time=11ms TTL=54
Reply from 151.101.130.133: bytes=64 time=8ms TTL=54
Reply from 151.101.130.133: bytes=64 time=7ms TTL=54
Reply from 151.101.130.133: bytes=64 time=30ms TTL=54
Reply from 151.101.130.133: bytes=64 time=90ms TTL=54

Ping statistics for 151.101.130.133:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 90ms, Average = 19ms
```

64 bytes
berkeley.edu



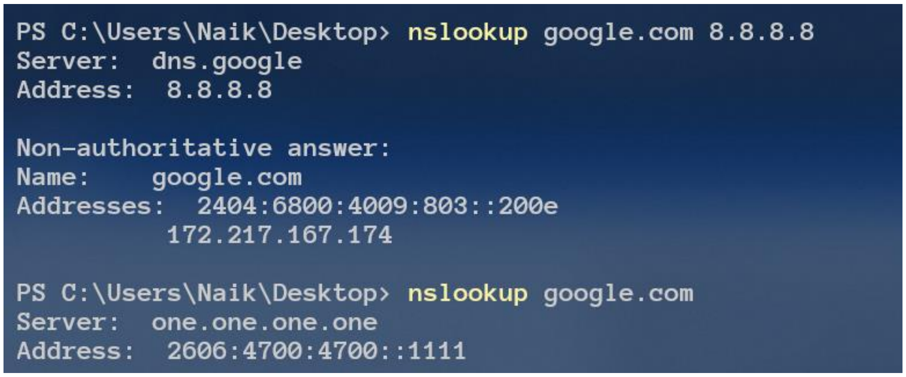
```
Pinging berkeley.edu [35.163.72.93] with 64 bytes of data:
Reply from 35.163.72.93: bytes=64 time=268ms TTL=37
Reply from 35.163.72.93: bytes=64 time=269ms TTL=37
Reply from 35.163.72.93: bytes=64 time=270ms TTL=37
Reply from 35.163.72.93: bytes=64 time=269ms TTL=37
Reply from 35.163.72.93: bytes=64 time=269ms TTL=37
Reply from 35.163.72.93: bytes=64 time=272ms TTL=37
Reply from 35.163.72.93: bytes=64 time=268ms TTL=37
Reply from 35.163.72.93: bytes=64 time=270ms TTL=37
Reply from 35.163.72.93: bytes=64 time=267ms TTL=37
Reply from 35.163.72.93: bytes=64 time=267ms TTL=37

Ping statistics for 35.163.72.93:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 267ms, Maximum = 272ms, Average = 268ms
```

Observations:

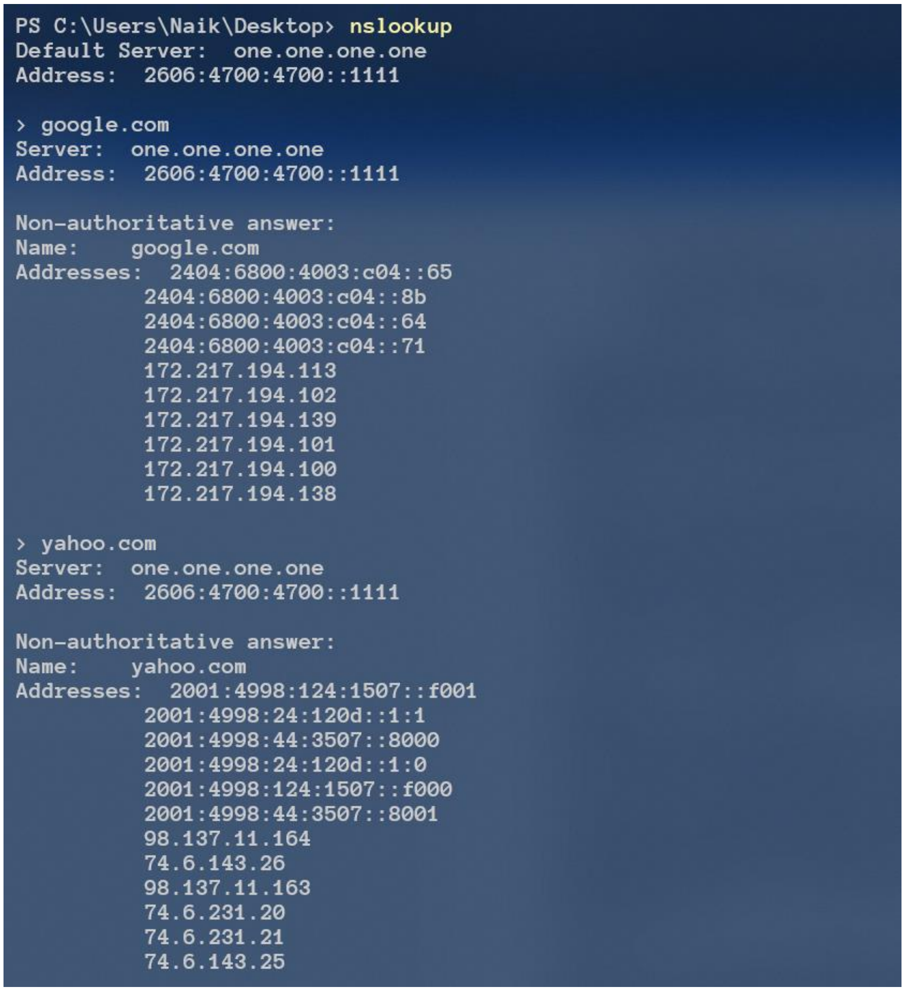
Ping time is different for differnet hosts because it depends upon physical distance

Physical distance – although a connection optimized by a CDN can often reduce the number of hops required to reach a destination, there is no way of getting around the limitation imposed by the speed of light; the distance between a start and end point is a limiting factor in network connectivity that can only be reduced by moving content closer to the requesting users. To overcome this obstacle, a CDN will cache content closer to the requesting users, thereby reducing RTT. [1]

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>

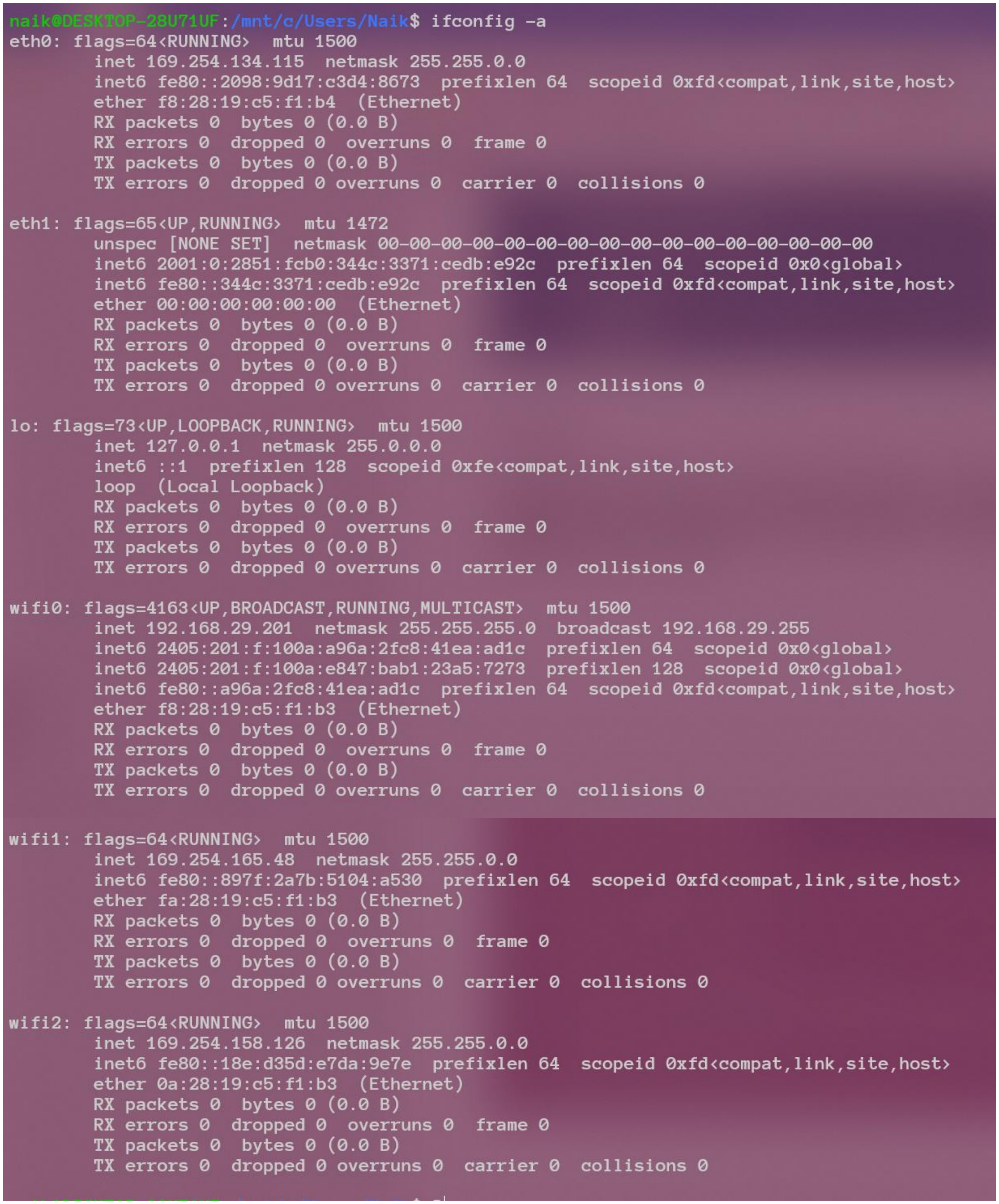


```
PS C:\Users\Naik\Desktop> nslookup google.com 8.8.8.8
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4009:803::200e
          172.217.167.174

PS C:\Users\Naik\Desktop> nslookup google.com
Server:  one.one.one.one
Address:  2606:4700:4700::1111
```



```
PS C:\Users\Naik\Desktop> nslookup
Default Server:  one.one.one.one
Address:  2606:4700:4700::1111

> google.com
Server:  one.one.one.one
Address:  2606:4700:4700::1111

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4003:c04::65
          2404:6800:4003:c04::8b
          2404:6800:4003:c04::64
          2404:6800:4003:c04::71
          172.217.194.113
          172.217.194.102
          172.217.194.139
          172.217.194.101
          172.217.194.100
          172.217.194.138

> yahoo.com
Server:  one.one.one.one
Address:  2606:4700:4700::1111

Non-authoritative answer:
Name:    yahoo.com
Addresses:  2001:4998:124:1507::f001
          2001:4998:24:120d::1:1
          2001:4998:44:3507::8000
          2001:4998:24:120d::1:0
          2001:4998:124:1507::f000
          2001:4998:44:3507::8001
          98.137.11.164
          74.6.143.26
          98.137.11.163
          74.6.231.20
          74.6.231.21
          74.6.143.25
```

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!!!.)



```
naik@DESKTOP-28U71UF:/mnt/c/Users/Naik$ ifconfig -a
eth0: flags=64<RUNNING>  mtu 1500
        inet 169.254.134.115  netmask 255.255.0.0
        inet6 fe80::2098:9d17:c3d4:8673  prefixlen 64  scopeid 0xfd<compat,link,site,host>
        ether f8:28:19:c5:f1:b4  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=65<UP,RUNNING>  mtu 1472
        unspec [NONE SET]  netmask 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
        inet6 2001:0:2851:fcb0:344c:3371:cedb:e92c  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::344c:3371:cedb:e92c  prefixlen 64  scopeid 0xfd<compat,link,site,host>
        ether 00:00:00:00:00:00  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 1500
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0xfe<compat,link,site,host>
        loop  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wifi0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.29.201  netmask 255.255.255.0  broadcast 192.168.29.255
        inet6 2405:201:f:100a:a96a:2fc8:41ea:ad1c  prefixlen 64  scopeid 0x0<global>
        inet6 2405:201:f:100a:e847:bab1:23a5:7273  prefixlen 128  scopeid 0x0<global>
        inet6 fe80::a96a:2fc8:41ea:ad1c  prefixlen 64  scopeid 0xfd<compat,link,site,host>
        ether f8:28:19:c5:f1:b3  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wifi1: flags=64<RUNNING>  mtu 1500
        inet 169.254.165.48  netmask 255.255.0.0
        inet6 fe80::897f:2a7b:5104:a530  prefixlen 64  scopeid 0xfd<compat,link,site,host>
        ether fa:28:19:c5:f1:b3  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wifi2: flags=64<RUNNING>  mtu 1500
        inet 169.254.158.126  netmask 255.255.0.0
        inet6 fe80::18e:d35d:e7da:9e7e  prefixlen 64  scopeid 0xfd<compat,link,site,host>
        ether 0a:28:19:c5:f1:b3  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

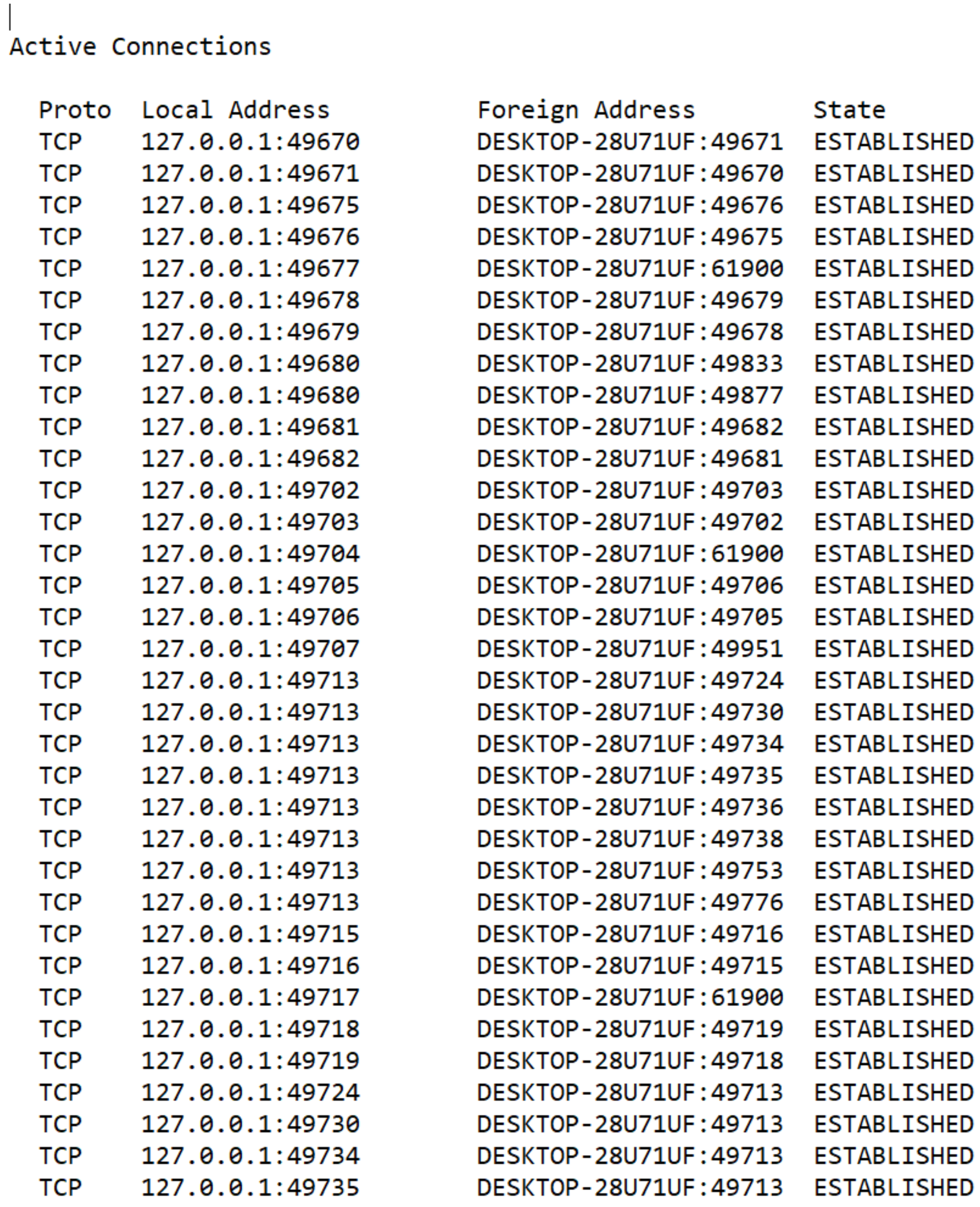
lo is a special virtual network interface called loopback device. Loopback is used mainly for diagnostics and troubleshooting, and to connect to services running on local host. [3]

inet 169.254.165.48 is ipv4 address.

inet6 is ipv6 address.

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.)

telnet — 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 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 to 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



```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49670        DESKTOP-28U71UF:49671  ESTABLISHED
  TCP    127.0.0.1:49671        DESKTOP-28U71UF:49670  ESTABLISHED
  TCP    127.0.0.1:49675        DESKTOP-28U71UF:49676  ESTABLISHED
  TCP    127.0.0.1:49676        DESKTOP-28U71UF:49675  ESTABLISHED
  TCP    127.0.0.1:49677        DESKTOP-28U71UF:61900  ESTABLISHED
  TCP    127.0.0.1:49678        DESKTOP-28U71UF:49679  ESTABLISHED
  TCP    127.0.0.1:49679        DESKTOP-28U71UF:49678  ESTABLISHED
  TCP    127.0.0.1:49680        DESKTOP-28U71UF:49833  ESTABLISHED
  TCP    127.0.0.1:49680        DESKTOP-28U71UF:49877  ESTABLISHED
  TCP    127.0.0.1:49681        DESKTOP-28U71UF:49682  ESTABLISHED
  TCP    127.0.0.1:49682        DESKTOP-28U71UF:49681  ESTABLISHED
  TCP    127.0.0.1:49702        DESKTOP-28U71UF:49703  ESTABLISHED
  TCP    127.0.0.1:49703        DESKTOP-28U71UF:49702  ESTABLISHED
  TCP    127.0.0.1:49704        DESKTOP-28U71UF:61900  ESTABLISHED
  TCP    127.0.0.1:49705        DESKTOP-28U71UF:49706  ESTABLISHED
  TCP    127.0.0.1:49706        DESKTOP-28U71UF:49705  ESTABLISHED
  TCP    127.0.0.1:49707        DESKTOP-28U71UF:49951  ESTABLISHED
  TCP    127.0.0.1:49713        DESKTOP-28U71UF:49724  ESTABLISHED
  TCP    127.0.0.1:49713        DESKTOP-28U71UF:49730  ESTABLISHED
  TCP    127.0.0.1:49713        DESKTOP-28U71UF:49734  ESTABLISHED
  TCP    127.0.0.1:49713        DESKTOP-28U71UF:49735  ESTABLISHED
  TCP    127.0.0.1:49713        DESKTOP-28U71UF:49736  ESTABLISHED
  TCP    127.0.0.1:49713        DESKTOP-28U71UF:49738  ESTABLISHED
  TCP    127.0.0.1:49713        DESKTOP-28U71UF:49753  ESTABLISHED
  TCP    127.0.0.1:49713        DESKTOP-28U71UF:49776  ESTABLISHED
  TCP    127.0.0.1:49715        DESKTOP-28U71UF:49716  ESTABLISHED
  TCP    127.0.0.1:49716        DESKTOP-28U71UF:49715  ESTABLISHED
  TCP    127.0.0.1:49717        DESKTOP-28U71UF:61900  ESTABLISHED
  TCP    127.0.0.1:49718        DESKTOP-28U71UF:49719  ESTABLISHED
  TCP    127.0.0.1:49719        DESKTOP-28U71UF:49718  ESTABLISHED
  TCP    127.0.0.1:49724        DESKTOP-28U71UF:49713  ESTABLISHED
  TCP    127.0.0.1:49730        DESKTOP-28U71UF:49713  ESTABLISHED
  TCP    127.0.0.1:49734        DESKTOP-28U71UF:49713  ESTABLISHED
  TCP    127.0.0.1:49735        DESKTOP-28U71UF:49713  ESTABLISHED
```

traceroute — Traceroute is discussed in man utility. The command traceroute <host> will show routers encountered by packets on their way from your computer to a specified <host>. For each n = 1, 2, 3,..., traceroute sends a packet with "time-to-live" (ttl) equal to n. Every time a router forwards a packet, it decreases the ttl of the packet by one. If the ttl drops to zero, the router discards the packet and sends an error message back to the sender of the packet. (Again, as with ping, the packets might be blocked or might not even be sent, so that the error messages will never be received.) The sender gets the identity of the router from the source of the error message. Traceroute will send packets until n reaches some set upper bound or until a packet actually gets through to the destination. It actually does this three times for each n. In this way, it identifies routers that are one step, two steps, three steps, ... away from the source computer. A packet for which no response is received is indicated in the output as a *.

Traceroute is installed on the computers. If was not installed in your virtual server last week, but you can install it with the command sudo apt-get install traceroute

The path taken through a network, can be measured using `traceroute`. The syntax for the command in Linux is:

```
traceroute <hostname>
```

The syntax in Windows is:

```
tracert <hostname>
```

You can specify either a hostname (e.g., `cs.iitb.ac.in`) or an IP address (e.g., `128.105.2.6`).

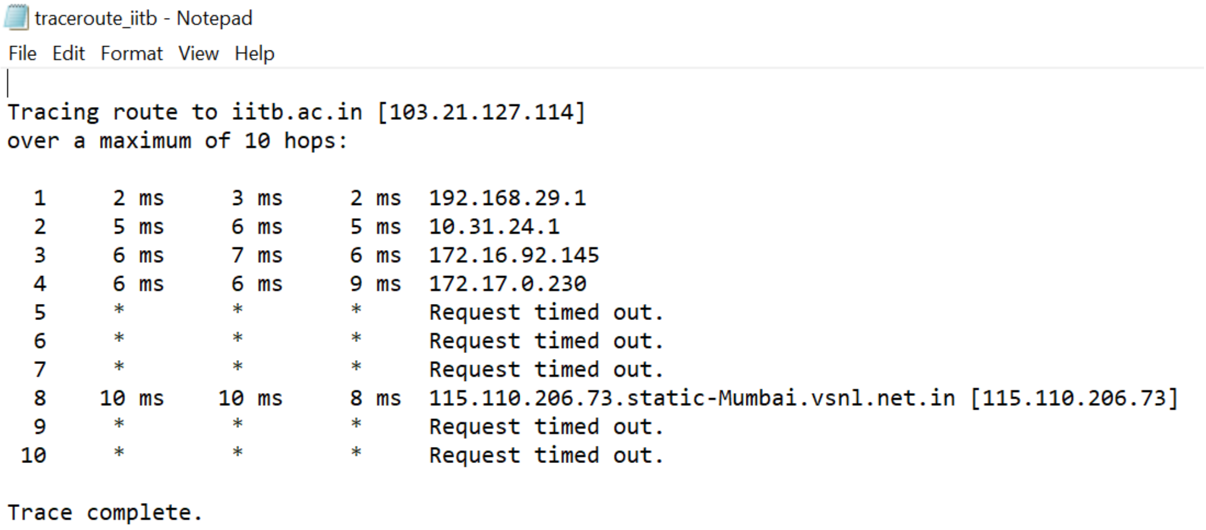
1.2.1 Experiments with Traceroute

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

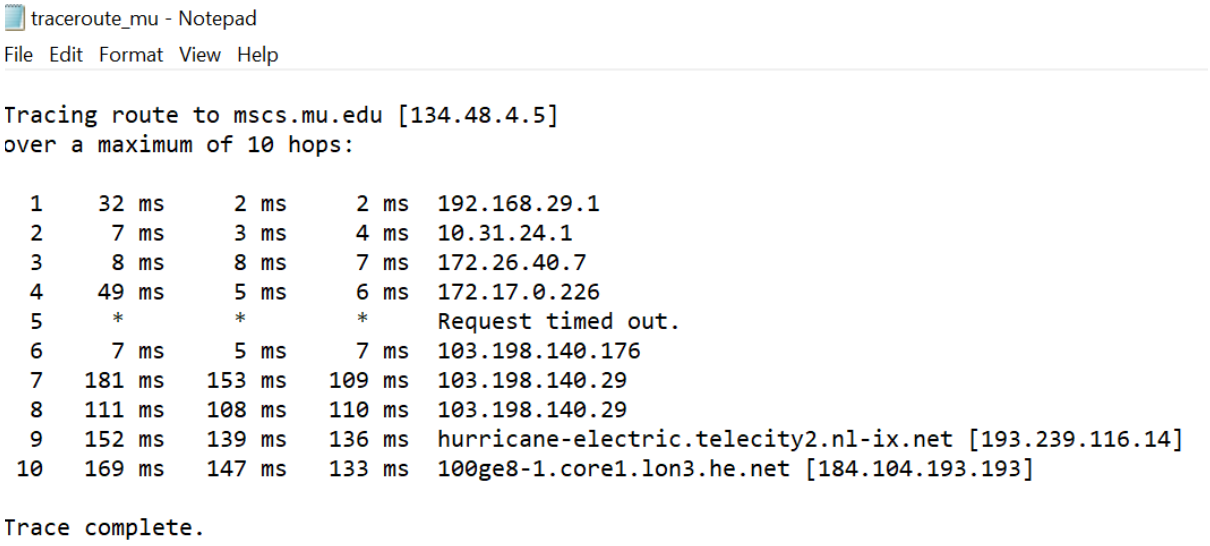
Store the output of each traceroute command in a separate file named `traceroute_HOSTNAME.log`, replacing `HOSTNAME` with the hostname for end-host you pinged
(e.g., `traceroute_ee.iitb.ac.in.log`).

1. iitb



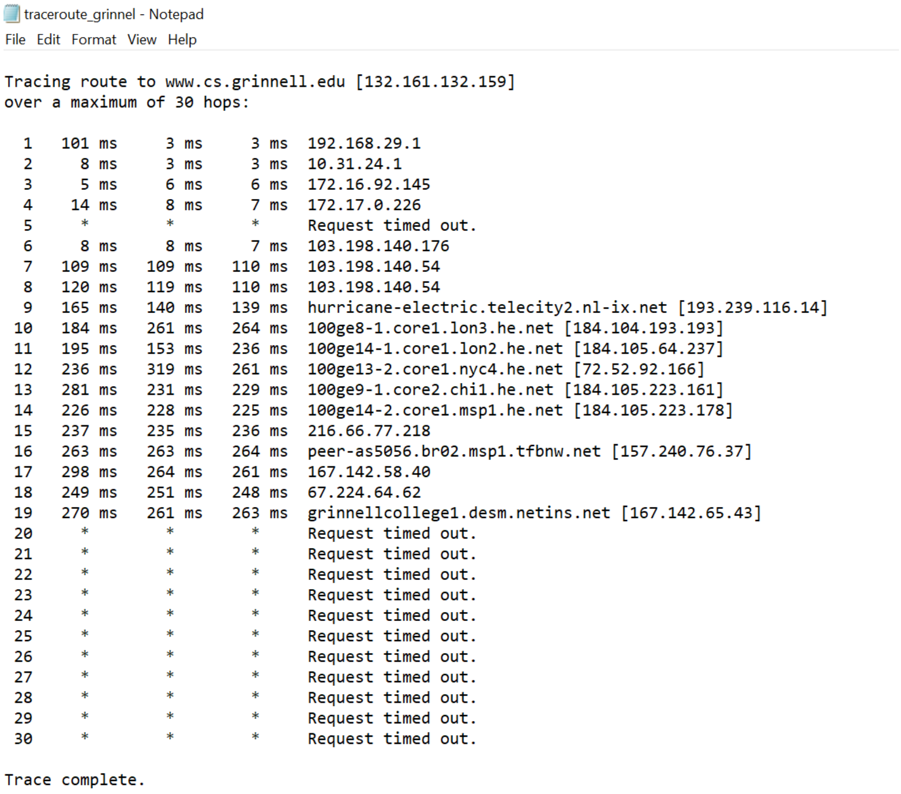
```
Tracing route to iitb.ac.in [103.21.127.114]
over a maximum of 10 hops:

  1     2 ms     3 ms     2 ms  192.168.29.1
  2     5 ms     6 ms     5 ms  10.31.24.1
  3     6 ms     7 ms     6 ms  172.16.92.145
  4     6 ms     6 ms     9 ms  172.17.0.230
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8    10 ms    10 ms     8 ms  115.110.206.73.static-Mumbai.vsnl.net.in [115.110.206.73]
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.

Trace complete.
```

2. mscs.mu.edu



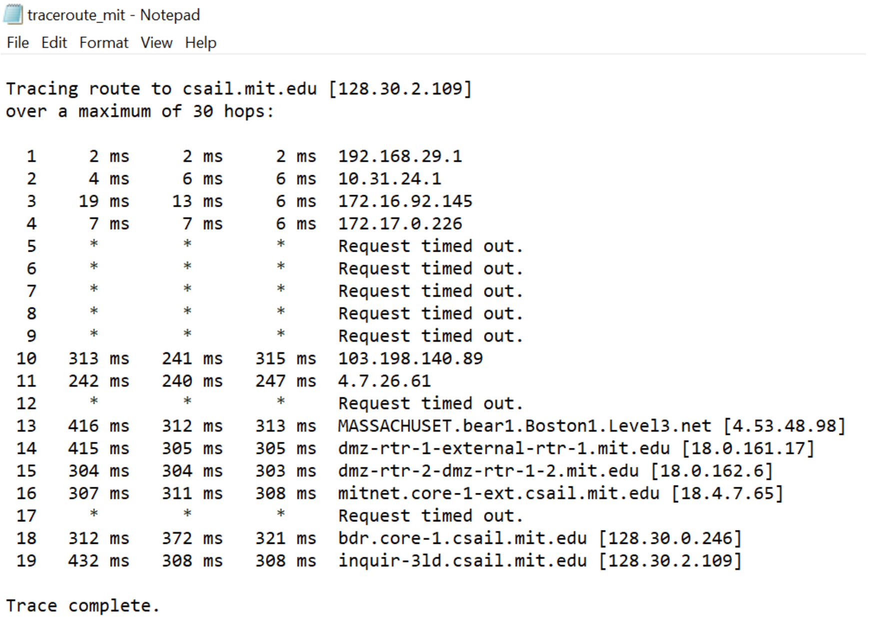
```
Tracing route to mscs.mu.edu [134.48.4.5]
over a maximum of 10 hops:

  1    32 ms     2 ms     2 ms  192.168.29.1
  2     7 ms     3 ms     4 ms  10.31.24.1
  3     8 ms     8 ms     7 ms  172.26.40.7
  4    49 ms     5 ms     6 ms  172.17.0.226
  5     *        *        *     Request timed out.
  6     7 ms     5 ms     7 ms  103.198.140.176
  7   181 ms   153 ms   109 ms  103.198.140.29
  8   111 ms   108 ms   110 ms  103.198.140.29
  9   152 ms   139 ms   136 ms  hurricane-electric.telecity2.nl-ix.net [193.239.116.14]
 10   169 ms   147 ms   133 ms  100ge8-1.core1.lon3.he.net [184.104.193.193]

Trace complete.
```

3. www.cs.grinnell.edu



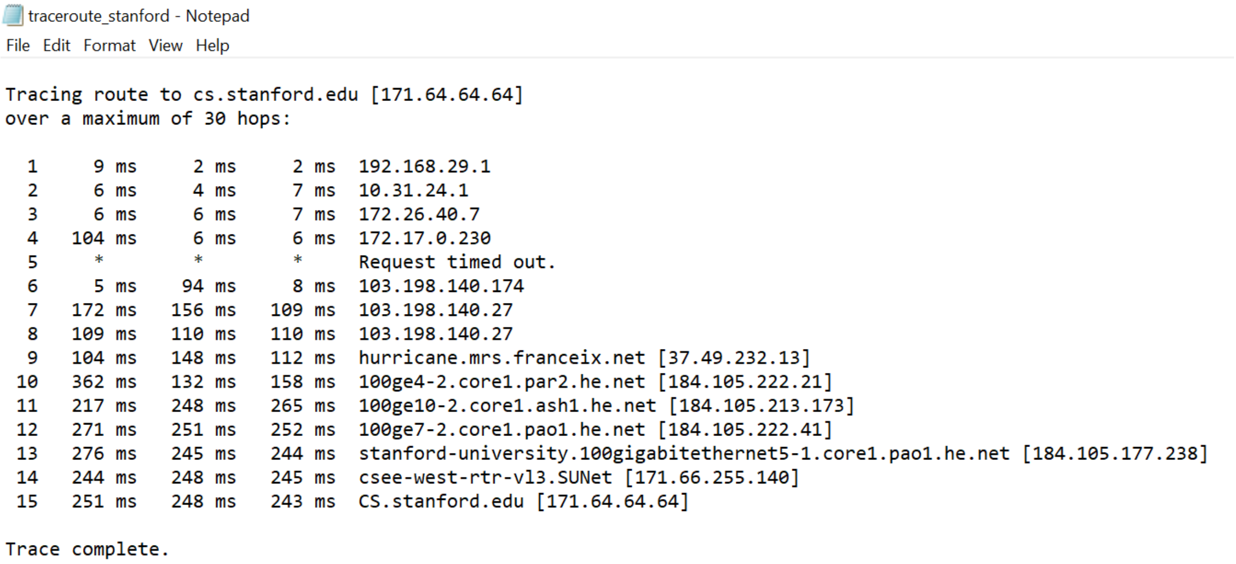
```
Tracing route to www.cs.grinnell.edu [132.161.132.159]
over a maximum of 30 hops:

  1   101 ms     3 ms     3 ms  192.168.29.1
  2     8 ms     3 ms     3 ms  10.31.24.1
  3     5 ms     6 ms     6 ms  172.16.92.145
  4    14 ms     8 ms     7 ms  172.17.0.226
  5     *        *        *     Request timed out.
  6     8 ms     8 ms     7 ms  103.198.140.176
  7   109 ms   109 ms   110 ms  103.198.140.54
  8   120 ms   119 ms   110 ms  103.198.140.54
  9   165 ms   140 ms   139 ms  hurricane-electric.telecity2.nl-ix.net [193.239.116.14]
 10   184 ms   261 ms   264 ms  100ge8-1.core1.lon3.he.net [184.104.193.193]
 11   195 ms   153 ms   236 ms  100ge14-1.core1.lon2.he.net [184.105.64.237]
 12   236 ms   319 ms   261 ms  100ge13-2.core1.nyc4.he.net [72.52.92.166]
 13   281 ms   231 ms   229 ms  100ge9-1.core2.chi1.he.net [184.105.223.161]
 14   226 ms   228 ms   225 ms  100ge14-2.core1.msp1.he.net [184.105.223.178]
 15   237 ms   235 ms   236 ms  216.66.77.218
 16   263 ms   263 ms   264 ms  peer-as5056.br02.msp1.tfbnw.net [157.240.76.37]
 17   298 ms   264 ms   261 ms  167.142.58.40
 18   249 ms   251 ms   248 ms  67.224.64.62
 19   270 ms   261 ms   263 ms  grinnellcollege1.desm.netins.net [167.142.65.43]
 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.
```

4. csail.mit.edu



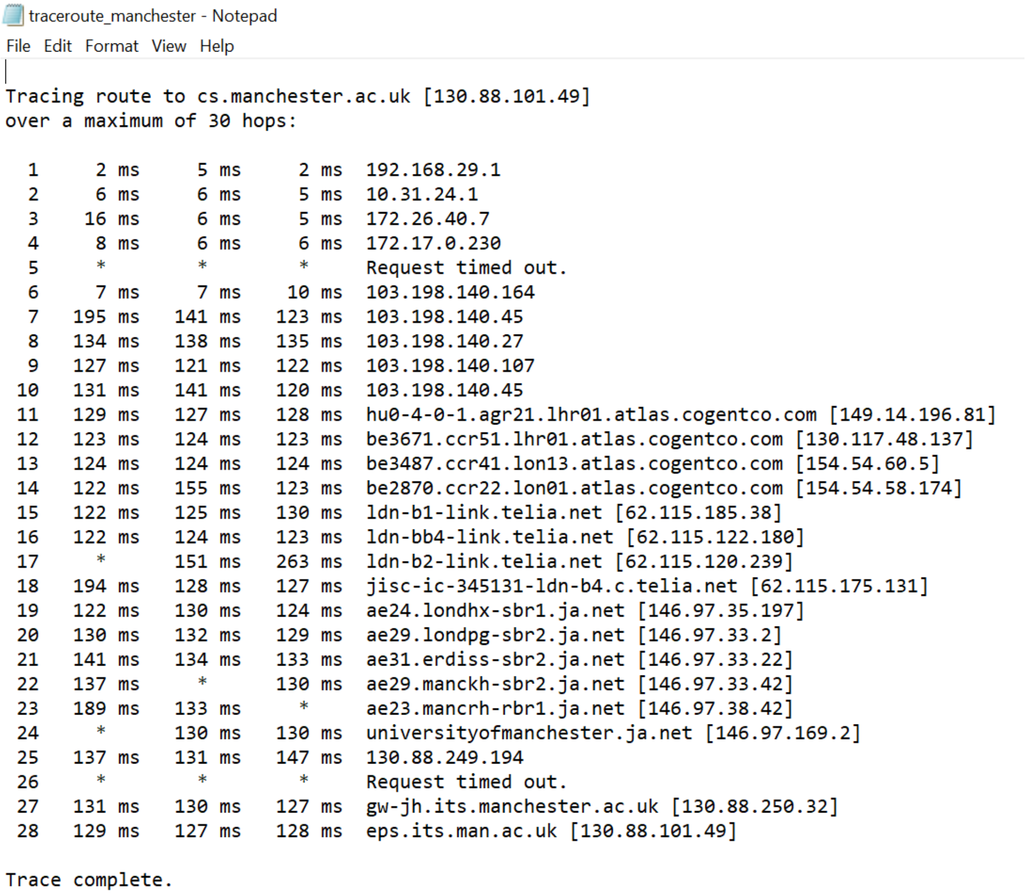
```
Tracing route to csail.mit.edu [128.30.2.109]
over a maximum of 30 hops:

  1     2 ms     2 ms     2 ms  192.168.29.1
  2     4 ms     6 ms     6 ms  10.31.24.1
  3    19 ms    13 ms     6 ms  172.16.92.145
  4     7 ms     7 ms     6 ms  172.17.0.226
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10   313 ms   241 ms   315 ms  103.198.140.89
 11   242 ms   240 ms   247 ms  4.7.26.61
 12     *        *        *     Request timed out.
 13   416 ms   312 ms   313 ms  MASSACHUSET.bear1.Boston1.Level3.net [4.53.48.98]
 14   415 ms   305 ms   305 ms  dmz-rtr-1-external-rtr-1.mit.edu [18.0.161.17]
 15   304 ms   304 ms   303 ms  dmz-rtr-2-dmz-rtr-1-2.mit.edu [18.0.162.6]
 16   307 ms   311 ms   308 ms  mitnet.core-1-ext.csail.mit.edu [18.4.7.65]
 17     *        *        *     Request timed out.
 18   312 ms   372 ms   321 ms  bdr.core-1.csail.mit.edu [128.30.0.246]
 19   432 ms   308 ms   308 ms  inquir-3ld.csail.mit.edu [128.30.2.109]

Trace complete.
```

5. cs.stanford.edu



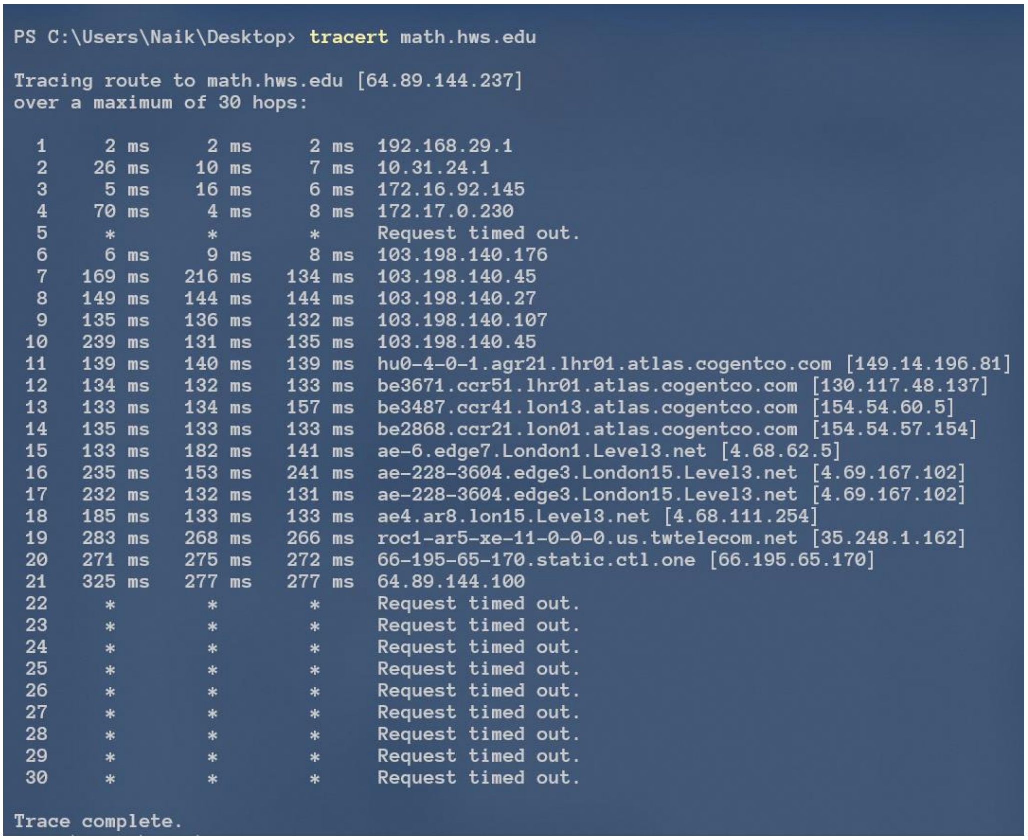
```
Tracing route to cs.stanford.edu [171.64.64.64]
over a maximum of 30 hops:

  1     9 ms     2 ms     2 ms  192.168.29.1
  2     6 ms     4 ms     7 ms  10.31.24.1
  3     6 ms     6 ms     7 ms  172.26.40.7
  4   104 ms     6 ms     6 ms  172.17.0.230
  5     *        *        *     Request timed out.
  6     5 ms    94 ms     8 ms  103.198.140.174
  7   172 ms   156 ms   109 ms  103.198.140.27
  8   109 ms   110 ms   110 ms  103.198.140.27
  9   104 ms   148 ms   112 ms  hurricane.mrs.franceix.net [37.49.232.13]
 10   362 ms   132 ms   158 ms  100ge4-2.core1.par2.he.net [184.105.222.21]
 11   217 ms   248 ms   265 ms  100ge10-2.core1.ash1.he.net [184.105.213.173]
 12   271 ms   251 ms   252 ms  100ge7-2.core1.pao1.he.net [184.105.222.41]
 13   276 ms   245 ms   244 ms  stanford-university.100gigabitethernet5-1.core1.pao1.he.net [184.105.177.238]
 14   244 ms   248 ms   245 ms  csee-west-rtr-vl3.SUNet [171.66.255.140]
 15   251 ms   248 ms   243 ms  CS.stanford.edu [171.64.64.64]

Trace complete.
```

6. cs.manchester.ac.uk

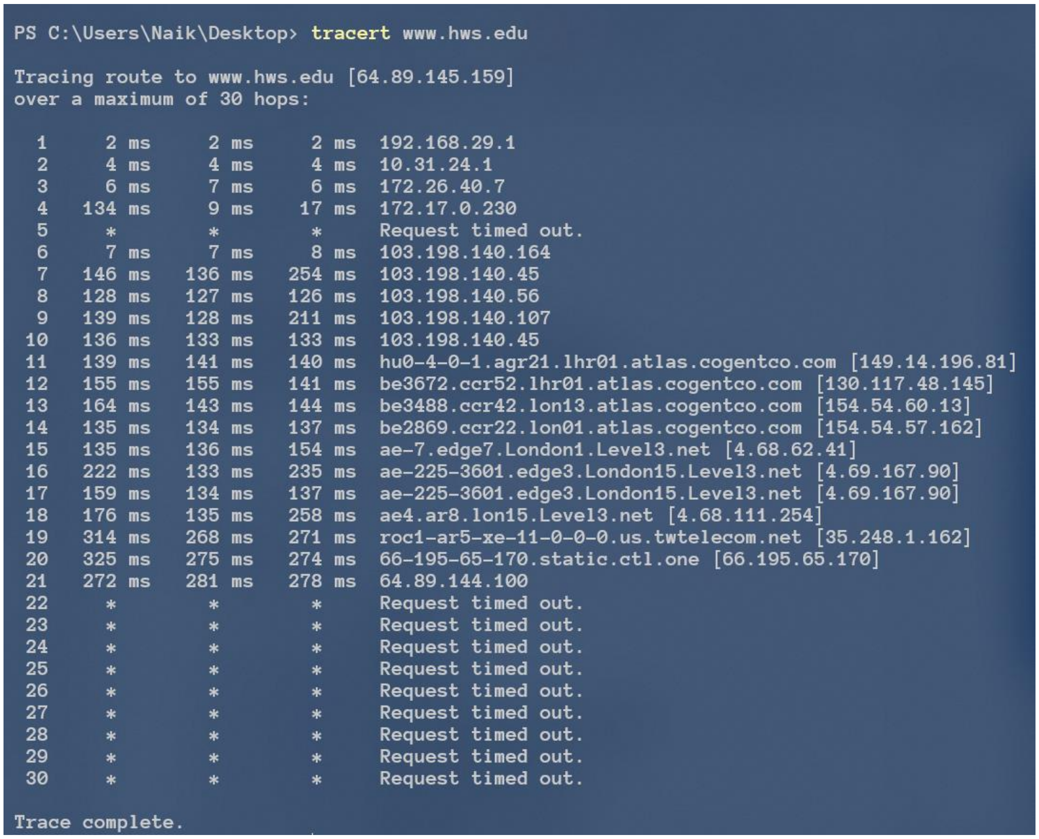


```
Tracing route to cs.manchester.ac.uk [130.88.101.49]
over a maximum of 30 hops:

  1     2 ms     5 ms     2 ms  192.168.29.1
  2     6 ms     6 ms     5 ms  10.31.24.1
  3    16 ms     6 ms     5 ms  172.26.40.7
  4     8 ms     6 ms     6 ms  172.17.0.230
  5     *        *        *     Request timed out.
  6     7 ms     7 ms    10 ms  103.198.140.164
  7   195 ms   141 ms   123 ms  103.198.140.45
  8   134 ms   138 ms   135 ms  103.198.140.27
  9   127 ms   121 ms   122 ms  103.198.140.107
 10   131 ms   141 ms   120 ms  103.198.140.45
 11   129 ms   127 ms   128 ms  hu0-4-0-1.agr21.lhr01.atlas.cogentco.com [149.14.196.81]
 12   123 ms   124 ms   123 ms  be3671.ccr51.lhr01.atlas.cogentco.com [130.117.48.137]
 13   124 ms   124 ms   124 ms  be3487.ccr41.lon13.atlas.cogentco.com [154.54.60.5]
 14   122 ms   155 ms   123 ms  be2870.ccr22.lon01.atlas.cogentco.com [154.54.58.174]
 15   122 ms   125 ms   130 ms  ldn-b1-link.telia.net [62.115.185.38]
 16   122 ms   124 ms   123 ms  ldn-bb4-link.telia.net [62.115.122.180]
 17     *      151 ms   263 ms  ldn-b2-link.telia.net [62.115.120.239]
 18   194 ms   128 ms   127 ms  jisc-ic-345131-ldn-b4.c.telia.net [62.115.175.131]
 19   122 ms   130 ms   124 ms  ae24.londhx-sbr1.ja.net [146.97.35.197]
 20   130 ms   132 ms   129 ms  ae29.londpg-sbr2.ja.net [146.97.33.2]
 21   141 ms   134 ms   133 ms  ae31.erdiss-sbr2.ja.net [146.97.33.22]
 22   137 ms     *      130 ms  ae29.manckh-sbr2.ja.net [146.97.33.42]
 23   189 ms   133 ms     *     ae23.mancrh-rbr1.ja.net [146.97.38.42]
 24     *      130 ms   130 ms  universityofmanchester.ja.net [146.97.169.2]
 25   137 ms   131 ms   147 ms  130.88.249.194
 26     *        *        *     Request timed out.
 27   131 ms   130 ms   127 ms  gw-jh.its.manchester.ac.uk [130.88.250.32]
 28   129 ms   127 ms   128 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.



```
PS C:\Users\Naik\Desktop> tracert math.hws.edu

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

  1     2 ms     2 ms     2 ms  192.168.29.1
  2    26 ms    10 ms     7 ms  10.31.24.1
  3     5 ms    16 ms     6 ms  172.16.92.145
  4    70 ms     4 ms     8 ms  172.17.0.230
  5     *        *        *     Request timed out.
  6     6 ms     9 ms     8 ms  103.198.140.176
  7   169 ms   216 ms   134 ms  103.198.140.45
  8   149 ms   144 ms   144 ms  103.198.140.27
  9   135 ms   136 ms   132 ms  103.198.140.107
 10   239 ms   131 ms   135 ms  103.198.140.45
 11   139 ms   140 ms   139 ms  hu0-4-0-1.agr21.lhr01.atlas.cogentco.com [149.14.196.81]
 12   134 ms   132 ms   133 ms  be3671.ccr51.lhr01.atlas.cogentco.com [130.117.48.137]
 13   133 ms   134 ms   157 ms  be3487.ccr41.lon13.atlas.cogentco.com [154.54.60.5]
 14   135 ms   133 ms   133 ms  be2868.ccr21.lon01.atlas.cogentco.com [154.54.57.154]
 15   133 ms   182 ms   141 ms  ae-6.edge7.London1.Level3.net [4.68.62.5]
 16   235 ms   153 ms   241 ms  ae-228-3604.edge3.London15.Level3.net [4.69.167.102]
 17   232 ms   132 ms   131 ms  ae-228-3604.edge3.London15.Level3.net [4.69.167.102]
 18   185 ms   133 ms   133 ms  ae4.ar8.lon15.Level3.net [4.68.111.254]
 19   283 ms   268 ms   266 ms  roc1-ar5-xe-11-0-0-0.us.twtelecom.net [35.248.1.162]
 20   271 ms   275 ms   272 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 21   325 ms   277 ms   277 ms  64.89.144.100
 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.
```

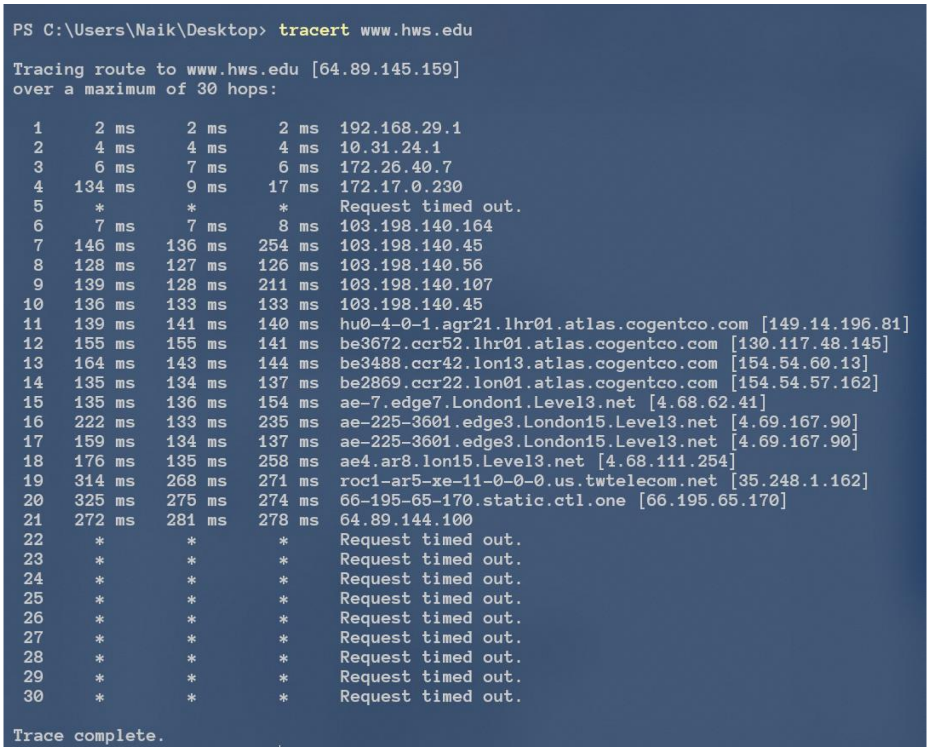


```
PS C:\Users\Naik\Desktop> tracert www.hws.edu

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

  1     2 ms     2 ms     2 ms  192.168.29.1
  2     4 ms     4 ms     4 ms  10.31.24.1
  3     6 ms     7 ms     6 ms  172.26.40.7
  4   134 ms     9 ms    17 ms  172.17.0.230
  5     *        *        *     Request timed out.
  6     7 ms     7 ms     8 ms  103.198.140.164
  7   146 ms   136 ms   254 ms  103.198.140.45
  8   128 ms   127 ms   126 ms  103.198.140.56
  9   139 ms   128 ms   211 ms  103.198.140.107
 10   136 ms   133 ms   133 ms  103.198.140.45
 11   139 ms   141 ms   140 ms  hu0-4-0-1.agr21.lhr01.atlas.cogentco.com [149.14.196.81]
 12   155 ms   155 ms   141 ms  be3672.ccr52.lhr01.atlas.cogentco.com [130.117.48.145]
 13   164 ms   143 ms   144 ms  be3488.ccr42.lon13.atlas.cogentco.com [154.54.60.13]
 14   135 ms   134 ms   137 ms  be2869.ccr22.lon01.atlas.cogentco.com [154.54.57.162]
 15   135 ms   136 ms   154 ms  ae-7.edge7.London1.Level3.net [4.68.62.41]
 16   222 ms   133 ms   235 ms  ae-225-3601.edge3.London15.Level3.net [4.69.167.90]
 17   159 ms   134 ms   137 ms  ae-225-3601.edge3.London15.Level3.net [4.69.167.90]
 18   176 ms   135 ms   258 ms  ae4.ar8.lon15.Level3.net [4.68.111.254]
 19   314 ms   268 ms   271 ms  roc1-ar5-xe-11-0-0-0.us.twtelecom.net [35.248.1.162]
 20   325 ms   275 ms   274 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 21   272 ms   281 ms   278 ms  64.89.144.100
 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.
```

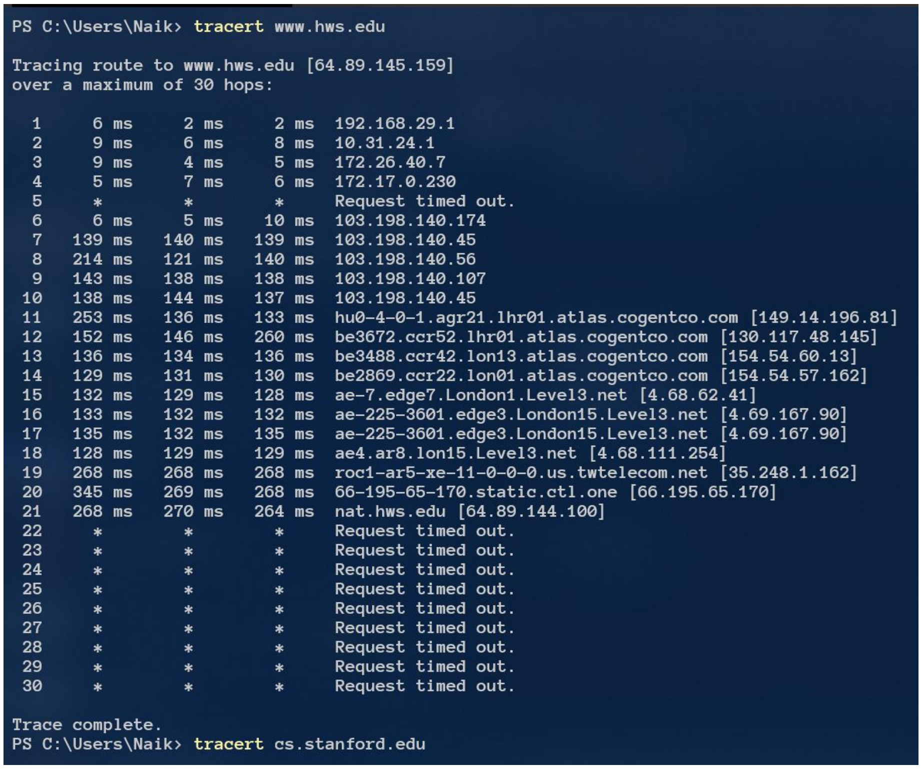
Observations:

Traceroute to math.hws.edu and to www.hws.edu both followed the same path (i.e the network address of the ip addresses were the same) till hop no. 21 following which all hops have status request timed out. However, the host addresses are different.

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.



```
PS C:\Users\Naik\Desktop> tracert www.hws.edu

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

  1     2 ms     2 ms     2 ms  192.168.29.1
  2     4 ms     4 ms     4 ms  10.31.24.1
  3     6 ms     7 ms     6 ms  172.26.40.7
  4   134 ms     9 ms    17 ms  172.17.0.230
  5     *        *        *     Request timed out.
  6     7 ms     7 ms     8 ms  103.198.140.164
  7   146 ms   136 ms   254 ms  103.198.140.45
  8   128 ms   127 ms   126 ms  103.198.140.56
  9   139 ms   128 ms   211 ms  103.198.140.107
 10   136 ms   133 ms   133 ms  103.198.140.45
 11   139 ms   141 ms   140 ms  hu0-4-0-1.agr21.lhr01.atlas.cogentco.com [149.14.196.81]
 12   155 ms   155 ms   141 ms  be3672.ccr52.lhr01.atlas.cogentco.com [130.117.48.145]
 13   164 ms   143 ms   144 ms  be3488.ccr42.lon13.atlas.cogentco.com [154.54.60.13]
 14   135 ms   134 ms   137 ms  be2869.ccr22.lon01.atlas.cogentco.com [154.54.57.162]
 15   135 ms   136 ms   154 ms  ae-7.edge7.London1.Level3.net [4.68.62.41]
 16   222 ms   133 ms   235 ms  ae-225-3601.edge3.London15.Level3.net [4.69.167.90]
 17   159 ms   134 ms   137 ms  ae-225-3601.edge3.London15.Level3.net [4.69.167.90]
 18   176 ms   135 ms   258 ms  ae4.ar8.lon15.Level3.net [4.68.111.254]
 19   314 ms   268 ms   271 ms  roc1-ar5-xe-11-0-0-0.us.twtelecom.net [35.248.1.162]
 20   325 ms   275 ms   274 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 21   272 ms   281 ms   278 ms  64.89.144.100
 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.
```



```
PS C:\Users\Naik> tracert www.hws.edu

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

  1     6 ms     2 ms     2 ms  192.168.29.1
  2     9 ms     6 ms     8 ms  10.31.24.1
  3     9 ms     4 ms     5 ms  172.26.40.7
  4     5 ms     7 ms     6 ms  172.17.0.230
  5     *        *        *     Request timed out.
  6     6 ms     5 ms    10 ms  103.198.140.174
  7   139 ms   140 ms   139 ms  103.198.140.45
  8   214 ms   121 ms   140 ms  103.198.140.56
  9   143 ms   138 ms   138 ms  103.198.140.107
 10   138 ms   144 ms   137 ms  103.198.140.45
 11   253 ms   136 ms   133 ms  hu0-4-0-1.agr21.lhr01.atlas.cogentco.com [149.14.196.81]
 12   152 ms   146 ms   260 ms  be3672.ccr52.lhr01.atlas.cogentco.com [130.117.48.145]
 13   136 ms   134 ms   136 ms  be3488.ccr42.lon13.atlas.cogentco.com [154.54.60.13]
 14   129 ms   131 ms   130 ms  be2869.ccr22.lon01.atlas.cogentco.com [154.54.57.162]
 15   132 ms   129 ms   128 ms  ae-7.edge7.London1.Level3.net [4.68.62.41]
 16   133 ms   132 ms   132 ms  ae-225-3601.edge3.London15.Level3.net [4.69.167.90]
 17   135 ms   132 ms   135 ms  ae-225-3601.edge3.London15.Level3.net [4.69.167.90]
 18   128 ms   129 ms   129 ms  ae4.ar8.lon15.Level3.net [4.68.111.254]
 19   268 ms   268 ms   268 ms  roc1-ar5-xe-11-0-0-0.us.twtelecom.net [35.248.1.162]
 20   345 ms   269 ms   268 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 21   268 ms   270 ms   264 ms  nat.hws.edu [64.89.144.100]
 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.
PS C:\Users\Naik> tracert cs.stanford.edu
```

Observations:

There was no change but it is not necessary. The path and RTT could be different for the same destinantions. The packet could be passed through different intermediate nodes. However, the source and destination would always be the same.

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`.

- **Is any part of the path common for all hosts you tracerouted?**

  The initial few hops are same across all traceroute commands regardless of destination address. The paths start diverging after the 5th hop. The first hop address is the home address and the second one is the ISP address.

- **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?**

  Usually, the farther the geographical distance more the hops are required for the trace to be complete. So, it is directly proportional. This is because the packet has to pass through multiple routers.

- **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?**

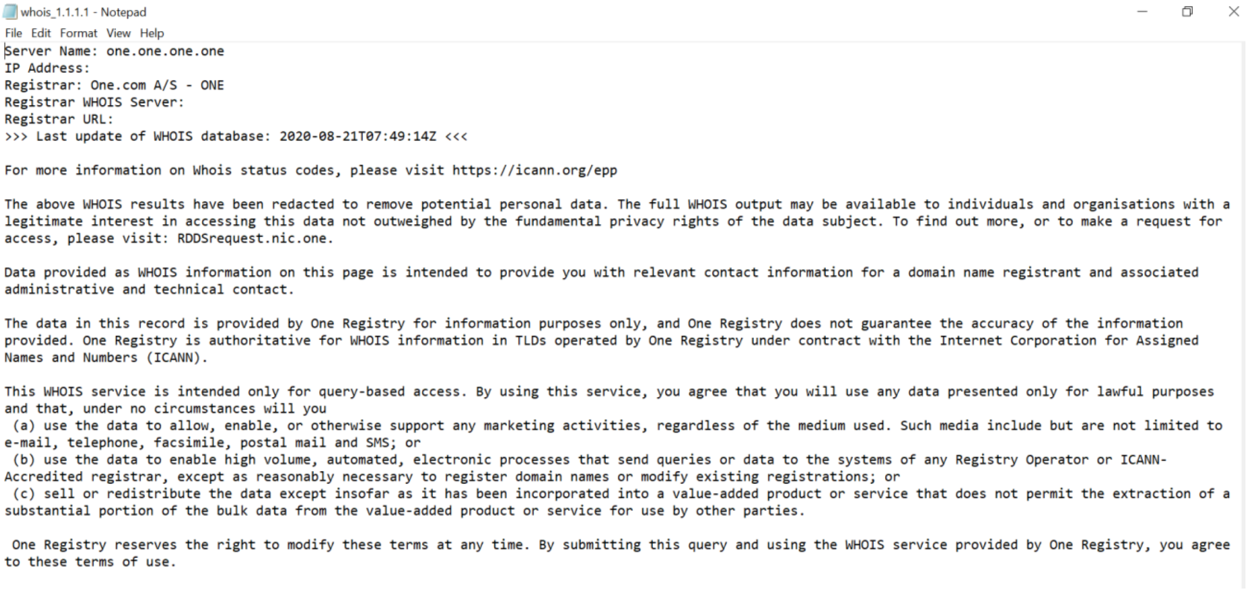
  The first few hops across all tracert commands have low latency (<10 ms). After about the 3rd hop the latency starts increasing to double digits. At the 7th or the 8th hop the latency is in the order of 10^2 ms. i.e as the number of nodes increases the latency increases. The pattern is similar across all hosts.

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*).

<u>Exercise 4:</u> (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.

whois 1.1.1.1



```
Server Name: one.one.one.one
IP Address:
Registrar: One.com A/S - ONE
Registrar WHOIS Server:
Registrar URL:
>>> Last update of WHOIS database: 2020-08-21T07:49:14Z <<<

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

The above WHOIS results have been redacted to remove potential personal data. The full WHOIS output may be available to individuals and organisations with a
legitimate interest in accessing this data not outweighed by the fundamental privacy rights of the data subject. To find out more, or to make a request for
access, please visit: RDDSrequest.nic.one.

Data provided as WHOIS information on this page is intended to provide you with relevant contact information for a domain name registrant and associated
administrative and technical contact.

The data in this record is provided by One Registry for information purposes only, and One Registry does not guarantee the accuracy of the information
provided. One Registry is authoritative for WHOIS information in TLDs operated by One Registry under contract with the Internet Corporation for Assigned
Names and Numbers (ICANN).

This WHOIS service is intended only for query-based access. By using this service, you agree that you will use any data presented only for lawful purposes
and that, under no circumstances will you
 (a) use the data to allow, enable, or otherwise support any marketing activities, regardless of the medium used. Such media include but are not limited to
e-mail, telephone, facsimile, postal mail and SMS; or
 (b) use the data to enable high volume, automated, electronic processes that send queries or data to the systems of any Registry Operator or ICANN-
Accredited registrar, except as reasonably necessary to register domain names or modify existing registrations; or
 (c) sell or redistribute the data except insofar as it has been incorporated into a value-added product or service that does not permit the extraction of a
substantial portion of the bulk data from the value-added product or service for use by other parties.

 One Registry reserves the right to modify these terms at any time. By submitting this query and using the WHOIS service provided by One Registry, you agree
to these terms of use.
```

<u>Observations:</u>
Running whois on a popular site returns a list consisting of Domain name, Registered domain id and other details. It also lists a notice and terms of use statement. Also has details like registrar email, phone and address.

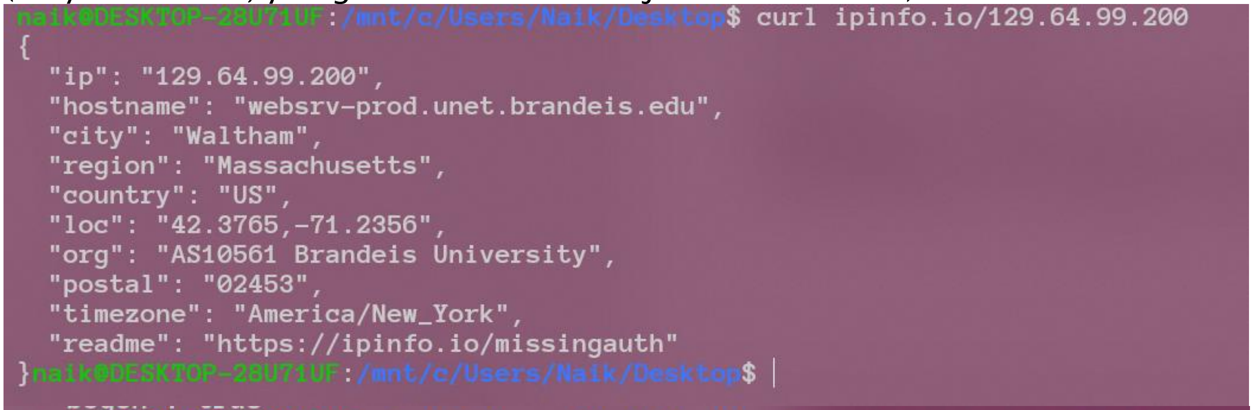
<u>Exercise 5:</u> (Should be short.) Because of NAT, the domain name *spit.ac.in* has a different IP address outside of SPIT than it does on campus. Using information in this lab and working on a home computer, find the outside IP address for spit.ac.in. Explain how you did it.

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.

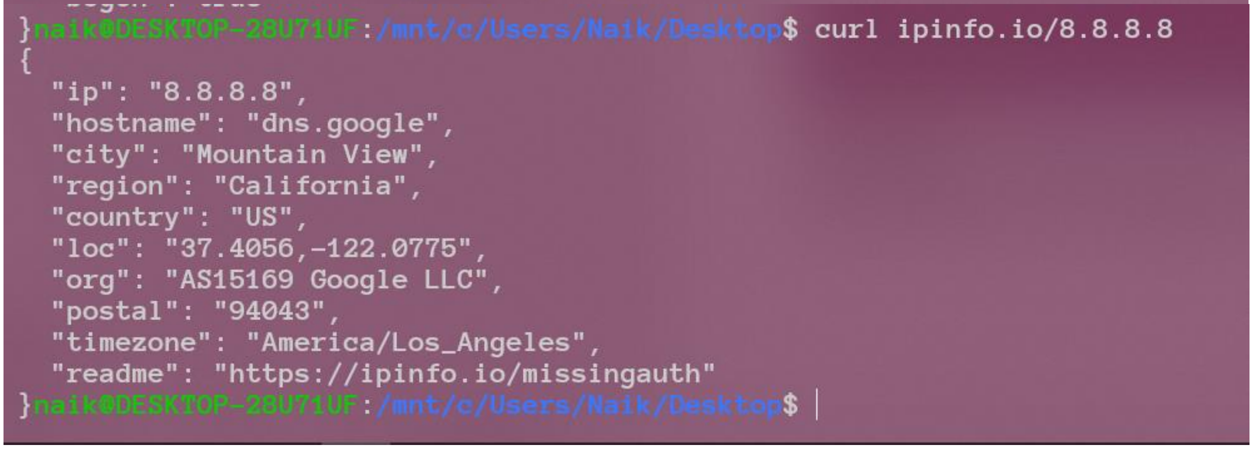
This geolocation program is not installed on our computers, but you can access one on the command line using the *curl* command, which can send HTTP reuests and display the response. The following command uses *curl* to contact a public web service that will look up an IP address for you: curl ipinfo.io/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



```
naik@DESKTOP-28U71UF:/mnt/c/Users/Naik/Desktop$ 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"
}naik@DESKTOP-28U71UF:/mnt/c/Users/Naik/Desktop$
```



```
}naik@DESKTOP-28U71UF:/mnt/c/Users/Naik/Desktop$ curl ipinfo.io/8.8.8.8
{
  "ip": "8.8.8.8",
  "hostname": "dns.google",
  "city": "Mountain View",
  "region": "California",
  "country": "US",
  "loc": "37.4056,-122.0775",
  "org": "AS15169 Google LLC",
  "postal": "94043",
  "timezone": "America/Los_Angeles",
  "readme": "https://ipinfo.io/missingauth"
}naik@DESKTOP-28U71UF:/mnt/c/Users/Naik/Desktop$
```

Exercise 6: Find a few IP addresses that are connected to the web server on spit.ac.in right now, and determine where those IP addresses are located. (I'm expecting that there will be several; if not, try again in a few minutes or sometime later.) Find one that is far from Geneva, NY. Explain how you did it.

CONCLUSION:

- Successfully implemented basic command line Networking utilities namely ping, ifconfig, traceroute, whois and curl.
- Geographical distance plays a major role in transferring packets.
- The first few addresses are same for every destination.
- The first address in tracert command is the local address and the second address is that of the ISP.

Link to all log files:

https://drive.google.com/drive/folders/10IskxIYimGrTXGybrB22dFmeqBtZ0yPi?usp=sharing

References

[1] https://www.cloudflare.com/learning/cdn/glossary/round-trip-time-rtt/
[2] https://en.wikipedia.org/wiki/Ping_(networking_utility)
[3] https://askubuntu.com/questions/247625/what-is-the-loopback-device-and-how-do-i-use-it