Name – Chirag Rana
C-batch
Roll No – 47
UID- 2018130043

Data Communication and Computer Networks

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

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).

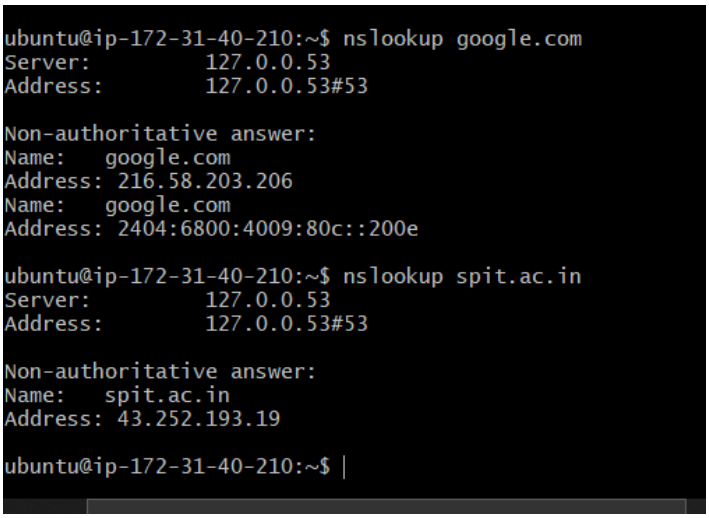
```
ubuntu@ip-172-31-40-210:~$ ping -c 10 -s 100 berkeley.edu
PING berkeley.edu (35.163.72.93) 100(128) bytes of data.
108 bytes from ec2-35-163-72-93.us-west-2.compute.amazonaws.com (35.163.72.93): icmp_seq=1 ttl=35 time=225 ms
108 bytes from ec2-35-163-72-93.us-west-2.compute.amazonaws.com (35.163.72.93): icmp_seq=2 ttl=35 time=224 ms
108 bytes from ec2-35-163-72-93.us-west-2.compute.amazonaws.com (35.163.72.93): icmp_seq=3 ttl=35 time=224 ms
108 bytes from ec2-35-163-72-93.us-west-2.compute.amazonaws.com (35.163.72.93): icmp_seq=4 ttl=35 time=225 ms
108 bytes from ec2-35-163-72-93.us-west-2.compute.amazonaws.com (35.163.72.93): icmp_seq=5 ttl=35 time=224 ms
108 bytes from ec2-35-163-72-93.us-west-2.compute.amazonaws.com (35.163.72.93): icmp_seq=6 ttl=35 time=224 ms
108 bytes from ec2-35-163-72-93.us-west-2.compute.amazonaws.com (35.163.72.93): icmp_seq=7 ttl=35 time=224 ms
108 bytes from ec2-35-163-72-93.us-west-2.compute.amazonaws.com (35.163.72.93): icmp_seq=8 ttl=35 time=225 ms
108 bytes from ec2-35-163-72-93.us-west-2.compute.amazonaws.com (35.163.72.93): icmp_seq=9 ttl=35 time=224 ms
108 bytes from ec2-35-163-72-93.us-west-2.compute.amazonaws.com (35.163.72.93): icmp_seq=10 ttl=35 time=224 ms

--- berkeley.edu ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9009ms
rtt min/avg/max/mdev = 224.832/225.007/225.584/0.475 ms
```

```
ubuntu@ip-172-31-40-210:~$ ping -c 10 -s 100 www.ox.ac.uk
PING www.ox.ac.uk (151.101.66.133) 100(128) bytes of data.
108 bytes from 151.101.66.133 (151.101.66.133): icmp_seq=1 ttl=52 time=1.08 ms
108 bytes from 151.101.66.133 (151.101.66.133): icmp_seq=2 ttl=52 time=1.15 ms
108 bytes from 151.101.66.133 (151.101.66.133): icmp_seq=3 ttl=52 time=1.14 ms
108 bytes from 151.101.66.133 (151.101.66.133): icmp_seq=4 ttl=52 time=1.13 ms
108 bytes from 151.101.66.133 (151.101.66.133): icmp_seq=5 ttl=52 time=1.16 ms
108 bytes from 151.101.66.133 (151.101.66.133): icmp_seq=6 ttl=52 time=1.15 ms
108 bytes from 151.101.66.133 (151.101.66.133): icmp_seq=7 ttl=52 time=1.10 ms
108 bytes from 151.101.66.133 (151.101.66.133): icmp_seq=8 ttl=52 time=1.15 ms
108 bytes from 151.101.66.133 (151.101.66.133): icmp_seq=9 ttl=52 time=1.14 ms
108 bytes from 151.101.66.133 (151.101.66.133): icmp_seq=10 ttl=52 time=1.14 ms

--- www.ox.ac.uk ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9012ms
rtt min/avg/max/mdev = 1.087/1.138/1.162/0.048 ms
```

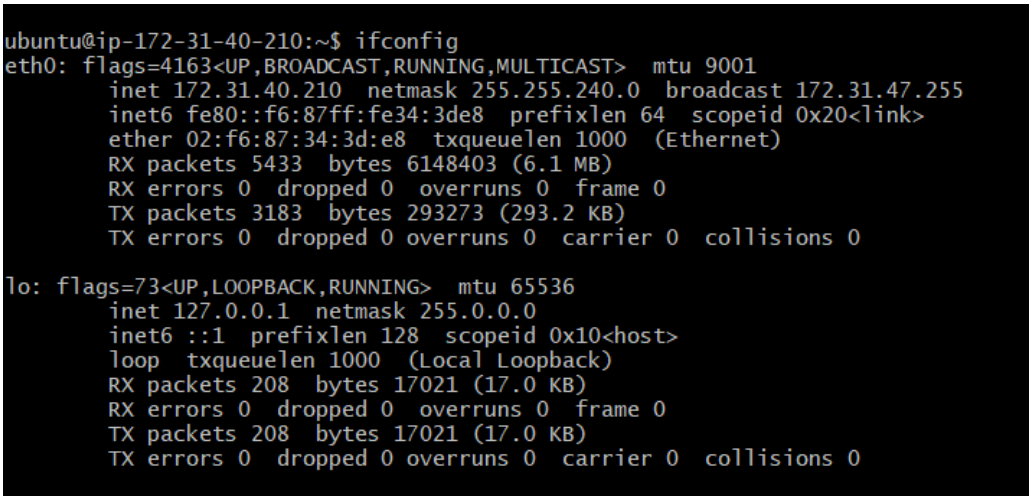
```
ubuntu@ip-172-31-40-210:~$ ping -c 10 -s 100 www.uw.edu
PING www.washington.edu (128.95.155.135) 100(128) bytes of data.
108 bytes from www2.cac.washington.edu (128.95.155.135): icmp_seq=1 ttl=35 time=240 ms
108 bytes from www2.cac.washington.edu (128.95.155.135): icmp_seq=2 ttl=35 time=241 ms
108 bytes from www2.cac.washington.edu (128.95.155.135): icmp_seq=3 ttl=35 time=241 ms
108 bytes from www2.cac.washington.edu (128.95.155.135): icmp_seq=4 ttl=35 time=241 ms
108 bytes from www2.cac.washington.edu (128.95.155.135): icmp_seq=5 ttl=35 time=240 ms
108 bytes from www2.cac.washington.edu (128.95.155.135): icmp_seq=6 ttl=35 time=241 ms
108 bytes from www2.cac.washington.edu (128.95.155.135): icmp_seq=7 ttl=35 time=241 ms
108 bytes from www2.cac.washington.edu (128.95.155.135): icmp_seq=8 ttl=35 time=241 ms
108 bytes from www2.cac.washington.edu (128.95.155.135): icmp_seq=9 ttl=35 time=240 ms
108 bytes from www2.cac.washington.edu (128.95.155.135): icmp_seq=10 ttl=35 time=241 ms

--- www.washington.edu ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9008ms
rtt min/avg/max/mdev = 240.972/241.107/241.902/0.639 ms
```

As seen from the above we see that as the distance from my location to the pinged place location increases the TTL time also increases. Like getting response from www.uk.edu (in United Kingdom) is faster then getting response from www.uw.edu (University of Washington). Hence it can be concluded that distance is a major factor in getting in the response and has good impact on the response time.

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 nslookup 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!!!.)



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.)

```
ubuntu@ip-172-31-40-210:~$ netstat -t -n
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 172.31.40.210:22        49.32.58.139:58083      ESTABLISHED
tcp        0    300 172.31.40.210:22        49.32.58.139:58180      ESTABLISHED
ubuntu@ip-172-31-40-210:~$ netstat -t -n -l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
ubuntu@ip-172-31-40-210:~$
```

```
ubuntu@ip-172-31-40-210:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 ip-172-31-40-210.ap:ssh 49.32.58.139:58083      ESTABLISHED
tcp        0    300 ip-172-31-40-210.ap:ssh 49.32.58.139:58180      ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    32057
/run/user/1000/systemd/notify
unix  3      [ ]         DGRAM                    13869    /run/systemd/notify
unix  2      [ ]         DGRAM                    13881    /run/systemd/journal/syslog
unix  9      [ ]         DGRAM                    13890    /run/systemd/journal/socket
unix  8      [ ]         DGRAM                    14422    /run/systemd/journal/dev-
log
unix  2      [ ]         DGRAM                    17750
unix  3      [ ]         DGRAM                    16245
unix  3      [ ]         STREAM     CONNECTED     17510    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     19129    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     18599    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     21405
unix  3      [ ]         DGRAM                    16107
unix  3      [ ]         DGRAM                    16244
unix  3      [ ]         STREAM     CONNECTED     19027
unix  3      [ ]         STREAM     CONNECTED     14885
unix  3      [ ]         STREAM     CONNECTED     19289
unix  3      [ ]         STREAM     CONNECTED     15320    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     21406
/var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     19026
unix  3      [ ]         STREAM     CONNECTED     17509
unix  3      [ ]         STREAM     CONNECTED     17642
unix  3      [ ]         STREAM     CONNECTED     16187
unix  3      [ ]         STREAM     CONNECTED     19712
/var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     16188    /run/systemd/journal/stdout
unix  3      [ ]         DGRAM                    13870
unix  2      [ ]         DGRAM                    16240
unix  2      [ ]         DGRAM                    15007
unix  3      [ ]         DGRAM                    13871
unix  3      [ ]         DGRAM                    16246
unix  3      [ ]         STREAM     CONNECTED     18953    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     18787    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     19053
/var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     17645    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     18786
unix  3      [ ]         STREAM     CONNECTED     19128
unix  3      [ ]         DGRAM                    16108
unix  2      [ ]         DGRAM                    14887
unix  3      [ ]         STREAM     CONNECTED     19290    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     21048
/var/run/dbus/system_bus_socket
```

```
unix  3      [ ]         STREAM     CONNECTED     18951
unix  2      [ ]         DGRAM                    17522
unix  3      [ ]         STREAM     CONNECTED     18598
unix  2      [ ]         DGRAM                    20311
unix  3      [ ]         DGRAM                    16243
unix  3      [ ]         STREAM     CONNECTED     19028    /run/systemd/journal/stdout
unix  2      [ ]         DGRAM                    14806
unix  3      [ ]         STREAM     CONNECTED     15316    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     19210
unix  3      [ ]         STREAM     CONNECTED     14646
unix  3      [ ]         STREAM     CONNECTED     19211    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     20939
unix  3      [ ]         STREAM     CONNECTED     22598
unix  2      [ ]         DGRAM                    33542
unix  3      [ ]         DGRAM                    14986
unix  3      [ ]         STREAM     CONNECTED     21411
/var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     18328
unix  3      [ ]         STREAM     CONNECTED     21046
/var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     22601
unix  2      [ ]         DGRAM                    31863
unix  3      [ ]         STREAM     CONNECTED     21178
unix  3      [ ]         DGRAM                    17535
unix  3      [ ]         STREAM     CONNECTED     18329
unix  3      [ ]         STREAM     CONNECTED     22594
unix  2      [ ]         DGRAM                    31981
unix  3      [ ]         STREAM     CONNECTED     19052
/var/run/dbus/system_bus_socket
unix  3      [ ]         DGRAM                    32059
unix  3      [ ]         STREAM     CONNECTED     20942    /run/systemd/journal/stdout
unix  3      [ ]         DGRAM                    17533
unix  3      [ ]         STREAM     CONNECTED     21410
unix  3      [ ]         STREAM     CONNECTED     19051
/var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     21371
unix  3      [ ]         STREAM     CONNECTED     21180    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     33735
unix  3      [ ]         STREAM     CONNECTED     31967
unix  3      [ ]         DGRAM                    14987
unix  3      [ ]         STREAM     CONNECTED     21370
unix  2      [ ]         DGRAM                    32013
unix  3      [ ]         STREAM     CONNECTED     19968
unix  3      [ ]         STREAM     CONNECTED     19711
unix  3      [ ]         STREAM     CONNECTED     32708
unix  3      [ ]         STREAM     CONNECTED     21045
unix  3      [ ]         STREAM     CONNECTED     20129    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     22600
unix  3      [ ]         STREAM     CONNECTED     22593
unix  3      [ ]         STREAM     CONNECTED     32707
unix  2      [ ]         DGRAM                    20818
unix  3      [ ]         STREAM     CONNECTED     22599
unix  3      [ ]         STREAM     CONNECTED     19049
unix  3      [ ]         DGRAM                    32058
unix  2      [ ]         DGRAM                    19789
unix  2      [ ]         DGRAM                    19042
unix  3      [ ]         DGRAM                    17532
unix  3      [ ]         STREAM     CONNECTED     31977    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     19050
unix  3      [ ]         STREAM     CONNECTED     33736
unix  3      [ ]         STREAM     CONNECTED     21047
unix  3      [ ]         STREAM     CONNECTED     19970    /run/systemd/journal/stdout
unix  3      [ ]         DGRAM                    17534
unix  3      [ ]         STREAM     CONNECTED     20127
```

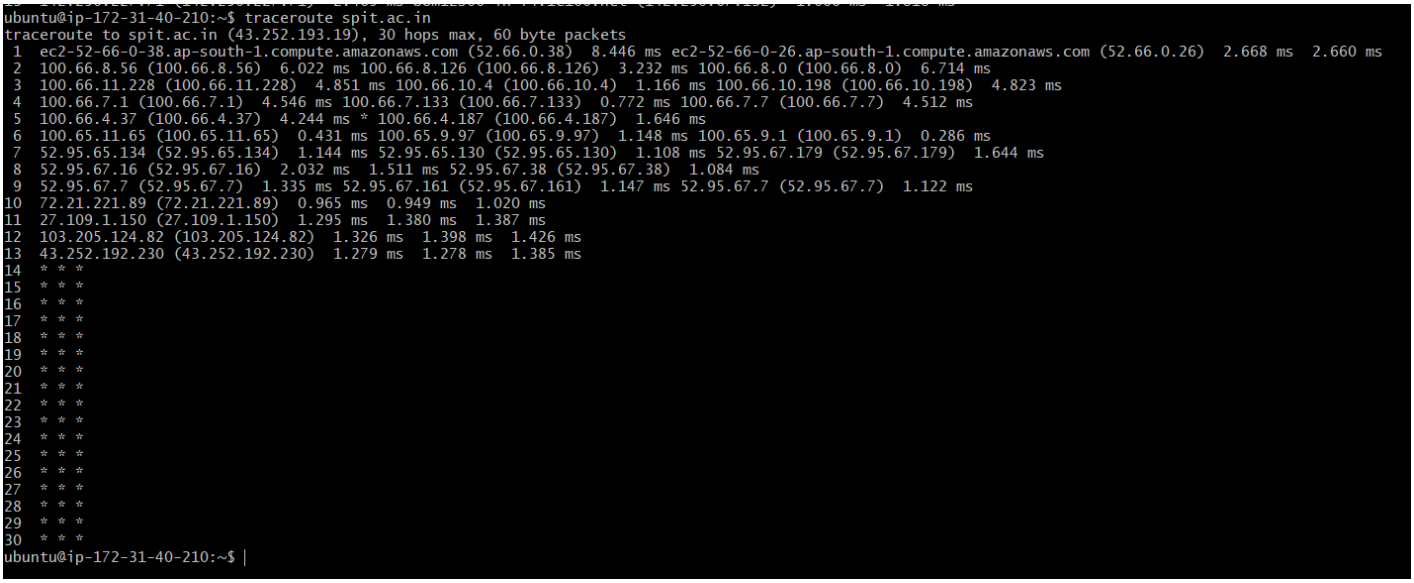
telnet — Telnet is an old program for remote login. It's not used so much for that any more, since it has no security features. But basically, all it does is open a connection to a server and allow server and client to send lines of plain text to each other. It can be used to check that it's possible 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>
```

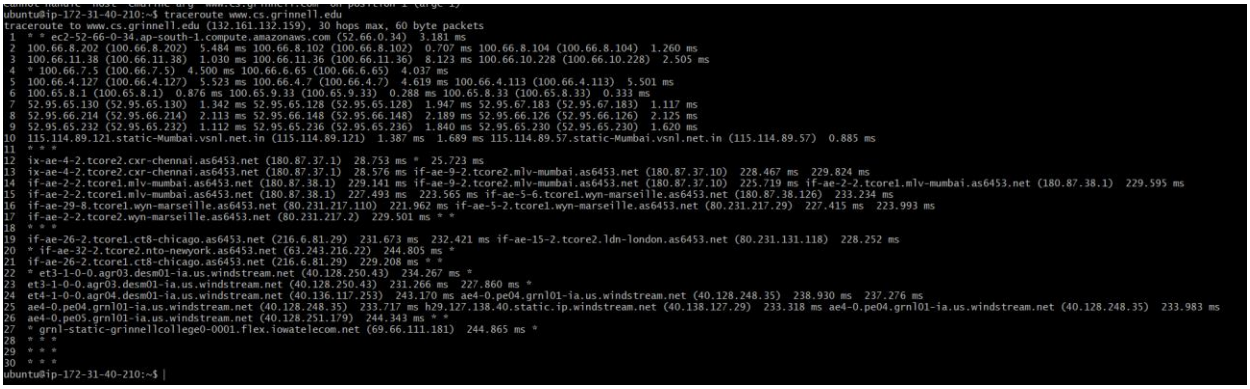


You can specify either a hostname (e.g., `cs.iitb.ac.in`) or an IP address (e.g., `128.105.2.6`).

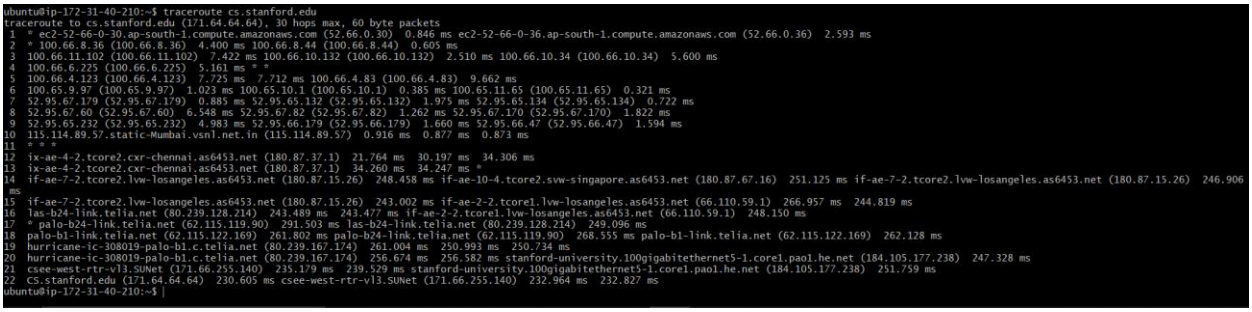
1.2.1 EXPERIMENTS WITH TRACEROUTE

From **your machine** traceroute to the following hosts:

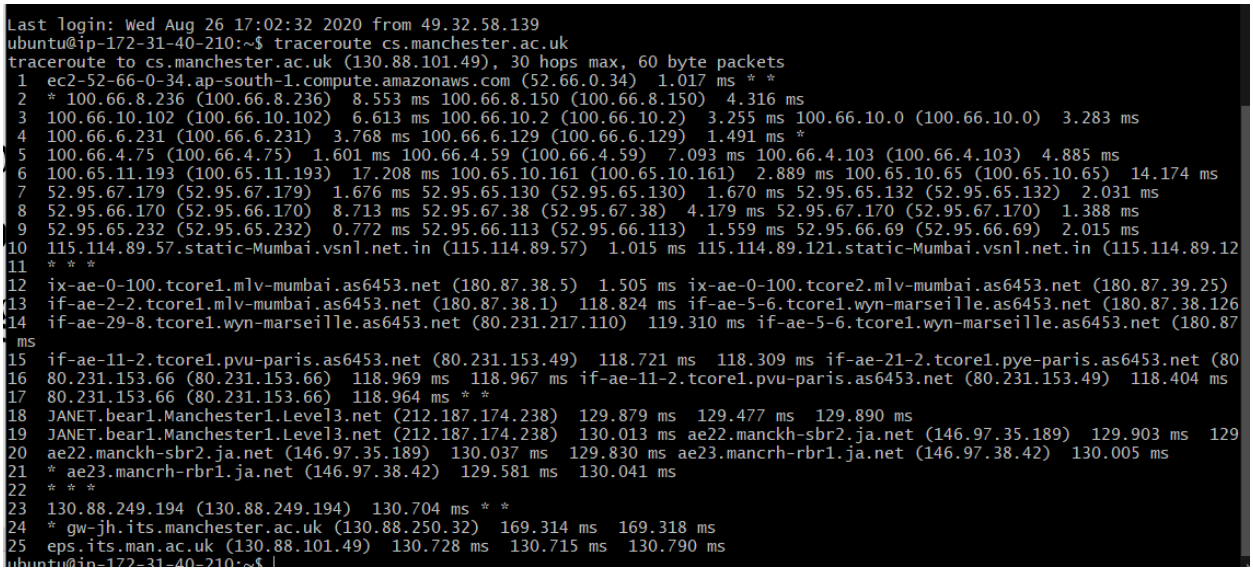
1. www.cs.grinnell.edu



2. cs.stanford.edu



3. cs.manchester.ac.uk



4) cs.standford.edu

```
ubuntu@ip-172-31-40-210:~$ traceroute cs.stanford.edu
traceroute to cs.stanford.edu (171.64.64.64), 30 hops max, 60 byte packets
 1  ec2-52-66-0-36.ap-south-1.compute.amazonaws.com (52.66.0.36)  8.654 ms ec2-52-66-0-32.ap-south-1.compute.amazonaws.com (5
2.66.0.32)  4.166 ms ec2-52-66-0-34.ap-south-1.compute.amazonaws.com (52.66.0.34)  3.290 ms
 2  * 100.66.8.248 (100.66.8.248)  3.643 ms 100.66.8.56 (100.66.8.56)  3.574 ms
 3  100.66.11.160 (100.66.11.160)  1.039 ms 100.66.10.226 (100.66.10.226)  11.292 ms 100.66.10.160 (100.66.10.160)  6.798 ms
 4  100.66.6.231 (100.66.6.231)  1.310 ms 100.66.6.67 (100.66.6.67)  2.712 ms 100.66.6.39 (100.66.6.39)  2.136 ms
 5  100.66.4.205 (100.66.4.205)  2.540 ms 100.66.4.207 (100.66.4.207)  2.605 ms 100.66.4.99 (100.66.4.99)  2.659 ms
 6  100.65.8.65 (100.65.8.65)  1.165 ms 100.65.10.161 (100.65.10.161)  0.393 ms 100.65.9.1 (100.65.9.1)  0.330 ms
 7  52.95.65.134 (52.95.65.134)  1.429 ms 52.95.67.181 (52.95.67.181)  2.103 ms 52.95.65.134 (52.95.65.134)  1.162 ms
 8  52.95.66.192 (52.95.66.192)  2.703 ms 52.95.66.170 (52.95.66.170)  3.423 ms 52.95.67.60 (52.95.67.60)  1.341 ms
 9  52.95.66.91 (52.95.66.91)  1.634 ms 52.95.65.234 (52.95.65.234)  1.766 ms 52.95.66.135 (52.95.66.135)  1.603 ms
10  115.114.89.57.static-Mumbai.vsnl.net.in (115.114.89.57)  0.944 ms  0.809 ms  1.361 ms
11  * * *
12  * * *
13  * ix-ae-4-2.tcore2.cxr-chennai.as6453.net (180.87.37.1)  23.261 ms  18.564 ms
14  if-ae-10-4.tcore2.svw-singapore.as6453.net (180.87.67.16)  245.419 ms if-ae-7-2.tcore2.lvw-losangeles.as6453.net (180.87.
15.26)  249.473 ms  243.383 ms
15  if-ae-7-2.tcore2.lvw-losangeles.as6453.net (180.87.15.26)  250.121 ms  253.403 ms  245.067 ms
16  las-b24-link.telia.net (80.239.128.214)  255.558 ms  247.441 ms if-ae-2-2.tcore1.lvw-losangeles.as6453.net (66.110.59.1)
 256.808 ms
17  * palo-b24-link.telia.net (62.115.119.90)  264.747 ms *
18  palo-b1-link.telia.net (62.115.122.169)  272.189 ms palo-b24-link.telia.net (62.115.119.90)  258.990 ms palo-b1-link.teli
a.net (62.115.122.169)  260.775 ms
19  palo-b1-link.telia.net (62.115.122.169)  259.603 ms hurricane-ic-308019-palo-b1.c.telia.net (80.239.167.174)  254.891 ms
 254.811 ms
20  stanford-university.100gigabitethernet5-1.core1.pao1.he.net (184.105.177.238)  249.299 ms  261.208 ms hurricane-ic-308019
-palo-b1.c.telia.net (80.239.167.174)  247.834 ms
21  stanford-university.100gigabitethernet5-1.core1.pao1.he.net (184.105.177.238)  249.606 ms csee-west-rtr-vl3.SUNet (171.66
.255.140)  239.063 ms  241.848 ms
22  * CS.stanford.edu (171.64.64.64)  236.606 ms csee-west-rtr-vl3.SUNet (171.66.255.140)  243.417 ms
ubuntu@ip-172-31-40-210:~$
```

5) csail.mit.edu

```
ubuntu@ip-172-31-40-210:~$ traceroute csail.mit.edu
traceroute to csail.mit.edu (128.30.2.109), 30 hops max, 60 byte packets
 1  ec2-52-66-0-34.ap-south-1.compute.amazonaws.com (52.66.0.34)  1.750 ms ec2-52-66-0-28.ap-south-1.compute.amazonaws.com (5
2.66.0.28)  3.044 ms ec2-52-66-0-38.ap-south-1.compute.amazonaws.com (52.66.0.38)  3.482 ms
 2  100.66.8.250 (100.66.8.250)  5.049 ms 100.66.8.210 (100.66.8.210)  5.824 ms 100.66.8.162 (100.66.8.162)  4.112 ms
 3  100.66.11.6 (100.66.11.6)  5.695 ms 100.66.10.194 (100.66.10.194)  2.141 ms 100.66.11.128 (100.66.11.128)  7.850 ms
 4  100.66.7.227 (100.66.7.227)  2.698 ms * 100.66.6.35 (100.66.6.35)  7.118 ms
 5  * 100.66.4.65 (100.66.4.65)  5.208 ms 100.66.4.207 (100.66.4.207)  1.568 ms
 6  100.65.9.161 (100.65.9.161)  0.360 ms 100.65.11.65 (100.65.11.65)  0.265 ms 100.65.11.1 (100.65.11.1)  0.365 ms
 7  52.95.65.132 (52.95.65.132)  2.043 ms 52.95.67.181 (52.95.67.181)  1.222 ms 52.95.67.183 (52.95.67.183)  1.432 ms
 8  52.95.66.60 (52.95.66.60)  1.912 ms 52.95.66.104 (52.95.66.104)  1.998 ms 52.95.66.214 (52.95.66.214)  2.471 ms
 9  52.95.66.135 (52.95.66.135)  3.158 ms 52.95.65.226 (52.95.65.226)  1.272 ms 52.95.66.91 (52.95.66.91)  3.219 ms
10  115.114.89.57.static-Mumbai.vsnl.net.in (115.114.89.57)  0.884 ms  0.875 ms  0.937 ms
11  * * *
12  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net (180.87.38.5)  1.729 ms ix-ae-0-100.tcore2.mlv-mumbai.as6453.net (180.87.39.25)
 1.493 ms ix-ae-0-100.tcore1.mlv-mumbai.as6453.net (180.87.38.5)  1.697 ms
13  if-ae-2-2.tcore1.mlv-mumbai.as6453.net (180.87.38.1)  192.792 ms  192.544 ms *
14  * * *
15  * * *
16  * * *
17  if-ae-8-49.tcore2.nto-newyork.as6453.net (216.6.81.34)  188.160 ms if-ae-4-2.tcore2.n0v-newyork.as6453.net (80.231.131.15
3)  198.381 ms if-ae-12-2.tcore1.n75-newyork.as6453.net (66.110.96.5)  193.881 ms
18  if-ae-7-5.tcore1.nto-newyork.as6453.net (63.243.128.141)  197.762 ms if-ae-12-2.tcore1.n75-newyork.as6453.net (66.110.96.
5)  193.873 ms  193.599 ms
19  66.110.96.142 (66.110.96.142)  194.790 ms be-10390-cr02.newyork.ny.ibone.comcast.net (68.86.83.89)  193.787 ms 66.110.96.
138 (66.110.96.138)  188.218 ms
20  66.110.96.134 (66.110.96.134)  192.577 ms be-10390-cr02.newyork.ny.ibone.comcast.net (68.86.83.89)  193.899 ms 66.110.96.
150 (66.110.96.150)  190.412 ms
21  66.110.96.134 (66.110.96.134)  192.659 ms be-10390-cr02.newyork.ny.ibone.comcast.net (68.86.83.89)  194.892 ms 66.110.96.
130 (66.110.96.130)  192.969 ms
22  96.110.42.6 (96.110.42.6)  193.013 ms ae0-0-eg-bstpmall74w.boston.ma.boston.comcast.net (68.86.238.34)  193.324 ms  193.2
53 ms
23  ae0-0-eg-bstpmall74w.boston.ma.boston.comcast.net (68.86.238.34)  238.939 ms  223.959 ms  218.143 ms
24  50-201-57-174-static.hfc.comcastbusiness.net (50.201.57.174)  195.003 ms  193.030 ms  193.104 ms
25  dmz-rtr-1-external-rtr-3.mit.edu (18.0.161.13)  193.231 ms  193.140 ms ae0-0-eg-bstpmall74w.boston.ma.boston.comcast.net
(68.86.238.34)  197.832 ms
26  dmz-rtr-1-external-rtr-3.mit.edu (18.0.161.13)  197.497 ms  196.919 ms mitnet.core-1-ext.csail.mit.edu (18.4.7.65)  193.2
40 ms
27  dmz-rtr-1-external-rtr-3.mit.edu (18.0.161.13)  197.437 ms mitnet.core-1-ext.csail.mit.edu (18.4.7.65)  195.156 ms  195.6
98 ms
28  mitnet.core-1-ext.csail.mit.edu (18.4.7.65)  197.665 ms  195.824 ms bdr.core-1.csail.mit.edu (128.30.0.246)  194.658 ms
29  * bdr.core-1.csail.mit.edu (128.30.0.246)  195.155 ms *
30  * bdr.core-1.csail.mit.edu (128.30.0.246)  197.965 ms *
ubuntu@ip-172-31-40-210:~$
```

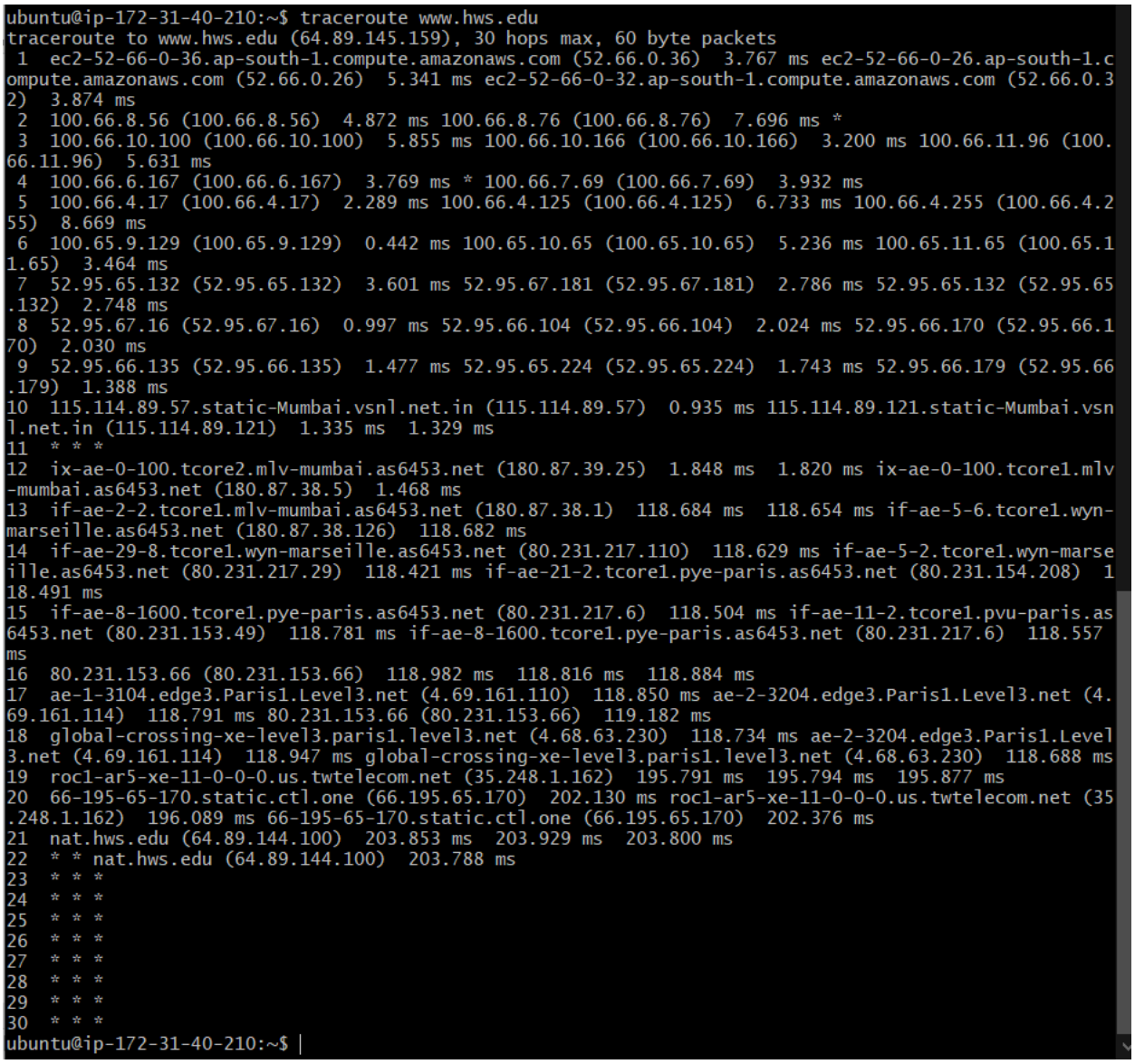
Store the output of each traceroute command in a separate file named `traceroute_HOSTNAME.log`, replacing `HOSTNAME` with the hostname for end-host you pinged (e.g., `traceroute_ee.iitb.ac.in.log`).

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

maths.hws.edu

```
ubuntu@ip-172-31-40-210:~$ traceroute math.hws.edu
traceroute to math.hws.edu (64.89.144.237), 30 hops max, 60 byte packets
 1  ec2-52-66-0-28.ap-south-1.compute.amazonaws.com (52.66.0.28)  4.121 ms ec2-52-66-0-36.ap-south-1.c
ompute.amazonaws.com (52.66.0.36)  7.484 ms  7.475 ms
 2  100.66.8.26 (100.66.8.26)  0.717 ms 100.66.8.22 (100.66.8.22)  1.703 ms 100.66.8.42 (100.66.8.42)
 6.522 ms
 3  100.66.10.162 (100.66.10.162)  7.414 ms  7.396 ms 100.66.10.198 (100.66.10.198)  6.549 ms
 4  100.66.7.135 (100.66.7.135)  8.430 ms 100.66.7.195 (100.66.7.195)  4.880 ms 100.66.7.99 (100.66.7.
99)  3.572 ms
 5  * 100.66.4.103 (100.66.4.103)  3.240 ms 100.66.4.207 (100.66.4.207)  4.688 ms
 6  100.65.11.225 (100.65.11.225)  0.510 ms 100.65.9.33 (100.65.9.33)  0.342 ms 100.65.11.129 (100.65.
11.129)  0.327 ms
 7  52.95.65.132 (52.95.65.132)  35.787 ms 52.95.65.128 (52.95.65.128)  35.769 ms 52.95.67.177 (52.95.
67.177)  35.239 ms
 8  52.95.67.170 (52.95.67.170)  1.847 ms 52.95.67.148 (52.95.67.148)  1.559 ms 52.95.66.170 (52.95.66
.170)  2.024 ms
 9  52.95.65.224 (52.95.65.224)  1.513 ms 52.95.65.234 (52.95.65.234)  1.357 ms 52.95.66.69 (52.95.66.
69)  1.557 ms
10  115.114.89.57.static-Mumbai.vsnl.net.in (115.114.89.57)  0.934 ms 115.114.89.121.static-Mumbai.vsn
l.net.in (115.114.89.121)  1.522 ms  1.449 ms
11  * * *
12  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net (180.87.38.5)  1.519 ms  1.415 ms  1.520 ms
13  if-ae-2-2.tcore1.mlv-mumbai.as6453.net (180.87.38.1)  118.648 ms  118.723 ms  118.684 ms
14  if-ae-8-1600.tcore1.pye-paris.as6453.net (80.231.217.6)  118.501 ms if-ae-5-2.tcore1.wyn-marseille
.as6453.net (80.231.217.29)  118.710 ms  137.561 ms
15  if-ae-11-2.tcore1.pvu-paris.as6453.net (80.231.153.49)  118.888 ms  119.651 ms if-ae-8-1600.tcore1
.pye-paris.as6453.net (80.231.217.6)  118.560 ms
16  if-ae-11-2.tcore1.pvu-paris.as6453.net (80.231.153.49)  119.786 ms *  119.645 ms
17  ae-1-3104.edge3.Paris1.Level3.net (4.69.161.110)  118.919 ms  118.958 ms  118.891 ms
18  ae-2-3204.edge3.Paris1.Level3.net (4.69.161.114)  118.981 ms ae-1-3104.edge3.Paris1.Level3.net (4.
69.161.110)  118.999 ms  119.900 ms
19  global-crossing-xe-level3.paris1.level3.net (4.68.63.230)  119.021 ms roc1-ar5-xe-11-0-0-0.us.twte
lecom.net (35.248.1.162)  196.040 ms global-crossing-xe-level3.paris1.level3.net (4.68.63.230)  118.94
2 ms
20  66-195-65-170.static.ctl.one (66.195.65.170)  202.049 ms roc1-ar5-xe-11-0-0-0.us.twtelecom.net (35
.248.1.162)  196.003 ms 66-195-65-170.static.ctl.one (66.195.65.170)  202.035 ms
21  66-195-65-170.static.ctl.one (66.195.65.170)  201.956 ms nat.hws.edu (64.89.144.100)  203.744 ms
203.876 ms
22  nat.hws.edu (64.89.144.100)  203.954 ms *  203.948 ms
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
ubuntu@ip-172-31-40-210:~$
```

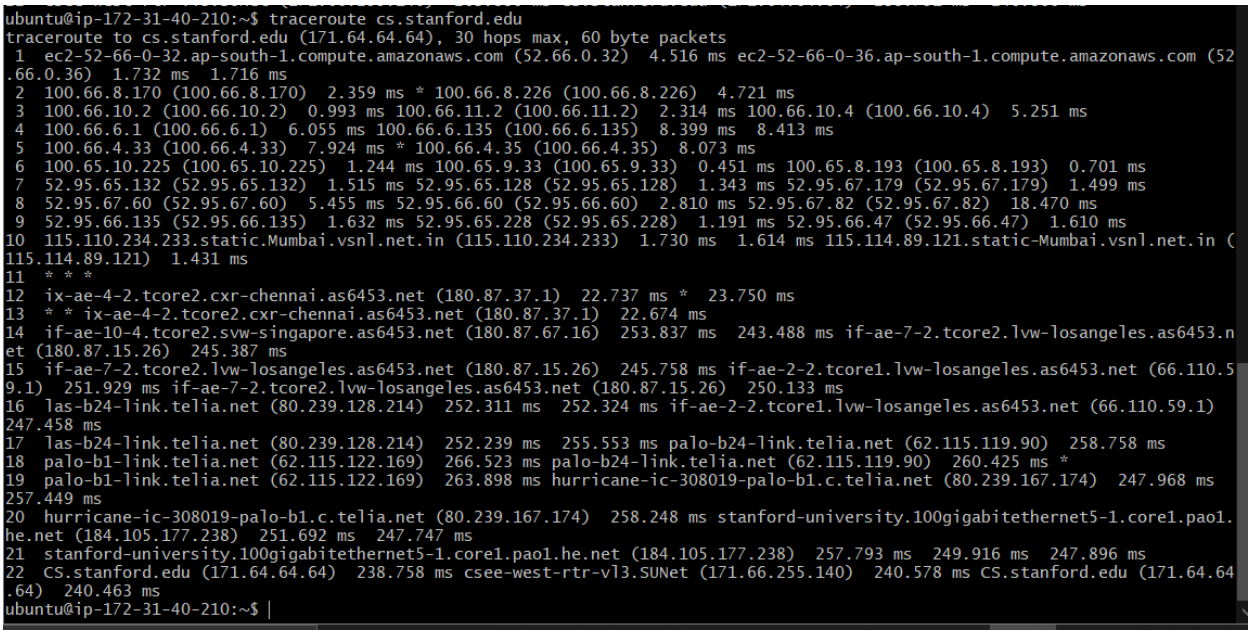
www.hws.edu



The first row shows that the process of route tracing has started as the last column shows the Default Gateway of the user. The next three rows in both the cases are similar as the route is being

traced starting from the ISP (Internet service provider) of the user. The next few rows, after which the tracing reaches the common IP address of 66.195.65.170 and then math.hws.edu [64.89.144.100], clearly show that the route is completely different after crossing the ISP for both the cases. A domain name might have multiple IP addresses associated. If this is the case, multiple traces may access two or more IP addresses. This will yield trace paths that differ from one another, even if the origin and destinations are the same. Domains may also use multiple servers for its subdomains. Tracing the path to the base domain might result in a completely different path when tracing to the subdomain. A URL with the **www** prefix is technically a subdomain, so it's possible that traces to **example.com** and **www.example.com** f ollow two very different paths.

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.



```
ubuntu@ip-172-31-40-210:~$ traceroute csail.mit.edu
traceroute to csail.mit.edu (128.30.2.109), 30 hops max, 60 byte packets
 1  ec2-52-66-0-26.ap-south-1.compute.amazonaws.com (52.66.0.26)  2.630 ms ec2-52-66-0-24.ap-south-1.compute.amazonaws.com (52
.66.0.24)  8.243 ms ec2-52-66-0-38.ap-south-1.compute.amazonaws.com (52.66.0.38)  3.831 ms
 2  * * 100.66.8.52 (100.66.8.52)  4.376 ms
 3  100.66.11.194 (100.66.11.194)  7.082 ms 100.66.11.70 (100.66.11.70)  5.042 ms 100.66.11.196 (100.66.11.196)  8.971 ms
 4  100.66.6.197 (100.66.6.197)  3.300 ms 100.66.6.37 (100.66.6.37)  7.982 ms 100.66.6.69 (100.66.6.69)  6.777 ms
 5  100.66.4.119 (100.66.4.119)  5.384 ms 100.66.4.91 (100.66.4.91)  8.147 ms 100.66.4.175 (100.66.4.175)  2.713 ms
 6  100.65.8.1 (100.65.8.1)  5.847 ms 100.65.11.129 (100.65.11.129)  0.304 ms 100.65.8.65 (100.65.8.65)  0.474 ms
 7  * 52.95.65.130 (52.95.65.130)  1.701 ms *
 8  52.95.67.126 (52.95.67.126)  1.125 ms * 52.95.66.192 (52.95.66.192)  9.715 ms
 9  52.95.65.234 (52.95.65.234)  0.906 ms 52.95.66.179 (52.95.66.179)  1.511 ms 52.95.66.113 (52.95.66.113)  1.529 ms
10  115.114.89.57.static-Mumbai.vsnl.net.in (115.114.89.57)  0.875 ms 115.114.89.121.static-Mumbai.vsnl.net.in (115.114.89.121
)  1.728 ms 115.114.89.57.static-Mumbai.vsnl.net.in (115.114.89.57)  0.988 ms
11  * * *
12  ix-ae-0-100.tcore2.mlv-mumbai.as6453.net (180.87.39.25)  1.643 ms ix-ae-0-100.tcore1.mlv-mumbai.as6453.net (180.87.38.5)
1.622 ms  1.682 ms
13  if-ae-2-2.tcore1.mlv-mumbai.as6453.net (180.87.38.1)  192.672 ms  194.074 ms if-ae-5-6.tcore1.wyn-marseille.as6453.net (18
0.87.38.126)  196.821 ms
14  if-ae-29-8.tcore1.wyn-marseille.as6453.net (80.231.217.110)  199.818 ms if-ae-5-2.tcore1.wyn-marseille.as6453.net (80.231.
217.29)  190.075 ms if-ae-5-6.tcore1.wyn-marseille.as6453.net (180.87.38.126)  197.097 ms
15  if-ae-2-2.tcore2.wyn-marseille.as6453.net (80.231.217.2)  196.376 ms if-ae-9-2.tcore2.l78-london.as6453.net (80.231.200.14
)  194.827 ms  195.358 ms
16  if-ae-9-2.tcore2.l78-london.as6453.net (80.231.200.14)  194.829 ms  194.773 ms if-ae-8-49.tcore2.nto-newyork.as6453.net (2
16.6.81.34)  193.696 ms
17  if-ae-8-49.tcore2.nto-newyork.as6453.net (216.6.81.34)  194.971 ms if-ae-4-2.tcore2.n0v-newyork.as6453.net (80.231.131.158
)  199.602 ms if-ae-32-2.tcore2.nto-newyork.as6453.net (63.243.216.22)  190.089 ms
18  if-ae-2-2.tcore1.n0v-newyork.as6453.net (216.6.90.21)  192.371 ms  192.953 ms if-ae-12-2.tcore1.n75-newyork.as6453.net (66
.110.96.5)  190.093 ms
19  be-10390-cr02.newyork.ny.ibone.comcast.net (68.86.83.89)  193.968 ms  195.123 ms if-ae-12-2.tcore1.n75-newyork.as6453.net
(66.110.96.5)  191.037 ms
20  be-10390-cr02.newyork.ny.ibone.comcast.net (68.86.83.89)  195.476 ms  195.851 ms if-ae-9-2.tcore1.n75-newyork.as6453.net (
63.243.128.122)  193.218 ms
21  be-10390-cr02.newyork.ny.ibone.comcast.net (68.86.83.89)  197.786 ms  196.744 ms  199.715 ms
22  96.110.42.14 (96.110.42.14)  193.901 ms  194.901 ms be-1402-cs04.newyork.ny.ibone.comcast.net (96.110.38.45)  196.367 ms
23  ae0-0-eg-bstpmal174w.boston.ma.boston.comcast.net (68.86.238.34)  195.329 ms  195.322 ms  195.268 ms
24  ae0-0-eg-bstpmal174w.boston.ma.boston.comcast.net (68.86.238.34)  197.575 ms dmz-rtr-1-external-rtr-3.mit.edu (18.0.161.13
)  192.890 ms  192.861 ms
25  dmz-rtr-1-external-rtr-3.mit.edu (18.0.161.13)  192.999 ms dmz-rtr-2-dmz-rtr-1-2.mit.edu (18.0.162.6)  193.065 ms dmz-rtr-
1-external-rtr-3.mit.edu (18.0.161.13)  194.924 ms
26  dmz-rtr-2-dmz-rtr-1-2.mit.edu (18.0.162.6)  192.964 ms mitnet.core-1-ext.csail.mit.edu (18.4.7.65)  193.281 ms dmz-rtr-2-d
mz-rtr-1-2.mit.edu (18.0.162.6)  195.125 ms
27  mitnet.core-1-ext.csail.mit.edu (18.4.7.65)  193.772 ms  193.231 ms dmz-rtr-2-dmz-rtr-1-2.mit.edu (18.0.162.6)  197.326 ms
28  dmz-rtr-2-dmz-rtr-1-2.mit.edu (18.0.162.6)  197.559 ms bdr.core-1.csail.mit.edu (128.30.0.246)  195.268 ms mitnet.core-1-e
xt.csail.mit.edu (18.4.7.65)  195.772 ms
29  bdr.core-1.csail.mit.edu (128.30.0.246)  197.059 ms * *
30  bdr.core-1.csail.mit.edu (128.30.0.246)  204.772 ms  204.759 ms  204.745 ms
ubuntu@ip-172-31-40-210:~$
```

Questions About Paths

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

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

   Yes, the tracerouting follows a particular path from the user's IP address through the IP addresses of the ISP and then the path really depends on which access point is ready to respond

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

   Yes , because if the distance between the location of the user and that of the destination url is more, then more hops will be required in order to reach the destination as more number of access points will be used for routing and the greater the number of access points involved, the greater are the chances of access points failing to respond and similarly for searching the alternative optimal path towards the destination.

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

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

WHOIS

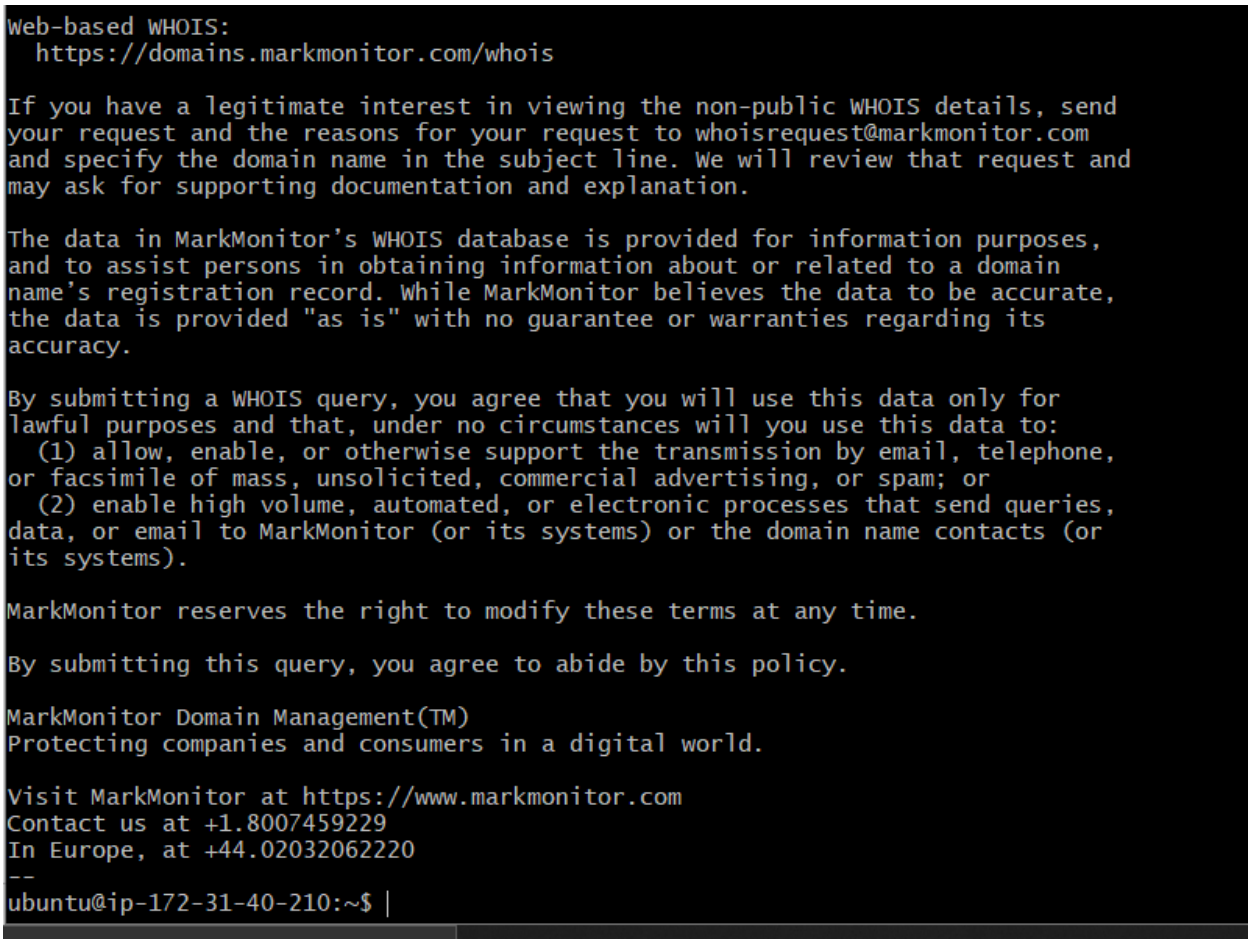
Whois — The *whois* command can give detailed information about domain names and IP addresses. If it is not installed on the computers then install it with command sudo apt-get install whois in.

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

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

```
ubuntu@ip-172-31-40-210:~$ whois google.com
   Domain Name: GOOGLE.COM
   Registry Domain ID: 2138514_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2019-09-09T15:39:04Z
   Creation Date: 1997-09-15T04:00:00Z
   Registry Expiry Date: 2028-09-14T04:00:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2083895740
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: NS1.GOOGLE.COM
   Name Server: NS2.GOOGLE.COM
   Name Server: NS3.GOOGLE.COM
   Name Server: NS4.GOOGLE.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2020-08-28T09:49:28Z <<<

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

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

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

```
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability.  VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: google.com
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-09-09T08:39:04-0700
Creation Date: 1997-09-15T00:00:00-0700
Registrar Registration Expiration Date: 2028-09-13T00:00:00-0700
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895770
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Registrant Organization: Google LLC
Registrant State/Province: CA
Registrant Country: US
Registrant Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Admin Organization: Google LLC
Admin State/Province: CA
Admin Country: US
Admin Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Tech Organization: Google LLC
Tech State/Province: CA
Tech Country: US
Tech Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Name Server: ns1.google.com
Name Server: ns3.google.com
Name Server: ns2.google.com
Name Server: ns4.google.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2020-08-28T02:41:24-0700 <<<

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

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

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



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

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

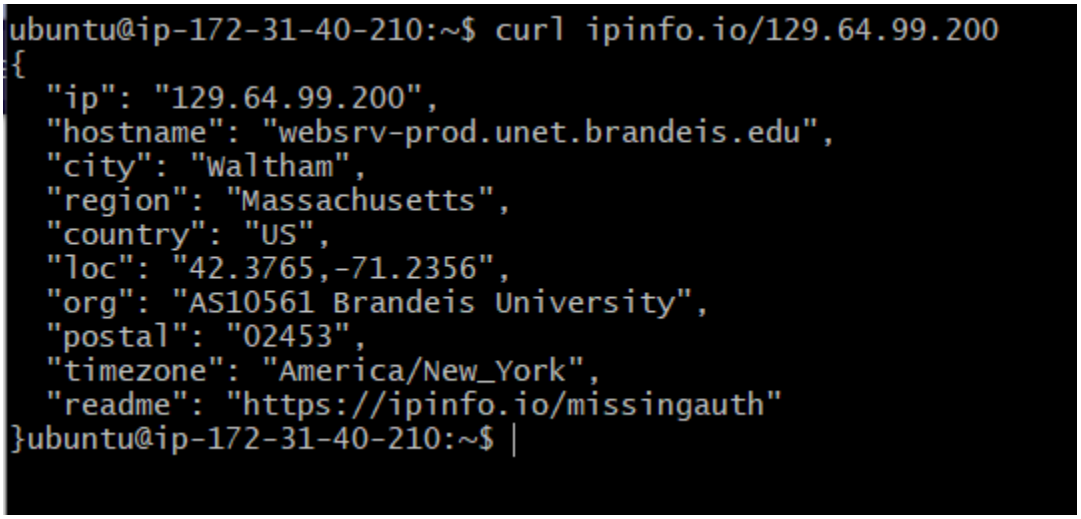
Geolocation — A geolocation service tries to tell, approximately, where a given IP address is located physically. They can't be completely accurate—but they probably get at least the country right most of the time.

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

curl ipinfo.io/129.64.99.200

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

Screenshot:



Conclusion:

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