Name: Bhargavi Poyekar

UID: 2018130040

Batch- C

Date: 14/08/2020

CEL 51, DCCN, Monsoon 2020

Lab 2: Basic Network Utilities

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

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

Some Basic command line Networking utilities

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

ping — The command ping <host> sends a series of packets and expects to receieve a response to each packet. When a return packet is received, ping reports the round trip time (the time between sending the packet and receiving the response). Some routers and firewalls block ping requests, so you might get no reponse at all. Ping can be used to check whether a computer is up and running, to measure network delay time, and to check for dropped packets

indicating network congestion. Note that <host> can be either a domain name or an IP address. By default, ping will send a packet every second indefinitely; stop it with Control-C

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

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

The syntax in Windows is:

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

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

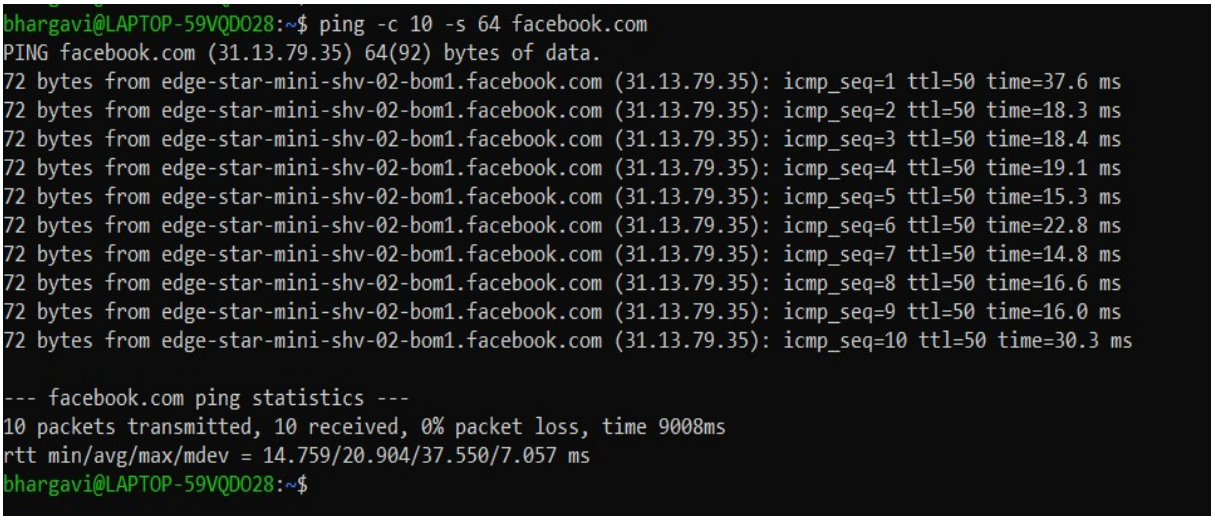
To save the output from ping to a file, include a greater than symbol and a file name at the end of the command. For example:

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

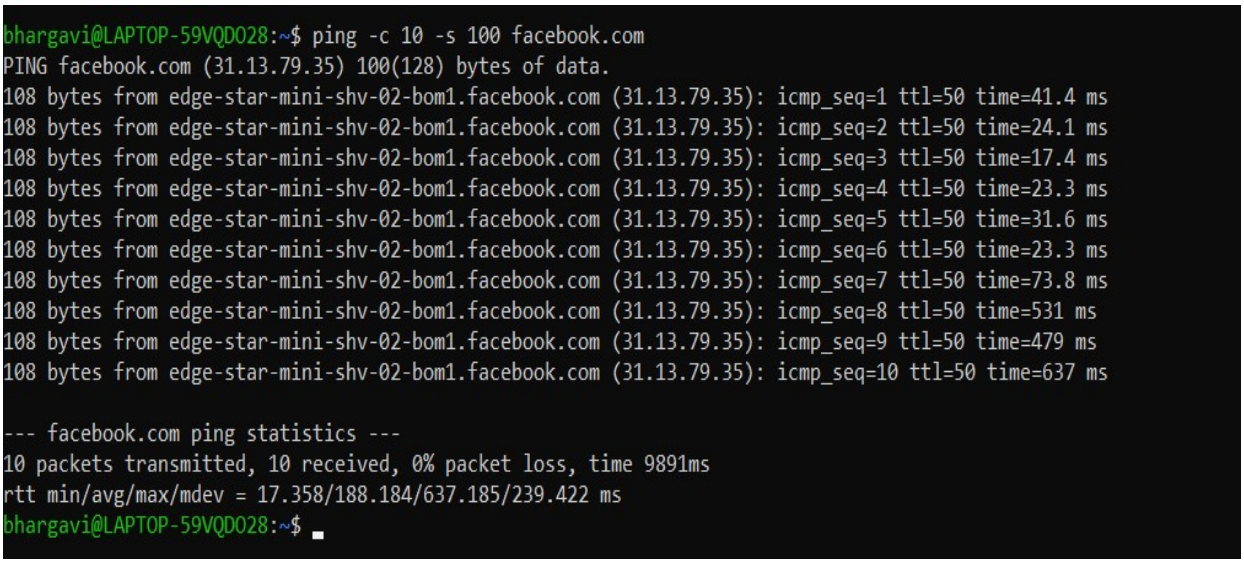
EXPERIMENTS WITH PING

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

    - 64 bytes



    - 100 bytes



- 500 bytes

```
bhargavi@LAPTOP-59VQDO28:~$ ping -c 10 -s 500 facebook.com
PING facebook.com (31.13.79.35) 500(528) bytes of data.
508 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=1 ttl=50 time=25.2 ms
508 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=2 ttl=50 time=57.0 ms
508 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=3 ttl=50 time=21.4 ms
508 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=4 ttl=50 time=22.7 ms
508 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=5 ttl=50 time=23.3 ms
508 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=6 ttl=50 time=20.7 ms
508 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=7 ttl=50 time=23.3 ms
508 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=8 ttl=50 time=30.4 ms
508 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=9 ttl=50 time=19.7 ms
508 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=10 ttl=50 time=20.8 ms

--- facebook.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9009ms
rtt min/avg/max/mdev = 19.683/26.450/56.986/10.580 ms
bhargavi@LAPTOP-59VQDO28:~$
```

- 1000 bytes

```
bhargavi@LAPTOP-59VQDO28:~$ ping -c 10 -s 1000 facebook.com
PING facebook.com (31.13.79.35) 1000(1028) bytes of data.
1008 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=1 ttl=50 time=27.0 ms
1008 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=2 ttl=50 time=32.6 ms
1008 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=3 ttl=50 time=26.3 ms
1008 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=4 ttl=50 time=27.4 ms
1008 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=5 ttl=50 time=24.9 ms
1008 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=6 ttl=50 time=74.2 ms
1008 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=7 ttl=50 time=32.6 ms
1008 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=8 ttl=50 time=28.1 ms
1008 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=9 ttl=50 time=29.4 ms
1008 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=10 ttl=50 time=23.4 ms

--- facebook.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9009ms
rtt min/avg/max/mdev = 23.444/32.583/74.169/14.142 ms
bhargavi@LAPTOP-59VQDO28:~$
```

- 1400 bytes

```
bhargavi@LAPTOP-59VQDO28:~$ ping -c 10 -s 1400 facebook.com
PING facebook.com (31.13.79.35) 1400(1428) bytes of data.
1408 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=1 ttl=50 time=27.8 ms
1408 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=2 ttl=50 time=76.1 ms
1408 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=3 ttl=50 time=32.6 ms
1408 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=4 ttl=50 time=29.5 ms
1408 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=5 ttl=50 time=142 ms
1408 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=6 ttl=50 time=59.6 ms
1408 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=7 ttl=50 time=125 ms
1408 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=8 ttl=50 time=36.3 ms
1408 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=9 ttl=50 time=39.2 ms
1408 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=10 ttl=50 time=39.8 ms

--- facebook.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9007ms
rtt min/avg/max/mdev = 27.816/60.792/141.986/39.119 ms
bhargavi@LAPTOP-59VQDO28:~$
```

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?

   The average RTT vary between different hosts. The following aspects of latency might impact this:

   - Propagation delay: It is the time taken by the first bit to travel from sender to receiver end of the link. In other words, it is simply the time required for bits to reach the destination from the start point. Factors on which Propagation delay depends are Distance and propagation speed. Different hosts can be situated at different locations hence there can be difference in the distances.
   - Queuing delay: Queuing delay is the time a job waits in a queue until it can be executed. It depends on congestion. It is the time

difference between when the packet arrived Destination and when the packet data was processed or executed. It may be caused by mainly three reasons i.e. originating switches, intermediate switches or call receiver servicing switches. The processing time can be different for each host.

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

   The average RTT vary with different packet sizes. The following aspects of latency might impact this:

   - Transmission delay: Time taken to put a packet onto link. In other words, it is simply time required to put data bits on the wire/communication medium. It depends on length of packet and bandwidth of network.

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).

- uw.edu

```
bhargavi@LAPTOP-59VQDO28:~$ ping -c 4 -s 32 uw.edu
PING uw.edu (128.95.155.134) 32(60) bytes of data.
40 bytes from www1.cac.washington.edu (128.95.155.134): icmp_seq=1 ttl=43 time=261 ms
40 bytes from www1.cac.washington.edu (128.95.155.134): icmp_seq=2 ttl=43 time=261 ms
40 bytes from www1.cac.washington.edu (128.95.155.134): icmp_seq=3 ttl=43 time=266 ms
40 bytes from www1.cac.washington.edu (128.95.155.134): icmp_seq=4 ttl=43 time=263 ms

--- uw.edu ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3331ms
rtt min/avg/max/mdev = 260.608/262.636/266.439/2.336 ms
```

- Cornell.edu

```
bhargavi@LAPTOP-59VQDO28:~$ ping -c 4 -s 32 cornell.edu
PING cornell.edu (128.253.173.245) 32(60) bytes of data.

--- cornell.edu ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3004ms
```

- Berkeley.edu

```
bhargavi@LAPTOP-59VQDO28:~$ ping -c 4 -s 32 berkeley.edu
PING berkeley.edu (35.163.72.93) 32(60) bytes of data.
40 bytes from ec2-35-163-72-93.us-west-2.compute.amazonaws.com (35.163.72.93): icmp_seq=1 ttl=32 time=269 ms
40 bytes from ec2-35-163-72-93.us-west-2.compute.amazonaws.com (35.163.72.93): icmp_seq=2 ttl=32 time=267 ms
40 bytes from ec2-35-163-72-93.us-west-2.compute.amazonaws.com (35.163.72.93): icmp_seq=3 ttl=32 time=273 ms
40 bytes from ec2-35-163-72-93.us-west-2.compute.amazonaws.com (35.163.72.93): icmp_seq=4 ttl=32 time=267 ms

--- berkeley.edu ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 266.500/268.895/272.963/2.629 ms
```

- Uchicago.edu

```
bhargavi@LAPTOP-59VQDO28:~$ ping -c 4 -s 32 uchicago.edu
PING uchicago.edu (34.200.129.209) 32(60) bytes of data.

--- uchicago.edu ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3004ms
```

- Ox.ac.uk

```
bhargavi@LAPTOP-59VQDO28:~$ ping -c 4 -s 32 ox.ac.uk
PING ox.ac.uk (151.101.130.133) 32(60) bytes of data.
40 bytes from 151.101.130.133 (151.101.130.133): icmp_seq=1 ttl=52 time=15.8 ms
40 bytes from 151.101.130.133 (151.101.130.133): icmp_seq=2 ttl=52 time=17.7 ms
40 bytes from 151.101.130.133 (151.101.130.133): icmp_seq=3 ttl=52 time=20.5 ms
40 bytes from 151.101.130.133 (151.101.130.133): icmp_seq=4 ttl=52 time=24.8 ms

--- ox.ac.uk ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 15.790/19.693/24.778/3.375 ms
```

- Yahoo.co.jp

```
bhargavi@LAPTOP-59VQDO28:~$ ping -c 4 -s 32 yahoo.co.jp
PING yahoo.co.jp (182.22.59.229) 32(60) bytes of data.
40 bytes from f1.top.vip.ssk.yahoo.co.jp (182.22.59.229): icmp_seq=1 ttl=38 time=146 ms
40 bytes from f1.top.vip.ssk.yahoo.co.jp (182.22.59.229): icmp_seq=2 ttl=38 time=146 ms
40 bytes from f1.top.vip.ssk.yahoo.co.jp (182.22.59.229): icmp_seq=3 ttl=38 time=145 ms
40 bytes from f1.top.vip.ssk.yahoo.co.jp (182.22.59.229): icmp_seq=4 ttl=38 time=149 ms

--- yahoo.co.jp ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 145.481/146.525/148.728/1.285 ms
bhargavi@LAPTOP-59VQDO28:~$
```

Observations:

- ➢ The round trip time depends on the distance between source and destination of the network requests.
- ➢ The RTT is more for the universities located in US than UK because distance for US is more than UK from India.
- ➢ The RTT for host in Japan is more than UK and less than US because its distance from India is more than UK and less than US.

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>

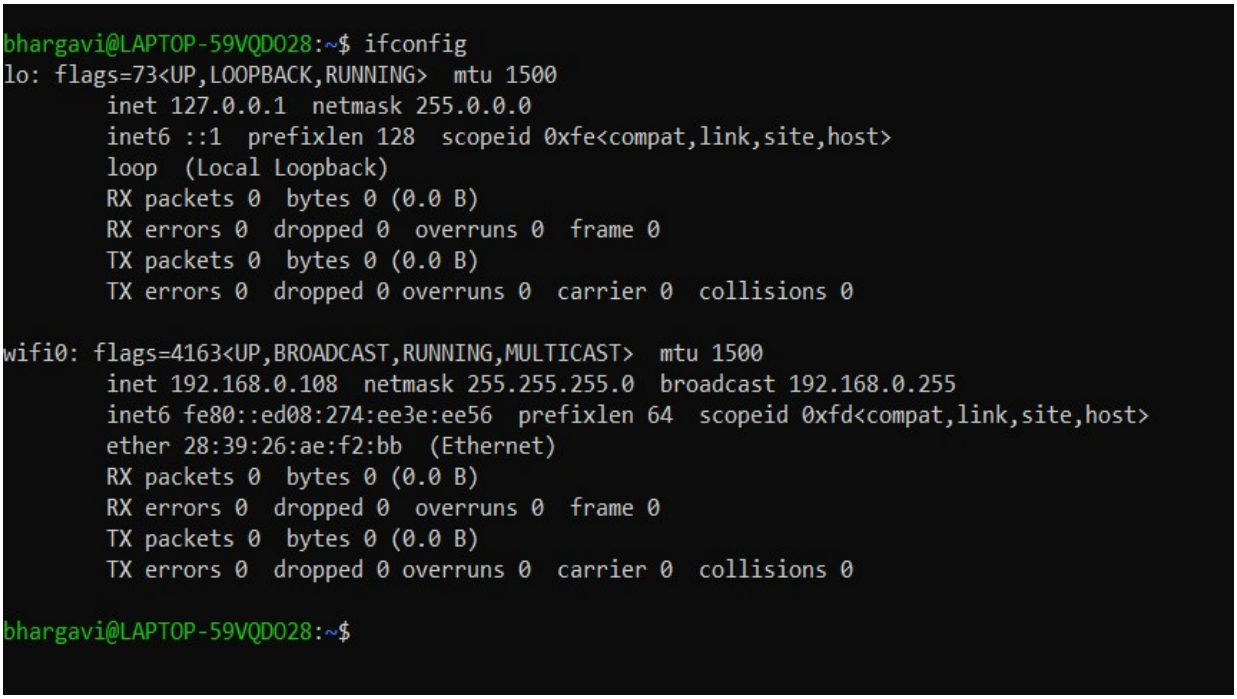
- yahoo.com

```
bhargavi@LAPTOP-59VQDO28:~$ nslookup yahoo.com
Server:         192.168.0.1
Address:        192.168.0.1#53

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

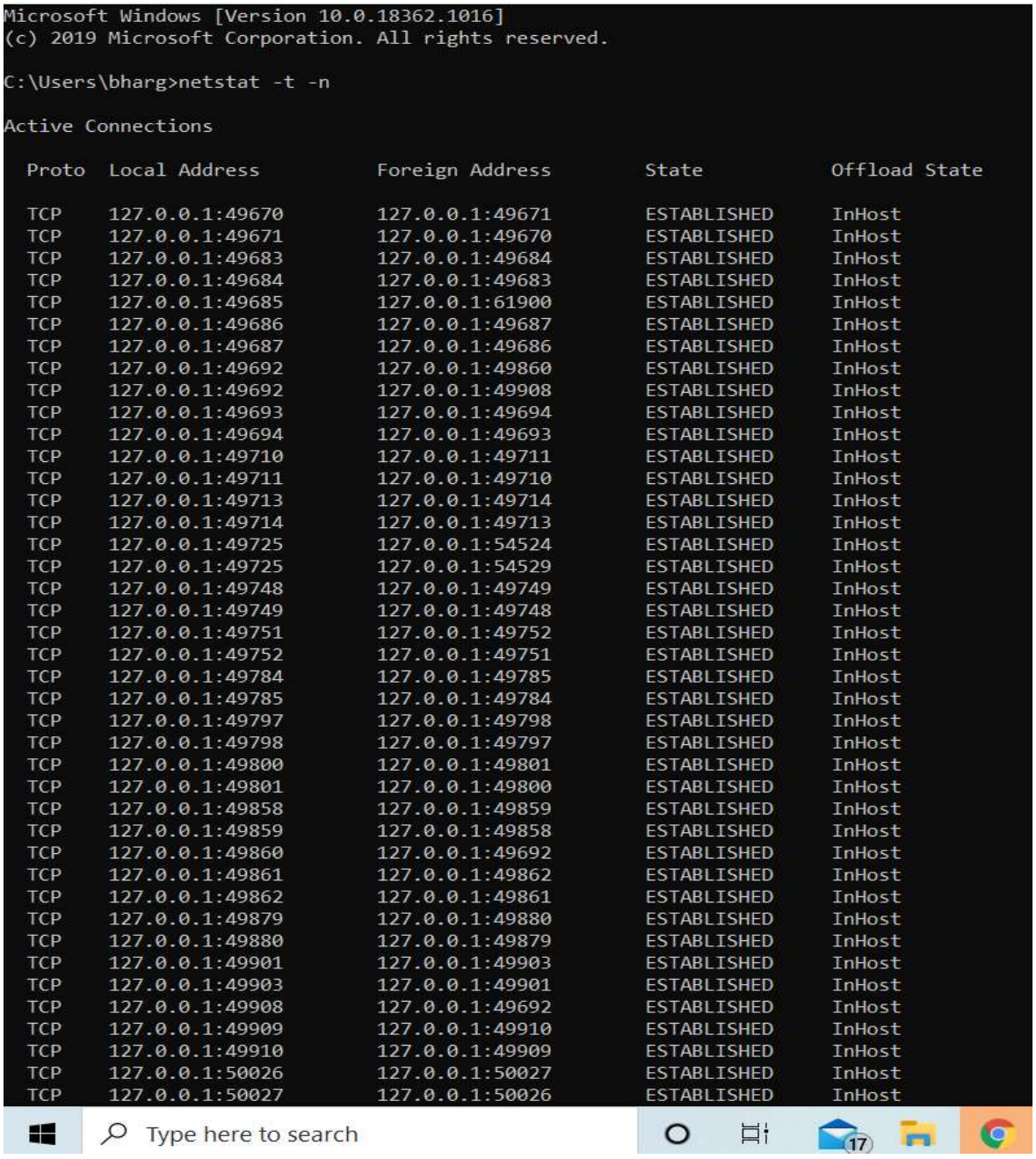
- Google.com

```
bhargavi@LAPTOP-59VQDO28:~$ nslookup google.com
Server:         192.168.0.1
Address:        192.168.0.1#53

Non-authoritative answer:
Name:   google.com
Address: 216.58.203.46
Name:   google.com
Address: 2404:6800:4009:80f::200e
```

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!!!.)

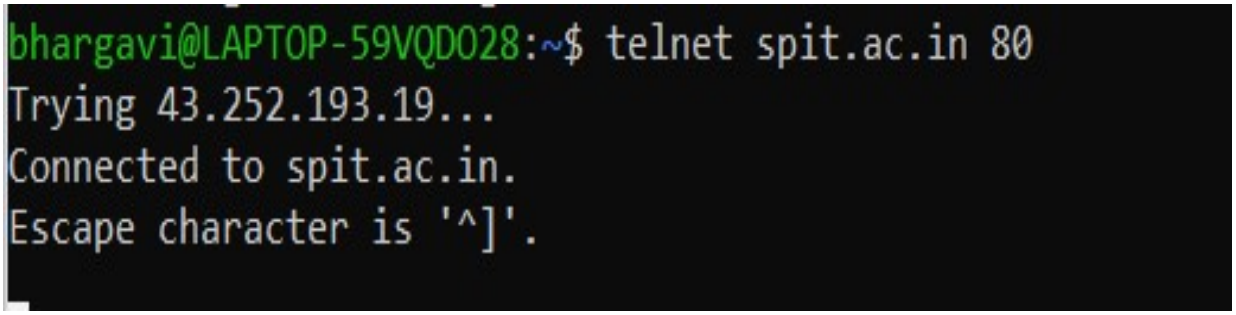


netstat — The netstat command gives information about network connections. I often use netstat -t -n which lists currently open TCP connections (that's the "-t" option) by IP address rather than domain name (that's the "-n" option). Add the option "-l" (lower case ell) to list listening sockets, that 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.)



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).

- Mscs.mu.edu

```
C:\Users\bharg>tracert mscs.mu.edu

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

  1     4 ms     3 ms     3 ms  192.168.0.1
  2    12 ms    13 ms    16 ms  10.210.0.1
  3    13 ms    22 ms    17 ms  192.168.3.62
  4    17 ms    11 ms    16 ms  172.19.0.205
  5    16 ms    14 ms    31 ms  10.74.47.53
  6    13 ms    17 ms    24 ms  10.74.47.54
  7    15 ms    16 ms    35 ms  203.212.193.30
  8    20 ms    17 ms    18 ms  202.88.130.245
  9    16 ms    16 ms    26 ms  mail.megtec.in [125.99.119.2]
 10    21 ms    14 ms    26 ms  136.232.27.245.static.jio.com [136.232.27.245]
 11    24 ms    21 ms    18 ms  103.198.140.58
 12   131 ms   130 ms   143 ms  103.198.140.27
 13   152 ms   144 ms   133 ms  103.198.140.27
 14   137 ms   120 ms   128 ms  hurricane.mrs.franceix.net [37.49.232.13]
 15   430 ms   144 ms   136 ms  100ge4-2.core1.par2.he.net [184.105.222.21]
 16   199 ms   196 ms   203 ms  100ge14-1.core1.nyc4.he.net [184.105.81.77]
 17   233 ms   240 ms   245 ms  100ge2-1.core2.chi1.he.net [184.104.193.173]
 18     *        *        *     Request timed out.
 19   272 ms   264 ms   262 ms  r-222wwash-isp-ae6-3926.wiscnet.net [140.189.8.126]
 20   280 ms   270 ms   286 ms  r-milwaukeeci-809-isp-ae3-0.wiscnet.net [140.189.8.230]
 21   261 ms   258 ms   255 ms  216.56.1.202
 22   272 ms   277 ms   266 ms  134.48.10.27
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```

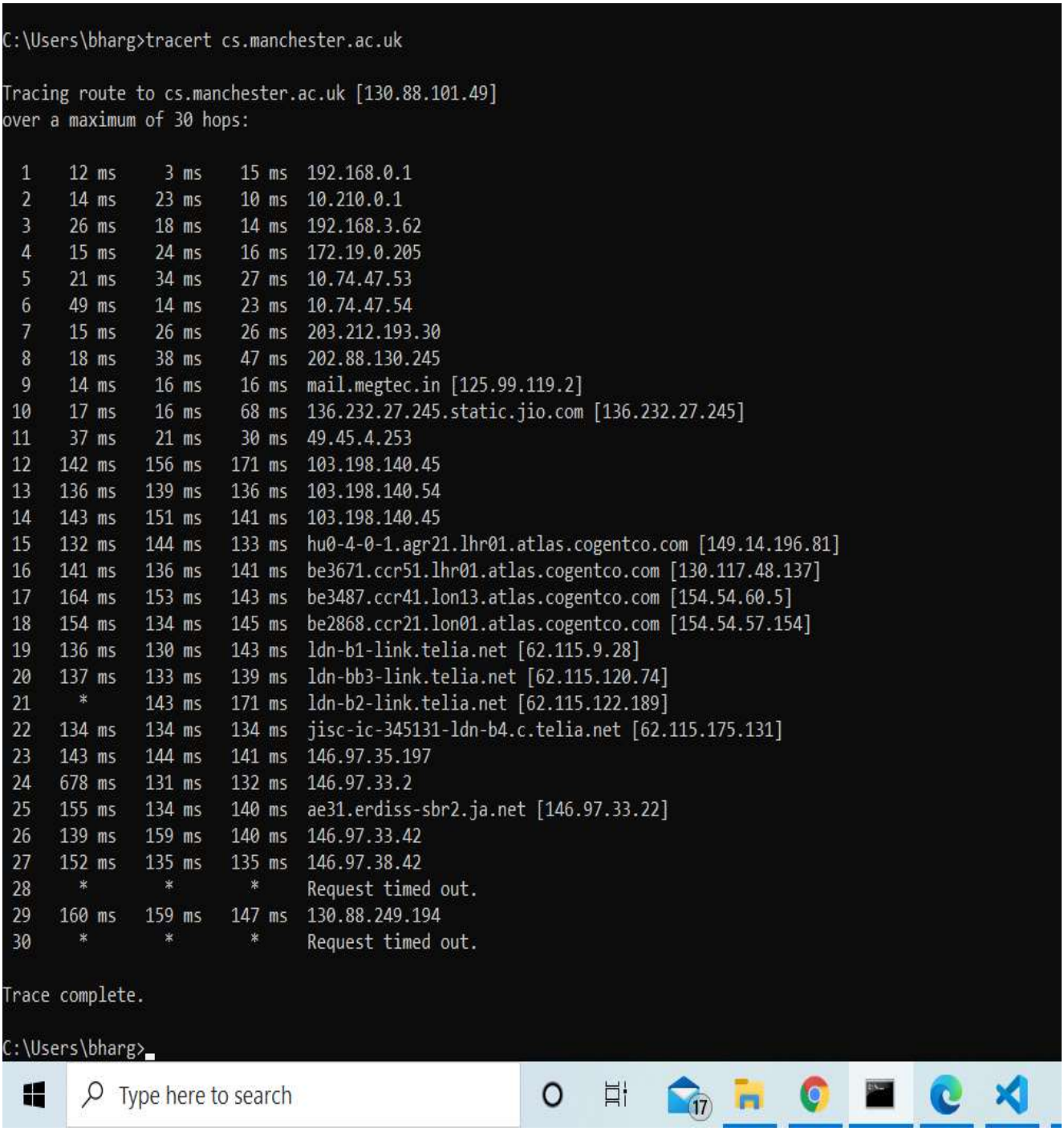
- Csail.mit.edu

```
C:\Users\bharg>tracert csail.mit.edu

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

  1     4 ms     4 ms     4 ms  192.168.0.1
  2    11 ms    12 ms    11 ms  10.210.0.1
  3    13 ms    15 ms    22 ms  192.168.3.62
  4    15 ms    16 ms    17 ms  172.19.0.205
  5    22 ms    17 ms    15 ms  10.74.47.53
  6    22 ms    19 ms    18 ms  10.74.47.54
  7    17 ms    15 ms    14 ms  203.212.193.30
  8    15 ms    15 ms    15 ms  202.88.130.245
  9    14 ms    14 ms    15 ms  mail.megtec.in [125.99.119.2]
 10    16 ms    14 ms    19 ms  136.232.27.245.static.jio.com [136.232.27.245]
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15   264 ms   273 ms   267 ms  103.198.140.15
 16     *      255 ms   260 ms  4.7.26.61
 17     *        *        *     Request timed out.
 18   319 ms   326 ms   317 ms  MASSACHUSET.bear1.Boston1.Level3.net [4.53.48.98]
 19   317 ms   317 ms   315 ms  18.0.161.17
 20   315 ms   313 ms   310 ms  dmz-rtr-2-dmz-rtr-1-2.mit.edu [18.0.162.6]
 21   316 ms   315 ms   315 ms  mitnet.core-1-ext.csail.mit.edu [18.4.7.65]
 22     *        *        *     Request timed out.
 23   316 ms   316 ms   319 ms  bdr.core-1.csail.mit.edu [128.30.0.246]
 24   321 ms   321 ms   322 ms  inquir-3ld.csail.mit.edu [128.30.2.109]

Trace complete.
```

- Cs.stanford.edu

```
C:\Users\bharg>cs.stanford.edu
'cs.stanford.edu' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\bharg>tracert cs.stanford.edu

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

  1     4 ms     3 ms     5 ms  192.168.0.1
  2    16 ms    19 ms    11 ms  10.210.0.1
  3    24 ms    17 ms    19 ms  192.168.3.62
  4    29 ms    23 ms    22 ms  172.19.0.205
  5    25 ms    19 ms    24 ms  10.74.47.53
  6    22 ms    18 ms    23 ms  10.74.47.54
  7    30 ms    25 ms    14 ms  203.212.193.30
  8    16 ms    40 ms    14 ms  202.88.130.245
  9    15 ms    18 ms    16 ms  mail.megtec.in [125.99.119.2]
 10    17 ms    16 ms    16 ms  136.232.27.245.static.jio.com [136.232.27.245]
 11    18 ms    38 ms    17 ms  49.45.4.253
 12   115 ms   119 ms   121 ms  103.198.140.54
 13   122 ms   116 ms   115 ms  103.198.140.54
 14   137 ms   139 ms   143 ms  hurricane-electric.telecity2.nl-ix.net [193.239.116.14]
 15   150 ms   164 ms   140 ms  100ge8-1.core1.lon3.he.net [184.104.193.193]
 16   155 ms   146 ms   137 ms  100ge14-1.core1.lon2.he.net [184.105.64.237]
 17   205 ms   208 ms   211 ms  100ge13-2.core1.nyc4.he.net [72.52.92.166]
 18   266 ms   268 ms   264 ms  100ge8-1.core1.sjc2.he.net [184.105.81.218]
 19   268 ms   265 ms   263 ms  100ge1-1.core1.pao1.he.net [72.52.92.158]
 20   265 ms   258 ms   259 ms  stanford-university.100gigabitethernet5-1.core1.pao1.he.net [184.105.177.238]
 21   299 ms   271 ms   270 ms  csee-west-rtr-vl3.SUNet [171.66.255.140]
 22   274 ms   271 ms   274 ms  CS.stanford.edu [171.64.64.64]

Trace complete.
```

- Cs.manchester.ac.uk



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.

- Math.hws.edu

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

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

  1     4 ms     3 ms     3 ms  192.168.0.1
  2    17 ms    12 ms    11 ms  10.210.0.1
  3   481 ms    13 ms    24 ms  192.168.3.62
  4    42 ms    11 ms    12 ms  172.19.0.205
  5    20 ms    14 ms    13 ms  10.74.47.53
  6    19 ms    13 ms    13 ms  10.74.47.54
  7    19 ms    60 ms    18 ms  203.212.193.30
  8    14 ms    13 ms    26 ms  202.88.130.245
  9  1485 ms    26 ms    14 ms  mail.megtec.in [125.99.119.2]
 10    24 ms    15 ms    16 ms  136.232.27.245.static.jio.com [136.232.27.245]
 11    40 ms    15 ms    14 ms  103.198.140.58
 12   172 ms   145 ms   142 ms  103.198.140.45
 13   182 ms   156 ms   149 ms  103.198.140.27
 14   137 ms   143 ms   136 ms  103.198.140.107
 15   155 ms   142 ms   143 ms  103.198.140.45
 16   134 ms   134 ms   132 ms  hu0-4-0-1.agr21.lhr01.atlas.cogentco.com [149.14.196.81]
 17   156 ms   137 ms   138 ms  be3671.ccr51.lhr01.atlas.cogentco.com [130.117.48.137]
 18   144 ms   152 ms   142 ms  be3487.ccr41.lon13.atlas.cogentco.com [154.54.60.5]
 19   136 ms   166 ms   130 ms  be2870.ccr22.lon01.atlas.cogentco.com [154.54.58.174]
 20   148 ms   155 ms   153 ms  ae-7.edge7.London1.Level3.net [4.68.62.41]
 21   182 ms   165 ms   132 ms  ae-227-3603.edge3.London15.Level3.net [4.69.167.98]
 22     *      138 ms   130 ms  ae-227-3603.edge3.London15.Level3.net [4.69.167.98]
 23   148 ms   170 ms   132 ms  ae4.ar8.lon15.Level3.net [4.68.111.254]
 24   276 ms   320 ms   278 ms  roc1-ar5-xe-11-0-0-0.us.twtelecom.net [35.248.1.162]
 25   270 ms   285 ms   277 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 26   289 ms   280 ms   278 ms  64.89.144.100
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```

- www.hws.edu

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

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

  1     3 ms     3 ms     3 ms  192.168.0.1
  2    22 ms    11 ms    12 ms  10.210.0.1
  3    13 ms    18 ms    15 ms  192.168.3.62
  4    15 ms    15 ms    17 ms  172.19.0.205
  5    13 ms    27 ms    14 ms  10.74.47.53
  6    14 ms    15 ms    14 ms  10.74.47.54
  7    15 ms    15 ms    15 ms  203.212.193.30
  8    15 ms    14 ms    16 ms  202.88.130.245
  9    30 ms    15 ms    15 ms  mail.megtec.in [125.99.119.2]
 10    16 ms    18 ms    14 ms  136.232.27.245.static.jio.com [136.232.27.245]
 11    16 ms    17 ms    17 ms  103.198.140.58
 12   157 ms   155 ms   156 ms  103.198.140.45
 13   133 ms   132 ms   130 ms  103.198.140.27
 14   135 ms   140 ms   136 ms  103.198.140.107
 15   143 ms   144 ms   145 ms  103.198.140.45
 16   136 ms   133 ms   146 ms  hu0-4-0-1.agr21.lhr01.atlas.cogentco.com [149.14.196.81]
 17   141 ms   140 ms   142 ms  be3672.ccr52.lhr01.atlas.cogentco.com [130.117.48.145]
 18   134 ms   132 ms   132 ms  be3488.ccr42.lon13.atlas.cogentco.com [154.54.60.13]
 19   132 ms   137 ms   142 ms  be2869.ccr22.lon01.atlas.cogentco.com [154.54.57.162]
 20   149 ms   156 ms   141 ms  ae-7.edge7.London1.Level3.net [4.68.62.41]
 21   148 ms   179 ms   174 ms  ae-225-3601.edge3.London15.Level3.net [4.69.167.90]
 22   146 ms   141 ms   143 ms  ae-225-3601.edge3.London15.Level3.net [4.69.167.90]
 23   141 ms   148 ms   158 ms  ae4.ar8.lon15.Level3.net [4.68.111.254]
 24   278 ms   274 ms   271 ms  roc1-ar5-xe-11-0-0-0.us.twtelecom.net [35.248.1.162]
 25   274 ms   269 ms   268 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 26   277 ms   277 ms   279 ms  64.89.144.100
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```

- In traceroute for math.hws.edu, the request to 22th node was timed out. Whereas in traceroute for hws.edu, 22th node is present as 4.69.167.90

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.

```
C:\Users\bharg>tracert spit.ac.in

Tracing route to spit.ac.in [43.252.193.19]
over a maximum of 30 hops:

  1     3 ms     4 ms     3 ms  192.168.0.1
  2    11 ms    12 ms    29 ms  10.210.0.1
  3    15 ms    16 ms    15 ms  192.168.3.62
  4    15 ms    15 ms    14 ms  172.19.0.205
  5    15 ms    16 ms    22 ms  10.74.47.53
  6  2269 ms    14 ms    14 ms  10.74.47.54
  7    17 ms    19 ms    18 ms  203.212.193.30
  8    26 ms    35 ms    14 ms  202.88.130.245
  9    15 ms    13 ms    14 ms  mail.megtec.in [125.99.119.2]
 10    28 ms    16 ms    16 ms  136.232.27.245.static.jio.com [136.232.27.245]
 11    13 ms    13 ms    18 ms  115.110.206.73.static-Mumbai.vsnl.net.in [115.110.206.73]
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14    22 ms    19 ms    28 ms  115.113.165.174.static-mumbai.vsnl.net.in [115.113.165.174]
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17    16 ms    16 ms    44 ms  223-30-0-0.lan.sify.net [223.31.147.250]
 18    43 ms    15 ms    90 ms  27.109.1.150
 19    20 ms    19 ms    22 ms  103.205.124.82
 20    20 ms    18 ms    23 ms  43.252.192.230
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```

```
Tracing route to spit.ac.in [43.252.193.19]
over a maximum of 30 hops:

  1   338 ms     6 ms    18 ms  192.168.0.1
  2    25 ms    26 ms    14 ms  10.210.0.1
  3    22 ms    14 ms    15 ms  192.168.3.62
  4    18 ms    19 ms    17 ms  172.19.0.205
  5    41 ms    26 ms    21 ms  10.74.47.53
  6    16 ms    15 ms    56 ms  10.74.47.54
  7    18 ms    14 ms    16 ms  203.212.193.30
  8    20 ms    18 ms    35 ms  125.99.55.254
  9    80 ms    62 ms   208 ms  125.99.55.253
 10    20 ms    32 ms    20 ms  136.232.27.245.static.jio.com [136.232.27.245]
 11    24 ms    21 ms    23 ms  115.110.206.73.static-Mumbai.vsnl.net.in [115.110.206.73]
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14    36 ms    66 ms   112 ms  115.113.165.174.static-mumbai.vsnl.net.in [115.113.165.174]
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17    17 ms    16 ms    17 ms  223-30-0-0.lan.sify.net [223.31.147.250]
 18    18 ms    25 ms    25 ms  27.109.1.150
 19    31 ms    26 ms    27 ms  103.205.124.82
 20    20 ms    37 ms    19 ms  43.252.192.230
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.

C:\Users\bhanu>
```

- There is difference at hop 8 and 9 in the nodes. First time, nodes visited were 202.88.130.245 and 125.99.119.2 for 8 and 9 respectively and 2nd time the nodes visited were125.99.55.254 and 125.99.55.253

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?

   - For all paths: the node 136.232.27.245.static.jio.com was common.

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

   - No, there is no relation between number of nodes and the distance between the hosts.

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

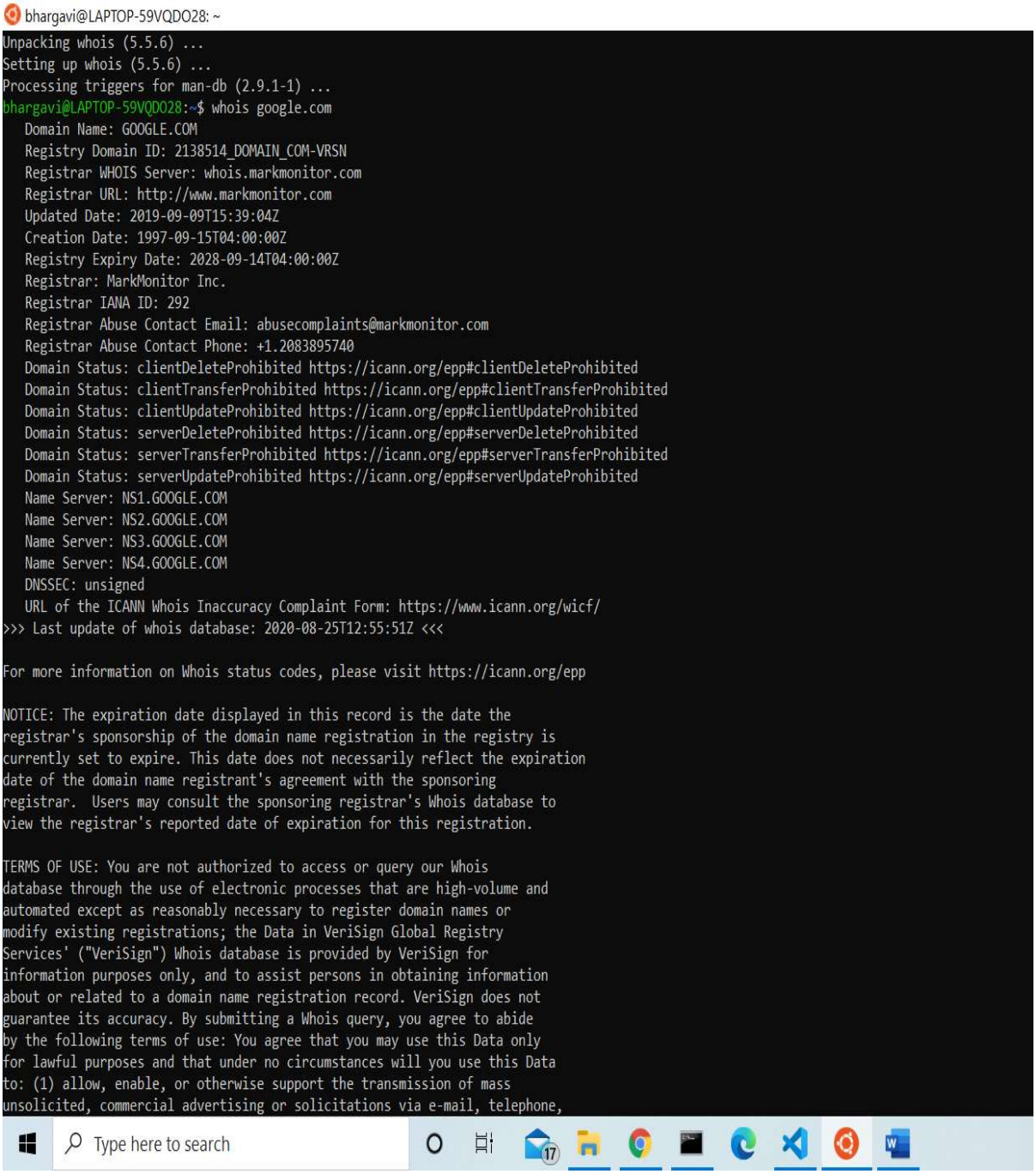
   - There can be propagation delay because of the more numbers of node

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.

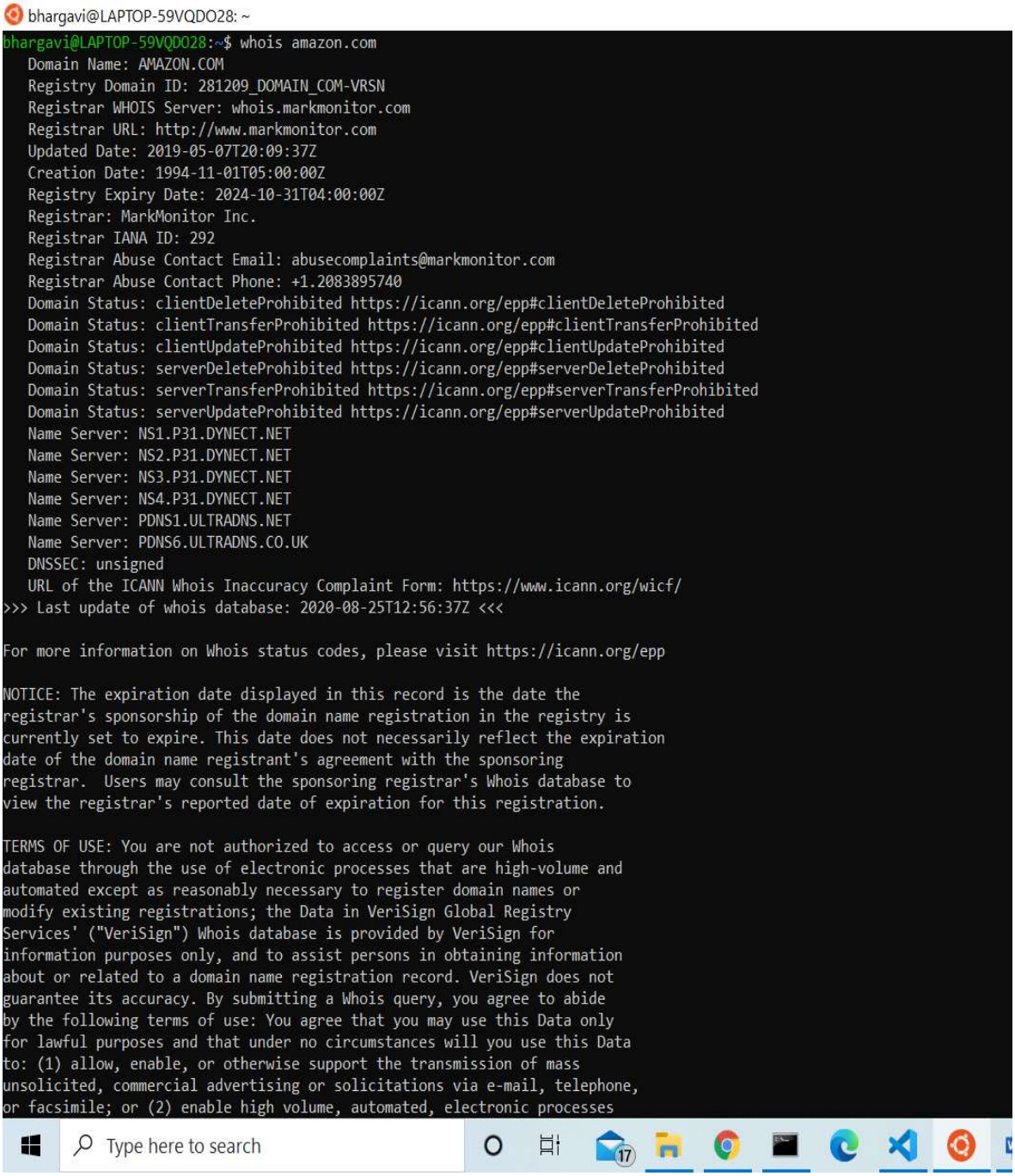
When using whois to look up a domain name, use the simple two-part network name, not an individual computer name (for example, whois spit.ac.in).

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.

- Google


bhargavi@LAPTOP-59VQDO28: ~
Unpacking whois (5.5.6) ...
Setting up whois (5.5.6) ...
Processing triggers for man-db (2.9.1-1) ...
bhargavi@LAPTOP-59VQDO28:~$ 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: 2020-08-25T12:55:51Z <<<
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,
Type here to search

Amazon.com


bhargavi@LAPTOP-59VQDO28: ~
bhargavi@LAPTOP-59VQDO28:~$ 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: 2020-08-25T12:56:37Z <<<
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
Type here to search

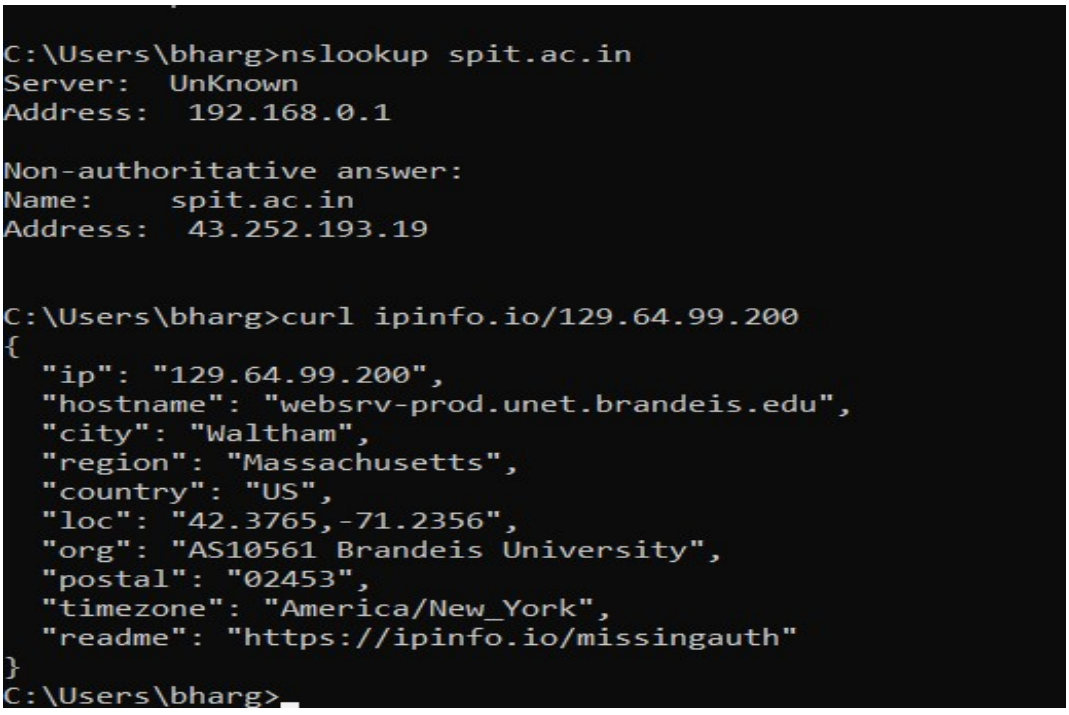
Exercise 5: (Should be short.) Because of NAT, the domain name spit.ac.in has a different IP address outside of SPIT than it does on campus. Using information in this lab and working on a home computer, find the outside IP address for spit.ac.in. Explain how you did it.

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.)



CONCLUSION:

1. In this experiment, I learned about basic network utilities such as ping, traceroute, ipconfig, etc.
2. I learned about their implementation and variation in them depending upon different factors such as distance, packet size, etc.