NAME : BHUSHAN KOYANDE
CLASS : TE COMPUTER
BATCH : B
UID : 2018130021
ROLL NO : 24

https://meet.google.com/nmg-oanc-hhj

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>
```

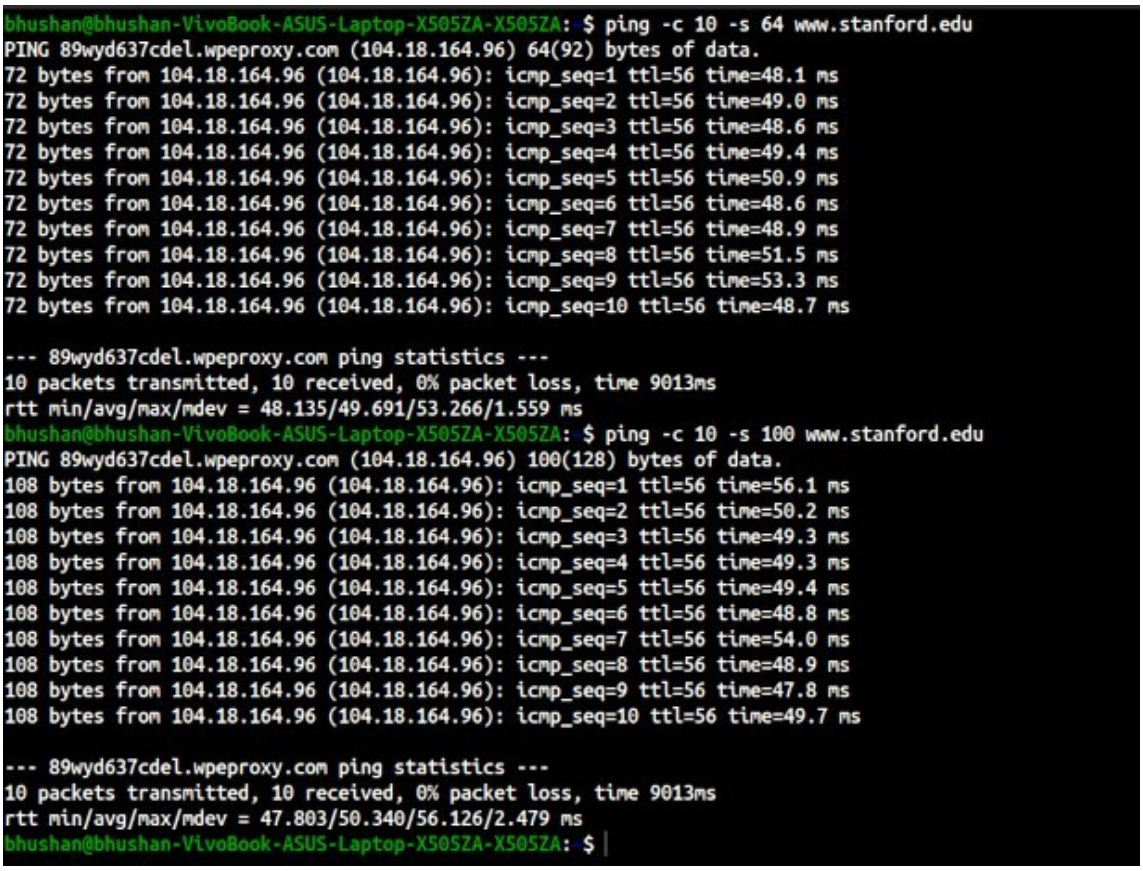
The default number of ICMP packets to send is either infinite (in Linux and Mac OS) or 4 (in Windows). The default packet size is either 64 bytes (in Linux) or 32 bytes (in Windows). You can specify either a hostname (e.g., `spit.ac.in`) or an IP address.

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



```
bhushan@bhushan-VivoBook-ASUS-Laptop-X505ZA-X505ZA:~$ ping -c 10 -s 500 www.stanford.edu
PING 89wyd637cdel.wpeproxy.com (104.18.168.96) 500(528) bytes of data.
508 bytes from 104.18.168.96 (104.18.168.96): icmp_seq=1 ttl=56 time=62.4 ms
508 bytes from 104.18.168.96 (104.18.168.96): icmp_seq=2 ttl=56 time=63.4 ms
508 bytes from 104.18.168.96 (104.18.168.96): icmp_seq=3 ttl=56 time=63.2 ms
508 bytes from 104.18.168.96 (104.18.168.96): icmp_seq=4 ttl=56 time=63.8 ms
508 bytes from 104.18.168.96 (104.18.168.96): icmp_seq=5 ttl=56 time=60.8 ms
508 bytes from 104.18.168.96 (104.18.168.96): icmp_seq=6 ttl=56 time=64.5 ms
508 bytes from 104.18.168.96 (104.18.168.96): icmp_seq=7 ttl=56 time=60.8 ms
508 bytes from 104.18.168.96 (104.18.168.96): icmp_seq=8 ttl=56 time=60.7 ms
508 bytes from 104.18.168.96 (104.18.168.96): icmp_seq=9 ttl=56 time=60.6 ms
508 bytes from 104.18.168.96 (104.18.168.96): icmp_seq=10 ttl=56 time=61.5 ms

--- 89wyd637cdel.wpeproxy.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9017ms
rtt min/avg/max/mdev = 60.637/62.170/64.506/1.410 ms
bhushan@bhushan-VivoBook-ASUS-Laptop-X505ZA-X505ZA:~$ ping -c 10 -s 1000 www.stanford.edu
PING 89wyd637cdel.wpeproxy.com (104.18.168.96) 1000(1028) bytes of data.
1008 bytes from 104.18.168.96 (104.18.168.96): icmp_seq=1 ttl=56 time=67.9 ms
1008 bytes from 104.18.168.96 (104.18.168.96): icmp_seq=2 ttl=56 time=66.5 ms
1008 bytes from 104.18.168.96 (104.18.168.96): icmp_seq=3 ttl=56 time=67.2 ms
1008 bytes from 104.18.168.96 (104.18.168.96): icmp_seq=4 ttl=56 time=68.4 ms
1008 bytes from 104.18.168.96 (104.18.168.96): icmp_seq=5 ttl=56 time=69.3 ms
1008 bytes from 104.18.168.96 (104.18.168.96): icmp_seq=6 ttl=56 time=63.4 ms
1008 bytes from 104.18.168.96 (104.18.168.96): icmp_seq=7 ttl=56 time=62.9 ms
1008 bytes from 104.18.168.96 (104.18.168.96): icmp_seq=8 ttl=56 time=62.6 ms
1008 bytes from 104.18.168.96 (104.18.168.96): icmp_seq=9 ttl=56 time=63.5 ms
1008 bytes from 104.18.168.96 (104.18.168.96): icmp_seq=10 ttl=56 time=63.1 ms

--- 89wyd637cdel.wpeproxy.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9014ms
rtt min/avg/max/mdev = 62.641/65.486/69.285/2.486 ms
bhushan@bhushan-VivoBook-ASUS-Laptop-X505ZA-X505ZA:~$ ping -c 10 -s 1400 www.stanford.edu
PING 89wyd637cdel.wpeproxy.com (104.18.168.96) 1400(1428) bytes of data.
1408 bytes from 104.18.168.96 (104.18.168.96): icmp_seq=1 ttl=56 time=70.9 ms
1408 bytes from 104.18.168.96 (104.18.168.96): icmp_seq=2 ttl=56 time=70.9 ms
1408 bytes from 104.18.168.96 (104.18.168.96): icmp_seq=3 ttl=56 time=70.9 ms
1408 bytes from 104.18.168.96 (104.18.168.96): icmp_seq=4 ttl=56 time=72.1 ms
1408 bytes from 104.18.168.96 (104.18.168.96): icmp_seq=5 ttl=56 time=70.1 ms
1408 bytes from 104.18.168.96 (104.18.168.96): icmp_seq=6 ttl=56 time=64.5 ms
1408 bytes from 104.18.168.96 (104.18.168.96): icmp_seq=7 ttl=56 time=65.4 ms
1408 bytes from 104.18.168.96 (104.18.168.96): icmp_seq=8 ttl=56 time=64.5 ms
1408 bytes from 104.18.168.96 (104.18.168.96): icmp_seq=9 ttl=56 time=64.7 ms
1408 bytes from 104.18.168.96 (104.18.168.96): icmp_seq=10 ttl=56 time=65.5 ms

--- 89wyd637cdel.wpeproxy.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9014ms
rtt min/avg/max/mdev = 64.464/67.942/72.137/3.079 ms
bhushan@bhushan-VivoBook-ASUS-Laptop-X505ZA-X505ZA:~$
```

```
bhushan@bhushan-VivoBook-ASUS-Laptop-X505ZA-X505ZA: $ ping -c 10 -s 64 www.geeksforgeeks.org
PING a1991.dscr.akamai.net (221.135.111.120) 64(92) bytes of data.
72 bytes from 221-135-111-120.sify.net (221.135.111.120): icmp_seq=1 ttl=58 time=5.98 ms
72 bytes from 221-135-111-120.sify.net (221.135.111.120): icmp_seq=2 ttl=58 time=7.52 ms
72 bytes from 221-135-111-120.sify.net (221.135.111.120): icmp_seq=3 ttl=58 time=5.29 ms
72 bytes from 221-135-111-120.sify.net (221.135.111.120): icmp_seq=4 ttl=58 time=11.0 ms
72 bytes from 221-135-111-120.sify.net (221.135.111.120): icmp_seq=5 ttl=58 time=5.63 ms
72 bytes from 221-135-111-120.sify.net (221.135.111.120): icmp_seq=6 ttl=58 time=28.6 ms
72 bytes from 221-135-111-120.sify.net (221.135.111.120): icmp_seq=7 ttl=58 time=6.21 ms
72 bytes from 221-135-111-120.sify.net (221.135.111.120): icmp_seq=8 ttl=58 time=4.70 ms
72 bytes from 221-135-111-120.sify.net (221.135.111.120): icmp_seq=9 ttl=58 time=3.98 ms
72 bytes from 221-135-111-120.sify.net (221.135.111.120): icmp_seq=10 ttl=58 time=4.83 ms

--- a1991.dscr.akamai.net ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9016ms
rtt min/avg/max/mdev = 3.978/8.378/28.643/7.009 ms
bhushan@bhushan-VivoBook-ASUS-Laptop-X505ZA-X505ZA: $ ping -c 10 -s 64 www.google.com
PING www.google.com (216.58.203.164) 64(92) bytes of data.
72 bytes from bom07s11-in-f4.1e100.net (216.58.203.164): icmp_seq=1 ttl=120 time=4.57 ms
72 bytes from bom07s11-in-f4.1e100.net (216.58.203.164): icmp_seq=2 ttl=120 time=14.4 ms
72 bytes from bom07s11-in-f4.1e100.net (216.58.203.164): icmp_seq=3 ttl=120 time=5.43 ms
72 bytes from bom07s11-in-f4.1e100.net (216.58.203.164): icmp_seq=4 ttl=120 time=764 ms
72 bytes from bom07s11-in-f4.1e100.net (216.58.203.164): icmp_seq=5 ttl=120 time=4.97 ms
72 bytes from bom07s11-in-f4.1e100.net (216.58.203.164): icmp_seq=6 ttl=120 time=3.93 ms
72 bytes from bom07s11-in-f4.1e100.net (216.58.203.164): icmp_seq=7 ttl=120 time=6.56 ms
72 bytes from bom07s11-in-f4.1e100.net (216.58.203.164): icmp_seq=7 ttl=120 time=23.7 ms (DUP!)
72 bytes from bom07s11-in-f4.1e100.net (216.58.203.164): icmp_seq=8 ttl=120 time=5.00 ms
72 bytes from bom07s11-in-f4.1e100.net (216.58.203.164): icmp_seq=9 ttl=120 time=8.78 ms
72 bytes from bom07s11-in-f4.1e100.net (216.58.203.164): icmp_seq=10 ttl=120 time=5.15 ms

--- www.google.com ping statistics ---
10 packets transmitted, 10 received, +1 duplicates, 0% packet loss, time 9013ms
rtt min/avg/max/mdev = 3.931/76.963/764.112/217.368 ms
```

```
bhushan@bhushan-VivoBook-ASUS-Laptop-X505ZA-X505ZA: $ ping -c 10 -s 64 www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (13.227.137.166) 64(92) bytes of data.
72 bytes from server-13-227-137-166.bom50.r.cloudfront.net (13.227.137.166): icmp_seq=1 ttl=245 time=6.57 ms
72 bytes from server-13-227-137-166.bom50.r.cloudfront.net (13.227.137.166): icmp_seq=2 ttl=245 time=29.3 ms
72 bytes from server-13-227-137-166.bom50.r.cloudfront.net (13.227.137.166): icmp_seq=3 ttl=245 time=27.5 ms
72 bytes from server-13-227-137-166.bom50.r.cloudfront.net (13.227.137.166): icmp_seq=4 ttl=245 time=17.2 ms
72 bytes from server-13-227-137-166.bom50.r.cloudfront.net (13.227.137.166): icmp_seq=5 ttl=245 time=16.7 ms
72 bytes from server-13-227-137-166.bom50.r.cloudfront.net (13.227.137.166): icmp_seq=6 ttl=245 time=22.7 ms
72 bytes from server-13-227-137-166.bom50.r.cloudfront.net (13.227.137.166): icmp_seq=7 ttl=245 time=6.01 ms
72 bytes from server-13-227-137-166.bom50.r.cloudfront.net (13.227.137.166): icmp_seq=8 ttl=245 time=8.46 ms
72 bytes from server-13-227-137-166.bom50.r.cloudfront.net (13.227.137.166): icmp_seq=9 ttl=245 time=22.2 ms
72 bytes from server-13-227-137-166.bom50.r.cloudfront.net (13.227.137.166): icmp_seq=10 ttl=245 time=6.20 ms

--- d3ag4hukkh62yn.cloudfront.net ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9014ms
rtt min/avg/max/mdev = 6.010/16.287/29.297/8.576 ms
bhushan@bhushan-VivoBook-ASUS-Laptop-X505ZA-X505ZA: $ ping -c 10 -s 64 www.yahoo.com
PING new-fp-shed.wg1.b.yahoo.com (202.165.107.49) 64(92) bytes of data.
72 bytes from media-router-fp73.prod.media.vip.sg3.yahoo.com (202.165.107.49): icmp_seq=1 ttl=51 time=201 ms
72 bytes from media-router-fp73.prod.media.vip.sg3.yahoo.com (202.165.107.49): icmp_seq=2 ttl=51 time=218 ms
72 bytes from media-router-fp73.prod.media.vip.sg3.yahoo.com (202.165.107.49): icmp_seq=3 ttl=51 time=243 ms
72 bytes from media-router-fp73.prod.media.vip.sg3.yahoo.com (202.165.107.49): icmp_seq=4 ttl=51 time=263 ms
72 bytes from media-router-fp73.prod.media.vip.sg3.yahoo.com (202.165.107.49): icmp_seq=5 ttl=51 time=287 ms
72 bytes from media-router-fp73.prod.media.vip.sg3.yahoo.com (202.165.107.49): icmp_seq=6 ttl=51 time=206 ms
72 bytes from media-router-fp73.prod.media.vip.sg3.yahoo.com (202.165.107.49): icmp_seq=7 ttl=51 time=228 ms
72 bytes from media-router-fp73.prod.media.vip.sg3.yahoo.com (202.165.107.49): icmp_seq=8 ttl=51 time=248 ms
72 bytes from media-router-fp73.prod.media.vip.sg3.yahoo.com (202.165.107.49): icmp_seq=9 ttl=51 time=274 ms
72 bytes from media-router-fp73.prod.media.vip.sg3.yahoo.com (202.165.107.49): icmp_seq=10 ttl=51 time=202 ms

--- new-fp-shed.wg1.b.yahoo.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9013ms
rtt min/avg/max/mdev = 200.979/236.942/286.541/29.454 ms
bhushan@bhushan-VivoBook-ASUS-Laptop-X505ZA-X505ZA: $ ping -c 10 -s 64 www.microsoft.com
PING e13678.dspb.akamaiedge.net (23.212.241.249) 64(92) bytes of data.
72 bytes from a23-212-241-249.deploy.static.akamaitechnologies.com (23.212.241.249): icmp_seq=1 ttl=60 time=1.88 ms
72 bytes from a23-212-241-249.deploy.static.akamaitechnologies.com (23.212.241.249): icmp_seq=2 ttl=60 time=3.71 ms
72 bytes from a23-212-241-249.deploy.static.akamaitechnologies.com (23.212.241.249): icmp_seq=3 ttl=60 time=4.17 ms
72 bytes from a23-212-241-249.deploy.static.akamaitechnologies.com (23.212.241.249): icmp_seq=4 ttl=60 time=11.3 ms
72 bytes from a23-212-241-249.deploy.static.akamaitechnologies.com (23.212.241.249): icmp_seq=5 ttl=60 time=4.03 ms
72 bytes from a23-212-241-249.deploy.static.akamaitechnologies.com (23.212.241.249): icmp_seq=6 ttl=60 time=3.91 ms
72 bytes from a23-212-241-249.deploy.static.akamaitechnologies.com (23.212.241.249): icmp_seq=7 ttl=60 time=3.80 ms
72 bytes from a23-212-241-249.deploy.static.akamaitechnologies.com (23.212.241.249): icmp_seq=8 ttl=60 time=5.46 ms
72 bytes from a23-212-241-249.deploy.static.akamaitechnologies.com (23.212.241.249): icmp_seq=9 ttl=60 time=3.83 ms
72 bytes from a23-212-241-249.deploy.static.akamaitechnologies.com (23.212.241.249): icmp_seq=10 ttl=60 time=5.60 ms

--- e13678.dspb.akamaiedge.net ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9015ms
rtt min/avg/max/mdev = 1.880/4.763/11.268/2.373 ms
```

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`.

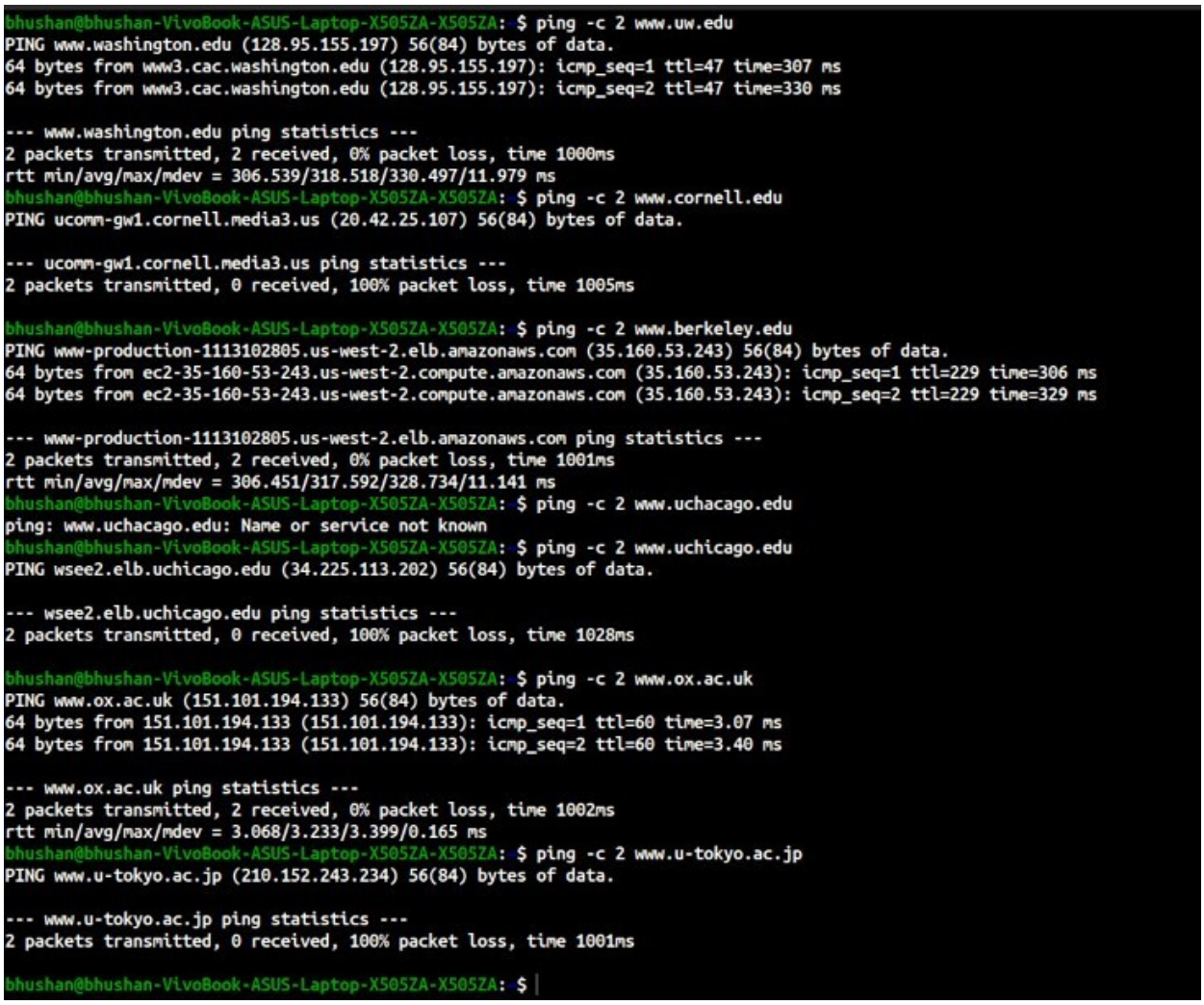
1. Does the average RTT vary between different hosts? What aspects of latency (transmit, propagation, and queueing delay) might impact this and why?

Ans : RTT varies between different hosts. RTT depends on the distance of host, the medium, number of network hops, traffic levels in the network and server response time of the host. Propogation delay depends on distance. Transmission delay depends on the efficiency of medium. Propogation and Transmission delay might have an impact in this case.

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 varies with packet size. RTT increases as packet size increases. Transmission delay depends on size of packet.So, transmission delay might have an impact on this.

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).



RTT increases as the physical distance of the host increases. Increase in physical distance causes an increase in propogation delay.

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>

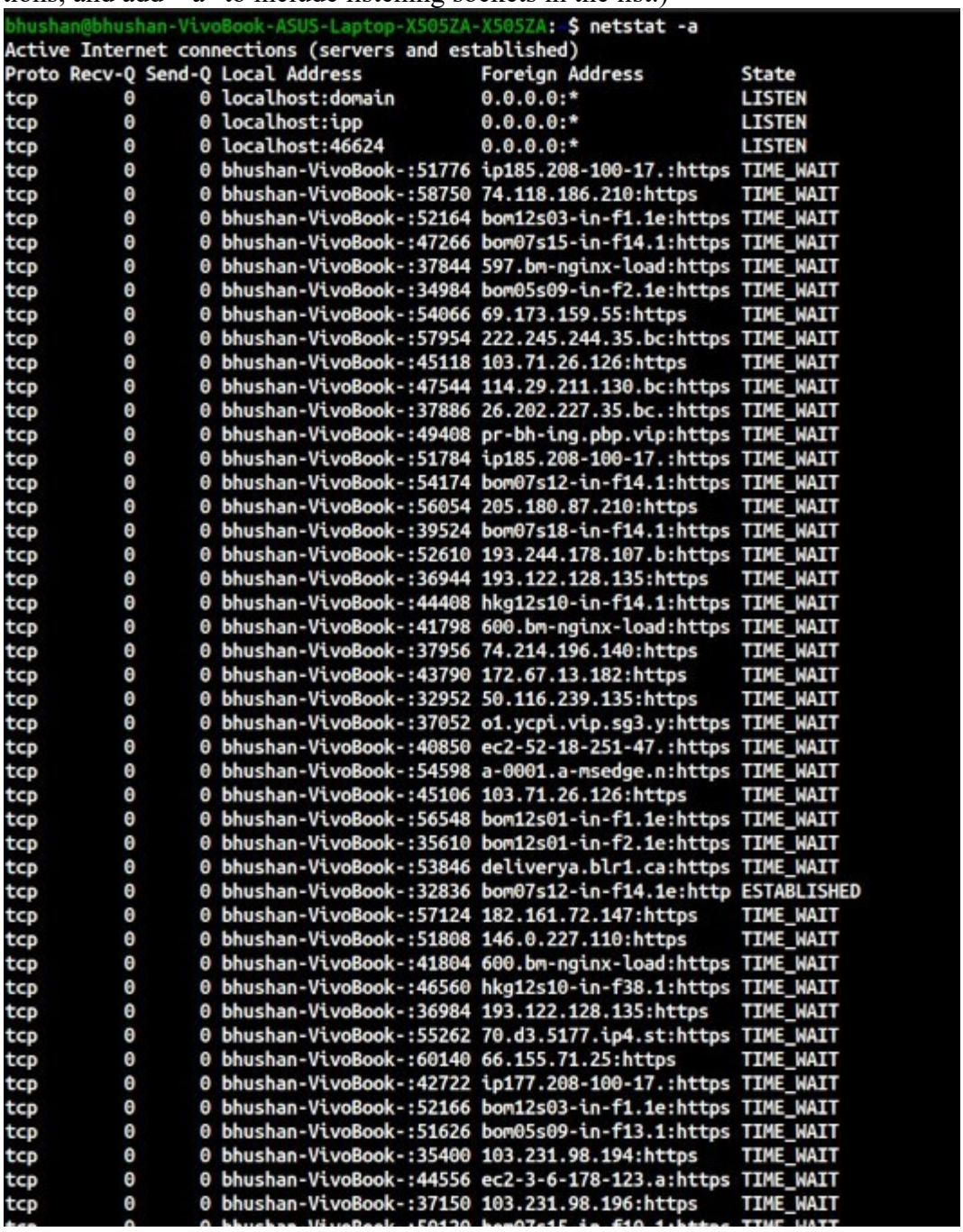
ifconfig — You used ifconfig in the previous lab. When used with no parameters, ifconfig reports some information about the computer's network interfaces. This usually includes lo which stands for localhost; it can be used for communication between programs running on the same computer. Linux often has 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!!!.)

The ifconfig command is used for displaying current network configuration information, setting up an IP address, creating an alias for a network interface, setting up hardware address and enable or disable network interfaces.

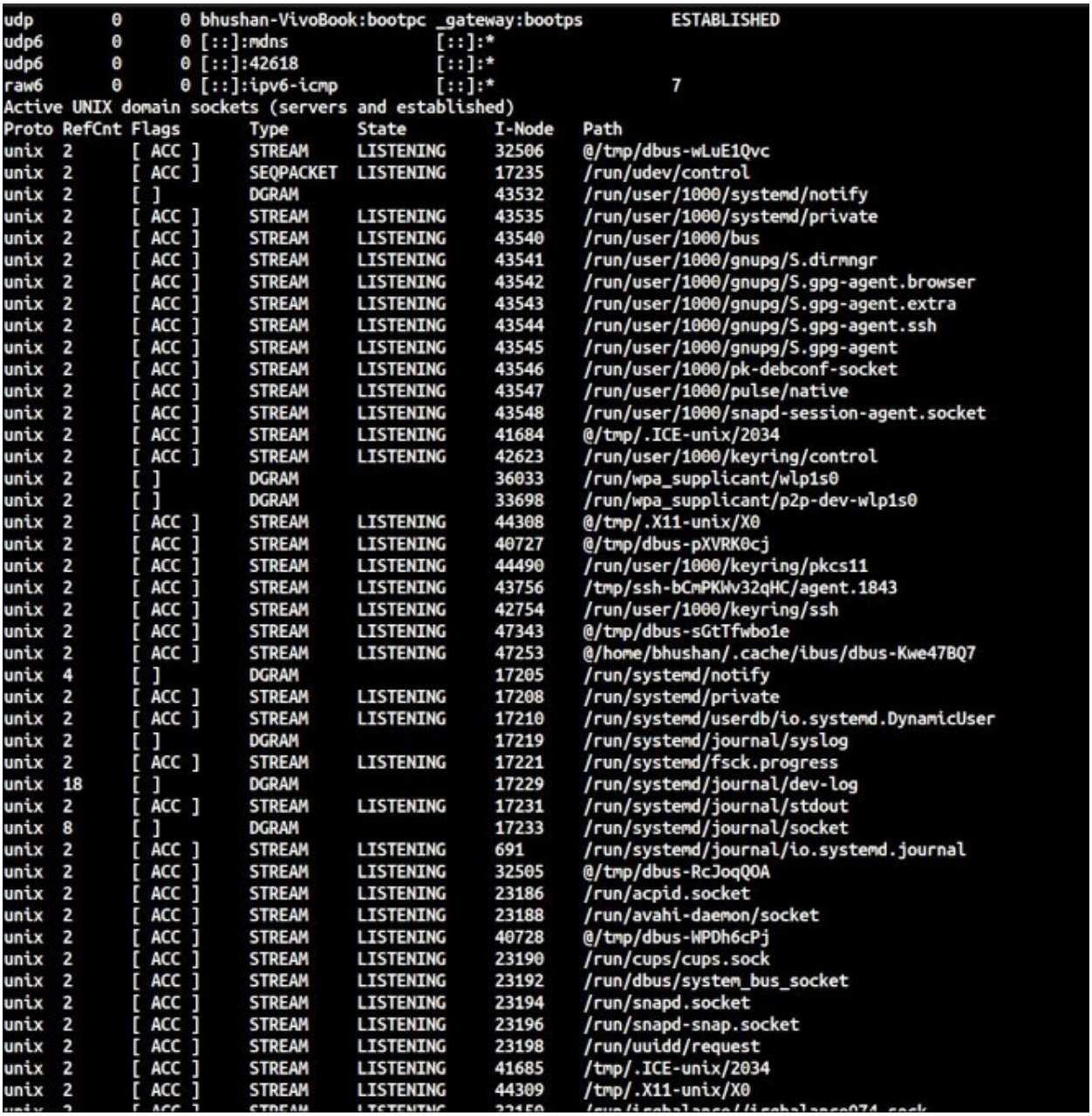
```
bhushan@bhushan-VivoBook-ASUS-Laptop-X505ZA-X505ZA:~$ ifconfig -a
enp2s0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 40:b0:76:0a:ac:66  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 441  bytes 41726 (41.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 441  bytes 41726 (41.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp1s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.103  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::4f13:111f:ffe5:c725  prefixlen 64  scopeid 0x20<link>
        ether f4:d1:08:04:da:4e  txqueuelen 1000  (Ethernet)
        RX packets 20951  bytes 25918356 (25.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7878  bytes 1506112 (1.5 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

bhushan@bhushan-VivoBook-ASUS-Laptop-X505ZA-X505ZA:~$
```

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.)



```
bhushan@bhushan-VivoBook-ASUS-Laptop-X505ZA-X505ZA: $ netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp        0      0 localhost:46624         0.0.0.0:*               LISTEN
tcp        0      0 bhushan-VivoBook-:51776 ip185.208-100-17.:https TIME_WAIT
tcp        0      0 bhushan-VivoBook-:58750 74.118.186.210:https    TIME_WAIT
tcp        0      0 bhushan-VivoBook-:52164 bom12s03-in-f1.1e:https TIME_WAIT
tcp        0      0 bhushan-VivoBook-:47266 bom07s15-in-f14.1:https TIME_WAIT
tcp        0      0 bhushan-VivoBook-:37844 597.bm-nginx-load:https TIME_WAIT
tcp        0      0 bhushan-VivoBook-:34984 bom05s09-in-f2.1e:https TIME_WAIT
tcp        0      0 bhushan-VivoBook-:54066 69.173.159.55:https     TIME_WAIT
tcp        0      0 bhushan-VivoBook-:57954 222.245.244.35.bc:https TIME_WAIT
tcp        0      0 bhushan-VivoBook-:45118 103.71.26.126:https     TIME_WAIT
tcp        0      0 bhushan-VivoBook-:47544 114.29.211.130.bc:https TIME_WAIT
tcp        0      0 bhushan-VivoBook-:37886 26.202.227.35.bc.:https TIME_WAIT
tcp        0      0 bhushan-VivoBook-:49408 pr-bh-ing.pbp.vip:https TIME_WAIT
tcp        0      0 bhushan-VivoBook-:51784 ip185.208-100-17.:https TIME_WAIT
tcp        0      0 bhushan-VivoBook-:54174 bom07s12-in-f14.1:https TIME_WAIT
tcp        0      0 bhushan-VivoBook-:56054 205.180.87.210:https    TIME_WAIT
tcp        0      0 bhushan-VivoBook-:39524 bom07s18-in-f14.1:https TIME_WAIT
tcp        0      0 bhushan-VivoBook-:52610 193.244.178.107.b:https TIME_WAIT
tcp        0      0 bhushan-VivoBook-:36944 193.122.128.135:https   TIME_WAIT
tcp        0      0 bhushan-VivoBook-:44408 hkg12s10-in-f14.1:https TIME_WAIT
tcp        0      0 bhushan-VivoBook-:41798 600.bm-nginx-load:https TIME_WAIT
tcp        0      0 bhushan-VivoBook-:37956 74.214.196.140:https    TIME_WAIT
tcp        0      0 bhushan-VivoBook-:43790 172.67.13.182:https     TIME_WAIT
tcp        0      0 bhushan-VivoBook-:32952 50.116.239.135:https    TIME_WAIT
tcp        0      0 bhushan-VivoBook-:37052 o1.ycpi.vip.sg3.y:https TIME_WAIT
tcp        0      0 bhushan-VivoBook-:40850 ec2-52-18-251-47.:https TIME_WAIT
tcp        0      0 bhushan-VivoBook-:54598 a-0001.a-msedge.n:https TIME_WAIT
tcp        0      0 bhushan-VivoBook-:45106 103.71.26.126:https     TIME_WAIT
tcp        0      0 bhushan-VivoBook-:56548 bom12s01-in-f1.1e:https TIME_WAIT
tcp        0      0 bhushan-VivoBook-:35610 bom12s01-in-f2.1e:https TIME_WAIT
tcp        0      0 bhushan-VivoBook-:53846 deliverya.blr1.ca:https TIME_WAIT
tcp        0      0 bhushan-VivoBook-:32836 bom07s12-in-f14.1e:http ESTABLISHED
tcp        0      0 bhushan-VivoBook-:57124 182.161.72.147:https    TIME_WAIT
tcp        0      0 bhushan-VivoBook-:51808 146.0.227.110:https     TIME_WAIT
tcp        0      0 bhushan-VivoBook-:41804 600.bm-nginx-load:https TIME_WAIT
tcp        0      0 bhushan-VivoBook-:46560 hkg12s10-in-f38.1:https TIME_WAIT
tcp        0      0 bhushan-VivoBook-:36984 193.122.128.135:https   TIME_WAIT
tcp        0      0 bhushan-VivoBook-:55262 70.d3.5177.ip4.st:https TIME_WAIT
tcp        0      0 bhushan-VivoBook-:60140 66.155.71.25:https      TIME_WAIT
tcp        0      0 bhushan-VivoBook-:42722 ip177.208-100-17.:https TIME_WAIT
tcp        0      0 bhushan-VivoBook-:52166 bom12s03-in-f1.1e:https TIME_WAIT
tcp        0      0 bhushan-VivoBook-:51626 bom05s09-in-f13.1:https TIME_WAIT
tcp        0      0 bhushan-VivoBook-:35400 103.231.98.194:https    TIME_WAIT
tcp        0      0 bhushan-VivoBook-:44556 ec2-3-6-178-123.a:https TIME_WAIT
tcp        0      0 bhushan-VivoBook-:37150 103.231.98.196:https    TIME_WAIT
```



```
udp        0      0 bhushan-VivoBook:bootpc _gateway:bootps         ESTABLISHED
udp6       0      0 [::]:mdns               [::]:*
udp6       0      0 [::]:42618              [::]:*
raw6       0      0 [::]:ipv6-icmp          [::]:*                  7
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ACC ]     STREAM     LISTENING     32506    @/tmp/dbus-wLuE1Qvc
unix  2      [ ACC ]     SEQPACKET  LISTENING     17235    /run/udev/control
unix  2      [ ]         DGRAM                    43532    /run/user/1000/systemd/notify
unix  2      [ ACC ]     STREAM     LISTENING     43535    /run/user/1000/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     43540    /run/user/1000/bus
unix  2      [ ACC ]     STREAM     LISTENING     43541    /run/user/1000/gnupg/S.dirmngr
unix  2      [ ACC ]     STREAM     LISTENING     43542    /run/user/1000/gnupg/S.gpg-agent.browser
unix  2      [ ACC ]     STREAM     LISTENING     43543    /run/user/1000/gnupg/S.gpg-agent.extra
unix  2      [ ACC ]     STREAM     LISTENING     43544    /run/user/1000/gnupg/S.gpg-agent.ssh
unix  2      [ ACC ]     STREAM     LISTENING     43545    /run/user/1000/gnupg/S.gpg-agent
unix  2      [ ACC ]     STREAM     LISTENING     43546    /run/user/1000/pk-debconf-socket
unix  2      [ ACC ]     STREAM     LISTENING     43547    /run/user/1000/pulse/native
unix  2      [ ACC ]     STREAM     LISTENING     43548    /run/user/1000/snapd-session-agent.socket
unix  2      [ ACC ]     STREAM     LISTENING     41684    @/tmp/.ICE-unix/2034
unix  2      [ ACC ]     STREAM     LISTENING     42623    /run/user/1000/keyring/control
unix  2      [ ]         DGRAM                    36033    /run/wpa_supplicant/wlp1s0
unix  2      [ ]         DGRAM                    33698    /run/wpa_supplicant/p2p-dev-wlp1s0
unix  2      [ ACC ]     STREAM     LISTENING     44308    @/tmp/.X11-unix/X0
unix  2      [ ACC ]     STREAM     LISTENING     40727    @/tmp/dbus-pXVRK0cj
unix  2      [ ACC ]     STREAM     LISTENING     44490    /run/user/1000/keyring/pkcs11
unix  2      [ ACC ]     STREAM     LISTENING     43756    /tmp/ssh-bCmPKWv32qHC/agent.1843
unix  2      [ ACC ]     STREAM     LISTENING     42754    /run/user/1000/keyring/ssh
unix  2      [ ACC ]     STREAM     LISTENING     47343    @/tmp/dbus-sGtTfwbo1e
unix  2      [ ACC ]     STREAM     LISTENING     47253    @/home/bhushan/.cache/ibus/dbus-Kwe47BQ7
unix  4      [ ]         DGRAM                    17205    /run/systemd/notify
unix  2      [ ACC ]     STREAM     LISTENING     17208    /run/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     17210    /run/systemd/userdb/io.systemd.DynamicUser
unix  2      [ ]         DGRAM                    17219    /run/systemd/journal/syslog
unix  2      [ ACC ]     STREAM     LISTENING     17221    /run/systemd/fsck.progress
unix  18     [ ]         DGRAM                    17229    /run/systemd/journal/dev-log
unix  2      [ ACC ]     STREAM     LISTENING     17231    /run/systemd/journal/stdout
unix  8      [ ]         DGRAM                    17233    /run/systemd/journal/socket
unix  2      [ ACC ]     STREAM     LISTENING     691      /run/systemd/journal/io.systemd.journal
unix  2      [ ACC ]     STREAM     LISTENING     32505    @/tmp/dbus-RcJoqQOA
unix  2      [ ACC ]     STREAM     LISTENING     23186    /run/acpid.socket
unix  2      [ ACC ]     STREAM     LISTENING     23188    /run/avahi-daemon/socket
unix  2      [ ACC ]     STREAM     LISTENING     40728    @/tmp/dbus-WPDh6cPj
unix  2      [ ACC ]     STREAM     LISTENING     23190    /run/cups/cups.sock
unix  2      [ ACC ]     STREAM     LISTENING     23192    /run/dbus/system_bus_socket
unix  2      [ ACC ]     STREAM     LISTENING     23194    /run/snapd.socket
unix  2      [ ACC ]     STREAM     LISTENING     23196    /run/snapd-snap.socket
unix  2      [ ACC ]     STREAM     LISTENING     23198    /run/uuidd/request
unix  2      [ ACC ]     STREAM     LISTENING     41685    /tmp/.ICE-unix/2034
unix  2      [ ACC ]     STREAM     LISTENING     44309    /tmp/.X11-unix/X0
```

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: telent <host> <port>. For example, to connect to the web server on www.spit.ac.in: telnet spit.ac.in 80

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`).

```
bhushan@bhushan-VivoBook-ASUS-Laptop-X505ZA-X505ZA: $ traceroute www.ee.iitb.ac.in
traceroute to www.ee.iitb.ac.in (103.21.125.132), 30 hops max, 60 byte packets
 1  _gateway (192.168.0.1)  1.866 ms  6.456 ms  8.189 ms
 2  45-164-87-103.digitalsatellite.in (103.87.164.45)  11.572 ms  11.639 ms  14.957 ms
 3  1-164-87-103.digitalsatellite.in (103.87.164.1)  16.658 ms  18.416 ms  20.606 ms
 4  106-164-87-103.digitalsatellite.in (103.87.164.106)  23.909 ms  23.910 ms  26.513 ms
 5  105-164-87-103.digitalsatellite.in (103.87.164.105)  26.758 ms  27.840 ms  28.067 ms
 6  1.6.74.200 (1.6.74.200)  32.911 ms  2.951 ms  2.763 ms
 7  100.66.8.23 (100.66.8.23)  7.351 ms 100.67.56.97 (100.67.56.97)  17.569 ms *
 8  100.67.70.146 (100.67.70.146)  37.659 ms 100.67.56.103 (100.67.56.103)  37.614 ms  37.625 ms
 9  115.113.165.173.static-mumbai.vsnl.net.in (115.113.165.173)  35.978 ms  21.331 ms  36.249 ms
10  * * *
11  * * *
12  115.113.165.62.static-mumbai.vsnl.net.in (115.113.165.62)  35.354 ms  20.234 ms  5.674 ms
13  * * *
14  * * *
15  115.110.234.170.static.Mumbai.vsnl.net.in (115.110.234.170)  15.286 ms  15.294 ms  15.259 ms
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
bhushan@bhushan-VivoBook-ASUS-Laptop-X505ZA-X505ZA: $
```

```
bhushan@bhushan-VivoBook-ASUS-Laptop-X505ZA-X505ZA: $ traceroute mscs.mu.edu
traceroute to mscs.mu.edu (134.48.4.5), 30 hops max, 60 byte packets
 1  _gateway (192.168.0.1)  1.333 ms  2.533 ms  3.747 ms
 2  45-164-87-103.digitalsatellite.in (103.87.164.45)  6.055 ms  7.137 ms  9.692 ms
 3  1-164-87-103.digitalsatellite.in (103.87.164.1)  11.099 ms  12.820 ms  13.062 ms
 4  106-164-87-103.digitalsatellite.in (103.87.164.106)  19.097 ms  19.103 ms  20.953 ms
 5  105-164-87-103.digitalsatellite.in (103.87.164.105)  20.950 ms  22.795 ms  24.058 ms
 6  1.6.74.200 (1.6.74.200)  25.440 ms  4.125 ms  6.108 ms
 7  100.67.110.97 (100.67.110.97)  101.654 ms  102.361 ms *
 8  100.67.110.101 (100.67.110.101)  104.398 ms 100.65.226.206 (100.65.226.206)  105.854 ms 100.67.110.97 (100.67.110.97)  105.854 ms
 9  hurricane.mrs.franceix.net (37.49.232.13)  132.056 ms  133.005 ms  134.069 ms
10  100ge4-2.core1.par2.he.net (184.105.222.21)  135.110 ms  135.794 ms  136.084 ms
11  100ge14-1.core1.nyc4.he.net (184.105.81.77)  274.972 ms  275.567 ms  275.776 ms
12  100ge9-1.core2.chi1.he.net (184.105.223.161)  268.584 ms 100ge2-1.core2.chi1.he.net (184.104.193.173)  242.946 ms  242.348 ms
13  * * *
14  r-222wwash-isp-ae6-3926.wiscnet.net (140.189.8.126)  241.658 ms  244.080 ms  245.680 ms
15  r-milwaukeeci-809-isp-ae3-0.wiscnet.net (140.189.8.230)  238.883 ms  241.213 ms  242.571 ms
16  MarquetteUniv.site.wiscnet.net (216.56.1.202)  310.105 ms  310.071 ms  308.883 ms
17  134.48.10.27 (134.48.10.27)  308.324 ms  211.404 ms  308.574 ms
18  * * *
19  * * *
20  euclid.mscs.mu.edu (134.48.4.5)  309.390 ms  309.361 ms  310.869 ms
bhushan@bhushan-VivoBook-ASUS-Laptop-X505ZA-X505ZA: $
```

```
bhushan@bhushan-VivoBook-ASUS-Laptop-X505ZA-X505ZA: $ traceroute www.cs.grinnell.edu
traceroute to www.cs.grinnell.edu (132.161.132.159), 30 hops max, 60 byte packets
 1  _gateway (192.168.0.1)  1.822 ms  3.616 ms  14.630 ms
 2  45-164-87-103.digitalsatellite.in (103.87.164.45)  16.866 ms  16.944 ms  17.036 ms
 3  1-164-87-103.digitalsatellite.in (103.87.164.1)  18.542 ms  18.750 ms  23.455 ms
 4  106-164-87-103.digitalsatellite.in (103.87.164.106)  18.489 ms  26.183 ms  28.008 ms
 5  105-164-87-103.digitalsatellite.in (103.87.164.105)  28.201 ms  30.069 ms  30.374 ms
 6  1.6.74.200 (1.6.74.200)  30.953 ms  6.587 ms  3.631 ms
 7  * 100.67.110.97 (100.67.110.97)  103.408 ms *
 8  100.67.110.101 (100.67.110.101)  113.550 ms 100.65.226.206 (100.65.226.206)  116.399 ms 100.67.110.101 (100.67.110.101)  117.867 ms
 9  hurricane.mrs.franceix.net (37.49.232.13)  144.494 ms  145.582 ms  147.217 ms
10  100ge4-2.core1.par2.he.net (184.105.222.21)  148.595 ms  149.563 ms  150.617 ms
11  100ge14-1.core1.nyc4.he.net (184.105.81.77)  318.595 ms  318.813 ms  319.113 ms
12  100ge2-1.core2.chi1.he.net (184.104.193.173)  316.078 ms 100ge9-1.core2.chi1.he.net (184.105.223.161)  233.191 ms  233.123 ms
13  100ge14-2.core1.msp1.he.net (184.105.223.178)  247.297 ms  247.317 ms  247.304 ms
14  216.66.77.218 (216.66.77.218)  218.595 ms * *
15  peer-as5056.br02.msp1.tfbnw.net (157.240.76.37)  223.034 ms  222.760 ms  249.356 ms
16  167.142.58.40 (167.142.58.40)  248.447 ms  248.205 ms *
17  67.224.64.62 (67.224.64.62)  250.262 ms  250.260 ms  240.700 ms
18  grinnellcollege1.desm.netins.net (167.142.65.43)  256.449 ms  270.317 ms  307.248 ms
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
bhushan@bhushan-VivoBook-ASUS-Laptop-X505ZA-X505ZA: $
```

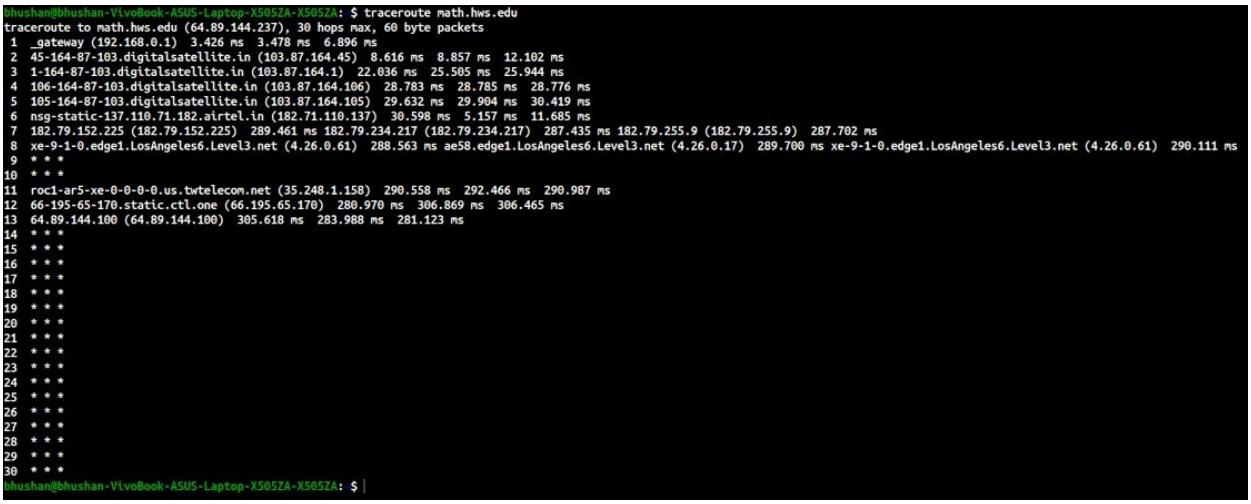
```
bhushan@bhushan-VivoBook-ASUS-Laptop-X505ZA-X505ZA: $ traceroute cs.stanford.edu
traceroute to cs.stanford.edu (171.64.64.64), 30 hops max, 60 byte packets
 1  _gateway (192.168.0.1)  1.819 ms  3.731 ms  5.466 ms
 2  45-164-87-103.digitalsatellite.in (103.87.164.45)  8.926 ms  8.963 ms  12.242 ms
 3  1-164-87-103.digitalsatellite.in (103.87.164.1)  28.848 ms  29.127 ms  29.464 ms
 4  106-164-87-103.digitalsatellite.in (103.87.164.106)  30.707 ms  30.705 ms  30.696 ms
 5  105-164-87-103.digitalsatellite.in (103.87.164.105)  30.688 ms  30.901 ms  31.186 ms
 6  1.6.74.200 (1.6.74.200)  34.239 ms  6.171 ms  7.937 ms
 7  100.67.110.97 (100.67.110.97)  102.791 ms *  103.358 ms
 8  100.67.110.101 (100.67.110.101)  103.350 ms 100.65.226.206 (100.65.226.206)  105.058 ms  105.053 ms
 9  hurricane.mrs.franceix.net (37.49.232.13)  148.454 ms  130.126 ms  130.375 ms
10  100ge4-2.core1.par2.he.net (184.105.222.21)  130.820 ms  131.484 ms  132.689 ms
11  100ge10-2.core1.ash1.he.net (184.105.213.173)  360.578 ms  361.129 ms  364.756 ms
12  100ge7-2.core1.pao1.he.net (184.105.222.41)  357.212 ms  258.400 ms  271.907 ms
13  stanford-university.100gigabitethernet5-1.core1.pao1.he.net (184.105.177.238)  242.484 ms  242.686 ms  244.090 ms
14  csee-west-rtr-vl3.SUNet (171.66.255.140)  248.222 ms  247.930 ms  249.035 ms
15  CS.stanford.edu (171.64.64.64)  243.433 ms  243.998 ms  244.820 ms
bhushan@bhushan-VivoBook-ASUS-Laptop-X505ZA-X505ZA: $
```

```
bhushan@bhushan-VivoBook-ASUS-Laptop-X505ZA-X505ZA: $ traceroute cs.manchester.ac.uk
traceroute to cs.manchester.ac.uk (130.88.101.49), 30 hops max, 60 byte packets
 1  _gateway (192.168.0.1)  1.810 ms  3.545 ms  5.344 ms
 2  45-164-87-103.digitalsatellite.in (103.87.164.45)  8.718 ms  9.018 ms  12.423 ms
 3  1-164-87-103.digitalsatellite.in (103.87.164.1)  24.489 ms  24.704 ms  25.758 ms
 4  106-164-87-103.digitalsatellite.in (103.87.164.106)  27.206 ms  27.200 ms  28.532 ms
 5  105-164-87-103.digitalsatellite.in (103.87.164.105)  28.523 ms  28.828 ms  29.224 ms
 6  1.6.74.200 (1.6.74.200)  29.853 ms  3.121 ms  7.707 ms
 7  100.67.110.97 (100.67.110.97)  101.240 ms * *
 8  100.67.110.97 (100.67.110.97)  101.264 ms 100.67.110.101 (100.67.110.101)  103.723 ms  104.423 ms
 9  mei-b2-link.telia.net (80.239.128.50)  103.721 ms  107.366 ms  107.667 ms
10  prs-bb3-link.telia.net (62.115.118.94)  132.228 ms  132.245 ms  132.238 ms
11  ldn-bb3-link.telia.net (62.115.123.68)  134.110 ms ldn-bb3-link.telia.net (62.115.134.93)  135.063 ms  136.244 ms
12  * * *
13  jisc-ic-345131-ldn-b4.c.telia.net (62.115.175.131)  126.608 ms  126.627 ms *
14  ae24.londhx-sbr1.ja.net (146.97.35.197)  124.674 ms  125.715 ms  124.184 ms
15  ae29.londpg-sbr2.ja.net (146.97.33.2)  124.279 ms  134.113 ms  132.644 ms
16  ae31.erdiss-sbr2.ja.net (146.97.33.22)  132.865 ms  133.265 ms  128.452 ms
17  ae29.manckh-sbr2.ja.net (146.97.33.42)  131.006 ms  133.253 ms  134.920 ms
18  ae23.mancrh-rbr1.ja.net (146.97.38.42)  129.889 ms  130.097 ms  130.260 ms
19  universityofmanchester.ja.net (146.97.169.2)  130.379 ms * *
20  130.88.249.194 (130.88.249.194)  206.089 ms  207.640 ms  201.473 ms
21  * * *
22  gw-jh.its.manchester.ac.uk (130.88.250.32)  207.698 ms  206.193 ms  208.083 ms
23  eps.its.man.ac.uk (130.88.101.49)  202.048 ms  204.790 ms  203.323 ms
bhushan@bhushan-VivoBook-ASUS-Laptop-X505ZA-X505ZA: $
```

```
bhushan@bhushan-VivoBook-ASUS-Laptop-X505ZA-X505ZA: $ traceroute csail.mit.edu
traceroute to csail.mit.edu (128.30.2.109), 30 hops max, 60 byte packets
 1  _gateway (192.168.0.1)  9.613 ms  9.629 ms  9.725 ms
 2  45-164-87-103.digitalsatellite.in (103.87.164.45)  9.823 ms  9.915 ms  16.629 ms
 3  1-164-87-103.digitalsatellite.in (103.87.164.1)  21.369 ms  25.532 ms  26.834 ms
 4  106-164-87-103.digitalsatellite.in (103.87.164.106)  29.803 ms  35.039 ms  35.803 ms
 5  105-164-87-103.digitalsatellite.in (103.87.164.105)  37.520 ms  39.163 ms  40.087 ms
 6  nsg-static-137.110.71.182.airtel.in (182.71.110.137)  40.440 ms  2.619 ms  2.816 ms
 7  182.79.211.194 (182.79.211.194)  256.639 ms 182.79.243.29 (182.79.243.29)  257.141 ms 182.79.152.227 (182.79.152.227)  257.359 ms
 8  ae58.edge1.LosAngeles6.Level3.net (4.26.0.17)  258.574 ms xe-5-1-0.edge1.LosAngeles6.Level3.net (4.26.0.89)  258.199 ms ae58.edge1.LosAngeles6.Level3.net (4.26.0.17)  258.806 ms
 9  * * *
10  MASSACHUSET.bear1.Boston1.Level3.net (4.53.48.98)  317.981 ms  308.844 ms  316.707 ms
11  dmz-rtr-1-external-rtr-1.mit.edu (18.0.161.17)  301.410 ms  308.234 ms  302.012 ms
12  dmz-rtr-2-dmz-rtr-1-2.mit.edu (18.0.162.6)  318.922 ms dmz-rtr-2-dmz-rtr-1-1.mit.edu (18.0.161.6)  408.954 ms  306.222 ms
13  mitnet.core-1-ext.csail.mit.edu (18.4.7.65)  296.813 ms  301.838 ms  291.971 ms
14  * * *
15  bdr.core-1.csail.mit.edu (128.30.0.246)  302.519 ms  309.859 ms  295.256 ms
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
bhushan@bhushan-VivoBook-ASUS-Laptop-X505ZA-X505ZA: $
```

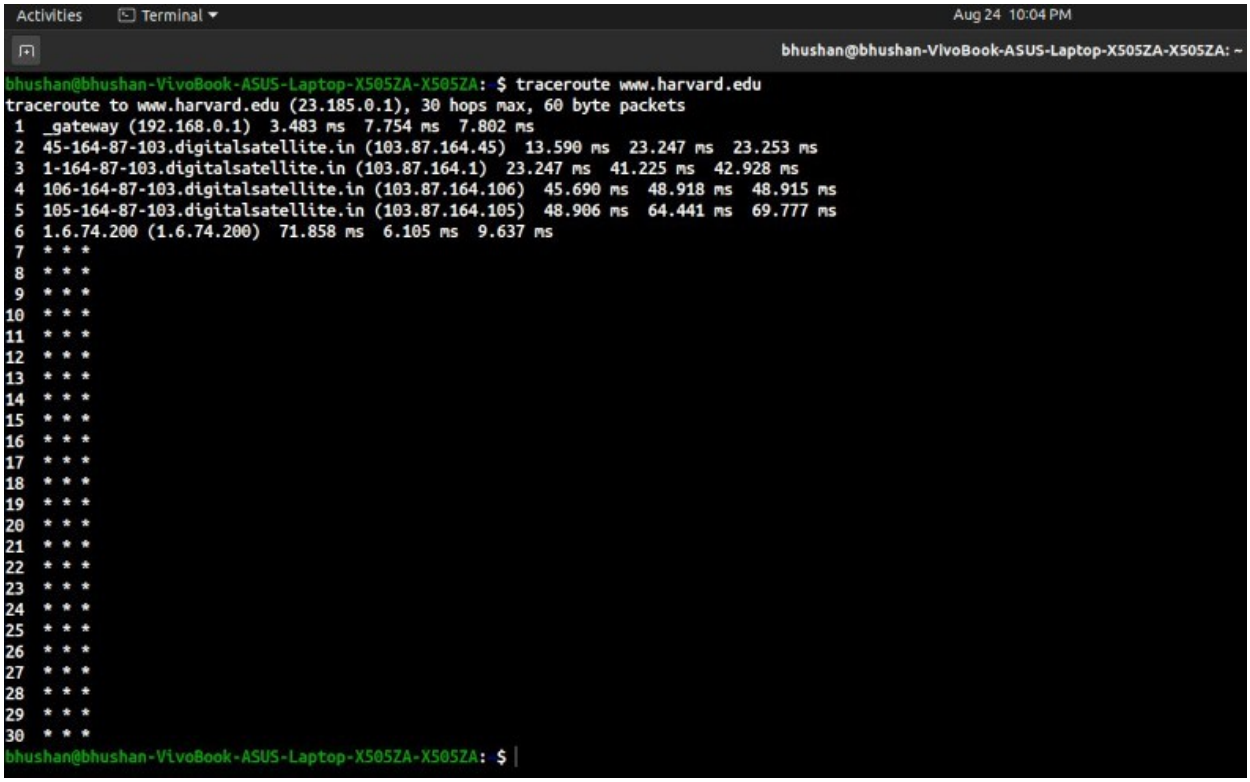
Exercise 2: (Very short.) Use traceroute to trace the route from your computer to math.hws.edu and to www.hws.edu. Explain the difference in the results.

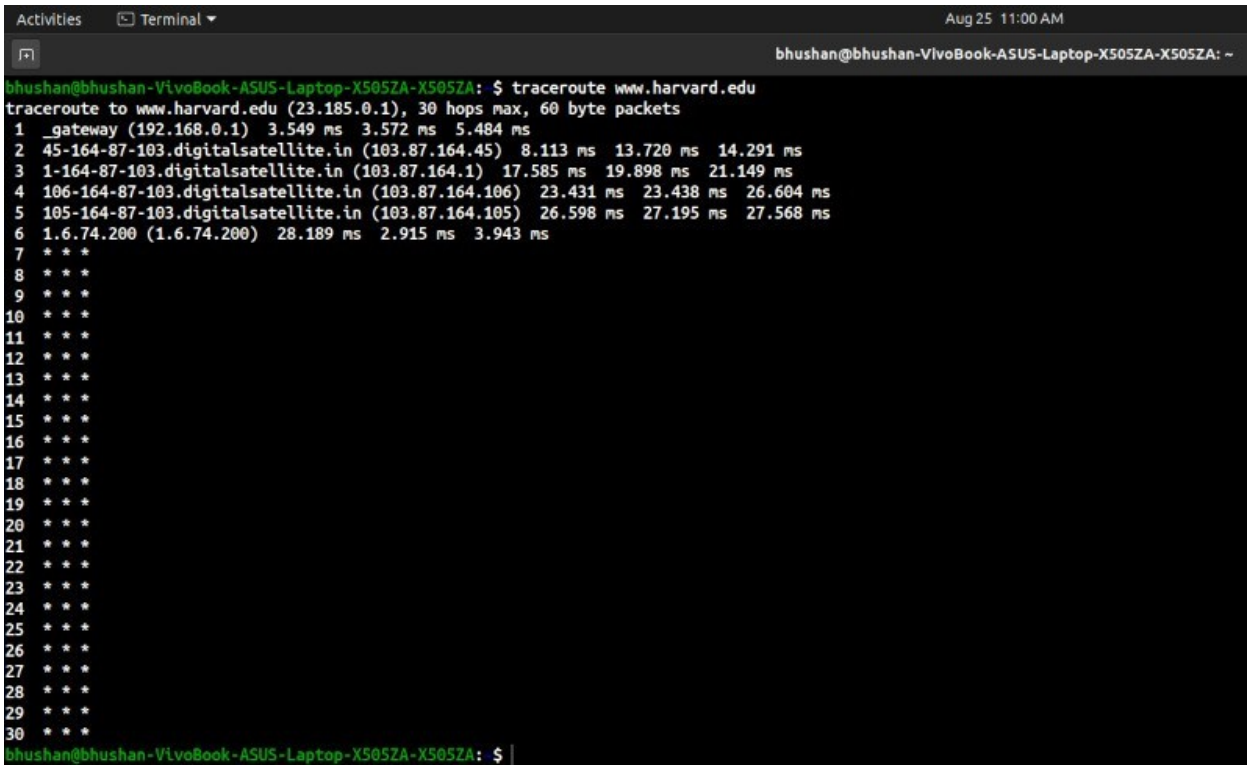
```
bhushan@bhushan-VivoBook-ASUS-Laptop-X505ZA-X505ZA: $ traceroute www.hws.edu
traceroute to www.hws.edu (64.89.145.159), 30 hops max, 60 byte packets
 1  _gateway (192.168.0.1)  4.678 ms  4.700 ms  6.671 ms
 2  45-164-87-103.digitalsatellite.in (103.87.164.45)  10.032 ms  10.114 ms  13.613 ms
 3  1-164-87-103.digitalsatellite.in (103.87.164.1)  19.434 ms  19.807 ms  24.602 ms
 4  106-164-87-103.digitalsatellite.in (103.87.164.106)  29.055 ms  29.057 ms  29.049 ms
 5  105-164-87-103.digitalsatellite.in (103.87.164.105)  31.579 ms  31.811 ms  33.582 ms
 6  nsg-static-137.110.71.182.airtel.in (182.71.110.137)  34.078 ms  4.538 ms  5.390 ms
 7  116.119.35.6 (116.119.35.6)  271.359 ms 182.79.245.69 (182.79.245.69)  269.035 ms 116.119.35.6 (116.119.35.6)  271.805 ms
 8  ae58.edge1.LosAngeles6.Level3.net (4.26.0.17)  272.966 ms xe-9-1-0.edge1.LosAngeles6.Level3.net (4.26.0.61)  273.341 ms xe-5-1-0.edge1.LosAngeles6.Level3.net (4.26.0.89)  272.067 ms
 9  * * *
10  * * *
11  roc1-ar5-xe-0-0-0-0.us.twtelecom.net (35.248.1.158)  273.975 ms  274.230 ms  270.767 ms
12  66-195-65-170.static.ctl.one (66.195.65.170)  286.910 ms  251.231 ms  241.671 ms
13  64.89.144.100 (64.89.144.100)  249.663 ms  288.496 ms  258.712 ms
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
bhushan@bhushan-VivoBook-ASUS-Laptop-X505ZA-X505ZA: $
```



On using traceroute command for www.hws.edu and math.hws.edu, we observe that path from node 1 to node 6 is same in both cases. Node 7 and node 8 are different. Path from node 11 to node 13 is same for both.

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.





Traceroute command was executed for the website www.harvard.edu first on 24 – 08 – 20 and for the second time on 25 – 08 – 20 . The path followed was the same on both occasions. The RTT was different as seen in the images.

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?

Ans : The path from first hop to sixth hop is common for the six hosts for which traceroute is used.

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?

Ans : The number of nodes increases as the distance at which the host lies increases. Thus, number of nodes depends on location. However, this is not true for all cases.

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?

Ans : RTT increases as the number of nodes increases. Thus, latency increases with increase in number of nodes due to increase in queuing delay. This is not true for 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*).

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.

```
bhushan@bhushan-VivoBook-ASUS-Laptop-X505ZA-X505ZA: $ whois amazon.com
   Domain Name: AMAZON.COM
   Registry Domain ID: 281209_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2019-05-07T20:09:37Z
   Creation Date: 1994-11-01T05:00:00Z
   Registry Expiry Date: 2024-10-31T04:00:00Z
   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.P31.DYNECT.NET
   Name Server: NS2.P31.DYNECT.NET
   Name Server: NS3.P31.DYNECT.NET
   Name Server: NS4.P31.DYNECT.NET
   Name Server: PDNS1.ULTRADNS.NET
   Name Server: PDNS6.ULTRADNS.CO.UK
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2020-08-24T13:38:27Z <<<

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

We find information like Domain Name, Domain ID, Registrar URL, Updated Date, Creation and Expiry Date, Registrar Contact details, IANA ID, Name Server and Domain Status.

Using *whois* we can get information about a specific ip address or we can get information regarding a registered domain.

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.

IP address can be found using ping, traceroute or nslookup.

Using the *nslookup* command we can find the ip address from domain name.

```
bhushan@bhushan-VivoBook-ASUS-Laptop-X505ZA-X505ZA: $ nslookup www.spit.ac.in
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.spit.ac.in
Address: 43.252.193.19

bhushan@bhushan-VivoBook-ASUS-Laptop-X505ZA-X505ZA: $
```

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.)

```
bhushan@bhushan-VivoBook-ASUS-Laptop-X505ZA-X505ZA: $ curl ipinfo.io/23.185.0.1
{
  "ip": "23.185.0.1",
  "city": "San Francisco",
  "region": "California",
  "country": "US",
  "loc": "37.7929,-122.4079",
  "org": "AS54113 Fastly",
  "postal": "94108",
  "timezone": "America/Los_Angeles",
  "readme": "https://ipinfo.io/missingauth"
}bhushan@bhushan-VivoBook-ASUS-Laptop-X505ZA-X505ZA: $
```

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.